The Curry-Howard Isomorphism

Student: Chuangjie Xu (1061493)

Supervisor: Achim Jung

January 28, 2011

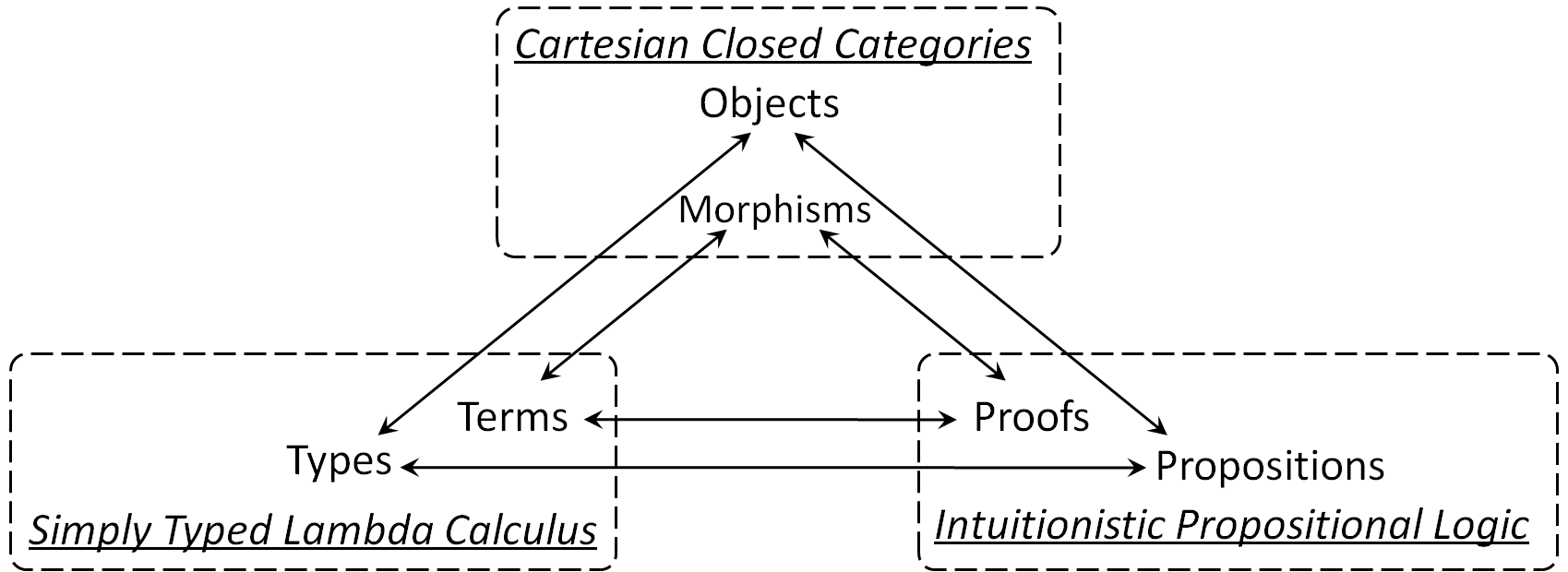
**Abstract**

**1. Introduction**

Logicians must be familiar with modus ponens , a very common rule of inference, saying that given implication and proposition , we have . Programmers may frequently use function application: if is a function of type and is an argument of type , then the application is of type . Interestingly, modus ponens behaves the same as function application. So, are proofs related to programs? Yes, there is an amazing precise correspondence between them which is described in the Curry-Howard Isomorphism.

In the 1930s, Haskell Curry observed a correspondence between types of combinators and propositions in intuitionist implicational logic. But, at that time, it was viewed as no more than a curiosity. About three decades later, William Howard extended this correspondence to first order logic by introducing dependent types. Therefore, this correspondence is called the Curry-Howard Isomorphism.

The Curry-Howard Isomorphism states a correspondence between systems of formal logic and computational calculi. For years, it has been extended to more expressive logics, e.g. higher order logic, and other mathematical systems, e.g. cartesian closed categories. In this project, I mainly probed into one of its extensions, the three-way-correspondence between intuitionistic propositional logic, simply-typed lambda calculus and cartesian closed categories, with propositions or types being interpreted as objects and proofs or terms as morphisms.



Intuitionistic logic is a formalization of Brouwer’s intuitionism. As the founder of intuitionism, L. E. J. Brouwer avoided use of formal language or logic all his life. But his attitude did not stop others considering formalizations of parts of intuitionism. In the 1930s, Arend Heyting, a former student of Brouwer, produced the first complete axiomatizations for intuitionistic propositional and predicate logic. In intuitionistic logic, the law of excluded middle and double negation elimination are no longer axioms.

The lambda calculus was introduced by Alonzo Church in the early 1930s as a formal system to provide a functional foundation for mathematics. Since Church’s original system was shown to be logically inconsistent, he gave just a consistent subtheory of his original system dealing only with the functional part. Then, in 1940, Church also introduced a typed interpretation of the lambda calculus by assigning types to terms. This typed lambda calculus serves as the foundation of the modern type systems in computer science.

Category first appeared in Samuel Eilenberg and Saunders Mac Lane’s paper written in 1945. It was originally introduced to describe the passage from one type of mathematical structure to another. In recent decades, category theory has found use for computer science. For instant, it has a profound influence on the design of functional and imperative programming languages, e.g. Haskell and Agda.

Looking from the historical perspective, these three different systems seem to have different origins, not related to each other. However, Joachim Lambek showed in the early 1970s that cartesian closed categories provided a formal analogy between proofs in intuitionistic propositional logic and types in combinatory logic. As a result, some people may use Curry-Howard-Lambek Isomorphism to refer to this three-way-correspondence.

**2. Background**

**2.1 Intuitionistic Logic**

**2.2 Lambda Calculus**

The -calculus is a family of prototype programming language. One of their main features is that they are *functional*, since they are based on the notion of function and include notion for function-abstraction and application. Also they are *higher-order*; that is, they give a systematic notation for functions whose input and output values may be other functions.

The simplest of these languages is the pure lambda calculus which studies only functions and their applicative behaviors but does not contain any constant or type. Its first primitive operation is *application*. The expression denotes the function applied to the argument . Another basic operation is *abstraction*. Let be an expression possibly containing or depending on . Then denotes the function.

To begin with, the set of -terms in type-free lambda calculus is defined.

**2.2.1 Definition (-terms)** Assume that an infinite sequence of *term-variables* is given. Then the *-terms* is defined as follows:

i) each term-variable is a *-*term, called an *atom* or *atomic term*;

ii) if and are *-*terms, then is a *-*term called an *application*;

iii) if is a term-variable and is a *-*term, then is a *-*term called an *abstraction* or *lambda abstraction*.

Parentheses and repeated ’s are often omitted in such a way that, to illustrate,  
  
where iterated abstraction uses *association to the right* while iterated application uses *association to the left*.

Let be a component of a term . The displayed component is called the *scope* of the *abstractor* . And the occurrence of in the abstractor is called a *binding occurrence* of . Then we can define free and bound variables in a term.

**2.2.2 Definition (Free, bound)** A variable is *free* in a term iff its occurrence is not in the scope of a in ; and is bound in iff contains an occurrence of .

According this definition, a variable may be both free and bound in a term , for instance if .

The set of all variables free in is denoted by , and can be obtained inductively in the following way:

* ;
* ;
* .

The first basic operation in lambda calculus is substitution.

**2.2.3 Definition (Substitution)** Define to be the result of substituting for each free occurrence in and making any changes of bound variables needed to prevent variables free in from becoming bound in . More precisely, define for all and all

* ;
* ;
* ;
* ;
* if ;
* if and ;
* if and .

In the last case, can be any variable that is not free in and , i.e. and .

For any and any distinct , the result of simultaneously substituting all for ( in term is defined similarly to the definition above and denoted as .

There are three kinds of equivalence playing an important role in lambda calculus. The first one is -equivalence.

**2.2.4 Definition (-equivalence)** Given a variable , we have  
  
called an -*conversion*, and the act of replacing an occurrence of in a term by is called a *change of bound variables*. and are -*equivalent*, notation , if results from by a series of changes of bound variables.

Another equality relation that can be analyzed by reduction is -equivalence.

**2.2.5 Definition (-equivalence)**

i) A -*redex* is any term of the form . It can be reduced by the following rule  
  
If contains a -redex and is the result of replacing it by , we say -*contracts* to , denoted as .

ii) A -*reduction* of a term is a finite or infinite ordered sequence of -contractions, i.e. . A finite -reduction is *from* *to* if it has contractions and or it is empty and . If there exists a reduction from to , we say -*reduces to ,* denoted as .

iii) and are -*equivalent*, notation , if can be changed to by a finite sequence of -reductions and -expansions (reversed -reductions).

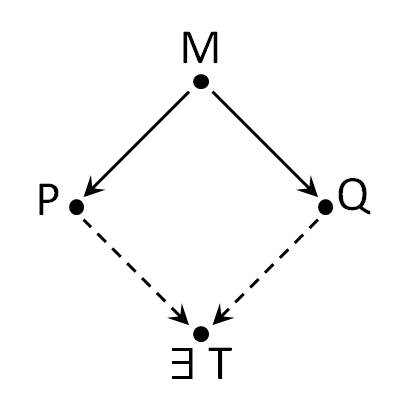
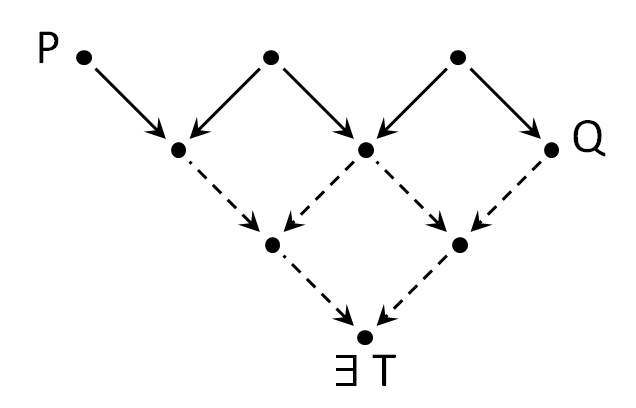
In a -reduction, -conversions are allowed.

A term may be able to -reduce to different terms at the same time. For example, the term can -reduce (in one step) to by substituting to in or by substituting to in . It is necessary for a calculus that the result of computation is independent from the order of reduction. This property holds for all -terms, which is described in the following theorem.

**2.2.6 Theorem (Church-Rosser Theorem for )**

i) If and , then there exists such that and .

ii) If , then there exists such that and .

A sequence of -reduction may come to an end where no further -reduction is possible. This brings the

**2.3 Categories**

As a relatively young branch of mathematics, category theory studies in an abstract way the properties of particular mathematical structures. It seeks to express all mathematical concepts in terms of “objects” and “morphisms” independently of what they are representing. Nowadays, categories appear in most branches of mathematics and many parts of computer science. Topoi, a kind of category, can even serve as a foundation for mathematics. Cartesian closed categories can work as a framework for describing the denotational semantics of typed lambda calculus, and more generally, programming languages.

**2.3.1 Definition (Categories)** A *category* consists of:

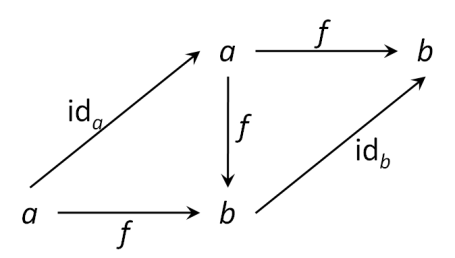
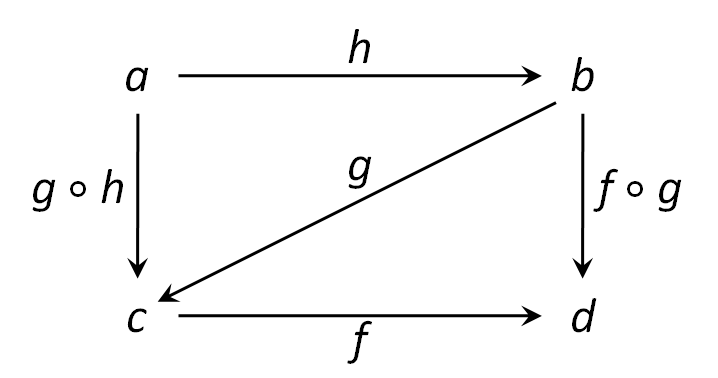
* a collection of *objects*;
* a collection of *morphisms* (also called *arrows or maps*) between objects, with two maps which give the domain and codomain of a morphism (we write to denote a morphism with and );
* a binary map “”, called composition, mapping each pair of morphisms with to a morphism such that and ;

such that the following axioms hold:

* identity: for every object , there exists a morphism , called the identity morphism for , such that for any morphism ;
* associativity: for every , and .

For any objects and of a category , the collection of all morphisms is called a *hom-set* and denoted as . A category is determined by its hom-sets.

Categorists use *diagrams* to express equations. In a diagram, a morphism is represented as an arrow form point to , labeled . A diagram *commutes* if the composition of the morphism along any path between two fixed objects is equal. The identity and associative laws in the definition of category can be represented by the following commutative diagrams:

** **

A common example of a category is the category **.** It is the category whose objects are sets and whose morphisms are functions. The identity of object in is the identity function . The composition of morphisms is the composition of functions. As a category, it satisfies the two category axioms:

i) , for every ;

It follows by using the definition of composite function and identity function:  
 and

ii) , for every , and .

This follows from the fact that composition of functions is associative:

One typical use of categories is to consider categories whose objects are sets with mathematical structure and whose morphisms are functions that preserve that structure. One of the common examples is the category whose objects are posets and whose morphisms are monotone functions. It will be discussed later as an example of a CCC.

There are many categorical constructions, i.e. particular objects and morphisms that satisfy a given set of axioms, which enrich the language of Category Theory. When studying constructions, one observes that all concepts are defined by their relations with other objects, and these relations are established by the existence and the equality of particular morphisms. In this dissertation, the following fundamental categorical constructions will be considered.

The simplest of these is the notion of initial object and its dual, terminal object.

**2.3.2 Definition (Initial and Terminal Objects)** Let be a category. An object of is *initial* if, for any object in , there is a unique morphism from to . An object in is *terminal* if, for any object in , there is a unique morphism from to .

In this dissertation, terminal objects are denoted as and, for object , the unique morphism is denoted as .

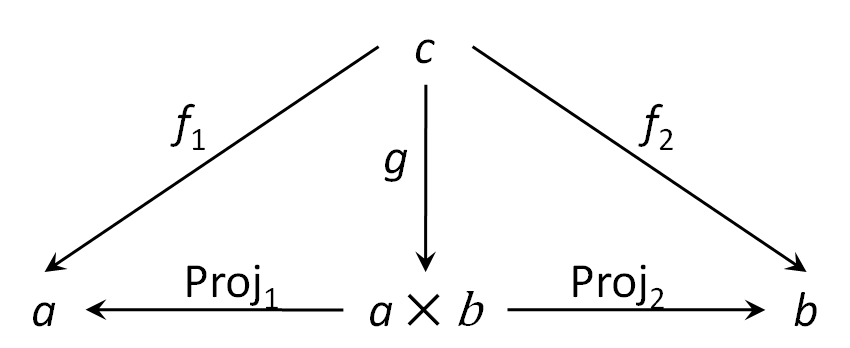
In , the initial object is the empty set , and the unique morphism with for its source is the empty function whose graph is empty. Any singleton set is terminal in since for any set , there is exactly one function from to this singleton set.

In set theory, we can form a cartesian product of two sets and define coordinate functions for it. Then we can even form a product function of two given functions which have the same domain. This motivates a general definition of categorical products (within a category).

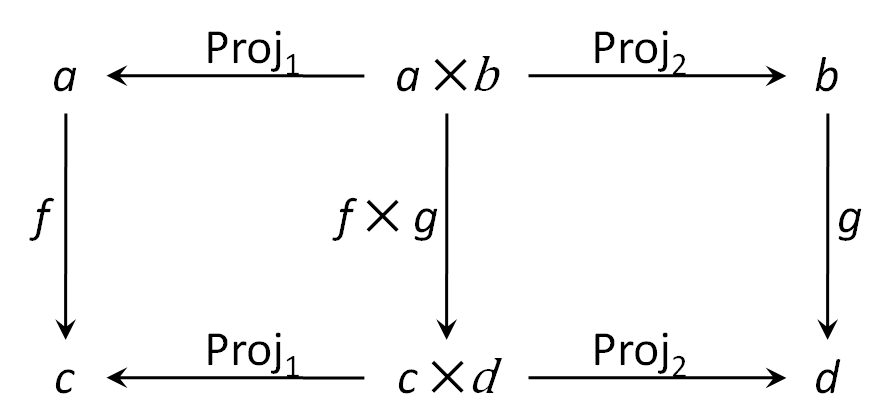
**2.3.3 Definition (Products)** Let and be objects of a category . The *product* of and is an object together with two morphisms and , and for every object in , an operation such that for all morphisms , , and , the following equations hold:

* ;
* .

Since equations in category theory can be represented by commutative diagrams, we can give another definition of categorical products based on diagrams: Let and be objects of category . The *product* of and is an object together with two morphisms and , and for every object in , an operation such that for every and , the morphism is the unique satisfying



The cartesian product construction for morphisms can also be given a categorical definition. Given morphisms and the product is defined by whose correspondent commutative diagram is the following:



**Proposition** Let be a category with products. Given , , and , we have .

**Proof**

Similarly, we have .

By the equation in definition 2.3.3,

According to the definition of products of morphisms,

.

Therefore, the equation holds.

□

The products in are the cartesian product of sets. Let and be two sets. The cartesian product is the set of pair with and , together with the coordinate functions and such that and . Given two functions and , the function is defined by for all . Then, given , and , the equations in definition 2.3.3 are satisfied:

i)

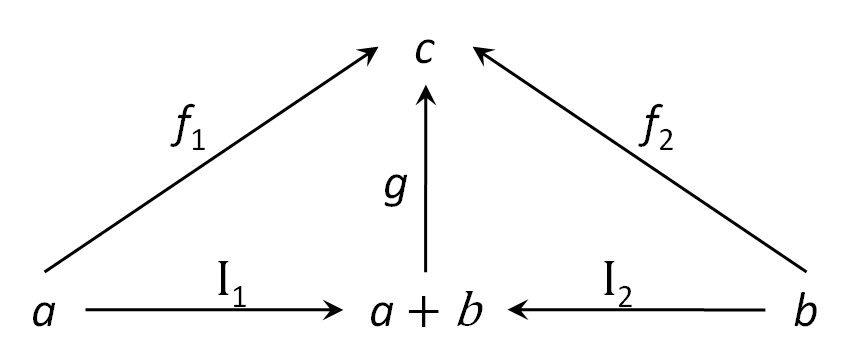
ii)

for all .

**2.3.4 Definition (Coproducts)** Let and be objects of a category . The *coproduct* of and is an object together with morphisms and , and for every object in an operation such that for every , and , , the following equations hold:

* ;
* .

The corresponding commutative diagram to the equations above is shown as follows:



where is the unique .

The coproducts in are the disjoint unions of sets. Let and be two sets. The disjoint union of them is defined by with two injection functions that takes all in to in and that takes all in to in . Given two functions and , the function is defined by for all . Given , and , the equations in the definition above are satisfied:

i)

ii)

for all .

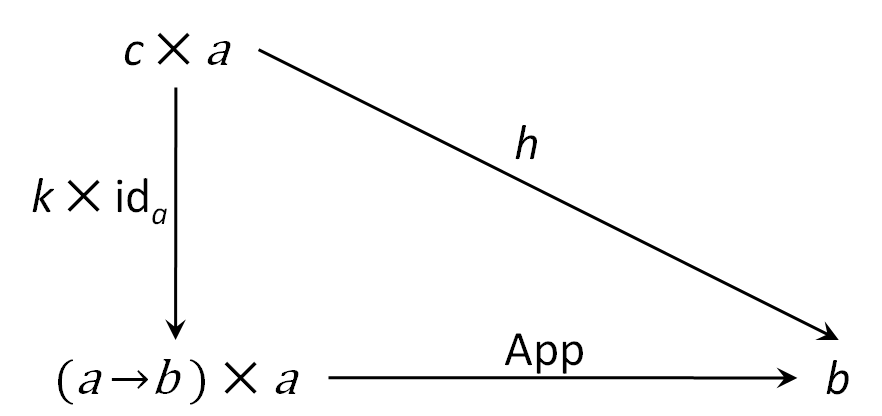
One can form a set of functions which have the same domain and codomain. Similarly, the hom-set of morphisms may form an object. This idea brings our last basic construction, exponentials.

**2.3.5 Definition (Exponentials)** Let be a category with products for all objects, and and be objects of . The *exponential*, also called *function object*, of and is an object together with a morphism , and for every object in , an operation such that for every and , the following equations hold:

* ;
* .

Using product of morphisms , the two equations above can be rewritten as and .

The commutative diagram representing the equations in the definition is shown as follows:



where the morphism is the unique .

In , the exponent set of and is the set of functions from to . The function is given by for all and . Given a function , the function is defined by for all and . Given and , the two equations hold:

i)

ii)

for all and .

Both products and exponentials have special importance for theories of computation. A two-argument function can be reduced to a one-argument function yielding a function from the second argument to the result. This passage is called *currying*. And exponentials give a categorical interpretation to the notion of currying. Therefore, categories with products and exponentials for every pair of objects are important enough to deserve a special name.

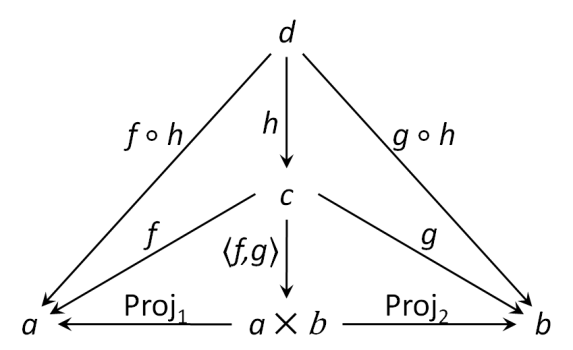
**2.3.6 Definition (Cartesian Closed Categories)** A category is *cartesian closed* iff

* It contains a terminal object ;
* For all objects and in , there is a product;
* For all objects and in , there is an exponential.

**Proposition** The following two useful identities hold in all cartesian closed categories:

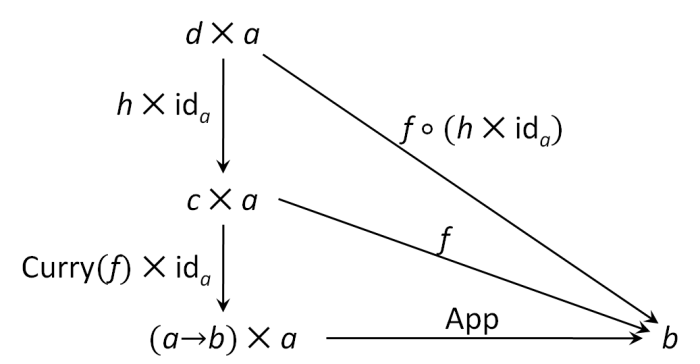
i)

where , and ;

**

ii)

where and .



**Proof**

These two equations have been proved by the diagrams following them. But they can also be proved by the equations given in definition 2.3.3 and definition 2.3.5:

i)

Since we have , then holds.

ii) (by )

(by )

(by )

□

The following gives some examples and one non-example of CCCs.

(1)

has been already given as an example of each categorical construction. It is cartesian closed since it satisfies the three conditions:

* Any singleton set can be the terminal object (it does not matter which one it exactly is since all the singleton sets are isomorphic);
* The product of sets and is the cartesian product of and ;
* The exponential of sets and is the set of functions from to .

(2)

is the category whose objects are posets and whose morphisms are monotone maps. The identity of object in is the identity map such that for all . The composition of morphisms is the composition of maps which still preserves the monotonicity property.

is cartesian closed:

* Any singleton poset can be the terminal object . The map from any poset in to this singleton poset is unique.
* The product of posets and is the cartesian product of set and with the ordering which is defined by iff and . The projections are the coordinate functions and . Given two monotone maps and , the map is defined by for all . Suppose and , then and . According to the definition of , we have , therefore, the map is monotone. In the same way as , satisfies the equations in definition 2.3.3.
* The object is a poset consisting of the set of monotone maps from to and a ordering defined by, given , iff for all . Given , the map is defined by for all and . Suppose , and , we have because ; therefore, the map is monotone. The map is defined by for all and . Suppose and with and , then by the definition of and ; therefore, is also monotone. satisfies the equations in definition 2.3.5. The proof is carried out in the same way of .

(3)

is same as the category except that each poset has a least element . We construct its identity, composition, terminal object, product, exponential in the same way of **.** Since the categorical constructions of morphism still preserve the monotonicity of morphisms; therefore, is cartesian closed.

(4) – non-example

is the category whose objects are posets with least element and whose morphisms are monotone maps with the property that in one poset is mapped to in another one, i.e. for any monotone map , .

However, is not cartesian closed. It has terminal object. But it does not have products and exponentials. Suppose that the products in are constructed in the same way of **.** (the monotonicity cannot be preserved)

**3. Correspondences**

**3.1 Every type-derivation in leads to a proof in intuitionistic implicational logic**

**3.2 Every proof in intuitionistic propositional logic can be encoded by a lambda term**

**3.3 Every lambda term can be interpreted as a morphism in a CCC**

As mentioned in the previous section, cartesian closed categories can work as a more general but also more abstract framework for describing the denotational semantics of typed lambda calculus.

The lambda calculus has terminal type, product types and function types. Correspondently, a CCC has terminal object, products and exponentials. A closed relation between them seems to be obvious. However, the lambda calculus without product type constructor is as expressive as . Therefore, both the type expressions and well-typed lambda terms in can be interpreted in any CCC, and this interpretation should be sound and complete.

**3.3.1 Definition (The Interpretation of Terms)** Given a typed lambda calculus and a cartesian closed category , we choose an object of for each type constant and a morphism for each term constant, and then all type expressions and typing contexts can be interpreted as objects and well-typed terms as morphisms. For notational simplicity, is omitted to denote the interpretation of type expressions, typing contexts and terms of in :

(1) The interpretation of type expression is defined as follows:

* , given as an object constant in ;
* .

(2) The interpretation of typing context is defined by induction on the length of the context:

* ;
* .

(3) The interpretation of a well-typed term is a morphism from to which is defined by induction on the proof of the typing judgement :

* ;
* , given as a morphism constant in ;
* ;
* ;
* where and contains all the free variables of .

In this definition, is an *m*,*n*-function. If is an ordered type assignment of length , the ordered type assignment of length is defined by . If is a well-typed term and contains all the free variables of , then the interpretation of can be related to the one of by using a combination of pairing and projection functions.

Before giving the definition of the combination, we need a few notational conventions. If is a morphism from object to , for , then we write for the morphism and for a composition of projection morphisms and so that .

Now, given an *m*,*n*-function , we can define by

.

The type terminal object is included in the type of since the interpretation of any typing context contains .

Some lemmas are needed in the proof of soundness and completeness of the interpretation defined in 3.3.1.

The first one is the substitution lemma, which will be used in the proof of soundness later.

**3.3.2 Lemma (CCC Substitution)** If and are well-typed terms, then .

**Proof**

The proof is carried out by induction on typing derivation. The base case is the one whose term is a term variable. The inductive steps have two cases: application and abstraction.

**Base case**

(by)

**Inductive steps**

**(1) Application**

Induction hypothesis:

and

.

**(2) Abstraction**

Induction hypothesis:

(by)

□

**3.3.3 Theorem (Soundness)** Given any well-typed terms and with , then the interpretations of them are same, i.e. , in every CCC.

**Proof**

**(1) -equivalence**

During the interpretation, we can see that the names of term variables never appear in the interpretation; therefore, -equivalence should hold in the interpretation. Here, an equational proof of a stronger form of -equivalence is given.

If and are well-typed, with , then

The proof can be carried out by induction on the term . The base case is the one when is a variable while the inductive steps contains application and abstraction.

Base case –

Inductive steps:

(a) Application –

with and .

Induction hypothesis:

and

(b) Abstraction –

with

Induction hypothesis:

Therefore, .

**(2) -equivalence**

We can represent -equivalence in the following form:

(by)

(by)

(by Substitution Lemma)

**(3) -equivalence**

We can represent -equivalence in the following form:

(by and )

(by)

□

**3.3.4 Theorem (Completeness)** Given any well-typed terms and , there exists a CCC such that if, then .

**Proof**

The category is generated by in the following way:

The objects of are sequences of type expressions. To be specific, the empty sequence is the terminal object and a sequence is the product of these types. For notational convenience, we write for a sequence of variables, similarly for a sequence of type expressions, and for typing context .

The morphisms from to are given by -tuples of terms over free variables. To put it more specifically, a morphism is an equivalence class of tuples of terms,

.

Composition in is defined by substitution. Given morphisms and , the composition of them is

**(1) is cartesian closed**

The cartesian closed structure of is obtained as follows:

**i)** Terminal object with unique morphism

As mentioned above, the empty sequence of types is the terminal object . According to the definition of morphisms above, a morphism from an object to is given by -tuples of terms. Then, the morphism from an object to , the empty sequence, should be given by the empty tuple. For every object , the morphism is defined by the empty tuple, i.e. . Clearly, it is unique for every object .

**ii)** Product objects with projection morphisms and function

Given two objects and , the product of them is obtained by their concatenation, . Then, the projection morphisms is given by

And, given and , the product function is defined by the concatenation of tuples:

The equations in definition 2.3.3 are satisfied. For any

,

, and

,

we have

Similarly, we have

**iii)** Exponentials with function and morphism

The exponential of objects and is the sequence of types of the following pattern .

Given any , the morphism is defined by

For any and , the morphism is defined by

The equations in definition 2.3.5 should hold. For any  
 and   
,

we have

Therefore, is cartesian closed.

**(2)**

Given any well-typed term in , its interpretation in obtained in (1) is the equivalence class of itself. Precisely,

Then, if and have the same interpretation, they should be in the same equivalence class, i.e. **.**

Therefore, given any well-typed terms and , there exists a CCC such that if, then .

□

**References**

1