Crafting Provers in Racket

Adrian Manea
Coordinator: Assoc. Prof. Traian Şerbănuţă

March 21, 2020

Contents

TO ADD/CLARIFY

INTRODUCTION AND MOTIVATION

The main motivation for starting the work on this project is my interest in the programming language Racket. This grew from me getting acquainted with Emacs and Lisps, from a user standpoint at first, but then my interest grew and I started reading more about lambda calculus and various other related subjects. Before long, I discovered John McCarthy's pioneering work in trying to make lambda calculus suitable for programming languages, but what really captured my interest were the theoretical foundations that McCarthy's articles [McC60, McC61, McC62] set for this task, in a time when programming was either electrical engineering or pure mathematics. His work was said to have introduced a paradigm shift in computer science that is comparable to the non-Euclidean geometry revolution. The next step was discovering [AS96], which showed me how an apparently simple programming language such as Scheme can be used for wonderful constructions and various degrees of abstraction. This is further supported by the thorough specification and revisions that were published by the Scheme Community, the latest being [S+13].

Further reading in the world of Lisp dialects, I have discovered Racket, whose appeal was instantaneous to me, since it is so often described not as a general purpose programming language derived from Scheme,[1] but rather as a toolbox for constructing languages to solve various problems. In fact, as I see it, it offers the necessary items for one to properly understand, craft and teach languages that exhibit particular behaviour.

This is precisely the aim of the current work. Having a background in mathematics, I quickly became interested on the one hand in proof assistants (or so-called "theorem provers") and type theory, on the other. The appeal of category theory mixed with (or, by some sources, morphed into) topos theory, type theory and the background of intuitionistic logic is very strong for me and I have been trying to approach the subject from many of its sides. Of equal interest for me is the teaching aspect. I believe in strong foundations, a thorough understanding of fundamentals before getting into more complex structures and I so often search for methods, tools and examples that I can use to showcase particular aspects of the subject I'm learning or teaching. Racket, for

[1] Racket used to be called PLT Scheme, where PLT is the name of the research group that has been working on this project since the very beginning, scattered throughout the world, as showcased at [plt20].

me, provides the perfect environment to fulfil most of such intentions. On the one hand, the language is big and flexible enough to be expressive for concepts of type theory, logic and proofs and on the other, it can be used in a piecemeal setup to serve as a great teaching toolbox for my purposes.

The plan of the work is as follows. We will start with some basic elements of type theory and intuitionistic logic. While the subject is hugely developed and used in many parts of (theoretical) computer science, we will try to make the work as self-contained as possible and as such, include in the preliminaries strictly the topics that will be developed further. For simplicity, but also for historical reasons, we will be focusing on the main work by one of the creators of the field, at least in terms of making its presentation appropriate for computer science applications, Per Martin-Löf, [ML80]. While Martin-Löf's lectures focus more on the theoretical side of things, the excellent [NP90] provides enough details to see how the concepts can be used in actual programming.

The second preliminary part of the dissertation will focus on Racket itself. We will try to provide a so-called "crash-course" to introduce some elements of syntax. Again, we will be focusing on items that will be used throughout the dissertation.

A first, excellent example will follow, along the lines of P. Ragde's article, [Rag16]. There, the author showcases a toy proof assistant, called *Proust*, that they have written in Racket, the purpose being twofold. On the one hand, it shows the power that the language has for such tasks and on the other, as the author mentions, it helps them and their students to understand at least a part of the inner workings of well established proof assistants, such as Coq and Agda. That is, they will be implementing a small portion of the tools that are available in Coq and Agda in an intentionally verbose style so that their functions are transparent.

Finally, further examples are provided, which will exhibit features of interest from type theory and intuitionistic logic.

change bib style to go well with websites

CHAPTER 1

MARTIN-LÖF TYPE THEORY

We start the theoretical part of this work focusing on Martin-Löf's take on intuitionistic logic and type theory. Before we do that, however, a quick note on the historical evolution of the subject. For brevity, we will use the abbreviation MLTT for Martin-Löf's Type Theory.

1.1 Brief Historical Overview

Type theory was first developed by Bertrand Russell and some of his collaborators and then expanded by Frank Ramsey and others. It was used first to introduce a kind of hierarchy of (mathematical) concepts that would "solve" Russell's paradox. At the same time, in the first part of the twentieth century, the Dutch mathematician L. E. J. Brouwer, then continuing with the American mathematician E. Bishop sowed the seeds of *constructive mathematics*. They put the emphasis on proofs that actually produce examples of the concepts existential quantifiers speak of. Thus, for example, any proof of a proposition of the form $\exists x$ such that P must contain a method of actually instantiating that x. This approach contrasted with the formalism developed by leading mathematicians such as D. Hilbert who proposed that mathematics should be performed simply following abstract rules and that showing a method to obtain an x in the previous example does not necessarily mean that that x should be obtained "practically", but only *in principle*.

At the same time, philosopher and logician A. Heyting summarized in his monograph [Hey66] the approach that became known as *intuitionistic logic*. This emphasized constructive proofs as well and was used by Brouwer as a formal basis for his mathematical program.

In the second half of the twentieth century, the Swedish mathematician and philosopher Per Martin-Löf exposed his take on intuitionistic logic and type theory into what became known as *Martin-Löf type theory*. This approach draws influences from the philosophical work of F. Brentano, G. Frege and E. Husserl, but also uses the *Curry-Howard correspondence* between propositions and programs, terms and proofs (excellently detailed in [SU06]).

Martin-Löf's approach became extremely influential and with the help of works such as [NP90], it was quickly implemented as a foundation for extremely powerful proof assistants such as NuPRL, Coq, Agda, Idris and others.

It is also worth mentioning that type theory and intuitionistic logic have continued to develop independently from applications in computer science. As such, types and toposes are seen as good candidates to provide "proper" foundations of mathematics instead of sets. Some very important contributions have come from the HoTT group ([Gro]).

We will not go into more historical or philosophical details of this subject and instead further focus on the mathematical aspects that were then implemented in proof assistants.

It is worth mentioning, however, that type theory (along with topos theory) has evolved into a domain which claims to serve as a better foundation for mathematics than set theory. As such, there are significant differences between sets and types, which are excellently summarized at [Gro, §1.1].

1.2 Fundamentals of MLTT

MLTT draws inspiration from Gentzen natural deduction system from the 1930s, explained in more modern terms in [Gir90]. As such, judgments will be written in the so-called *proof tree form*, such as:

$$\frac{A}{A \vee B}$$

where above the line we have the hypotheses and below the inferences. In particular, the above rule takes for granted that we have some formulas A and B and it infers that $A \vee B$ is true given the hypothesis that A is true.

Given some A, which can be a set or a proposition, we write $a \in A$ to mean, using the Curry-Howard correspondence, that either:

- a is an element of the set A;
- a is a proof of the proposition A.

Also, the judgment $a = b \in A$ means more than meets the eye:

- A is a proposition or a set;
- a and b are proofs or elements respectively;
- a and b are identical elements of the set A or represent identical proofs of the proposition A.

In fact, more than these readings can be given for the simple judgment $a \in A$, as shown in the table of figure 1.1.

A set	$a \in A$	implies
A is a set	a is an element of the set A	A is nonempty
A is a proposition	a is a (constructive) proof of A	A is true
A is an intention (expectation)	a is a method of fulfilling A	A is fulfillable (realizable)
A is a problem (task)	a is a method of solving A	A is solvable

Figure 1.1: Readings of the judgment $a \in A$, cf. [ML80, p. 4]

In particular, the reading which refers to problem-solving is commonly attributed to A. Kolmogorov ([Kol32]) and called the *Brouwer-Heyting-Kolmogorov interpretation*.

What is characteristic of MLTT is that in order to ascertain that we have a set (proposition), we must prescribe an *introduction* rule, by means of showing how a *canonical* element of the set (proof of the proposition, respectively) is constructed an *equality* rule which shows how we know that two canonical elements are equal.

For example, for the set of positive integers (using the Peano approach and denoting by a' the successor of the element a), we can give the rules:

- for the canonical elements: $0 \in \mathbb{N}$ and $\dfrac{a \in \mathbb{N}}{a' \in \mathbb{N}}$;
- equality of canonical elements: $0 = 0 \in \mathbb{N}$ and $\dfrac{a = b \in \mathbb{N}}{a' = b' \in \mathbb{N}}$.

Another example, for the product of two sets (propositions) $A \times B$, we have:

- canonical elements:
$$\frac{a \in A \qquad b \in B}{(a, b) \in A \times B};$$
- equality of canonical elements:
$$\frac{a = c \in A \qquad b = d \in B}{(a, b) = (c, d) \in A \times B}$$

Now, equality of the sets (propositions) as a whole is prescribed by showing how equal and canonical elements are formed for the sets (propositions). For example, for sets (propositions), the equality is simply:
$$\frac{a = b \in A}{a = b \in B}.$$

For non-canonical elements, to explain what it means for them to be elements of a set (proposition) A, we must specify a method (proof, program) which, when executed (performed), it yields a *canonical* element of the set as a result.

Then, finally, two arbitrary (not necessarily canonical) elements of a set A are equal if, when executed as above, yield equal *canonical* elements of the set.

It is now worth focusing our attention on the particular cases of propositions. Given the setup above, we can write the table in figure 1.2.

a proof of	consists of
$\bot$	—
$A \wedge B$	a proof of A and a proof of B
$A \vee B$	a proof of A or a proof of B
$A \supset B$	a method taking any proof of A into a proof of B
$(\forall x)B(x)$	a method taking any individual a into a proof of $B(a)$
$(\exists x)B(x)$	an individual a and a proof of $B(a)$

Figure 1.2: Proofs of propositions, cf. [ML80, p. 7]

We can be more precise than that, noting further:

- the proposition $\bot$ has no possible proof;
- (a, b) is a proof of $A \wedge B$, provided that a is a proof of A and b is a proof of B;
- $i(a)$ or $j(b)$ are proofs of $A \vee B$, provided that a is a proof of A and b is a proof of B, where i and j are the canonical inclusions (which we detail later);
- $\lambda x.b(x)$ is a proof of $A \supset B$, provided that $b(a)$ is a proof of B under the hypothesis that a is a proof of A;
- $\lambda x.b(x)$ is a proof of $(\forall x)B(x)$, provided that $b(a)$ is a proof of $B(a)$, where a is some individual;
- (a, b) is a proof of $(\exists x)B(x)$, given that a is an individual and b is a proof of $B(a)$.

Also, the presentation can be extended further to *types*. From a historical, philosophical and mathematical point of view, types themselves are taken as primary notions, hence not properly defined. Intuitively though, one can think of types as "hierarchies", "levels" of certain kinds of elements or rather use the computer science intuition of *data types*.

For this case, the judgment "a is an element of type A" is commonly denoted by $a : A$ and if this is the case, we say that the type A is *inhabited*.

It can be formally shown that the type-theoretical approach is isomorphic to the propositional approach and the set-theoretical approach, making what is commonly known as the *formulas-as-types* or *propositions-as-sets* interpretations (for intuitionistic logic).

1.3 Untyped Lambda Calculus

Since in the Proust application that we present in §3 we will build a small proof assistant to verify proofs based on untyped lambda calculus, we will spend some space here to rigorously introduce some basic notions of this formalism. The simply typed version is not much more complicated and we will try to cover it briefly in the next section, in the context of dependent types.

This short presentation follows [Pie02, §5]. Much details, along with its connection to propositional logic, can be found in [SU06].

Therefore, the grammar of the untyped lambda calculus can be described in BNF as below:

$$t ::= x \mid \lambda x.t \mid tt,$$

meaning, respectively, variables, lambda abstractions and applications.

Two keywords are essential at this point:

- *metavariables* are the variables that are abstracted. So for example, in the expression $\lambda x.x^2$, x is a metavariable, since it can be renamed (consistently) without losing any meaning of the term. That is, $\lambda x.x^2$ is the same term as $\lambda y.y^2$, for example;
- the *scope* of variables is the region of the expression where it is *bound*. In the lambda term above, the variable x is bound in the whole body of the expression, λx being the actual binder. But in the term $\lambda x.\lambda y.x \cdot y$, x is bound in both the interior and the exterior lambda, while y is bound only in the interior expression. Finally, in the term $\lambda x.xy$, y is free.

  A term that has no free variables is called a *combinator*. The simplest example is the *identity function*, $\lambda x.x$.

We should also note that lambda application *associates to the left*. Hence, for example, in the expression:

$$(\lambda x.\lambda y.xy)ab,$$

we first bind x to a.

Although seemingly simple, untyped lambda calculus can be used to express some essential programming features, such as Booleans, numerals and branching expressions. They are usually called with A. Church's name as a prefix, i.e. *Church Booleans, Church numerals* and (less common) *Church branching*.

For this purpose, we introduce:

$$\texttt{true} = \lambda t.\lambda f.t$$
$$\texttt{false} = \lambda t.\lambda f.f.$$

To test this, we introduce a combinator `test`, which is basically a branching expression. That is, let:

$$\texttt{test} = \lambda l.\lambda m.\lambda n.lmn.$$

We will see how this expression reduces to m if l is `true` and it reduces to n if l is `false`. That is, we can understand the expression as:

$$\texttt{test} = \texttt{if l then m else n}.$$

Here is an example computation:

$$\begin{aligned}
\texttt{test true v w} &= (\lambda l.\lambda m.\lambda n.lmn)\texttt{true}vw \\
&\longrightarrow (\lambda m.\lambda n.\texttt{true}mn)vw \\
&\longrightarrow (\lambda n.\texttt{true}vn)w \\
&\longrightarrow \texttt{true}vw \\
&= (\lambda t.\lambda f.t)vw \\
&\longrightarrow (\lambda f.v)w \\
&= v.
\end{aligned}$$

More expressions can be defined, such as:

$$\begin{aligned}
\texttt{and} &= \lambda b.\lambda c.bc\texttt{false} \\
\texttt{pair} &= \lambda f.\lambda s.\lambda b.bfs \\
\texttt{first} &= \lambda p.p\texttt{true} \\
\texttt{second} &= \lambda p.p\texttt{false}.
\end{aligned}$$

They are detailed at [Pie02, pp. 59-60].

Finally, we reach *Church numerals*. They are lambda expressions which "act like numbers". That is, when the numeral c_n is fed as an argument to a function, it makes the function apply n times. Here are the definitions of the first few:

$$\begin{aligned}
c_0 &= \lambda s.\lambda z.z \\
c_1 &= \lambda s.\lambda z.sz \\
c_2 &= \lambda s.\lambda z.s(sz) \\
c_3 &= \lambda s.\lambda z.s(s(sz))
\end{aligned}$$

Notice the suggestive naming of variables, z reminding of zero and s reminding of the successor function. Another remark is that c_0 is actually `false`, with its variables renamed.

But we can define the successor function for Church numerals as well:

$$\texttt{succ} = \lambda n.\lambda s.\lambda z.s(nsz).$$

When applied to a Church numeral c_p, it will produce the expression of the succeeding Church numeral c_{p+1}.

We won't get into any more details here, for multiple reasons. On the one hand, the theory is reach enough to be hard to cover it extensively in this dissertation, therefore pointers to literature suffice for our purposes. On the other hand, we will not be concerned with more technical results or complications in what follows, so what we presented so far should serve as a reasonable prerequisite. We are also convinced that should novelties appear, they will be easy to grasp on the go. As we mentioned, we will be focusing on untyped lambda calculus only in presenting the Proust "nano prover" in §3.

1.4 Dependent Types — Judgments and Inference Rules

In many cases, it is very useful to have *dependent types*, namely types which, in a way, are *parametrized* by other types. A particular illustrating example is when we want to define, say, a function that selects the first element of a list, but we don't want to define it separately for lists of integers, then for lists of strings, then for lists of floats etc. We just want one function that does the job regardless of the types of the arguments.

A similar situation may be familiar from elementary mathematics. For example, if we have a *sequence of functions*, such as:

$$f_n : \mathbb{R} \longrightarrow \mathbb{R}, n \in \mathbb{N}$$

and each of the terms of the sequence is a different function, e.g.:

$$f_1(x) = \cos x, \quad f_2(x) = x^2, \quad f_3(x) = \exp(x) \dots,$$

we can say that we have *parametrized* the function f by the positive integers n which serve as the indices of the sequence.

Now imagine that the indices can be of different types, e.g. we can have $f_{a[]}$ and f_5 and $f_{'a'}$ in the same sequence and depending on the case, we know how to define the function. For example:

- for any $a \in \mathbb{Z}$, define $f_a = a^2 - 3a + 1$;
- for any vector `a[]`, define $f_{\texttt{a[]}}$ to be the sum of the elements of `a[]`;
- for any character `c`, define $f_{\texttt{c}}$ to be the ASCII code of `c`.

What we have "defined" in the toy example above is actually a *dependent function* which has one extra argument that is not obvious. So to be precise, we are defininining something like $f(x, T)$ (also written as $f(T)(x)$ or $f_T(x)$), where T is the type of x and depending on this T we actually know how to compute the value of the function in x accordingly. Once we have a fixed type T, the function is computed with a uniform formula for all arguments. So in the example above, the three rules that separate the cases for the types of the argument are each uniform: for *any integer* we compute that polynomial expression, for *any vector* we take the sum of its elements and for *any character*, we take its ASCII code.

While this may seem complicated and the example above may not be the most illuminating, we emphasize once again that dependent types are extremely useful for the case when we want to define functions that work in a similar way for various types. For example, we can modify the definitions above so that they do similar things regardless of the type of the argument:

- for any integer $a \in \mathbb{Z}$, define $f_a = a^2 - 3a + 1$;
- for any vector `a[]`, define $f_{\texttt{a[]}}$ to first compute the sum of the elements in `a[]`, store it in `s` and then compute $s^2 - 3s + 1$;
- for any character `c`, define $f_{\texttt{c}}$ to first take the ASCII code of `c`, store it in c, then compute $c^2 - 3c + 1$.

In such a situation, the function acts *as if* it is the polynomial $X^2 - 3X + 1$, computed *regardless* of the types of its arguments (integers, vectors, characters). That is, we have implemented a sort of "general polynomial" whose definition is *dependent* on the type of the argument, but the overall look is "the same".

These are the basic ideas which can also serve as motivations for what follows. We now go into a more rigorous presentation, following [Rij].

As it was seen in the theory developed by Martin-Löf, it is fundamental to specify what kinds of types, terms and judgments are primitive to one theory. In the case of the dependent type theory, we start with four primitive judgments:

(1) A is a well formed *type* in a context Γ, written as:

$$\Gamma \vdash A \text{ type};$$

(2) A and B are *judgmentally equal types* in a context Γ, written as:

$$\Gamma \vdash A \equiv B \text{ type};$$

(3) a is a well-formed *term* of type A in a context Γ, in symbols:

$$\Gamma \vdash a : A;$$

(4) a and b are *judgmentally equal terms* of type A in a context Γ, in symbols:

$$\Gamma a \equiv b : A.$$

In all the above, a *context* is just an expression which puts together all we assume to know so far. In symbols, it can be written as:

$$\Gamma = x_1 : A_1, x_2 : A_2(x_1), \dots, x_n : A_n(x_1, \dots, x_{n-1}),$$

and interpreted as being made of the statement $x_1 : A_1$ (where x_1 is a well-formed term and A_1 is a well-formed type), then $x_2 : A_2$, *but* knowing already information about x_1 and so forth, until the last statement, which presupposes the previous $n - 1$ statements.

Most of the times, we will be omitting the presuppositions, in the sense that we will just write $x_1 : A_1, \dots, x_n : A_n$. However, the presuppositions are essential, since they actually mean, for any $1 \leq k \leq n$ that:

$$x_1 : A_1, x_2 : A_2, \dots, x_{k-1} \vdash A_k \text{ type},$$

namely that they all make up the necessary hypothesis which allows us to conclude that the next item is a well-formed type (under this hypothesis).

Another item of terminology is that we say that the context Γ above *declares the variables* $x_1, \dots, x_n$. An *empty context* declares no variable and a type that is well-formed in an empty context will be called a *closed type*, as well as a well-formed of such a type will be called a *closed term*.

Getting towards dependent types, we may enrich a context with one more declaration then obtain a judgment there, such as:

$$\Gamma, x : A \vdash B \text{ type}. \tag{1.1}$$

This means that if we enlarge the context Γ with the declaration $x : A$ we can then judge that B is a well-formed type, which will be called a *type dependent on* A. An alternate name for B is actually a *family of types* over A (in context Γ), since by changing x, we can change A, which in turn could change B, but such that the judgment in (1.1) remains valid.

We should also point out that we have been emphasizing *judgments* and *judgmental* equalities. They contrast *definitions* and *definitional* equalities respectively in the sense that judgments are *derived*, whereas definitions are postulated.

Hence, in order to derive judgments, we need *inference rules*. They actually say that *judgmental equality is an equivalence relation* between judgments:

- reflexivity for types: $\dfrac{\Gamma \vdash A \text{ type}}{\Gamma \vdash A \equiv A \text{ type}}$;
- reflexivity for terms: $\dfrac{\Gamma \vdash a : A}{\Gamma a \equiv a : A}$;
- symmetry for types: $\dfrac{\Gamma \vdash A \equiv A' \text{ type}}{\Gamma \vdash A' \equiv A \text{ type}}$;
- symmetry for terms: $\dfrac{\Gamma a \equiv a' : A}{\Gamma \vdash a' \equiv a : A}$;
- transitivity for types: $\dfrac{\Gamma \vdash A \equiv A' \text{ type} \qquad \Gamma \vdash A' \equiv A'' \text{ type}}{\Gamma \vdash A \equiv A'' \text{ type}}$;

- transitivity for terms: $\dfrac{\Gamma \vdash a \equiv a' \,:\, A \qquad \Gamma \vdash a' \equiv a'' \,:\, A}{\Gamma \vdash a \equiv a'' \,:\, A}$.

Aside from these basic rules, we also have *structural rules*, which can be used in more complex derivations. They specify how *weakening*, *substitutions* and *use of variables* are performed.

(1) *Weakening a context:* As in the case of any deductive thinking, to weaken a hypothesis means to add more information to it (as opposed to strengthening it by removing information). Hence, the rule for weakening a context (denoted by W_A) is the following:

$$\frac{\Gamma \vdash A \text{ type} \qquad \Gamma, \Delta \vdash J}{\Gamma, x \,:\, A, \Delta \vdash J} W_A.$$

the explanation of the rule is as follows. We start with a context Γ where we make a typing judgment about A. Then we also assume we have a larger context, comprised of Γ and Δ in which we have a judgment J (which can be any of the four kinds introduced earlier). We conclude that in a weakened context where we include both Γ and Δ, as well as a typing judgment which makes use of A, namely the declaration of the *fresh variable* $x \,:\, A$, we can still judge J.

(2) *Variable rule:* This rule basically introduces an identity function for any type A, denoted by δ_A:

$$\frac{\Gamma \vdash A \text{ type}}{\Gamma, x \,:\, A \vdash x \,:\, A} \delta_A. \tag{1.2}$$

What we're seeing is that starting from a well-formed type, the judgment of a well-formed term of that type is automatic if we enlarge the context to contain that term as well. The identity function basically maps identically the $x \,:\, A$ from the hypothesis (context) to the conclusion (judgment).

(3) *Substitution rule:* We know already that we can rename variables consistently without changing anything in the judgments. This rule shows that we can perform substitutions consistently and this well preserve well-formedness of types, terms and judgmental equality (for types and terms):

$$\frac{\Gamma \vdash a \,:\, A \qquad \Gamma, x \,:\, A, \Delta \vdash J}{\Gamma, \Delta[a/x] \vdash J[a/x]} S_a.$$

This rule of substituting a for x basically says that we can safely substitute x with a consistently in a context and what will happen is that the substitution will propagate to the initial judgment.

The variations of this rule are for terms and types, which we write below and assume they are self-explanatory, following the explanations above:

$$\frac{\Gamma \vdash a \equiv a' \,:\, A \qquad \Gamma, x \,:\, A, \Delta \vdash B \text{ type}}{\Gamma, \Delta[a/x] \vdash B[a/x] \equiv B[a'/x] \text{ type}};$$

$$\frac{\Gamma \vdash a \equiv a' : A \qquad \Gamma, x : A, \Delta \vdash b : B}{\Gamma, \Delta[a/x] \vdash b[a/x] \equiv b[a'/x] : B[a/x]}.$$

Taking from geometry, when B is a family of types over A and we have some $a : A$, we call $B[a/x]$ *the fiber* of B at a and sometimes denote it shorter with $B(a)$.

1.5 Dependent Π Types

How do we actually "parametrize" a type in general by another type? And assume we did that. What are the well-formed terms that inhabit such types? We are about to find the answers to these questions: the types are called *(dependent) function types* or Π-types and their terms will be lambda abstractions.

Again taking from Martin-Löf, in order to specify a type, it is enough to give its *formation rule* (called *introduction* by Martin-Löf) and a rule which shows how to identify identical types of this sort. They are, respectively, the Π-formation rule and the Π-equality rule, presented below:

- Π formation: $\dfrac{\Gamma, x : A \vdash B(x) \text{ type}}{\Gamma \vdash \Pi_{(x:A)} B(x) \text{ type}} \Pi - \text{intro};$
- Π-equality: $\dfrac{\Gamma : A \equiv A' \text{ type} \qquad \Gamma, x : A \vdash B(x) \equiv B'(x) \text{ type}}{\Gamma \vdash \Pi_{(x:A)} B(x) \equiv \Gamma_{(x:A')} B'(x) \text{ type}} \Pi - \text{eq.}$

In words, if we start with a context Γ and weaken it with a declaration of a fresh variable $x : A$ (assumed arbitrary) and if in this (weakened) context we have a well-formed type which is denoted by $B(x)$ precisely to emphasize that it holds for any x, the conclusion is that we can form a type which engulfs this arbitrary x and the respective family $B(x)$. This is the so-called *product type* or Π-type and is denoted by $\Pi_{(x:A)} B(x)$. Again, we emphasize the fact that this holds for all x which is fixed for a particular type, but can be varied freely and the judgment still holds.

The situation is not dissimilar to the one we explained intuitively at the beginning of the previous section: we have some judgment (in this case, the well-formedness of the type $B(x)$) which is parametrized by some x in the sense that it can be different when changing x, but what's not different is that the judgment of well-formedness still holds true. So basically we have a sort of a *family of judgments*, that are accounted by the possible change of x.

This still holds true if we uniformly rename the parameter x. That is, assuming that $x' : A$ is a fresh variable that does not occur in the hypothesis $\Gamma, x : A$ (i.e. $x \notin \Gamma$ and $x' \neq x$), we have the Π-renaming rule:

$$\frac{\Gamma, x : A \vdash B(x) \text{ type}}{\Gamma \vdash \Pi_{(x:A)} B(x) \equiv \Pi_{(x':A)} B(x') \text{ type}} \Pi - x'/x.$$

The well-formed terms that inhabit such Π-types are special cases of λ-abstractions. Their special quality consists in that they can produce outputs of different types, *depending* (pun intended!) on the type of the input, but they do this in a uniform way, in the sense that it can be

captured in an inference rule:

$$\frac{\Gamma, x : A \vdash b(x) : B(x)}{\Gamma \vdash \lambda x.b(x) : \Pi_{(x:A)}B(x)}\lambda_A.$$

Notice how we specified everywhere that both the terms b and the types B *depend* on the choice of $x : A$.

The term $\lambda x.b(x)$ outputs a well-formed term of the product type. Intuitively, it is a general rule that can be applied "in the same way" regardless of the types of its input and which can produce different types of output.

For example, we are taught in elementary geometry that two plane vectors, understood as drawn arrows, are perpendicular if we superimpose a geometric tool for measuring angles and we see the indication of 90°. But then in high school, we learn that vectors are also pairs of reals and perpendicularity can be translated in terms of the dot product being null. Then in college, abstraction increases and we see that the same dot product can be adapted (almost identically) to functions, matrices, polynomials and other algebraic structures in the context of Euclidean vector spaces. Now we realize we know a *dependent function:* the dot product. It is computed "essentially the same" regardless of the type of its inputs: pairs or triples of reals, matrices, continuous functions, polynomials etc. The output is still a real number, so the output type does not change once the input type changes, but this is irrelevant. The basic idea is to have a uniform (rule-like) method of associating something functionally to an input, regardless of its type.

What follows now is to give a rule which enables us to infer that two lambda abstractions are identical:

$$\frac{\Gamma, x : A \vdash b(x) \equiv b'(x) : B(x)}{\Gamma \vdash \lambda x.b(x) \equiv \lambda x.b'(x) : \Pi_{(x:A)}B(x)}\lambda_A - \text{eq}$$

What this rule says is that if we start with identical terms (more precisely, *pairs* of identical terms, one pair for each parameter x), then the lambda abstractions that associates to the parameter x any of these terms are themselves identical.

Remark 1.1: A technical word of caution is appropriate here. Both in mathematics and in philosophy, we have the complementary terms of *intensional* and *extensional* equality or definitions. Their distinction is relevant here.

We call the *extension* of a concept the collection of examples or items that are characterized by that concept. For example, if the concept is "cuteness", all the cute objects belong to the extension of that concept. Mathematically, the extension of a functional concept (i.e. of a function) $f : A \longrightarrow B$ is the image of the function, namely $f(A)$.

The *intension* of a concept is the actual definition of the concept, seen in the most abstract way possible. Mathematically, the intension of a functional concept (a function) $f : A \longrightarrow B$ is the actual definition that makes up the function. So, say, if $f(x) = x^2$, the intension of f is "squaring the argument".

Now, for functions, which are one of the core concepts of this work, we have two kinds of equality:

- *extensional equality*, which says that two functions $f, g : A \longrightarrow B$ are equal iff $f(x) = g(x), \forall x \in A$, namely if $f(A) = g(A)$, i.e. their extensions coincide (as sets). This is usually called in mathematics *pointwise equality*.

- *intensional equality*, which makes two functions as above equal iff their actual definitions coincide (perhaps after algebraic manipulation). In mathematics, this is usually called *identity*, a very strong and rare relation between nontrivial objects. So for example, the functions $x \mapsto x^2$ and $y \mapsto (y + 1 - 1)^2$ are intensionally equal (they are also extensionally equal).

In general, the two notions are not the same, although it is not easy to provide counterexamples.

The point of this remark is that the rule λ_A – eq is an item of *intensional equality*, since we're assuming that the output expression of the two lambda terms are the same (as it was the case of x^2 and $(y + 1 - 1)^2$ in our example).

This distinction used to be central in the early days of type theory, especially when it was infused with philosophy (more precisely, logicism). But in (theoretical computer science) practice, intensional concepts are usually preferred, as they provide a "tighter" form of identification.

Back to the λ_A–eq rule, we also have the variation which uses fresh variables. Hence, if $x' : A$ is fresh, i.e. $x' \neq x$ and $x' \notin \Gamma$, then we have:

$$\frac{\Gamma, x : A \vdash b(x) : B(x)}{\Gamma \vdash \lambda x.b(x) \equiv \lambda x' b(x') : \Pi_{(x:A)} B(x)} \lambda_A - x'/x.$$

Whenever it is possible, we will still use the more common notation for functions, hence a *dependent function*, which is a well-formed term of a Π-type will be denoted either explicitly by the lambda notation, such as $\lambda x.b(x) : \Pi_{(x:A)} B(x)$, or implicitly, by $f : \Pi_{(x:A)} B(x)$, being understood that the argument of f is x.

The actual use of functions is contained in the *evaluation rule*:

$$\frac{\Gamma \vdash f : \Pi_{(x:A)} B(x)}{\Gamma, x : A \vdash f(x) : B(x)} \mathrm{ev}_A.$$

Moreover, basic conversions can be performed inside functional terms, both of implying that evaluation and lambda abstraction are mutually inverse operations:

- β-reduction: $\dfrac{\Gamma, x : A \vdash b(x) : B(x)}{\Gamma, x : A \vdash (\lambda y.b(y))(x) \equiv b(x) : B(x)} \beta$. This shows how λ expressions work, in general, so nothing special here.

- η-conversion: $\dfrac{\Gamma \vdash f : \Pi_{(x:A)} B(x)}{\Gamma \vdash \lambda x.f(x) \equiv f : \Pi_{(x:A)} B(x)} \eta$, which says nothing else that another name for a lambda abstraction of the form $\lambda x.f(x)$ is f.

Note that as in the case of regular (untyped) lambda calculus, functions of multiple arguments can be written as iterating lambda abstraction (which in turn produces terms of iterated Π-types). As such, a function of two arguments $(x, y) \in A \times B$ can be written as $\lambda x.\lambda y.f(x, y)$ or simply $\lambda xy.f(x, y)$, which is a term of type $\Pi_{(x:A)}\Pi_{(y:B)}B(x, y)$.

1.6 Dependent Function Types

We can obtain such types as a particular case of Π types. As such, assume A and B are both types in context Γ. First we weaken B by A (i.e. add A to the context), then form the corresponding Π-type:

$$\frac{\Gamma \vdash A\ \mathrm{type} \qquad \Gamma \vdash B\ \mathrm{type}}{\dfrac{\Gamma, x : A \vdash B\ \mathrm{type}}{\Gamma \vdash \Pi_{(x:A)}B\ \mathrm{type}}}.$$

What we achieve by this is that we somehow *fix* the type A in the intermediate step where we weakened the context Γ, since now A (by means of all its arbitrary inhabitants $x : A$) is added to the hypothesis. This means that such particular Π types contain ordinary functions $A \to B$, which is also the notation that we use for this *function type*.

It follows that all the inference rules for this type can be obtained as a particular case of Π types, so we just list them accordingly:

- $\to$-introduction (formation): $\dfrac{\Gamma \vdash A\ \mathrm{type} \qquad \Gamma \vdash B\ \mathrm{type}}{\Gamma \vdash A \to B\ \mathrm{type}}\to\text{-intro}$;
- lambda abstraction: $\dfrac{\Gamma \vdash B\ \mathrm{type} \qquad \Gamma, x : A \vdash b(x) : B}{\Gamma \vdash \lambda x.b(x) : A \to B}\lambda$;
- evaluation: $\dfrac{\Gamma \vdash f : A \to B}{\Gamma, x : A \vdash f(x) : B}\mathrm{ev}$;
- β-reduction: $\dfrac{\Gamma \vdash B\ \mathrm{type} \qquad \Gamma, x : A \vdash b(x) : B}{\Gamma, x : A \vdash (\lambda y.b(y))(x) \equiv b(x) : B}\beta$;
- η-conversion: $\dfrac{\Gamma \vdash f : A \to B}{\Gamma \vdash \lambda x.f(x) \equiv f : A \to B}\eta$.

Note that we explicitly omitted mentioning A in any of the rules (i.e. we wrote λ and not λ_A for the rule of λ-abstraction, similarly for evaluation), since as explained at the beginning of this section, function types are obtained precisely by *fixing* A, so it is understood.

Now we can obtain the proper identity function of any type A by using the variable rule (1.2):

$$\frac{\dfrac{\Gamma \vdash A\ \mathrm{type}}{\Gamma, x : A \vdash x : A}}{\Gamma \vdash \mathrm{id}_A :\equiv \lambda x.x : A \to A}.$$

We won't be getting into more complex constructions with dependent types, but we only mention that function composition is now easy to define:

$$\frac{\Gamma \vdash A \text{ type} \qquad \Gamma \vdash B \text{ type} \qquad \Gamma \vdash C \text{ type}}{\Gamma \vdash \text{comp} : (B \to C) \to ((A \to B) \to (A \to C))}.$$

In particular, the common mathematical notation $g \circ f$ will mean $\text{ev}(\text{ev}(\text{comp}, g), g)$ in this context.

1.7 Example: The Natural Numbers

As a closing theoretical example of this chapter, we show how the natural numbers can be formed as a type, using the Peano triple and the induction principle.

Therefore, we introduce $\mathbb{N}$, the *type of natural numbers*, which is a closed type, equipped with two special *closed terms*, one for zero and another one, for the successor function:

$$0 : \mathbb{N}, \quad S : \mathbb{N} \to \mathbb{N}.$$

Next, the *induction principle*:

$$\frac{\Gamma, n : \mathbb{N} \vdash P \text{ type} \qquad \Gamma \vdash p_0 : P(0) \qquad \Gamma \vdash p_S : \Pi_{(n:\mathbb{N})} P(n) \to P(S(n))}{\Gamma \vdash \text{ind}_{\mathbb{N}}(p_0, p_S) : \Pi_{(n:\mathbb{N})} P(n)} \mathbb{N}\text{ – ind.}$$

In words, this says that if we start with a type and a fixed natural n in a certain context (understood as a set of hypotheses) such that in that context, the (dependent) type $P(0)$ is inhabited by a term p_0 and the (dependent) function type $P(n) \to P(S(n))$ is also inhabited by a term p_S, then the type $P(n)$ will be inhabited. As this latter type is also dependent, it could be read as "$P(n)$ is inhabited for all $n : \mathbb{N}$".

With these at hand, we can define *addition*:

$$\text{add} : \mathbb{N} \to (\mathbb{N} \to \mathbb{N})$$

by induction. It means that we need to construct a function $\text{add}_0 : \mathbb{N} \to \mathbb{N}$ (for the base case) and another function for the inductive step:

$$\text{add}_S(f) : \mathbb{N} \to \mathbb{N},$$

under the hypotheses $n : \mathbb{N}$ and $f : \mathbb{N} \to \mathbb{N}$.

This is easy: take add_0 to be $\text{id}_{\mathbb{N}}$, the identity function, since it adds nothing to its argument (actually, it does add, *zero*) and then define the inductive step to be:

$$\text{add}_S(f) = \lambda m.S(f(m)),$$

which basically means that we are adding one to f pointwise (i.e. $\text{add}_S(f)(m) = (f(m) \mapsto f(m)+1)$).

We can derive this formally, but we skip the details and refer the reader to [Rij, pp. 12-13].

So what we get is a general addition function, add which works as expected:

$$\text{add}(n, m) = n + m$$

and using the basic terms of type $\mathbb{N}$, we can derive:

$$0 + m \equiv m, \qquad S(n) + m \equiv S(n + m).$$

We stop here with the theoretical presentation and examples, pointing the reader to the article [MM04] for another great reference that contains both excellent theoretical insight, as well as illuminating practical examples in functional programming.

Furthermore, the implementation of most elements of Martin-Löf's type theory is presented in a very readable manner in [NP90].

CHAPTER 2

RACKET CRASH COURSE

skip it and explain directly on code?

Historically speaking, Racket is based on Scheme, being formerly called PLT Scheme. As such, it expands on the standards R5RS (1998) and R6RS (2009) of Scheme and diverge more significantly from R7RS (2013). However, we will not be concerned about the differences between the languages and we will assume that all Racket syntax that we introduce is valid Scheme syntax and vice versa, unless explicitly mentioned otherwise.

Both languages emerged from a common ancestor, Lisp and as such, they use a *list syntax*. Furthermore, they use a prefix notation for the functions, predicates and mathematical operations, the so-called Polish (Łukasiewicz) notation.

The only delimiters Scheme uses are parentheses (and double quotations for strings) whereas Racket strongly suggests the use of square brackets inside parentheses for delimiting more important statements[1]

Loosely speaking, both Scheme and Racket are untyped, but they do recognize three basic types: *lists, functions* and *symbols*, the latter encompassing variables and "everything else".

A specific feature is the so-called *quoting mechanism*, denoted by a single quote (`'`) or a backtick (`` ` ``) which turns anything into a symbol and the reverse, the *unquoting mechanism*, denoted by a comma (`,`) which enforces evaluation, as in the case of a call by name versus call by value approach. For example, `'(+ 1 2)` is interpreted as the symbol (string) `(+ 1 2)`, whereas `,(+ 1 2)` means `3`.

For simple expressions, quoting can be done either with a single quote or with a backtick. However, in more complex expressions, a difference appears. The backtick is actually called *quasiquote* and it can be used in expressions containing unquote. So basically we have:

```
'(+ 1 2)                    ;; => (+ 1 2)
```

[1] Some Scheme implementations allow the use of square brackets as well, but do not enforce it and furthermore, there are interpreters that reject this syntax.

```
(define x 3)
`(+ 2 ,x)                ;; => 5     (used quasiquote)
'(+ 2 ,x)               ;; error    (used quote)
```

Moreover, there is also the *splice unquote* syntax, which is used to unquote lists. Instead of returning the whole list, as a regular unquote would do, splice unquote, denoted by `,@`, actually inserts the elements of the list:

```
(define x '(1 2 3))
`(+ 4 ,@x)               ;; => 10
```

Notice also the use of the quote in the first line, because we are just defining a (literal) list to store in `x`, whereas in the second line, we used the quasiquote, since the expression contains an unquote (the spliced one).

Another aspect of syntax is that a semicolon is used for comments and the convention is to use a single semicolon for an inline comment and two or more semicolons for comments spanning multiple lines. The output of a program is commonly written as `;; => output` inside the source code or documentation.

Remark 2.1: A short word on implementation: all the examples that we will be showcasing, as well as the included source code is tested on a Manjaro Linux operating system using the Emacs 26 editor, the included Scheme mode and the third party Racket mode.

After writing the source code, `C-c` loads the file into the respective REPL.

Some simple examples follow.

```
(+ (* 5 3) 1)       ;; => 16

(define (mod2 x)
  (lambda (x) (rem x 2)))
(mod2 5)            ;; => 1

(define (mod3 x)
  "Write the remainder of x when divided by 3"
  (cond                                          ; multiple branching
     ((equal (rem x 3) 1) write "it's 1")        ; if (x % 3 == 1)
     ((equal (rem x 3) 2) write "it's 2")        ; if (x % 3 == 2)
     (#t write "it's 0")))                       ; default (true) case

(define (add-or-quote x)
  "Add 3 if x is even or write 'hello' else"
  (cond
    ((equal (mod2 x) 0) (lambda (x) ,(+ 1 2)))
    (#t (lambda (x) 'hello))))
```

```
(set sum '(+ 1 2 3))        ; defines the variable "sum"
(set x (* ,sum 2))           ; defines x to be 12
```

Hopefully, the rest of the syntax can be understood directly from the examples that will follow. For further investigation, we recommend the official Racket documentation [rac20] and the book [FF14]. As the need requires, we will also further explain the syntax.

CHAPTER 3

PROUST

This chapter will provide an example of a great use of Racket to craft a "nano proof assistant", called Proust. The presentation closely follows [Rag16] and it will contain further clarifications as needed.

As the author mentions, the article is intended as a DIY approach for a simple proof assistant (in fact, the name derives from a weird contraction of the expression "proof assistant"). The general goal is much more interesting than that, in that it will also delve into the inner works of the underlying mechanisms of proof asistants, for the purpose of implementing them in a simpler manner.

Note that since Racket is rather a toolbox for crafting one's own toy languages, any source code must start with a `#lang` pragma, which mentions what part of Racket one wants to use. Common pragmas (formally, *modules*) include:

- `htdp` – the special module with syntax used in the [FF14] book;
- `racket` – the full-fledged module with all syntax and features;
- `racket/base` – the simplest submodule of `racket`;
- `racket/typed` – the module of Racket with strong typing;
- `scheme` – the backwards compatible module allowing one to use Scheme syntax.

To not overcomplicate the example and to skip any decision process, we will just use `#lang racket`. This will also mean that we will be working in an *untyped* environment, although we will define custom syntax for explicit type annotations and functional types.

3.1 The Grammar and Basic Parsing

First, we specify the language that we will use to make proof terms, which will be a mix of untyped lambda calculus and simple and function types. As such, the BNF grammar of the language is as follows:

$$\begin{aligned}
\texttt{expr} &::= (\lambda x \Longrightarrow \texttt{expr}) \\
&\mid (\texttt{expr}\ \texttt{expr}) \\
&\mid (\texttt{expr} : \texttt{type}) \\
&\mid x \\
\texttt{type} &::= (\texttt{type} \longrightarrow \texttt{type}) \\
&\mid X.
\end{aligned}$$

The reader will recognize, respectively: lambda abstraction, application, type inhabitance (also known as typed variable declaration) and free variables. These are the legal expressions and the types are either simple or functional.

To recognize the structures that appear, we will use the standard Racket structures (records), which will also allow pattern-matching to extract the parts that are needed. This works more or less as a DIY approach to typing, where we make things as verbose as possible, allowing for easy recognition and pattern matching for such types:

```
(struct Lam (var body) #:transparent)          ; lambda abstractions
(struct App (func arg) #:transparent)          ; application
(struct Ann (expr type) #:transparent)         ; explicit type annotations
(struct Arrow (domain range) #:transparent)    ; functional types
```

A little remark about *transparent* vs. *opaque* structures. By default, all structures defined in Racket are opaque. What this means for our purposes is that if one prints such a structure, it doesn't show anything about its internal contents. For example, printing a `Lam` will output `#<Lam>` (see the code examples that follow below). On the other hand, a transparent structure shows its internals when printed, i.e. it will print something like `(Lam 'x 'y)`.

Since by default, all Racket structures are opaque, transparency must be enabled explicitly.

The first goal of the simple proof assistant will be to parse expressions, in order to understand them appropriately and extract the needed parts. For this, we define a function `parse-expr`, which takes a so-called S-expression (standard Racket/Lisp expression) and produces an element that is a legal `expr`.

```
(define (parse-expr s)
  (match s                                ; pattern-match s
    [`(lambda ,(? symbol? x) => ,e)       ; is it a lambda expression?
        (Lam x (parse-expr e))]           ; make it a Lam
    [`(,e0 ,e1)                           ; is it an application?
        (App (parse-expr e0)              ; make it an App
```

```
          (parse-expr e1))]
    [`(,e : ,t)                          ; is it a type annotation (e : t)?
        (Ann (parse-expr e)              ; make it an Ann
             (parse-expr t))]
    [`(,e1 ,e2 ,e3 ,r ...)               ; is it a general list?
        (parse-expr
            `((,e1 ,e2) ,e3 ,@r))]       ; parse it by parts
    [(? symbol? x) x]                    ; else, it's a symbol, return it
    [else (error 'parse "bad syntax: ~a" s)]))
```

Notice the very clever use of the quoting and unquoting (including splice) mechanism in the definition of `parse-expr`, as well as the square bracket delimitation of the matching cases. The quote for the patterns ensures that we are searching for expressions that are either (literally) `(lambda ...)` or `(... ...)`, but inside the quoting we actually want to see what's there, so we evaluate the components using the unquote. The special predicate `(? symbol? x)` is used only in pattern matching, where the first question mark matches anything (similar to `*` in regular expressions). Also note that there is a convention in Lisps to name predicates (i.e. functions that return true or false) ending with a question mark. So basically the last successful case of pattern matching is used for symbols (literals).

Most of the syntax should be clear and it is also accompanied by comments which should ease understanding. The only new piece of syntax which we comment on is the *ellipse* (`...`), which is used to match anything that follows ("the rest").

Similarly, we parse type expressions:

```
(define (parse-type t)
  (match t
    [`(,t1 -> ,t2)                               ; is it a functional type?
        (Arrow (parse-type t1)                   ; make it an Arrow
               (parse-type t2))]
    [`(,t1 -> ,t2 -> ,r ...)                     ; maybe it's a multi-arg function
        (Arrow (parse-type t1)
               (parse-type `(,t1 -> ,@r)))]
    [(? symbol? X) X]                            ; is it a simple type? return it
    [else (error "can't parse this type")]))
```

To make printing clear enough, we define helper functions that do "unparsing", both for expressions and for types:

```
;; pretty-print-expr : expr -> String
(define (pretty-print-expr e)
  (match e
    [(Lam x b) (format "(lambda ~a => ~a)" x (pretty-print-expr b))]
    [(App e1 e2) (format "(~a ~a)"
                         (pretty-print-expr e1)
```

```
                          (pretty-print-expr e2))]
    [(? symbol? x) (format "~a" x)]
    [(Ann e t) (format "(~a : ~a)"
                       (pretty-print-expr e)
                       (pretty-print-expr t))]))

;; pretty-print-type : Type -> String
(define (pretty-print-type t)
  (match t
    [(Arrow t1 t2) (format "(~a -> ~a)"
                           (pretty-print-type t1)
                           (pretty-print-type t2))]
    [else t]))
```

Notice another piece of new syntax in formatted printing, where the `a` placeholder is used, i.e. it will be replaced by the arguments that follow. For example, the syntax `(format "~a" 'x)` will put the symbol `x` in place of `"~a"` when printing.

When evaluating and checking proofs, we will need a *context*, which is defined as a `(listof (List Symbol Type))`. The `listof` keyword is called a *contract* in this case and in short, it *asserts* that what it expects is a list with a symbol and a type. If the context does not respect the contract, we get a specific error. Racket provides extensive support for software contracts, for various items such as structures, functions, variables, but we do not actually need any such complexity here, so we will only indicate [Com] for further information. Also, for (judgments in) contexts, we refer the reader to our §1.4, where we see that a context Γ is basically made of lists of typed variable declarations of the form $x : A$.

Now, given the fact that a context is a list of a symbol and a type, we can `pretty-print` it as well using the function:

```
(define (pretty-print-context ctx)
  (cond
    [(empty? ctx) ""]
    [else (string-append (format "\n~a : a"
                                 (first (first ctx))
                                 (pretty-print-type (second (first ctx))))
          (pretty-print-context (rest ctx)))]))
```

3.2 Checking Lambdas

Now, given this setup, we can actually start writing the functions for the proofs. **We remark explicitly that for the purposes of this chapter, we will only present the part that uses lambda terms for proofs.**

First, type-checking, which checks whether an expression has a certain type in a given context.

```
;; type-check : Context Expr Type -> Boolean
;; produces true if expr has type t in context ctx
;; (else, error)
(define (type-check ctx expr type)
  (match expr
    [(Lam x t)              ; is expr a lambda expression?
      (match type           ; then the type must be an arrow
        [(Arrow tt tw) (type-check (cons `(,x ,tt) ctx) t tw)]
        [else (cannot-check ctx expr type)])]
  [else (if (equal? (type-infer ctx expr) type) true    ; fail for other types
            (cannot-check ctx expr type))]))

;; the error function
(define (cannot-check ctx expr type)
  (error 'type-check "cannot typecheck ~a as ~a in context:\n~a"
    (pretty-print-expr expr)
    (pretty-print-type type)
    (pretty-print-context ctx)))
```

Then the function that tries to make a type inference.

```
;; type-infer : Context Expr -> Type
;; tries to produce type of expr in context ctx
;; (else, error)
(define (type-infer ctx expr)
  (match expr
    [(Lam _ _) (cannot-infer ctx expr)]     ; lambdas are handled in type-check
    [(Ann e t) (type-check ctx e t) t]      ; check type annotations
    [(App f a)                              ; function application
        (define tf (type-infer ctx f))
          (match tf                         ; must be arrow type
            [(Arrow tt tw) #:when (type-check ctx a tt) tw] ; when the rest typechecks
            [else (cannot-infer ctx expr)])]
    [(? symbol? x)                          ; for symbols
       (cond
         [(assoc x ctx) => second]          ; if it's a list, the second is the type
         [else (cannot-infer ctx expr)])])) ; else, not okay

;; the error function
(define (cannot-infer ctx expr)
  (error 'type-infer "cannot infer type of ~a in context:\n~a"
    (pretty-print-expr expr)
    (pretty-print-context ctx)))
```

3.3 Basic Testing

Now we can define a function that checks some basic proofs like so:

```
(define (check-proof p)
    (type-infer empty (parse-expr p)) true)
```

This way, if errors do not appear, the function will successfully apply the `type-infer` procedure and return `true`, which can be seen as a "successful exit code".

Using this, we can use the Racket testing module to check some basic proofs, such as:

```
(require test-engine/racket-tests)              ; import the test module

;; check whether check-proof returns true => good proof
;; lambda xy.x : A -> (B -> A)
(check-expect
  (check-proof '((lambda x => (lambda y => x)) : (A -> (B -> A))))
    true)

;; lambda xy.yx : (A -> ((A -> B) -> B))
(check-expect
  (check-proof '((lambda x => (lambda y => (y x))) : (A -> ((A -> B) -> B))))
    true)

;; lambda fgx.f(gx) : ((B -> C) -> ((A -> B) -> (A -> C)))
(check-expect
  (check-proof '((lambda f => (lambda g => (lambda x => f (g x)))) :
                    ((B -> C -> ((A -> B) -> (A -> C))))))
    true)

(test)          ;; => All 3 tests passed.
```

Formally, what `check-proof` does is to verify well-formedness of typing judgments for lambda expressions (see our §1). As such, for example, the first proof checks the typing for the Church Boolean `true` in our §1.3.

The other two proofs are just simple exercises. We can also write, for example, the typing for the Church numeral c_1 (again, see §1.3). Given that:

$$c_1 = \lambda s.\lambda z.sz = \lambda sz.sz,$$

we have:

```
;; c1 = lambda sz . sz : ((A -> B) -> (A -> B))
(check-expect
```

```
  (check-proof '((lambda s => (lambda z => (s z))) : ((A -> B) -> (A -> B))))
    true)
(test)                    ;; => All 1 test passed.
```

is it OK?

CHAPTER 4

PIE

BIBLIOGRAPHY

[AS96] Harold Abelson and Gerald Sussman. *Structure and Interpretation of Computer Programs*. MIT Press, 1996.

[Com] The Racket Community. Contracts. https://docs.racket-lang.org/guide/contracts.html. Accessed March 2020.

[FF14] Matthias Felleisen and Bruce Findler. *How to Design Programs*. MIT Press, 2014.

[Gir90] Jean-Yves Girard. *Proofs and Types*. Cambridge University Press, 1990.

[Gro] The HoTT Group. Homotopy type theory. https://homotopytypetheory.org/. Accessed March 2020.

[Hey66] Arend Heyting. *Intuitionism, an Introduction*. Dover, 1966.

[Kol32] Andrei Kolmogorov. Zur deutung der intuitionistichen logik. *Mathematische Zeitschrift*, 1932.

[McC60] John McCarthy. Recursive functions of symbolic expressions and their computation by machine. *Commun. ACM*, 3(4):184–195, April 1960.

[McC61] John McCarthy. A basis for a mathematical theory of computation. *Western Joint Computer Conference*, 1961.

[McC62] John McCarthy. Towards a mathematical science of computation. *IFIP-62*, 1962.

[ML80] Per Martin-Löf. Intuitionistic type theory. Lectures in Padua, 1980. Notes by Giovanni Sambin.

[MM04] Conor McBride and James McKinna. The view from the left. *Journal of Functional Programming*, 14(1):69–111, 2004.

[NP90] Bengt Nordström and Kent Petersson. *Programming in Martin-Löf Type Theory*. Oxford University Press, 1990. Freely available at http://www.cse.chalmers.se/research/group/logic/book/.

[Pie02] Benjamin Pierce. *Types and Programming Languages*. MIT Press, 2002.

[plt20] The PLT group. https://racket-lang.org/people.html, 2020. Accessed: March 2020.

[rac20] Racket. https://racket-lang.org/, 2020. Accessed: March 2020.

[Rag16] Prabhakar Ragde. Proust: A nano proof assistant. In Johan Jeuring and Jay McCarthy, editors, *Trends in Functional Programming in Education*, pages 63–75. arXiv/cs.PL, 2016.

[Rij] Egbert Rijke. Introduction to homotopy type theory. .

[S+13] Gerald Sussman et al. Revised7 Report on the Algorithmic Language Scheme. Technical report, Scheme Working Group, 7 2013.

[SU06] Morten Sørensen and Pawel Urzyczyn. *Lectures on the Curry-Howard Isomorphism*. Elsevier Science, 2006.