Contents

1 Introduction

This serves as a brief starting point for understanding how the Curry-Howard correspondence appears in Lean, as well as being an introduction to the language itslef. Lean is both a **functional programming language** and a **theorem prover**. We'll focus primarily on its role as a theorem prover. But what does this mean, and how can that be achieved?

A programming language defines a **set of rules, semantics, and syntax** for writing programs. To achieve a goal, a programmer must write a program that meets given specifications. There are two primary approaches: **program derivation** and **program verification** ([NPS90] Section 1.1). In **program verification**, the programmer first writes a program and then proves it meets the specifications. This approach checks for errors at **runtime** when the code executes. In **program derivation**, the programmer writes a proof that a program with certain properties exists, then extracts a program from that proof. This approach enables specification checking during **compilation**, catching errors before execution. This distinction corresponds to **dynamic** versus **static type systems**. Most programming languages employ both approaches. For example, C checks operations on `int` at compile time but requires the programmer to ensure correctness with `void*` at run time. Lean emphasizes program derivation. Its type system is highly advanced and flexible, allowing the expression and verification of a wide range of mathematical statements, and this is what makes Lean a powerful **theorem prover**. Lean's type system is based on **Type Theory**, a branch of marthematics and logic tahta aims to provide a foundation for all mathematics and wich is a programming language itself.

It's important to note that Type Theory is not a single, unified theory, but rather a family of related theories with various extensions and ongoing developments and rich hiostorical ramifications. Creating a language like Lean require careful consideration of which rules and features to include. We shall give a brief overview of the historical development of type theory, and an a introduction on what comes next.

(From [Car19]) Type theory emerged as a fundamental response to Bertrand Russell's paradox. Considers the set $S = \{x \mid x \notin x\}$ (the set of all sets that do not contain themselves). This is a paradoxical construction, leading to the contradiction $S \in S \iff S \notin S$. Ernst Zermelo and Fraenkel addressed the contradiction by introducing Zermelo-Fraenkel set theory (ZFC), which became the standard axiomatization in modern mathematics. ZFC provides an untyped but stratified view of the mathematical universe, maintaining classical logical principles while avoiding paradoxes through careful axiomatization. Russell

chose a fundamentally different path. He recognized expressions like $A(A)$ or $x \in x$ as ill-typed, introducing his theory of types. Hs's first systematic response was **Ramified Type Theory**, wich turned out to be problematic. In the 1930s, Alonzo Church developed **Lambda Calculus** as a foundation for mathematics, initially pursuing a type-free approach. However, Church's original untyped system suffered from inconsistencies. To address these issues, Church introduced the **Simply Typed Lambda Calculus** in 1940 ([Chu40]). This system is a version of **Simple Type Theory**, a framework able to replace set-theory and propositional logic. Lambda calculus influenced the development of many programming languages as being a foundation for functional programming. Per Martin-Löf revolutionized type theory in the 1970s by introducing **dependent types** that can depend on values of other types. Think for instance of a of vectors of length n or a sequnce of n elements. **Dependent Type Theory** extends the expressive power of type systems by allowing the representation of quantifiers, providing a framework capable of replacing set theory and predicate logic. Dependent Type Theory is a derivation of **Martin-Löf Type Theory** (also known as **Intuitionistic Type Theory**). Martin-Löf's system embraced constructive principles, requiring that the existence of mathematical objects be demonstrated through explicit construction rather than classical proof by contradiction. Martin-Löf Type Theory also introduced **identity types** to represent equality. In the 1980s, Thierry Coquand and Gérard Huet introduced the **Calculus of Constructions** (CoC), synthesizing insights from Martin-Löf's dependent type theory with higher-order **polymorphism**. The Calculus of Constructions served as the theoretical foundation for the Coq proof assistant, one of the most influential interactive theorem provers. The original CoC was later extended with **inductive types** to form the **Calculus of Inductive Constructions** (CIC). Inductive types allow for the definition of data structures like natural numbers, lists, and trees. The Lean theorem prover, developed by Leonardo de Moura and others, is also based on CIC but incorporates several important refinements and differences from Coq's implementation.

A central insight in type theory is the **Curry-Howard correspondence**, which establishes a profound connection between logic and computation. Also known as the **propositions-as-types** principle, this correspondence represents one of the most elegant discoveries in the foundations of mathematics and computer science. It serves also well as a good introduction to type theory, and will be used in this discussion. Nontheless it continuelsy shows new applications and interpretations in modern type theories. The Curry-Howard correspondence was independently discovered by multiple researchers. **Haskell Curry** (1934) first observed the connection between combinatory logic and Hilbert-style proof systems. **William Alvin Howard** (1969) significantly extended the correspondence to natural deduction and the simply typed lambda calculus in his seminal work "The Formulae-as-Types Notion of Construction." The correspondence was further developed through **N.G. de Bruijn's AUTOMATH system** (1967), which was the first working proof checker and demonstrated the practical viability of mechanical proof verification. Amongst its technical innovations are a discussion of the irrelevance of proofs when working in a classical

context, which is one of the reasons advanced by de Bruijn for the separation between the notions of type and prop in the system [Tho99]. Lean also adopts this separation . **Per Martin-Löf's type theory** extended the correspondence to dependent types, allowing for the representation of quantifiers and identity types. Modern proof assistants like Coq, Lean, Agda, and Isabelle/HOL all leverage variants of the Curry-Howard correspondence to enable formal verification of mathematical theorems and software correctness properties.

2 Introduction to Logic

Logic is the study of reasoning, branching into various systems. We refer to **classical logic** as the one that underpins much of traditional mathematics. It's the logic of the ancient Greeks (not fair) and truthtables, and it remains used nowadays for pedagogical reasons. We first introduce **propositional logic**, which is the simplest form of classical logic. Later we will extend this to **first-order logic**, which includes quantifiers and predicates. In this setting, a **proposition** is a statement that is either true or false, and a **proof** is a logical argument that establishes the truth of a proposition. Propositions are constructed via **formulas** built from **propositional variables** (also called atomic propositions) combined with logical **connectives** such as "and" ($\wedge$), "or" ($\vee$), "not" ($\neg$), "implies" ($\Rightarrow$), and "if and only if" ($\Leftrightarrow$). These connectives allow the creation of complex or compound propositions.

Definition 2.1 (Propositional Formula) *([Tho99]) A **propositional formula** is either:*

- *A **propositional variable:** $X_0, X_1, X_2, \ldots$, or*
- *A **compound formula** formed by combining formulas using connectives:*

$$(A \wedge B), \quad (A \Rightarrow B), \quad (A \vee B), \quad \bot, \quad (A \Leftrightarrow B), \quad (\neg A)$$

  where A and B are formulas themselves.

We are going to describe classical logic though a formal framework called **deduction system** that specifies rules for deriving **conclusions** from **premises** (assumptions from other propositions). These rules, called **inference rules**, determine how new statements follow from existing ones.

Example 2.2 (Deductive style rule) *Here is an hypothetical example.*

$$\frac{P_1 \qquad P_2 \qquad \cdots \qquad P_n}{C}$$

where the premises $P_1, P_2, \ldots, P_n$ and the conclusion C.

The inference rules needed are:

- **Introduction rules** specify how to form compound propositions from simpler ones, and

- **Elimination rules** specify how to use compound propositions to derive information about their components.

Let's look at how we can define some connectives.

Conjunction ($\wedge$)

- Introduction

$$\frac{A \qquad B}{A \wedge B} \wedge\text{-Intro}$$

- Elimination

$$\frac{A \wedge B}{A} \wedge\text{-Elim}_1$$

$$\frac{A \wedge B}{B} \wedge\text{-Elim}_2$$

Disjunction ($\vee$)

- Introduction

$$\frac{A}{A \vee B} \vee\text{-Intro}_1$$

$$\frac{B}{A \vee B} \vee\text{-Intro}_2$$

- Elimination (Proof by cases)

$$\frac{A \vee B \qquad [A] \vdash C \qquad [B] \vdash C}{C} \vee\text{-Elim}$$

Implication ($\rightarrow$)

- Introduction

$$\frac{[A] \vdash B}{A \rightarrow B} \rightarrow\text{-Intro}$$

- Elimination (Modus Ponens)

$$\frac{A \rightarrow B \qquad A}{B} \rightarrow\text{-Elim}$$

Notation 2.3 *We use $A \vdash B$ (called turnstile) to designate a deduction of B from A. Normally the symbol used is*

$$\begin{array}{c} A \\ \vdots \\ B \end{array}$$

There are some minor differences, in fact, which I don't fully understand. The square brackets around a premise $[A]$ mean that the premise A is meant to be ***discharged*** *at the conclusion. The classical example is the introduction rule for the implication connective. To prove an implication $A \to B$, we assume A (shown as $[A]$), derive B under this assumption, and then discharge the assumption A to conclude that $A \to B$ holds without the assumption. The turnstile is predominantly used in judgments and type theory with the meaning of "entails that".*

Lean has its own syntax for connectives and their relative inference rules. For instance $A \wedge B$ can be presented as `A ∧ B`, `And(A, B)`, `⟨A, B⟩` or explicitly by the introduction rule `And.intro`. The pair $A \wedge B$ can be then consumed using elimination rules `And.left` and `And.right`.

Example 2.4 *Let's look at our first code example*

```
example (H_A : A) (H_B : B) : (A ∧ B) := And.intro H_A H_B
```

Lean aims to resemble the language used in mathematics. For instance, when defining a function or expression, one can use keywords such as `theorem` or `def`. Here, I used `example`, which is handy for defining anonymous expressions for demonstration purposes. After that comes the statement to be proved:

```
(H_A : A) (H_B : B) : (A ∧ B)
```

Meaning given a proof of A and a proof of B we can form a proof of $(A \wedge B)$. The operator `:=` expects a proof of the previous statezment. `And.intro` is implemented as:

```
And.intro: p → q → (p ∧ q).
```

It says: if you give me a proof of p and a proof of q, then i return a proof of $p \wedge q$. We therefore conclude the proof by directly giving `And.intro H_A H_B`. Here another way of writing the same statment.

```
example (H_p : p) (H_B : B) : And(A, B) := ⟨H_p, H_B⟩
```

This system of inference rules allows us to construct proofs in an algorithmic and systematical way, organized in what is called a **proof tree**. To reduce complexity, we follow a **top-down** approach (see [Tho99] and [NPS90]). This methodology forms the basis of **proof assistants** like Lean, Coq, and Agda, which help verify the correctness of mathematical proofs by checking each step

against these rules. We will see later that Lean, in fact, provides an info view of the proof tree which helps us understand and visualize the proof structure. Let's examine a concrete example of a proof.

Example 2.5 (Associativity of Conjunction) *We prove that $(A \wedge B) \wedge C$ implies $A \wedge (B \wedge C)$. First, from the assumption $(A \wedge B) \wedge C$, we can derive A:*

$$\dfrac{\dfrac{(A \wedge B) \wedge C}{A \wedge B} \wedge E_1}{A} \wedge E_1$$

Second, we can derive $B \wedge C$:

$$\dfrac{\dfrac{\dfrac{(A \wedge B) \wedge C}{A \wedge B} \wedge E_1}{B} \wedge E_2 \qquad \dfrac{(A \wedge B) \wedge C}{C} \wedge E_2}{B \wedge C} \wedge I$$

Finally, combining these derivations we obtain $A \wedge (B \wedge C)$:

$$\dfrac{(A \wedge B) \wedge C \vdash A \qquad (A \wedge B) \wedge C \vdash B \wedge C}{A \wedge (B \wedge C)} \wedge I$$

Example 2.6 (Lean Implementation) *Let us now implement the same proof in Lean.*

```
theorem and_associative : (A ∧ B) ∧ C → A ∧ (B ∧ C) :=
  fun h : (A ∧ B) ∧ C =>
    -- First, from the assumption (A ∧ B) ∧ C, we can derive A:
    have ab : A ∧ B := h.left -- extracts (A ∧ B) from the assumption
    have a : A := ab.left -- extracts A from (A ∧ B)
    -- Second, we can derive B ∧ C (here we only extra b and c
    separately and combined them in the next step)
    have c : C := h.right
    have b : B := ab.right
    -- Finally, combining these derivations we obtain A ∧ (B ∧ C)
    show A ∧ (B ∧ C) from ⟨a, ⟨b, c⟩⟩
```

Listing 1: Associativity of Conjunction in Lean

We introduce the `theorem` *with the name* `and_associative`*, which can be referenced in subsequent proofs. The type signature* `(A ∧ B) ∧ C → A ∧ (B ∧ C)` *represents our logical implication. The* `:=` *operator introduces the proof term that establishes the theorem's validity. In the previous code example this proof was directly given. Here, we construct it using the a function with the* `fun` *keyword. Why a function? We have already encountered the Curry-Howard correspondence in Lean previously, though without explicitly stating it. According to this correspondence, a proof of an implication can be understood as a function that takes a hypothesis as input and produces the desired conclusion as output. We will revisit this concept in more detail later. The* `have` *keyword introduces local lemmas within our proof scope, allowing us to break down complex reasoning into manageable intermediate steps, mirroring our natural deduction proof. Finally, the* `show` *keyword presents our final result.*

To capture more complex mathematical ideas, we extend our system from propositional logic to **predicate logic**. A **predicate** is a statement or proposition that depends on a variable. In propositional logic we represent a proposition simply by P. In predicate logic, this is generalized: a predicate is written as $P(a)$, where a is a variable. This extension allows us to introduce **quantifiers**: $\forall$ ("for all") and $\exists$ ("there exists"). These quantifiers express that a given formula holds either for every object or for at least one object, respectively.

When introducing variables into a formal system, typically denoted by lowercase letters, we must keep in mind that the specific choice of a variable name can be substituted without changing the meaning of the predicate or statement. This should feel familiar from mathematics, where the meaning of an expression does not depend on the names we assign to variables. Some variables are **bound** (constrained), while others remain **free** (arbitrary, in programming often called "dummy" variables). When substituting variables, it is important to ensure that this distinction is preserved. This phenomenon,called **variable capture**, parallels familiar mathematical practice: if $f(x) \coloneqq \int_1^2 \frac{dt}{x-t}$, then $f(t)$ equals $\int_1^2 \frac{ds}{t-s}$, not the ill-defined $\int_1^2 \frac{dt}{t-t}$. The same principle applies to logic. Variable capture occurs when a free variable becomes bound by a quantifier during substitution, fundamentally changing the meaning of the expression. For example, consider

$$\exists y.\, (y > x).$$

This states that for a given x there exists a y such that $y > x$. If we naively substitute $y + 1$ for x, we would obtain

$$\exists y.\, (y > y + 1),$$

where the y in $y + 1$ has been **captured** by the quantifier $\exists y$. This transforms the original statement from "there exists some y greater th an the free variable x" into the always-false statement "there exists some y greater than itself plus one."

To avoid capture, we must use **capture-avoiding substitution**. In the above example, we would first rename the bound variable to something fresh (say z), obtaining $\exists z.\, (z > x)$, and then safely substitute to get $\exists z.\, (z > y + 1)$. In programming, this concept is also familiar through block-structured code and scope. In Lean, for instance, when you are inside a block such as a function, theorem, or section, all the variables inside this context are bound to this specific scope (block) and cannot be referenced outside. We use the notation $\phi[t/x]$ for **substitution**, meaning all occurrences of the free variable x in formula ϕ are replaced by term t. This notation can be read as "t falling over and squishing x" — a helpful mnemonic for remembering that t replaces x, not the other way around.

We can now present the inference rules for quantifiers.

For all ($\forall$)

- Introduction

$$\frac{A}{\forall x.\, A}\,\forall I$$

- Elimination

$$\frac{\forall x.\, A}{A[t/x]}\,\forall E$$

Exixst ($\exists$)

- Introduction

$$\frac{A[t/x]}{\exists x.\, A}\,\exists I$$

- Elimination

$$\frac{[A] \vdash B}{B}\,\forall E$$

Lean espresses quantifiers with dependent types.

```
∀ (x : X), P x
```

Listing 2: For All

Three syntactic forms:

- Explicit: `∀ (x : X), P x`
- Type inference: `∀ x, P x` (when Lean can infer the type)
- Implicit binding: `∀ \{x : X\}, P x` (Lean infers the value automatically)

Proof techniques:

- **Introduction**: Use the `intro` tactic to introduce an arbitrary element
- **Elimination**: Apply the hypothesis to a specific value using function application
- **Specialization**: Use the `specialize` tactic to instantiate a general hypothesis

References

[Car19] Mario Carneiro. *The Type Theory of Lean*. Manuscript. Accessed: September 1, 2025. Apr. 2019. URL: https://github.com/digama0/lean-typetheory/.

[Chu40] Alonzo Church. *A Formulation of the Simple Theory of Types*. Vol. 5. 2. Association for Symbolic Logic, 1940, pp. 56–68.

[NPS90] Bengt Nordström, Kent Petersson, and Jan M. Smith. *Programming in Martin-Löf's Type Theory: An Introduction*. Now available from https://www.cse.chalmers.se/research/group/logic/book/book.pdf. Oxford, UK: Oxford University Press, 1990. URL: https://www.cse.chalmers.se/research/group/logic/book/book.pdf.

[Tho99] Simon Thompson. *Type Theory & Functional Programming*. March 1999. Computing Laboratory, University of Kent, 1999.