

Formal Verification of Central Limit Theorem in HOL Theorem Prover

Thi Cam Tu Phan

A thesis submitted for the degree of

Master of Computing (Advanced)

The Australian National University

School of Computing



Australian
National
University

May 2025

© Copyright by Thi Cam Tu Phan, 2025

All Rights Reserved

Abstract

Contents

Introduction

The idea of a formalised mechanist is simple but powerful: if we want to trust mathematics in software, we must mechanise not only calculations but also proofs. A mechanist builds a logic engine where every theorem arises from a small set of primitive rules. If those rules are sound, then everything derived from them inherits that soundness.

HOL4 supports this mechanised philosophy ?. It encodes logic using a typed λ -calculus and enforces soundness by restricting theorem creation to a protected MetaLanguage (ML) type. The only way to construct a theorem is by applying primitive inference rules written in Standard ML. This ensures that the proof kernel checks every line of reasoning with absolute rigour.

In this thesis, we formalise one of the most important results in probability theory: the Central Limit Theorem (CLT). When many independent effects accumulate, their combined influence often resembles a bell curve. We observe this phenomenon across a wide range of domains—from biological traits and human measurements to economic indicators and communication errors. The CLT explains this universality.

We follow the version of the Central Limit Theorem stated in ? and proved using Lindeberg’s method. Let $\{X_j\}_{j=1}^n$ be a sequence of independent random variables such that:

$$\mathbb{E}[X_j] = 0, \quad \mathbb{E}[X_j^2] = \sigma_j^2, \quad \mathbb{E}[|X_j|^3] = \gamma_j < \infty.$$

Define the sum $S_n = \sum_{j=1}^n X_j$, the total variance $s_n^2 = \sum_{j=1}^n \sigma_j^2$, and the total third moment $\Gamma_n = \sum_{j=1}^n \gamma_j$. If the Lyapunov condition

$$\lim_{n \rightarrow \infty} \frac{\Gamma_n}{s_n^3} = 0$$

holds, then the normalised sum $\frac{S_n}{s_n}$ converges in distribution to the standard normal:

$$\frac{S_n}{s_n} \xrightarrow{d} \mathcal{N}(0, 1).$$

This convergence result explains why the normal distribution emerges from a wide

variety of processes, even when individual random variables follow skewed or irregular distributions.

We do not assume probability theory or integration as axioms. Instead, we construct them from first principles in HOL4 using its existing real number, measure theory, and Lebesgue integration libraries. We define random variables, convergence in distribution, and weak limits in this framework. We then prove the CLT using the Lindeberg replacement method and Taylor expansion bounds, following the structure outlined in ?. Here is the Lyapunov's form of the Central Limit Theorem in HOL4:

```
Theorem central_limit_theorem :
  ⊢ ∀p X N. prob_space p ∧
  ext_normal_rv N p 0 1 ∧
  (∀i. real_random_variable (X i) p) ∧
  (∀n. indep_vars p X (λi. Borel) (count n)) ∧
  (∀i. expectation p (X i) = 0) ∧
  (∀i. expectation p (λx. (abs (X i x)) pow 3) < +∞) ∧
  (∀i. variance p (X i) < +∞) ∧
  (∀i. variance p (X i) ≠ 0) ∧
  (∀n. (sqrt (second_moments p X n)) ≠ 0) ∧
  ((λn. (third_moments p X n) / ((sqrt (second_moments p X n)) pow 3)) --> 0)
  sequentially ⇔
  ((λn x. (SIGMA (λi. X i x) (count n)) / (sqrt (second_moments p X n))) --> N)
  (in_distribution p)
```

Despite not yet completing the final convergence proof, this thesis represents a significant step toward a fully mechanised proof of Lyapunov's Central Limit Theorem in HOL4. The author developed over 6000 lines of formalisation code, building most of the necessary measure-theoretic and probabilistic infrastructure. Early progress was slowed by the need to learn the HOL4 system and an initial attempt to formalise the CLT using moment-generating functions—a path that proved impractical due to missing theorems in the HOL4 library at the time. The current approach, based on Lindeberg's method and Taylor expansion, has succeeded in formalising all major components of the proof. The only remaining step—formalising the Taylor error bound and completing the convergence argument—involves calculating the absolute third moment of the normal distribution. This means formalizing integrals using the gamma function and complex numbers, which are currently not yet fully realized in HOL4. At the time of writing the report, the author is still in the midst of this last step. Even if it is still incomplete at the submission deadline, the overall structure and supporting lemmas are all in place, and the last bound is now a question of careful implementation instead of conceptual difficulty.

1.1 Motivation

The Central Limit Theorem (CLT) is more than just a result in probability theory—it is the mathematical explanation behind the bell curve that appears across nature, science, and data. When we take a large number of independent random variables with finite variance, their properly normalised sum tends toward a normal distribution, regardless of the original distributions of the individual variables. This effect manifests in physical measurements, biological readings, economic results, and even in computation roundoff errors. The CLT illustrates the reasons why such behavior is not accidental but is necessary mathematically under gentle hypotheses.

Although succinctly phrased, the CLT is of very deep mathematical organization. Most textbook proofs rely on informal approximations or skip foundational details. In formal verification, this level of vagueness is unacceptable. We need a version of the CLT where every assumption is explicit, every step justified, and the entire argument checked by machine.

Some existing formal proofs of the CLT, such as the one in Isabelle/HOL, focus on the independent identical distribution (i.i.d.) case and rely on characteristic functions and the Lévy Continuity Theorem. That approach is elegant, but it depends on complex analysis and Fourier transforms, and does not generalise easily to sums of non-identically distributed variables. Moreover, HOL4's complex number library is still underdeveloped and lacks many of the theorems needed to support such an approach effectively. Attempting to formalise the necessary complex theory would demand substantial additional effort—likely more than what is needed for the Lindeberg-based approach we follow in this work.

In this thesis, we aim for something different. We want to formalise a version of the CLT that:

- allows non-identically distributed variables;
- avoids characteristic functions entirely;
- uses only measure-theoretic and analytical tools available in HOL4.

We follow the proof given in [1], based on Lindeberg's replacement trick and Taylor expansion bounds. This approach aligns closely with classical analysis and is modular enough to support future generalisations—such as multidimensional CLTs or stable laws.

By formalising this proof in HOL4, we not only demonstrate that the CLT is derivable in a foundational logical system, but also contribute tools and theorems that strengthen HOL4's probability theory library for future formalisation work.

1.2 Thesis Contributions

The contribution of this work is the formalisation of Lyapunov’s form of the Central Limit Theorem in HOL4, using the Lindeberg replacement strategy and Taylor approximation techniques. This required building up the necessary infrastructure for real-valued random variables, expectations, variances, and convergence in distribution from the ground up.

In particular:

- We constructed the formal setting for expressing the CLT in Lyapunov form, augmenting HOL4 with normalisation tools, moment summation tools, and standardisation tools.
- We established the background required to define and establish bounds on expectations using Taylor expansion, including a remainder term of order three.
- We proved key lemmas for the Lindeberg substitution trick, which summarizes how to replace original variables by Gaussian approximations and bound resulting error.
- We defined the final convergence goal in terms of convergence in distribution with a well-defined formulation and separation of technical specifications.

1.3 Structure of the Thesis

The remainder of this thesis is organised as follows. Chapter 2 reviews the Central Limit Theorem, its historical development, and the version we aim to formalise. It also surveys related work, including formal proofs in systems such as Isabelle/HOL. Chapter 3 introduces the HOL4 theorem prover and outlines the relevant libraries and foundational setup. Chapter 4 presents the core of the formalisation, including the supporting lemmas and structure of the proof. Chapter 5 discusses the results and places this work in the context of other efforts in formalised mathematics. Chapter 6 summarises the thesis by stating the contributions and providing guidance for future development of probability theory in HOL4. This research proves that a formalisation of the Central Limit Theorem in HOL4 is possible. It strengthens the basis of HOL4’s probability library, provides reusable tools for future developments, and establishes the system as a platform for fully verified mathematics.

Background and Related Work

The Central Limit Theory is one of the main theoretical results from the Probability theory, a bridge from individual randomness to aggregate predictability. It marks the gradual approach of mathematical rigor and upgrading of the theorem used by addressing more and more difficult problems. Over centuries, different forms of CLTs have been derived, each of which has added to its understanding convergence and applications. This chapter will present the historical development of the CLT that describes its milestones and contributions. It will also examine the modern theorem proving tools and ways of formalization, focusing on Lyapunov's approach.

2.1 Historical Background

Let us just trace briefly the historical evolution of the CLT, critical milestones, key contributors, and the gradual refinement of its conditions and scope. The roots of the CLT go back to the dispute of the eighteenth century, specifically to the time Abraham de Moivre laid the foundation for this theorem. In 1733, de Moivre showed that the sum of a large number of independent and identically distributed random variables converges to the normal distribution-an elegant approximation to problems such as the rolling of dice or repeated coin flips ?. His work initiated the interplay between discrete distributions-such as the Binomial-and their continuous approximations, and laid the ground for developments to come.

In 1810, Pierre-Simon Laplace independently extended de Moivre's insights by proving a much more general form of this theorem. Under broader conditions, Laplace demonstrated convergence of the sum of independent random variables to a normal distribution, thereby establishing CLT as a universal principle. His work was used in applying the CLT to population statistics and measurement errors ? and cemented its usefulness for aggregate phenomena analysis.

The 19th century would see the formalization of the central limit theorem (CLT) by Pafnuty Chebyshev, who also gave the theorem a rigorous foundation by the introduction of variance and expectation conditions. With that work, Chebyshev rendered the CLT mathematically precise, linking it to the developing area of probability theory ?. Building

on this work was further advancing the generalization of the CLT by Alexander Lyapunov to sequences of independent random variables that are not identically distributed. His version of the theorem brought forth Lyapunov's condition, which contained definite criteria for convergence ?.

In the early years of the 20th century, contributions by Lyapunov represented such a change in the evolution of the CLT. Unlike his predecessors, Lyapunov sought a "direct" and "elementary" proof. It would try to make the theorem internal relations simpler and relax the theorem's assumptions. His papers published in 1900 and 1901 reconstructed previous methods with a rigor of Weierstrass, and introduced new precision to the theorem by establishing explicit bounds on the normalized sum and the limiting normal distribution. This specificity answers Chebyshev's earlier demand for sharper probabilistic results although it should have simplified the proof through some clever but much deeper refinements of Poisson's arguments ?.

Lyapunov's goals extended beyond mere generalization; he aimed to illuminate the theorem's internal structure and make it more accessible. Avoiding the complexities of characteristic functions and complex analysis, he focused on moment-based criteria, relying on real-valued tools like Taylor expansions, bounding techniques, and Lyapunov's inequality. Thus the balance here is theoretical rigor and practical applicability, two characteristics that still resonate well with modern efforts at formal verification as that undertaken in this thesis.

In contemporary times, further refinements of the CLT were provided by William Feller bringing it to discrete random variables ?, and all subsequent developments that are probabilistic have been geared towards this common extension to stable distributions and higher dimensional data. These extensions demonstrate the theorem's adaptability to various contexts, from stochastic processes to machine learning and data analysis.

Lyapunov's version of the CLT represents a key milestone in this journey. It generalizes the theorem for independent random variables with finite moments so that it becomes an observed but pliant frame of reference for convergence. It is this balancing between abstractness and concreteness that is a characteristic of the whole development of probability during the modern period. Contemporaries of Lyapunov such as von Mises, Lévy, Cramér, Khinchin, and Kolmogorov likewise pursued abstract relations in probability theory while keeping an eye on practical relevance. This tension is paradigmatically present in Lyapunov's work, which illustrates the way in which results which are purely formal mathematics may nonetheless satisfy external criteria of applicability and utility. For more information about the history and the proofs of the Central Limit Theorem, see ??.

This thesis is based on the generalization of CLT as expressed in Lyapunov's version. Because of its focus on real-valued methods and moment-based criteria, it avoids any

complex tools like characteristic functions or complex analysis, hence being particularly suitable for formalization in HOL4. In this respect, Lyapunov's approach not only advances the mathematical generalization but also provides a practical framework to meet the rigor and accessibility requirements of automated reasoning systems by directly addressing convergence under relaxed conditions.

2.2 Related Work

Formalization of mathematical theorems as proofs has been a singular research focus in modern computational mathematics. The systems such as Isabelle/HOL (?), Coq (?), and HOL4 (?) have been heavily relied on over the years to encode and prove basic properties but offer several features and challenges.

One of the most significant achievements in this area was the formalization of CLT within the Isabelle/HOL proof assistant. This was made possible mainly by the rich library related to complex analysis in Isabelle/HOL, which provided the means to make use of characteristic functions within the proof. Characteristic functions are Fourier transforms of probability distributions that make convergence easier to analyze by drawing on their special mathematical properties. Central to the approach are two key steps: first, pointwise convergence of the characteristic function for the normalized sum of independent random variables to that of the standard normal distribution should be demonstrated; and second, by the application of the Lévy Continuity Theorem, one obtains the desired convergence in distribution. These two steps are actually the core of the proof that eventually leads to the verification of CLT ?.

The characteristic function approach is beautifully complemented by the infrastructure provided by Isabelle/HOL, which supports careful manipulation of complex-valued functions, differentiation, and limits. This thereby enables Isabelle/HOL to achieve the rigorous performance that is demanded by Fourier analysis and probability theory. Among the striking personalities behind this effort is Luke Serafin, who has produced a giant leap forward in the formalization of the CLT ?. Serafin's systematic encoding of the characteristic function method has ensured that it was entirely generic and modular. His contributions involved the formalization of key intermediate results such as the for sums of independent random variables and the fact that components of his work are reusable, enabling extension into applications that relate to probabilistic theorems.

The strength of Isabelle/HOL is to borrow from its excellent complex analysis library. The characteristic function-based proofs are formalized smoothly, and the modular and extensible framework allows researchers to always build on previous work, gradually increasing the scope of formalized mathematics. The CLT formalization within Isabelle/HOL is exemplary in showing how even the most intricate probabilistic results

can be encoded rigorously with the help of proof assistants. But this also points to some of the challenges with this approach: it is very much based on Fourier transforms and complex-valued methods, an infrastructure which may not always be as easily available when moving to other proof systems. Also, characteristic functions are powerful but often complicate proofs in situations where simpler real-valued methods, such as those based on moments, would suffice.

The formalization of CLT in Isabelle/HOL serves as an inspiration and comparison for the research presented in this thesis. The Example of Isabelle/HOL shows that the CLT can be formalized with the help of characteristic functions but also brings into relief the limitations of such a strategy-if proof assistants like HOL4 lack libraries comparable for complex analysis with it. This thesis takes a different site following the approach with the theorem of Lyapunov, which involves real-valued moment conditions rather than characteristic functions. Following this path, the work in HOL4 demonstrates how easier and less convoluted tools enable formulating the CLT while considering the inherent challenges of formal verification.

Preliminaries

This chapter describes an overview of the theoretical and formal theories required for the formalization of the Central Limit Theorem . This includes HOL Formalization, Measure Theory, Lebesgue Integration, and Probability Theory.

3.1 HOL Formalization

Higher Order Logic (HOL) ?? is derived from the Logic of Computable Functions (LCF) ?? created by Robin Milner and colleagues in 1972. HOL is an adaptation of Church's Simple Theory of Types (STT) ?, where a higher-order version of Hilbert's choice operator ϵ , Axiom of Infinity, and Rank-1 polymorphism have been added. HOL4 implements the original HOL framework, while other theorem provers in the HOL family, such as Isabelle/HOL, include important extensions. Such a simple logical basis makes HOL more accessible than those systems founded on much more advanced dependent type theories, such as the Calculus of Inductive and Co-Inductive Constructions constructed by Coq. Therefore, theories and proofs founded on HOL are easier for a layman to comprehend rather than being lost in a complicated type theory.

HOL refers both to the logical system and the software implementing it. HOL4 is the latest version of this software and written in Standard ML (SML), a general-purpose functional programming language. SML has played the most vital role in the HOL4 for implementing its core engine, enabled automation due to which proof tactics have been written in that and also for interaction, whether it is through a proof script or in direct correspondence with the user. Integrated SML gives a way in which HOL4 is versatile and can easily be extended such that complex verification tools are provided to develop the management of proofs by a user efficiently.

HOL terms are representatives of such things and the grammar includes constants, variables, applications (function calls) and lambda abstractions. Quantifiers, for instance universal ($\forall x. P(x)$) and existential ($\exists x. P(x)$), are also provided in HOL - they are defined as specific lambda functions.

The type system of HOL establishes the structural framework within which all terms and expressions are guaranteed to be well-defined and logically consistent. Types in

HOL denote sets within the universe U , and every term bears a certain type. The type grammar is simple and very expressive, and thus able to construct a wide variety of mathematical and logical objects.

The type grammar is defined as:

$$\sigma ::= \alpha \mid c \mid (\sigma_1, \dots, \sigma_n)\text{op} \mid \sigma_1 \rightarrow \sigma_2$$

where:

1. **Type Variables** (α, β, \dots): Generic placeholders that allow polymorphism to provide functions and predicates over different types.
 - Example: The type variable α could indicate integers, Booleans, or functions.
2. **Atomic Types** (c): Fixed and pre-defined types within HOL. The two initial atomic types are:
 - `bool`: The set of Boolean values $\{T, F\}$.
 - `ind`: The set composed by individuals (an infinite set).
3. **Compound Types** $((\sigma_1, \dots, \sigma_n)\text{op})$: Formed by applying type operators to other types. Their examples include Cartesian products, which designate the tuples over the elements.
 - Example: The type $(\text{bool}, \text{ind})\times$ represents pairs of a Boolean and an individual.
4. **Function Types** $(\sigma_1 \rightarrow \sigma_2)$: Represent total functions mapping elements from a domain (σ_1) to a codomain (σ_2) .
 - Example: The type $\text{bool} \rightarrow \text{ind}$ indicates a function mapping both Boolean-values to individual-elements.

For example, consider the following types:

1. A function from integers to Booleans:

$$f : \text{int} \rightarrow \text{bool}$$

This type indicates that $f(x)$ is a function taking an integer x and returning a Boolean.

2. A tuple containing a Boolean and a function:

$$p : (\text{bool}, (\text{int} \rightarrow \text{bool}))$$

This is a pair type $p = (b, f)$, where b is a Boolean, and f is a function mapping integers to Booleans.

3. The type system guarantees the consistency by making sure all terms are properly typed. So if $g : \text{int} \rightarrow \text{bool}$, then $g(5)$ as 5 is an integer, but, $g(T)$ would be invalid since T is a Boolean, not an integer. Such stringent typing is at the level of terms to avoid self-contradictory values and assure that proofs built up in HOL are sound.

In HOL, terms are representatives for elements of sets represented by their types. The grammar of the term defines the syntax and structure for the logical expressions that can be expressed and hence statements that could be well typed and logically valid. Terms in HOL are constructed from the following components:

$$t ::= x \mid c \mid t \ t' \mid \lambda x. t$$

where:

1. **Variables** (x, y, \dots) :

- Represent placeholders for elements of a type.
- Example: $x : \text{bool}$ stands for a Boolean variable.

2. **Constants** (c):

- Fixed entities such as T , F , mathematical operators, or predefined functions.
- Example: The constant $+$ defines addition for numeric types.

3. **Function Applications** ($t \ t'$):

- Define the application of a function to an argument. The term $f(x)$ applies the function f to the variable x .
- Example: If $f : \text{int} \rightarrow \text{real}$ and $x : \text{int}$, then $f(x)$ is a valid term of type real .

4. **λ -Abstractions** ($\lambda x. t$):

- Denote anonymous functions where x is the input variable, and t is the function body.
- Example: $\lambda x. x + 1$ defines a function that increments its input by 1.

To ensure consistency, the terms of HOL should be well typed. Given a term t_σ of type σ , its grammar can be generalized with type annotations:

$$t_\sigma ::= x_\sigma \mid c_\sigma \mid (t_{\sigma_1 \rightarrow \sigma_2} t'_{\sigma_1})_{\sigma_2} \mid (\lambda x_{\sigma_1}. t_{\sigma_2})_{\sigma_1 \rightarrow \sigma_2}$$

HOL's deductive system is considered the logical foundation for forming and checking a proof. HOL's deductive system may consist of eight primitive rules of inference, the definition of new theorems by existing theorems. These rules are the basic components and are required for all logical reasoning within HOL, ensuring that proofs are consistent, logically valid, and traced. The following are the eight main primitive inference rules in HOL:

1. Assumption Introduction (ASSUME):

- Introduces a formula as an assumption.
- Rule:

$$\frac{}{t \mid - t}$$

- Example: From the assumption P , we conclude P .

2. Reflexivity (REFL):

- States that any term is equal to itself.
- Rule:

$$\frac{}{\mid - t = t}$$

- Example: For $x : \text{int}$, $x = x$ is always true.

3. Beta Conversion (BETA_CONV):

- Applies substitution in lambda abstractions.
- Rule:
- Example: $(\lambda x. x + 1)(5) \vdash 5 + 1$.

4. Substitution (SUBST):

- Replaces a term in a formula with another term proven to be equal.
- Rule:

$$\frac{\Gamma_1 \mid - t_1 = t'_1 \quad \dots \quad \Gamma_n \mid - t_n = t'_n \quad \Gamma \mid - t[t_1, \dots, t_n]}{\Gamma_1 \cup \dots \cup \Gamma_n \cup \Gamma \mid - t[t'_1, \dots, t'_n]}$$

- Example: From $x = y$ and $P(x)$, infer $P(y)$.

5. Abstraction (ABS):

- Generalizes an equation by abstracting a variable.
- Rule:

$$\frac{\Gamma \vdash t_1 = t_2}{\Gamma \vdash (\lambda x. t_1) = (\lambda x. t_2)}$$

- Example: From $5 + 1 = 6$, infer $\lambda x. x + 1 = \lambda x. 6$.

6. Type Instantiation (INST_TYPE):

- Specializes polymorphic functions or predicates to specific types.
- Rule:

$$\frac{\Gamma \vdash t}{\Gamma[\sigma_1, \dots, \sigma_n / \alpha_1, \dots, \alpha_n] \vdash t[\sigma_1, \dots, \sigma_n / \alpha_1, \dots, \alpha_n]}$$

7. Discharging Assumptions (DISCH):

- Converts an assumption into an implication.
- Rule:

$$\frac{\Gamma \vdash t_2}{\Gamma - \{t_1\} \vdash t_1 \Rightarrow t_2}$$

- Example: From $P \wedge Q$, infer $P \Rightarrow (Q \wedge P)$.

8. Modus Ponens (MP):

- Combines an implication and its premise to infer the conclusion.
- Rule:

$$\frac{\Gamma_1 \vdash t_1 \Rightarrow t_2 \quad \Gamma_2 \vdash t_1}{\Gamma_1 \cup \Gamma_2 \vdash t_2}$$

- Example: From $x > 0 \Rightarrow x^2 > 0$ and $x > 0$, infer $x^2 > 0$.

These inference rules ensure that all logical derivations are traceable to basic axioms and established theorems. Additionally, the deductive system forms the backbone of HOL4, ensuring that proofs are both rigorous and reliable.

All proofs in HOL are fundamentally derived from a set of primitive inference rules and a core logical foundation. These rules define the semantics of two fundamental logical connectives: **equality** ($=$) and **implication** (\Rightarrow). Other logical connectives and firstorder quantifiers, such as logical truth (T), falsehood (F), conjunction (\wedge), disjunction (\vee), and existential quantification (\exists), are defined as lambda (λ) functions for consistency within the HOL framework:

1. Logical Truth (T)

- Rule

$$T_DEF \quad \quad \quad |- T = ((\lambda x:bool. x) = (\lambda x. x))$$

- True is represented as the equality of two identical boolean functions.

2. Logical Falsehood (F)

- Rule

$$F_DEF \quad \quad \quad |- F = !t. t$$

- False is defined to satisfy any boolean implication.

3. Negation (\neg)

- Rule

$$NOT_DEF \quad \quad \quad |- \neg = (\lambda t. t ==> F)$$

- Negation is the implication of a boolean value leading to falsehood.

4. Conjunction (\wedge)

- Rule

$$AND_DEF \quad \quad \quad |- /\ = \lambda t1 t2. !t. (t1 ==> t2 ==> t) ==> t$$

- Conjunction is defined as a logical function that evaluates nested implications.

5. Disjunction (\vee)

- Rule

$$OR_DEF \quad \quad \quad |- \vee = \lambda t1 t2. !t. (t1 ==> t) ==> (t2 ==> t) ==> t$$

- Disjunction is expressed through sequential implications.

6. Universal Quantifier (\forall)

- Rule

$$FORALL_DEF \quad \quad \quad |- ! = \lambda P:'a->bool. P = (\lambda x. T)$$

- Universality asserts that a predicate holds for all elements of a type.

7. Existential Quantifier (\exists)

- Rule

$$\text{EXISTS_DEF} \quad |- \ ? = \backslash P: 'a \rightarrow \text{bool}. P(\$@ P)$$

- Existence is defined using Hilbert's choice operator (ϵ).

HOL also defines constructs for mathematical operations, such as **one-to-one functions** (*One_One*) and **onto functions** (*Onto*), to extend logical capabilities:

8. One-to-One (*ONE_ONE_DEF*)

- Rule

$$\vdash \text{ONE_ONE} = (\lambda f. \forall x1\ x2. f\ x1 = f\ x2 \Rightarrow x1 = x2)$$

9. Onto (*ONTO_DEF*)

- Rule

$$\vdash \text{ONTO} = (\lambda f. \forall y. \exists x. y = f\ x)$$

HOL includes the constant *Type_Definition*, which defines new types as bijections of subsets of existing types:

10. Type Definition *Type_Definition*

- Rule

$$\begin{aligned} &|- \text{TYPE_DEFINITION } (P: 'a \rightarrow \text{bool}) \ (\text{rep}: 'b \rightarrow 'a) = \\ &(!x' \ x''. (\text{rep } x' = \text{rep } x'')) ==> (x' = x'')) /\ \\ &(!x. P\ x = (?x'. x = \text{rep } x')) \end{aligned}$$

- This process is automated by the HOL Datatype package, simplifying the creation of new types.

HOL's standard theory is built upon four foundational axioms:

1. Boolean Cases (*BOOL_CASES_AX*)

- Rule

$$\vdash \forall t. (t \Leftrightarrow T) \vee (t \Leftrightarrow F)$$

- This axiom ensures that any boolean value is either true or false.

2. Eta Conversion (ETA_AX)

- Rule

$$\vdash \forall t. (\lambda x. t \ x) = t$$

- Eta conversion describes the extensionality of functions.

3. Hilbert's Choice (SELECT_AX)

- Rule

$$\vdash \forall P \ x. P \ x \Rightarrow P \ (\$@ \ P)$$

- This axiom relates the choice operator to existential quantification.

4. Infinity (INFINITY_AX)

- Rule

$$\vdash \exists f. \text{ONE_ONE } f \wedge \neg \text{ONTO } f$$

- The Axiom of Infinity ensures the existence of an infinite set.

These axioms are generally sufficient for conventional formalization projects in HOL4. Adding new axioms is strongly discouraged, as it can compromise logical consistency.

3.2 Measure Theory

Measure theory in HOL4 is the theoretical foundation on which measurements like size, content, or probability can be given to sets. It bases its formalizations on measures, which are functions taking specific collections of subsets, called sigma algebras, as arguments.

1. Measures and Sigma Algebra

A measure in HOL4 is defined as a set function of type $(\alpha \rightarrow \text{bool}) \rightarrow \text{extreal}$, where extreal accounts for extended real numbers to handle infinities. For example, the

measure of the entire real line \mathbb{R} under the Lebesgue measure is represented as $+\infty$ (PosInf).

In order for measures to be consistent, they should satisfy the following properties:

- (a) **Non-Negativity:** $\mu(A) \geq 0$ for all measurable sets A .
- (b) **Null Empty Set:** $\mu(\emptyset) = 0$.
- (c) **Countable Additivity:** For any countable collection of disjoint sets $\{A_n\}$:

$$\mu\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mu(A_n).$$

Measures form over some sigma algebra (σ -algebra) which are systems of subsets that preserve their countable operations like unions, intersections, and complements. A formal definition of σ -algebra is:

sigma_algebra(a)

where ‘subsets(a)’ denotes the subsets of a σ -algebra.

An equivalent definition of σ -algebra is also provided in HOL4 making their construction flexible:

```
SIGMA_ALGEBRA_ALT_SPACE
⊢ ∀a. sigma_algebra a ⇔
  subset_class (space a) (subsets a) ∧ space a ∈ subsets a ∧
  (∀s. s ∈ subsets a ⇒ space a DIFF s ∈ subsets a) ∧
  ∀f. f ∈ (ℕ(:num) → subsets a) ⇒
    BIGUNION (IMAGE f ℕ(:num)) ∈ subsets a
```

2. **Measure Spaces** The tuples $(sp; sts; \mu)$ refer to a measure space in HOL4. In HOL4, the tuple (sp, sts, μ) refer to a **measure space**, where:

- sp : The underlying set (space).
- sts : The σ -algebra of measurable subsets.
- μ : The measure function.

Three functions, `m_space`, `measurable_sets`, and `measure` give sp , sts , and μ . or a measure space, the following conditions must hold:

- σ -algebra property: (sp, sts) is a valid σ -algebra.
- **Positivity:** $\mu(\emptyset) = 0$ and $\mu(A) \geq 0$ for all $A \in sts$.

- **Countable Additivity:** For any countable disjoint collection $\{A_n\} \subseteq \text{sts}$:

$$\mu\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mu(A_n).$$

In some occasions, the measures defined on smaller systems of sets like semirings are extended to full σ -algebra by using Carathéodory's extension theorem. Such intermediate measures are said to be premeasures.

3. Semirings and Generated σ -algebra

A semiring is a simpler system of subsets that can generate a σ -algebra. It satisfies:

- (a) Stability under intersection: $A, B \in S \implies A \cap B \in S$.
- (b) Decomposition of differences: For $A, B \in S$, $A \setminus B$ can be expressed as a finite disjoint union of subsets from S .

An example is the set of all right-open intervals $[a, b)$ in \mathbb{R} , which forms a semiring. For any system of sets (sp, sts) , the smallest σ -algebra containing it, denoted $\sigma(\text{sp}, \text{sts})$, is defined as:

$$\sigma(\text{sp}, \text{sts}) = (\text{sp}, \bigcap \{s \mid \text{sts} \subseteq s \wedge \text{sigma_algebra}(\text{sp}, s)\}).$$

4. Borel Sigma Algebras

The **Borel Sigma Algebra** is the σ -algebra generated by the open subsets of \mathbb{R} , denoted $\mathcal{B}(\mathbb{R})$. In HOL4, it is formally defined as:

$$\text{borel} = \sigma(\mathbb{R}, \{\text{open sets in } \mathbb{R}\}).$$

Alternate characterizations include:

- (a) Using intervals, e.g., half-open intervals $(a, b]$:

$$\text{borel} = \sigma(\mathbb{R}, \{\{x \mid a < x \leq b\} \mid a, b \in \mathbb{R}\}).$$

- (b) Using half-spaces:

$$\text{borel} = \sigma(\mathbb{R}, \{\{x \mid x \leq a\} \mid a \in \mathbb{R}\}).$$

```

right_open_interval
⊢ ∀a b. right_open_interval a b = {x | a ≤ x ∧ x < b}

right_open_intervals
⊢ right_open_intervals = (U(:real), {right_open_interval a b | T})

```

```

right_open_intervals_semiring
⊢ semiring right_open_intervals

right_open_intervals_sigma_borel
⊢ sigma (space right_open_intervals) (subsets right_open_intervals) =
  borel

```

The Borel σ -algebra is also important in the definition of measurable functions and measurable spaces in analysis.

5. Measurable Functions

In HOL4, a function $f : \text{space}(a) \rightarrow \text{space}(b)$ is measurable if:

$$\forall s \in \text{subsets}(b). f^{-1}(s) \cap \text{space}(a) \in \text{subsets}(a).$$

This ensures that the preimage of every measurable set in the codomain is measurable in the domain.

```

measurable_def
⊢ ∀a b.
measurable a b =
{f |
f ∈ (space a → space b) ∧
∀s. s ∈ subsets b ⇒ PREIMAGE f s ∩ space a ∈ subsets a}

```

HOL4's formalization of measure theory provides a rigorous framework for constructing and reasoning about measures, σ -algebra, and measurable functions. The definitions and mathematics make theorems that can be extended to more advanced levels and results.

3.3 Lebesgue Integration Theory

3.4 Probability Theory

Central Limit Theorem

Future Work

Conclusion

References

William J Adams. *The life and times of the central limit theorem*, volume 35. American Mathematical Soc., 2009.

Yves Bertot and Pierre Castéran. *Interactive theorem proving and program development: Coq'Art: the calculus of inductive constructions*. Springer Science & Business Media, 2013.

Patrick Billingsley. *Probability and measure*. John Wiley & Sons, 2017.

Pafnutii Lvovich Chebyshev. Sur deux théorèmes relatifs aux probabilités. *Acta math*, 14 (1):305–315, 1890.

Alonzo Church. A formulation of the simple theory of types. *The journal of symbolic logic*, 5(2):56–68, 1940.

HOL4 contributors. The hol system logic (kananaskis-13 release). Available online at <http://sourceforge.net/projects/hol/files/hol/kananaskis-13/kananaskis-13-logic.pdf>, 2024. Accessed: 2024-12-13.

Abraham De Moivre. *Approximatio ad summam terminorum binomii $(a + b)^n$ in seriem expansi*. Royal Society, 1733.

Willy Feller. The fundamental limit theorems in probability. *Bulletin of the American Mathematical Society*, 51:800–832, 1945. Reprinted in Adams 2009, pp. 80–113.

Hans Fischer. *A history of the central limit theorem: from classical to modern probability theory*, volume 4. Springer, 2011.

Michael J Gordon, Arthur J Milner, and Christopher P Wadsworth. *Edinburgh LCF: a mechanised logic of computation*. Springer, 1979.

Pierre Simon Laplace. *Oeuvres complètes de Laplace*. Gautier-Villars, 1835.

Aleksandr Mikhailovich Lyapunov. Pafnutii Lvovich chebyshev, 1895. Reprinted in parts in Chebyshev (1946), pp. 9–21.

Robin Milner. *Logic for Computable Functions: description of a machine implementation*. Stanford University, 1972.

Luke Serafin. *A formally verified proof of the Central Limit Theorem*. Master's thesis, Carnegie Mellon University, 2015.

Konrad Slind and Michael Norrish. A brief overview of hol4. In *International Conference on Theorem Proving in Higher Order Logics*, pages 28–32. Springer, 2008.

Isabelle Team. Isabelle/hol, 2015. URL <https://isabelle.in.tum.de/>. Accessed: 2024-12-01.

Index

“modern syntax”, *see* special syntactic forms

for scripts