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

Abstract

Contents

Chapter 1

Introduction

Formal verification has continued revolutionizing the understanding and application of foundational theorems in mathematics: the surety of accompanying rigor and its implementation in computational systems. Thus have built chances for innovative mathematical services. Probability theory is a domain with both important theoretical results and practical applications, and it has increasingly become a focus of formalization efforts. The most important from such results is the Central Limit Theorem (CLT), which carries very strong implications in theory and practice.

The CLT is perhaps the most prominent result in probability theory describing how the sum of independent random variables, if suitably normalized, approximates a standard normal distribution when the number of terms increases indefinitely. It closes the gap between random single events and predictable behavior in the aggregate, forms the basis of inferential statistics, and underpins models in a vast variety of fields such as physics, finance, and artificial intelligence. Given this importance, formal verification of the CLT using proof assistants will be an important step toward proving its correctness in automated reasoning systems.

However, formalizing CLT is far from straightforward. There exist numerous variants of this theorem, together with their numerous proofs, ranging from classical independent and identically distributed (i.i.d.) to some more general versions. Notably, Lyapunov's theorem extends the CLT to independent, non-identically distributed (i.n.i.d.) random variables, offering a broader applicability than the classical i.i.d. case **?**. Each of those proofs uses advanced mathematical tools, including characteristic functions, moment generating functions, or even higher-order moments, according to the situation. These proofs require advanced mathematical infrastructure, which is not available with all proof assistants. In particular, the case of HOL4 Slind and Norrish (2008) has found it impossible to use some of the approaches, particularly the one based on characteristic functions, because the strong complex analysis library was lacking.

Instead, this thesis follows another path: leveraging Lyapunov's theorem and the Lindeberg approach, which avoids characteristic functions in favor of real-valued, moment-based techniques. Additionally, it pays attention to moment-based convergence criteria, trying to provide its conditions for convergence using Taylor expansions, Big-O notation of error bounds, and Lyapunov's inequality. This approach aligns well with the existing

mathematical infrastructure of HOL4 while simultaneously expanding its capabilities.

1.1 Motivation

The formalization of the Central Limit Theorem in HOL4 involved interesting challenges because of the highly mathematical nature of the theorem and the specific limitations of existing libraries in HOL4. Another difference between the proof assistants, Isabelle/HOL, which has a very mature library for complex analysis and HOL4, is that there are no built-in key concepts for working with characteristic functions and others associated with the common classical proofs of CLT.

Lack of a well-developed library has been one of the major setbacks of HOL4. Proving the central limit theorem using the more traditional kinds of proofs, such as the one formalized in Isabelle/HOL, involves the use of characteristic functions for convergence proof. Characteristic functions are essentially Fourier transforms and thereby hinge a lot on complex analysis. It would have been very difficult to follow this approach in HOL4, since the proof assistant currently lacks support for these advanced tools.

An alternative approach was explored using moment generating functions (MGFs). MGFs are much more popular for proving the CLT, wherein their specialized property is utilized to show convergence to the standard normal distribution. However, it soon became evident that formally establishing the uniqueness property of MGFs would become a serious blocker. While this property is a triviality in classical analysis, the formalization work involved was highly intricate and beyond the scope of what is currently practical within HOL4's libraries. As a result, this approach was abandoned, leading to the need for a new direction.

The breakthrough came with the adoption of Lyapunov's theorem as the basis for formalizing the CLT. Lyapunov's argument has a very direct and elementary approach to the theorem without using complex analysis or moment-generating functions but rather basing on real-valued, moment-based convergence criteria; hence, it being particularly fitted into the existing framework of HOL4. Lyapunov's proof is a milestone of abstraction in the probability theory, but it is still beautifully simple and thus met the practical and strict requirements of formal verification.

However, Linderberg's method introduced its own set of challenges for formalization in HOL4:

- **Taylor Expansions:** The proof relies heavy on Taylor expansions to approximate test functions and bound errors. These had to be rigorously formalized in HOL4 from first principles.

- **Big-O Notation:** Reasoning about the asymptotic behavior of error terms involved the formalization of Big-O notation, which did not exist in HOL4 until now.

- **Lyapunov's Inequality:** An important part of the proof was the formalization of Lyapunov's inequality, which gives sufficient conditions for convergence. It was carefully adapted to fit into HOL4's logical framework.

Following the Linderberg's approach, with its valuation on real techniques and elementary methods, proved most important: it served to encapsulate the CLT under the constraints of HOL4 and was entirely consistent toward building reusable mathematics libraries. Taylor series developments, Big-O notion, and Lyapunov's inequality are indispensable not only for this proof but also as a basis of further formalizations in the realm of probability theory and elsewhere.

This shift from characteristic functions and MGFs to the more concrete, moment-based approach of Lyapunov underlines flexibility and problem-solving ingenuity necessary in formal verification projects. It thus shows how advanced mathematical results can be formalized in HOL4, even when serious deficiencies in its infrastructure must first be overcome. Moreover, it emphasizes the role of Lyapunov's approach as a turning point in the history of probability theory and as one of the bases for modern formalization.

1.2 Thesis Contributions

This thesis formalizes Lyapunov's inequality in HOL4, hence establishing a rigorous framework for convergence in probability proofs. In particular, the necessary mathematical theories and lemmas for the proof of CLT: Taylor expansions to bound errors, Big-O notation for asymptotic behavior analysis, and telescoping techniques for incremental replacements. These lemmas are used to formalize the Lyapunov's theorem and Lindeberg's approach, with a subsequent complete proof of CLT within HOL4. Unlike other approaches using characterization or moment-generating functions, this work does not use complex analysis, but works with the methods compatible with the real-valued nature of HOL4.

This thesis, beyond formalizing CLT, enriches libraries for probabilistic analysis that can be reused beyond, such as statistical inference and machine learning. This addresses some foundational gaps in HOL4 and demonstrates the use of HOL4 in advancing formalized mathematics.

1.3 Structure of the Thesis

The rest of the thesis is organized as follows. Chapter 2 provides background on the Central Limit Theorem, its history, and the setting of Lyapunov's proof. Related work, including other formalizations, using proof assistants like Isabelle/HOL is also covered. Chapter 3 then details the preliminaries, including HOL4 as proof engineering and related libraries. The key components of the proof, its completion, and its validation of the CLT are given in Chapter 4. Chapter 5 presents a discussion of results, and positioning of this work with respect to related efforts on formal verification. Finally, the thesis is concluded in Chapter 6 by summarizing the contributions made by this work and presenting the vision on future directions that probability theory in HOL4 may take.

This thesis not only shows that a formalization of the CLT in HOL4 is possible but also opens up further opportunities for work on the formal probability theory. It fills in some foundational gaps and provides reusable tools, which illustrates more general potential of HOL4 to make serious contributions to the fully verified mathematics corpus.

Chapter 2

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 De Moivre (1733). 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 Laplace (1835) 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 Chebyshev

(1890). 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 Lyapunov (1895).

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 Fischer (2011).

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 Feller (1945), 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 Fischer (2011); **?**.

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 Team (2015), Coq Bertot and Castéran (2013), and HOL4 Slind and Norrish (2008) 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, grad-

ually 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.

Chapter 3

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) Slind and Norrish (2008); **?** 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 such 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 (!x. P(x)) and existential (?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:

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

where:

1. **Type Variables ($\alpha, \beta, \ldots$):** 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 ($(\sigma_1, \ldots, \sigma_n)$op):** Formed by applying type operators to other types. Their examples include Cartesian products, which designate the tuples over the elements.
    - Example: The type (`bool`, `ind`)$\times$ represents pairs of a Boolean and an individual.
4. **Function Types ($\sigma_1 \to \sigma_2$):** Represent total functions mapping elements from a domain (σ_1) to a codomain (σ_2).
    - Example: The type `bool` $\to$ `ind` indicates a function mapping both Boolean-values to individual-elements.

For example, consider the following types:

1. A function from integers to Booleans:

    $$f : \texttt{int} \to \texttt{bool}$$

    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:

$$p : (\texttt{bool}, (\texttt{int} \to \texttt{bool}))$$

   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 $g : \texttt{int} \to \texttt{bool}$, 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, ...):
   - Represent placeholders for elements of a type.
   - Example: $x : \texttt{bool}$ 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 $f : \texttt{int} \to \texttt{real}$ and $x : \texttt{int}$, 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:

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

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:

$$\frac{}{t \ \vdash\ t}$$

   - Example: From the assumption P, we conclude P.
2. **Reflexivity (REFL):**
   - States that any term is equal to itself.
   - Rule:

$$\frac{}{\vdash\ t = t}$$

   - Example: For $x : \texttt{int}$, $x = x$ 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:

$$\frac{\Gamma_1 \ \vdash\ t_1 = t'_1 \quad \cdots \quad \Gamma_n \ \vdash\ t_n = t'_n \quad \Gamma \ \vdash\ t[t_1, \ldots, t_n]}{\Gamma_1 \cup \cdots \cup \Gamma_n \cup \Gamma \ \vdash\ t[t'_1, \ldots, t'_n]}$$

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

5. **Abstraction (ABS):**
   - Generalizes an equation by abstracting a variable.
   - Rule:
$$\frac{\Gamma \ |- \ t_1 \ = \ t_2}{\Gamma \ |- \ (\backslash x . t_1) \ = \ (\backslash x . t_2)}$$
   - 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:
$$\frac{\Gamma \ |- \ t}{\Gamma[\sigma_1, \ \ldots \ , \sigma_n/\alpha_1, \ \ldots \ , \alpha_n] \ |- \ t[\sigma_1, \ \ldots \ , \sigma_n/\alpha_1, \ \ldots \ , \alpha_n]}$$

7. **Discharging Assumptions (DISCH):**
   - Converts an assumption into an implication.
   - Rule:
$$\frac{\Gamma \ |- \ t_2}{\Gamma - \{t_1\} \ |- \ t_1 \ ==> \ t_2}$$
   - 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:
$$\frac{\Gamma_1 \ |- \ t_1 \ ==> \ t_2 \qquad \Gamma_2 \ |- \ t_1}{\Gamma_1 \cup \Gamma_2 \ |- \ t_2}$$
   - 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** ($\Longrightarrow$). 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                |- T  = ((\x:bool. x) = (\x. x))
      ```

    - True is represented as the equality of two identical boolean functions.
2. **Logical Falsehood (F)**
    - Rule

      ```
      F_DEF                |- F  = !t. t
      ```

    - False is defined to satisfy any boolean implication.
3. **Negation ($\neg$)**
    - Rule

      ```
      NOT_DEF              |- ¬  = (\t. t ==> F)
      ```

    - Negation is the implication of a boolean value leading to falsehood.
4. **Conjunction ($\wedge$)**
    - Rule

      ```
      AND_DEF              |- /\ = \t1 t2. !t. (t1 ==> t2 ==> t) ==> t
      ```

    - Conjunction is defined as a logical function that evaluates nested implications.
5. **Disjunction ($\vee$)**
    - Rule

      ```
      OR_DEF               |- \/ = \t1 t2. !t. (t1 ==> t) ==> (t2 ==> t) ==> t
      ```

    - Disjunction is expressed through sequential implications.
6. **Universal Quantifier ($\forall$)**
    - Rule

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

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

7. **Existential Quantifier (∃)**

   - Rule

```
EXISTS_DEF          |- ?  = \P:'a->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

$$\vdash \texttt{ONE\_ONE} = (\lambda \texttt{f}.\ \forall \texttt{x1}\ \texttt{x2}.\ \texttt{f x1} = \texttt{f x2} \Rightarrow \texttt{x1} = \texttt{x2})$$

9. **Onto (*ONTO_DEF*)**

   - Rule

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

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

10. **Type Definition** *Type_Definition*

    - Rule

```
|- TYPE_DEFINITION (P:'a->bool) (rep:'b->'a) =
(!x' x''. (rep x' = rep x'') ==> (x' = x'')) /\
(!x. P x = (?x'. x = rep x'))
```

    - 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

   $$\vdash \exists f.\ \mathrm{ONE\_ONE}\ f \wedge \neg \mathrm{ONTO}\ f$$

   - 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 $(\alpha \to \text{bool}) \to \text{extreal}$, 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:

$$\text{sigma\_algebra}(a)$$

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 ∈ (𝕌(:num) → subsets a) ⇒
BIGUNION (IMAGE f 𝕌(:num)) ∈ subsets a
```

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

- **Countable Additivity:** For any countable disjoint collection $\{A_n\} \subseteq$ 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 $f : \text{space}(a) \to \text{space}(b)$ 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

Chapter 4

Central Limit Theorem

asldfjkldasjflkdfjldsa;f

Chapter 5

Future Work

Future Work

Chapter 6

Conclusion

asdfsdfasdf

asdasasfdfdf

References

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

Manfred Broy, Bengt Jonsson, J-P Katoen, Martin Leucker, and Alexander Pretschner. Model-based testing of reactive systems. In *Volume 3472 of Springer LNCS*. Springer, 2005.

Jerry R Burch, Edmund M Clarke, Kenneth L McMillan, David L Dill, and Lain-Jinn Hwang. Symbolic model checking: 1020 states and beyond. *Information and computation*, 98 (2):142–170, 1992.

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

Kai Lai Chung. *A course in probability theory*. Elsevier, 2000.

Edmund M Clarke, Thomas A Henzinger, Helmut Veith, Roderick Bloem, et al. *Handbook of model checking*, volume 10. Springer, 2018.

Abraham De Moivre. *Approximatio ad summam terminorum binomii (a+ b) n in seriem expansi*. 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.

John Harrison. Hol light, 2015. URL `http://www.cl.cam.ac.uk/~jrh13/hol-light/`. Accessed: 2024-12-01.

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

Aleksandr Mikhailovich Lyapunov. Pafnutii lvovich chebyshev, 1895.

Sheldon Ross. *First Course in Probability, A*. Pearson Higher Ed, 2019.

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