

APE-Bench I: Towards File-level Automated Proof Engineering of Formal Math Libraries

Huajian Xin^{*†1,2}, Luming Li¹, Xiaoran Jin¹, Jacques Fleuriot², Wenda Li²

¹ByteDance Seed, ²University of Edinburgh

^{*}Work done at ByteDance Seed, [†]Corresponding authors

Abstract

Recent progress in large language models (LLMs) has shown promise in formal theorem proving, yet existing benchmarks remain limited to isolated, static proof tasks, failing to capture the iterative, engineering-intensive workflows of real-world formal mathematics libraries. Motivated by analogous advances in software engineering, we introduce the paradigm of *Automated Proof Engineering (APE)*, which aims to automate proof engineering tasks such as feature addition, proof refactoring, and bug fixing using LLMs. To facilitate research in this direction, we present **APE-Bench I**, the first realistic benchmark built from real-world commit histories of Mathlib4, featuring diverse file-level tasks described in natural language and verified via a hybrid approach combining the Lean compiler and LLM-as-a-Judge. We further develop Eleanstic, a scalable parallel verification infrastructure optimized for proof checking across multiple versions of Mathlib. Empirical results on state-of-the-art LLMs reveal a syntax–semantics gap: while some models perform well on localized edits, overall success rates drop sharply on structurally complex tasks. This work lays the foundation for developing agentic workflows in proof engineering, with future benchmarks targeting multi-file coordination, project-scale verification, and autonomous agents capable of planning, editing, and repairing formal libraries.

Correspondence: Huajian Xin at H.Xin-3@sms.ed.ac.uk

1 Introduction

Large language models (LLMs) have recently demonstrated impressive capabilities in formal mathematics, achieving state-of-the-art results on isolated theorem-proving tasks. However, existing benchmarks operate in static, goal-driven settings and fail to reflect the full complexity of real-world formal mathematics workflows. Maintaining large formal libraries such as **Mathlib4** entails more than solving standalone problems—it involves iteratively refactoring, extending, and debugging an interconnected and evolving codebase. This gap between isolated problem-solving and real-world proof engineering highlights the need for a fundamentally different evaluation paradigm.

While analogous limitations in code generation have led to increasingly realistic software engineering benchmarks—e.g., from *HumanEval* [3] to *SWE-bench* [7]—the formal mathematics community has yet to adopt a similar shift. We introduce the paradigm of **Automated Proof Engineering (APE)**—a setting where each task presents a natural language instruction along with a pre-edit version of Lean files, and the model generates a corresponding code patch. While human edits are not guided by explicit instructions, we distill their underlying intent into instruction–patch pairs, enabling modular, interpretable, and scalable evaluation

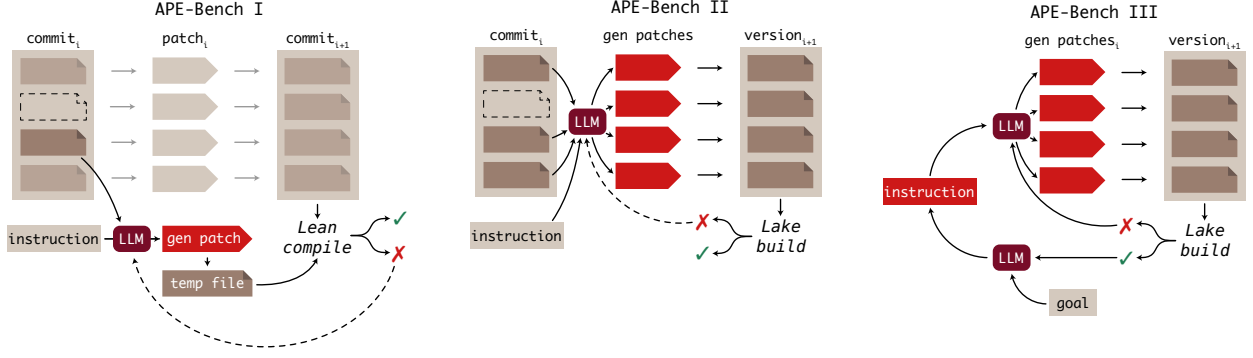


Figure 1 The APE-Bench series: A staged roadmap for automated proof engineering. The benchmark suite progresses from single-file edits (APE-Bench I) to multi-file coordination (APE-Bench II) and ultimately to autonomous workflows (APE-Bench III). This staged design reflects the increasing complexity of real-world proof engineering tasks.

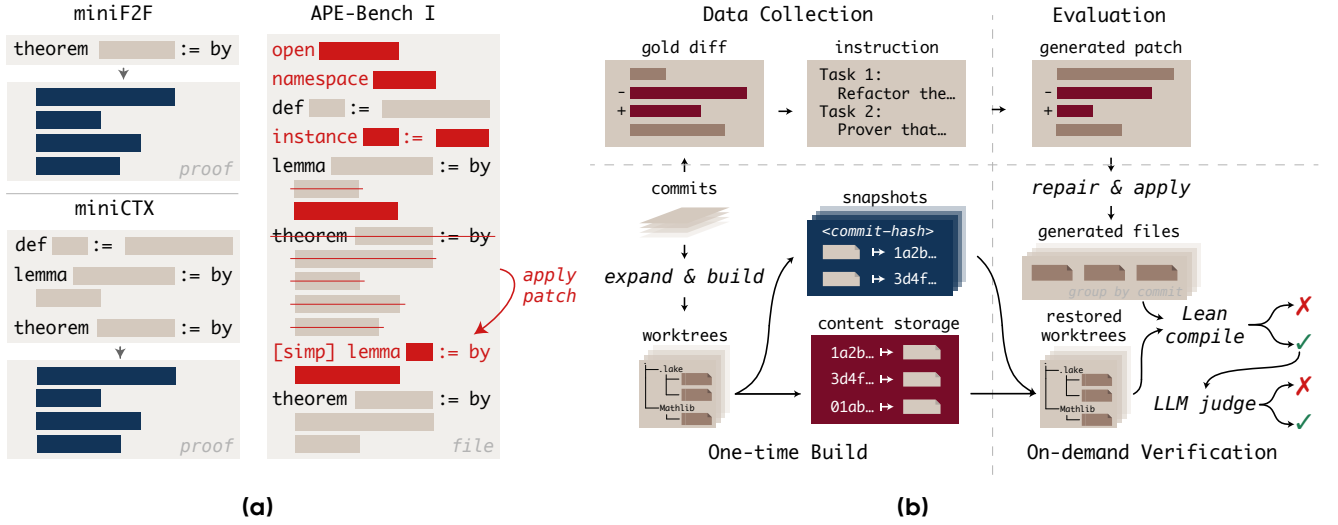


Figure 2 APE-Bench I: Benchmark structure and evaluation pipeline. (a) Unlike earlier benchmarks focusing on isolated theorem-proving, APE-Bench I targets realistic file-level proof engineering tasks from real-world Mathlib commits. (b) The data pipeline includes commit mining, diff extraction, instruction synthesis, and verification using *Eleanstic*-a multi-version infrastructure for efficient Lean verification.

units.

To operationalise this paradigm, we introduce the **APE-Bench** series—a staged suite of benchmarks for increasingly sophisticated proof engineering capabilities. As shown in Figure 1, **APE-Bench I** focuses on single-file instruction-guided edits with localised scope. **APE-Bench II** will introduce multi-file coordination and project-level verification. Finally, **APE-Bench III** aims to support autonomous workflows, where agents plan, edit, and iteratively repair formal libraries via feedback-driven strategies.

This paper presents **APE-Bench I**, the first step in this roadmap. Built from thousands of real-world commits in Mathlib4, it targets localised, instruction-driven edits at the file level. Its design is guided by four core goals:

- **Realism:** Reflect real development practices by extracting file-level edits from actual Mathlib4 commits, preserving their structural integrity.
- **Stratification:** Support diverse task types and complexities through a multi-stage filtering pipeline that removes trivial edits and categorizes tasks by function and difficulty.

- **Scalable Syntax-Semantics Evaluation:** Enable efficient assessment through syntactic verification via the Lean compiler and semantic judgement via an LLM-as-a-judge system.
- **Continual Evolvability:** Support automated updates with the evolution of the underlying library through fully automated construction pipelines.

APE-Bench I enables a comprehensive evaluation of leading language models on realistic proof engineering tasks. Our experiments reveal that o3-mini leads in syntactic success rate, while Gemini 2.5 Pro Preview achieves the highest semantic correctness under LLM judgement. Most models degrade sharply as task size increases, and many produce syntactically valid but semantically incorrect patches. These results highlight substantial gaps between current capabilities and real-world proof engineering requirements.

We summarize our core contributions as follows:

1. We introduce the paradigm of *Automated Proof Engineering (APE)*, which reframes formal mathematics as instruction-driven code editing aligned with real-world development workflows.
2. We construct APE-Bench I, the first large-scale, file-level benchmark for proof engineering, built from over 10,000 real-world commits in `Mathlib4`.
3. We develop a two-stage evaluation protocol combining syntax-level checking via Lean compilation with semantic judgement via an LLM-as-a-judge system.
4. We conduct a comprehensive empirical study on leading LLMs, revealing substantial performance differences, sharp degradation on complex tasks, and frequent semantic failures.
5. We release all data, code, and infrastructure to support reproducible evaluation and continual benchmark expansion as `Mathlib4` evolves.

2 Background and Related Work

Formal proof engineering refers to the disciplined application of software engineering principles to the construction, maintenance, and evolution of large-scale formal mathematical libraries [10]. In contrast to traditional theorem proving, which typically centres on isolated logical goals, proof engineering entails a broader and more structurally intricate set of tasks, such as extending libraries with new features, restructuring existing proofs (refactoring), and correcting erroneous logic (bug fixing). For a more comprehensive discussion of proof engineering practices and challenges, see Appendix A.1.

Most existing benchmarks emphasise single-goal theorem proving within static contexts, diverging significantly from the demands of real-world proof maintenance. As shown in Table 1, conventional benchmarks evaluate success based on isolated proof completion, neglecting the broader engineering workflows needed to evolve and maintain large formal mathematics libraries. Recent efforts have explored richer proof generation scenarios [1, 4–6, 11–13], but still typically focus on isolated reasoning tasks rather than realistic proof engineering workflows (see Appendix A.2 for an extended analysis). A clear gap remains in systematic, task-diverse benchmarks that reflect the full scope of real-world proof engineering.

Aspect	Current Benchmarks	Real-world Practice
Scope	Isolated, static theorem proving	Dynamic, evolving large libraries
Objectives	Individual proof completion	Feature addition, proof refactoring, bug fixing

Table 1 Comparison between conventional benchmarks and real-world proof engineering practices.

3 APE-Bench I: A Realistic Benchmark for File-Level Proof Engineering

To concretely realise the paradigm of Automated Proof Engineering (APE), we introduce APE-Bench I, a realistic and instruction-driven benchmark constructed from real-world edits in the `Mathlib4` formal mathematics library. This section describes the design and construction of the benchmark, including its task

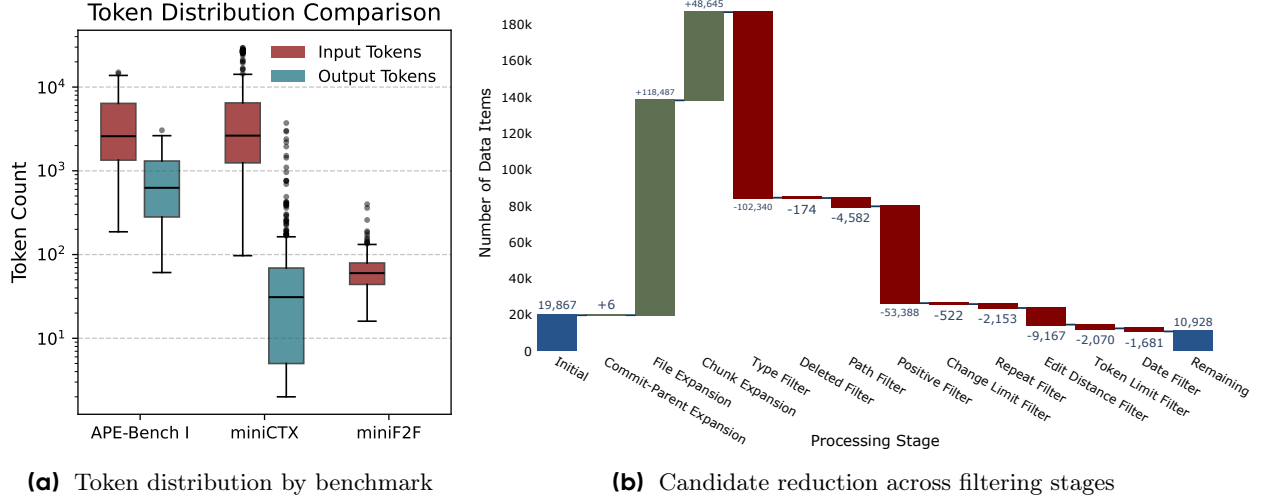


Figure 3 APE-Bench I: Scale and complexity of extracted tasks. (a) APE-Bench I tasks span significantly longer input-output contexts than prior datasets. (b) Starting from 19k commits, the pipeline produces 185k+ candidates, filtered to 10,928 high-quality tasks.

format, the methodology for extracting file-level edits from version history, and the automatic synthesis of natural-language instructions and semantic labels.

3.1 Task Format and Objective

Each task in APE-Bench I defines a localised file-level proof engineering problem, grounded in an actual edit to a Lean source file. The objective is to apply a valid patch that fulfills a natural-language instruction by transforming a given pre-edit file into a structurally correct and semantically meaningful post-edit version.

Formally, each task is specified as a triplet (**Instruction**, **PreFile**, **Patch**), where:

- **Instruction** is a concise imperative-style natural language command describing the intended modification. It typically requests the addition of a definition, the restructuring of an existing proof, or the correction of a specific error.
- **PreFile** contains the complete Lean source code of the target file before the edit. It provides the context necessary to interpret the instruction and generate a corresponding structural change.
- **Patch** is a unified diff that encodes the intended edit, specifying insertions and deletions relative to **PreFile**. The diff format supports modular and interpretable editing, and facilitates automated application, verification, and evaluation.

This triplet formulation reflects the real-world dynamics of proof maintenance, characterized by developers dynamically modifying multiple, often interdependent, parts of entire files as they evolve, rather than statically addressing isolated subgoals.

3.2 Task Extraction from Mathlib4 Commits

To construct realistic and diverse proof engineering tasks, we extract file-level edits from the version history of **Mathlib4**. Our extraction pipeline, illustrated in Figure 3b, proceeds in four stages:

Step 1: Commit Sourcing and Diff Decomposition. We begin with 19,867 Git commits made between August 2023 and March 2025. Each commit is decomposed into file-level diffs, isolating modified files and their corresponding changes. These diffs are further segmented into semantically scoped chunks by hunk or declaration boundaries.

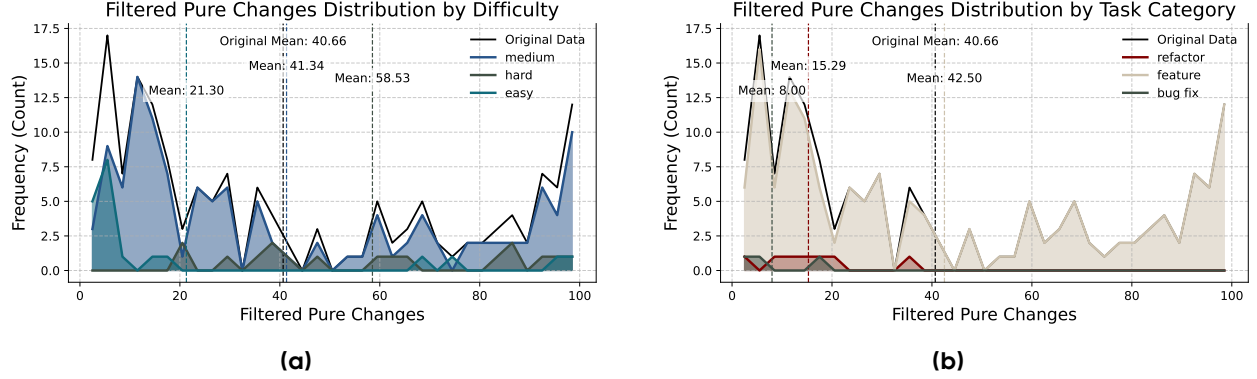


Figure 4 Distribution of code change magnitudes across semantic labels in the test set. (a) Based on non-comment line counts from gold patches, grouped by difficulty. (b) Patch sizes grouped by functional category.

Step 2: Granular Chunk Expansion. To improve modelling tractability and enhance semantic interpretability, we decompose large diffs into smaller, contiguous edit fragments. Each fragment is applied incrementally to the evolving file state, yielding fine-grained task units. This expansion increases the total number of edit candidates to over 187,000.

Step 3: Multi-Stage Filtering. We apply a sequence of automated filters targeting semantic relevance (retaining only commits with recognisable editing intent), content quality (discarding comment-only or whitespace edits), and structural integrity (restricting to at most 100 lines of changes and 16,000 tokens). The overall retention trajectory is visualised in Figure 3b. For additional details on our filtering methodology, see Appendix B.1.

Step 4: Compilation Validation. To ensure structural soundness, all retained patches are compiled under their post-edit environments using Lean. Only patches that successfully typecheck in the restored version context are included in the final benchmark.

The final benchmark consists of 10,928 structurally coherent tasks. As shown in Figure 3a, these tasks exhibit significantly longer input and output sequences than prior benchmarks, reflecting the higher structural complexity of proof engineering tasks.

3.3 Instruction Synthesis and Task Labelling

Each task is paired with a natural language instruction and annotated with semantic labels describing its functional category and structural difficulty. For instruction generation, we use Claude Sonnet 3.7 (thinking mode) to extract and summarise the developer’s intent from the raw diff in an imperative style. We apply a reverse validation procedure to ensure semantic alignment between instruction and patch (detailed methodology in Appendix B.2).

For task labelling, we assign three types of labels to the test set:

- **Task Category:** Feature, Refactor, or Bug Fix, aligned with common proof engineering operations.
- **Difficulty Level:** Easy, Medium, Hard, or Very Hard, estimating structural and reasoning complexity.
- **Task Nature:** Substantial or Superficial, used for filtering; only Substantial tasks are retained.

Figure 4 shows the distribution of code changes across difficulty levels and functional categories. These labels enable stratified evaluation and help reveal capability gaps across models, as confirmed by our experimental results in Section 5. Appendix B.3 provides additional statistical validation of these label distributions.

4 Evaluation Infrastructure and Protocol

To enable reliable assessment of model-generated edits in APE-Bench I, we establish a two-stage evaluation framework that reflects the dual demands of proof engineering: syntactic correctness and semantic adequacy. As illustrated in Figure 5, each candidate patch is evaluated for both grammatical validity under Lean’s type system and alignment with the task’s instruction-level intent. The first stage, *syntactic verification*, checks whether the resulting file passes Lean verification within the corresponding versioned environment. This process is implemented via *Eleanstic*, a scalable verification infrastructure that supports reproducible, parallelisable, and version-aware Lean verification (Section 4.1). The second stage, *semantic judgement*, determines whether the patch satisfies the instruction as intended. This is carried out by a large language model acting as an instruction-conditioned judge (Section 4.2). A task is marked as successful only if a model-generated patch passes both verification stages. This protocol provides a standardised and scalable basis for computing success metrics, enabling detailed analyses across syntax-level and semantics-level dimensions.

4.1 Syntactic Verification via Eleanstic

Syntactic verification in APE-Bench I requires compiling model-generated patches within the exact versioned environment from which each task was derived. In large-scale formal libraries like Mathlib4, where definitions and dependencies evolve rapidly across commits, such version fidelity is critical for meaningful evaluation.

We introduce *Eleanstic*, a dedicated infrastructure for scalable, version-aware syntactic verification. Eleanstic decouples the high-cost process of building Mathlib4 from the low-cost process of validating edits by collapsing each post-build state into a compact, content-addressable snapshot. This architecture significantly reduces redundant computation, minimises storage usage, and supports efficient parallel evaluation across thousands of distinct versions (technical implementation details in Appendix C.1).

For verification, a model-generated patch is applied to the target Lean file in an isolated environment, and the Lean compiler verifies only the modified file without affecting the restored environment. A patch is considered syntactically valid if it compiles successfully and does not emit warnings.

4.2 Semantic Judgement via LLM-as-a-Judge

While syntactic verification ensures that a model-generated patch is type-correct under the Lean compiler, it does not guarantee that the patch fulfils the intended transformation described in the natural language instruction. Common failure modes include omitting key components, misinterpreting the instruction, or modifying unrelated content.

We use Claude Sonnet 3.7 (thinking) as the semantic evaluator. Given a task triplet—comprising the instruction, the pre-edit Lean file, and the candidate patch—the model assesses whether the patch fulfils the instruction in both structure and intent. To improve robustness, we adopt a **sample@4** strategy with majority voting, where a task is considered semantically successful only if most samples agree that all subcomponents of the instruction are correctly implemented.

Our choice of Claude Sonnet 3.7 (thinking) as the primary semantic judge is supported by empirical validation. As demonstrated in Section 5.5, when comparing judgements across multiple LLM judges (Claude Sonnet 3.7 thinking, Gemini 2.5 Pro Preview, DeepSeek V3, and DeepSeek R1), Claude Sonnet 3.7 (thinking) exhibits the lowest deviation from majority consensus. This suggests it provides the most balanced assessment across diverse proof engineering styles, with minimal bias toward specific model families or proof strategies.

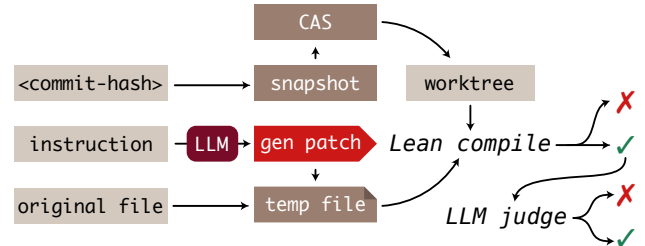


Figure 5 Evaluation pipeline for APE-Bench I. Given a commit hash, the corresponding Lean environment is restored by a snapshot from content-addressable storage (CAS), reproducing the exact worktree state. An LLM generates a patch based on the instruction and the original file. This patch is applied to a temporary file and evaluated through Lean compile and LLM judge.

While a multi-judge system with cross-model voting could theoretically provide more robust evaluation, particularly for models that exhibit high judge-to-judge variance, our experiments indicate that Claude Sonnet 3.7 (thinking) offers a reasonable approximation of consensus judgment. This approach balances evaluation quality with system simplicity, enabling efficient assessment across thousands of tasks without sacrificing reliability.

5 Experiments

5.1 Experimental Setup

We evaluate eight state-of-the-art language models on APE-Bench I: Gemini 2.5 Pro Preview, o3-mini, Claude Sonnet 3.7 (with and without thinking mode), DeepSeek R1, DeepSeek V3, GPT-4o, and Doubao 1.5 Pro. All models generate patches in unified diff format without task-specific fine-tuning. We process outputs using DiffRepair, a post-processing mechanism that rewrites imprecise diffs into structurally consistent patches (described in Appendix D.3). We adopt the standard pass@ k evaluation [3] to estimate task success rates. For each task, $n = 20$ candidate patches are sampled, and pass@16 is computed using the unbiased estimator:

$$\text{pass}@k := \mathbb{E} \left[1 - \frac{\binom{n-c}{k}}{\binom{n}{k}} \right],$$

where $c \leq n$ is the number of patches passing both syntactic and semantic judgement. For most models, we use temperature $T=0.6$ to improve output diversity.

5.2 Main Results

We evaluate model performance using the pass@16 metric, which estimates the probability that at least one of 16 generated candidates satisfies specified criteria. Specifically, we distinguish between:

- **Verification pass@16:** The proportion of tasks for which at least one candidate compiles successfully using Lean 4.
- **Judgement pass@16:** The proportion of tasks for which at least one compiled candidate additionally satisfies the instruction according to semantic evaluation.
- **Relative Decrease:** The percentage decrease from Verification to Judgement success, reflecting how often syntactically valid outputs fail to meet the intended edits.

Model	Verification pass@16	Judgement pass@16	Relative Decrease (%)
Gemini 2.5 Pro Preview	18.79%	18.04%	3.99%
DeepSeek R1	15.30%	12.55%	17.97%
Claude Sonnet 3.7 (thinking)	12.73%	12.73%	0.001%
o3-mini	20.13%	8.60%	57.28%
Claude Sonnet 3.7	11.33%	10.83%	4.41%
DeepSeek V3	12.44%	11.81%	5.06%
GPT-4o	15.16%	6.73%	55.61%
Doubao 1.5 Pro	6.19%	2.98%	51.86%

Table 2 Overall model performance on APE-Bench I using pass@16. Relative Decrease is computed as the percentage of Lean-compilable outputs that fail LLM-based semantic judgement.

As shown in Table 2, Gemini 2.5 Pro Preview achieves the highest judgement success rate at 18.04%, while o3-mini leads in verification pass rate (20.13%) but suffers from a substantial relative decrease (57.28%). Claude Sonnet 3.7 (thinking) exhibits nearly perfect semantic consistency with a negligible relative decrease (0.001%), though at a lower overall success rate. GPT-4o shows the largest semantic gap with a relative

decrease of 55.61%, indicating that half of its syntactically valid outputs fail to meet the semantic requirements of the tasks.

Notably, even the best-performing model succeeds on only about one-sixth of the benchmark tasks, highlighting the substantial gap between present capabilities and the demands of real-world proof engineering. Additional performance metrics across different pass@k values are available in D.

5.3 Structural Robustness and Task-Scale Sensitivity

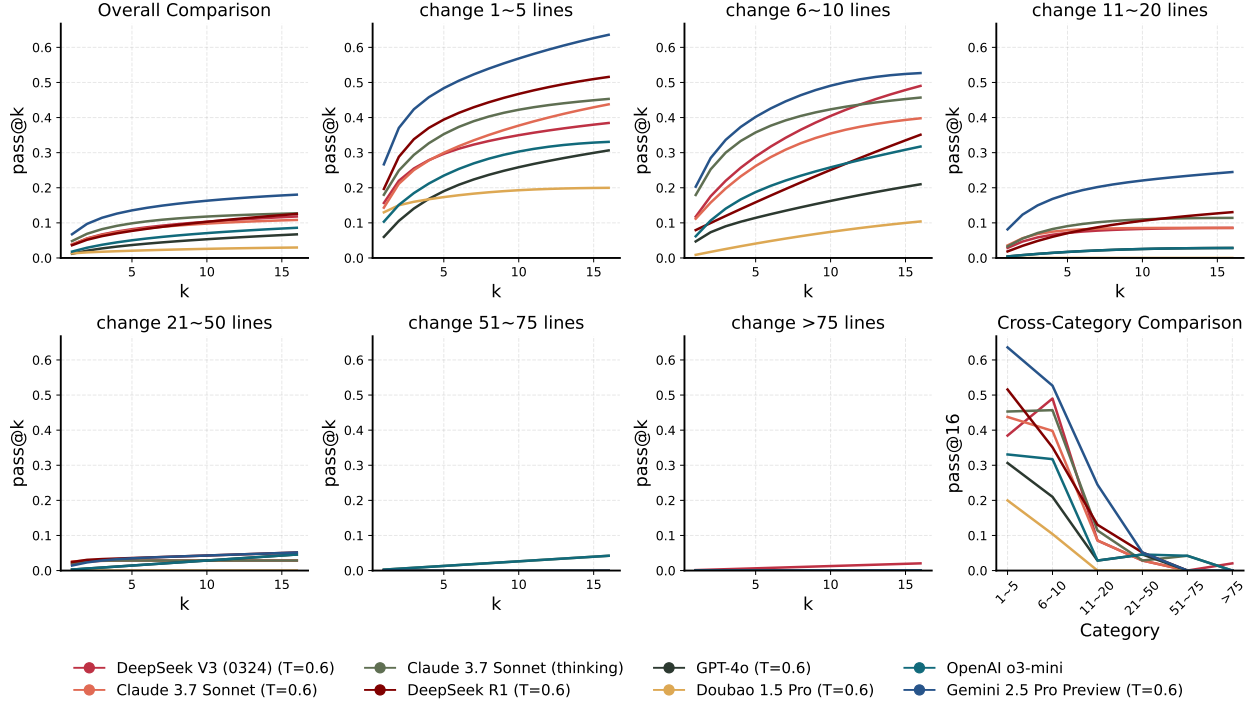


Figure 6 Model pass@16 success rate grouped by ground-truth patch size. Larger edits cause sharp performance degradation. Gemini 2.5 Pro Preview leads across most bins up to 20 lines, no model shows robustness on large edits.

We first group benchmark tasks by the size of their ground-truth patches and evaluate model pass@16 within each bin. As shown in Figure 6, most models exhibit sharp performance degradation as the size of the target edit increases. While all models achieve moderate to high success rates on small-scale edits (1–5 lines), performance drops significantly for medium (11–20 lines) and large-scale (>20 lines) tasks. Notably, Gemini 2.5 Pro Preview consistently achieves the highest pass@16 across small and medium bins, while all models collapse to near-zero beyond 50 lines of change, underscoring the challenge of scaling to structurally complex edits.

To further investigate structural sensitivity, we evaluate model performance across different task categories, difficulty levels, and mathematical domains. Figure 7 presents a unified heatmap showing pass@16 evaluation results for each model across these dimensions. Tasks labeled as bug fixes are handled reasonably well by all models, likely due to their localized and low-risk nature. Refactoring tasks reveal more pronounced model differences: Gemini and Claude variants perform relatively well, likely due to their bias toward structural preservation, whereas GPT-4o and Doubao underperform. Feature addition tasks are the most challenging, with Gemini 2.5 Pro Preview demonstrating the strongest performance in this category.

Difficulty-based analysis reveals a sharp capability cliff. While several models perform well on easy tasks, performance drops significantly on medium-difficulty tasks, and no model achieves non-zero success on hard tasks. These hard tasks, which typically involve large-scale edits or cross-declaration dependencies, remain virtually unsolved by all leading models. Domain-based variation is also evident: dynamics and tactic modules

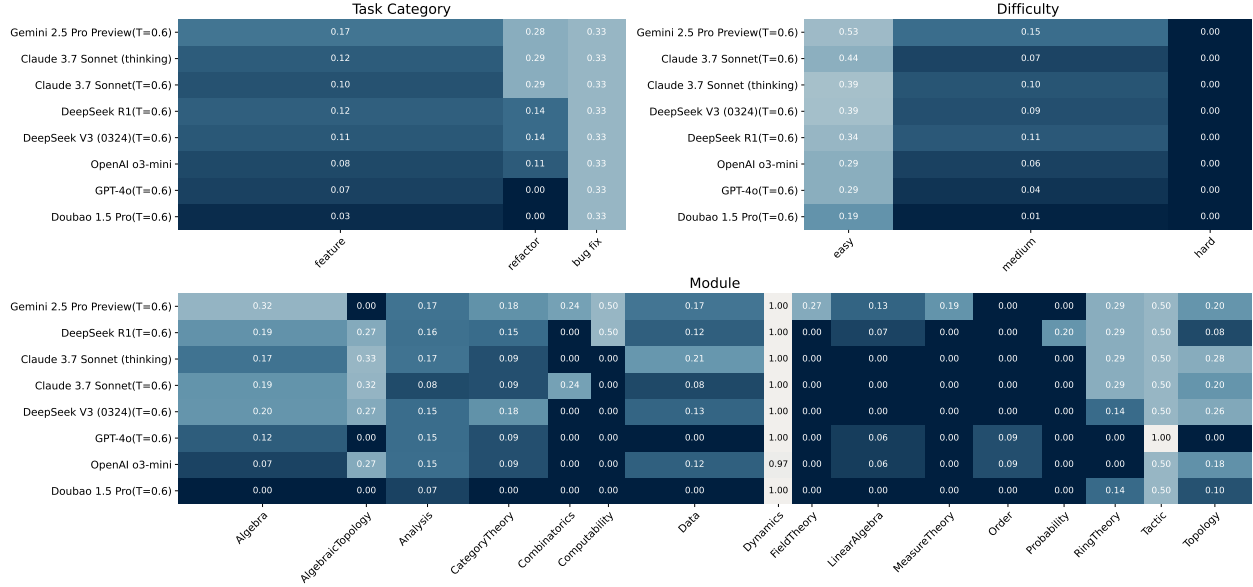


Figure 7 Heatmap of evaluation pass@16 success rates across different task types, difficulty levels, and mathematical modules. Column widths represent the proportion of each class in the test set. Color intensity indicates model performance.

are consistently easier for most models, whereas combinatorics, measure theory, probability theory, and set theory present the greatest challenges.

5.4 Semantic Robustness and Failure Characterization

Error Class	Description
Component Omission	Required definitions, proofs, or examples are missing
Incompleteness Issue	The edit is structurally partial, unfinished, or placeholder
Mathematical Error	The logic is invalid or inconsistent with Lean’s formal semantics
Quality Defect	Redundant or unabstracted edits, or lack of documentation
Requirement Mismatch	Misalignment with the intended instruction

Table 3 Semantic error classes and their typical manifestations.

To understand why many syntactically valid patches nonetheless fail semantically, we analyse failure cases using a taxonomy of five high-level semantic error types (Table 3). Figure 8 shows the distribution of these errors as a proportion of failure cases for each model. Across the board, component omission emerges as the most dominant failure mode, where models skip required definitions, theorems, or implementation elements. Closely following are quality defects (e.g., redundant edits, poor formatting, or missing documentation) and **incompleteness issues**, where patches are partially implemented or left unfinished. GPT-4o and o3-mini exhibit notably high error frequencies in all categories, not only producing mathematically incorrect or incomplete outputs, but also failing to align edits with task instructions—reflecting a lack of planning, verification, and structural awareness. By contrast, Claude Sonnet 3.7 (thinking) maintains the lowest error rates across all dimensions, demonstrating strong consistency and semantic robustness.

These findings indicate that semantic failures are not random, but exhibit clear structural patterns. Most errors arise from insufficient edit planning, incomplete satisfaction of instructions, or a lack of global structural understanding. While mechanisms like *DiffRepair* (see Appendix D.3) can correct syntactic misalignments, they cannot compensate for omitted logic or misinterpreted intent. Future improvements will require models

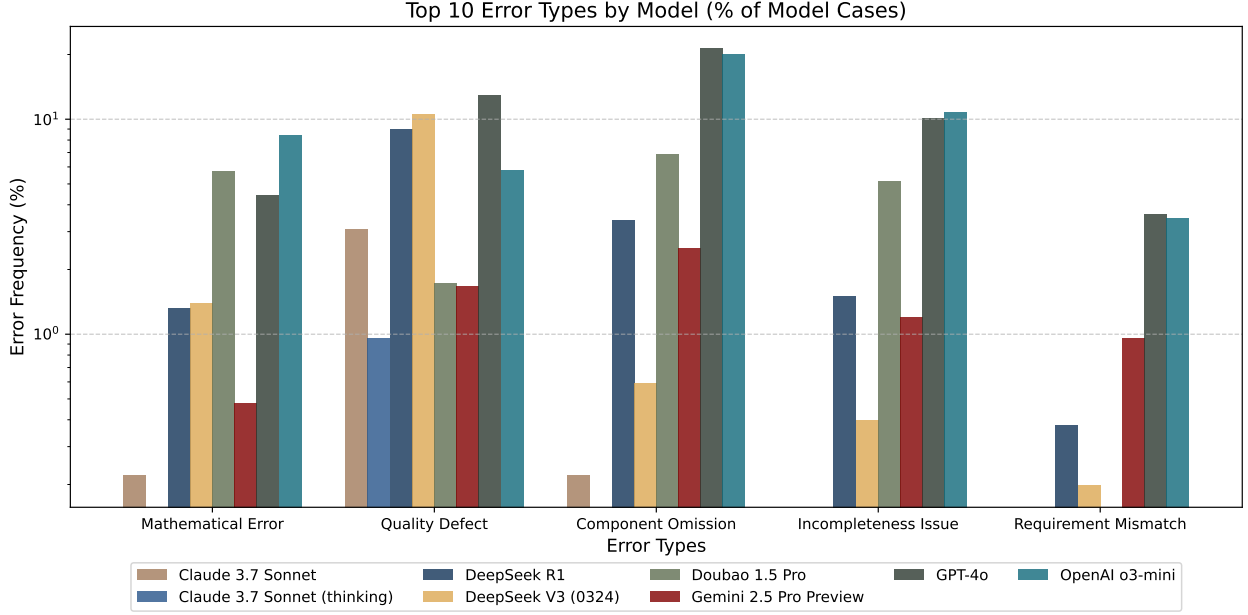


Figure 8 Distribution of semantic error types across models (log-scaled y-axis). Component omission, quality defects, and incompleteness are the most frequent error types, with Claude Sonnet 3.7 (thinking) showing consistently minimal error rates.

to engage in multi-step planning, instruction verification, and iterative refinement to bridge the gap between syntactic validity and semantic correctness.

5.5 Judge Model Selection and Evaluation Bias

While syntactic validity can be objectively determined by the Lean compiler, semantic evaluation requires subjective judgment. In our framework, this is delegated to large language models acting as instruction-conditioned judges. However, since these judges are themselves LLMs, a natural concern arises: do they exhibit systematic bias, particularly favoring outputs from models within their own family?

To measure this effect, we introduce a **Family Preference Index (FPI)**, which quantifies the relative deviation between a judge’s ratings of same-family versus other-family models. Formally, for judge J ,

$$\text{FPI}_J = \mathbb{E}_{m \in M_{\text{same}}}[\Delta_{J,m}] - \mathbb{E}_{m \in M_{\text{other}}}[\Delta_{J,m}]$$

where $\Delta_{J,m}$ is the deviation between J ’s score and the majority consensus for model m . A positive FPI suggests preferential scoring toward same-family outputs.

As summarized in Table 4, most judges display mild but measurable family preferences. Gemini and DeepSeek V3 exhibit positive FPIs, indicating upward bias for their own models. Claude Sonnet 3.7 (thinking) shows the smallest FPI and the lowest deviation from majority voting, reflecting high consistency and relative neutrality. In contrast, DeepSeek R1 reveals a reversed pattern, assigning more favorable ratings to non-family outputs.

While no judge displays extreme favoritism—most FPI values remain within $\pm 2\%$ —such biases can subtly influence evaluations, especially when models are closely matched. These findings motivate our choice of Claude Sonnet 3.7 (thinking) as the primary semantic evaluator, based on its empirical alignment with consensus and minimal systemic bias. To further improve robustness, future work may incorporate multi-judge aggregation, adversarial calibration, or dedicated reference evaluators.

Model Evaluated	Claude Thinking (%)		Gemini (%)		DeepSeek R1 (%)		DeepSeek V3 (%)		Majority Vote (%)
Gemini 2.5 Pro Preview	18.04	+0.55	16.20	-1.29	17.66	+0.17	18.05	+0.56	17.49
DeepSeek R1	12.55	-0.38	10.56	-2.37	13.80	+0.87	14.80	+1.87	12.93
Claude Sonnet 3.7 (thinking)	12.73	+0.31	11.47	-0.95	12.73	+0.31	12.73	+0.31	12.42
o3-mini	8.60	-2.22	5.94	-4.88	15.31	+4.49	13.42	+2.60	10.82
Claude Sonnet 3.7	10.83	+0.25	8.84	-1.74	11.33	+0.75	11.33	+0.75	10.58
DeepSeek V3	11.81	+0.53	9.44	-1.84	11.93	+0.65	11.92	+0.64	11.28
GPT-4o	6.73	-1.85	5.71	-2.87	13.31	+4.73	8.58	0.00	8.58
Doubao 1.5 Pro	2.98	-0.68	3.48	-0.18	4.08	+0.42	4.08	+0.42	3.66
Squared Deviation from Majority	3.31		78.02		233.61		81.69		-
Family Preference Index (FPI)	+0.95%		+2.12%		-1.16%		+1.10%		-

Table 4 Judge model comparison: Success rates across different LLM judges. Each judge column shows score and deviation from majority (colored: green for positive, red for negative). The bottom rows report total deviation from consensus (squared) and the Family Preference Index (FPI), which quantifies each judge’s average relative bias toward its own model family.

6 Conclusion

This work introduces the paradigm of Automated Proof Engineering (APE) and presents APE-Bench I, the first large-scale benchmark grounded in real-world proof development workflows from **Mathlib4**. By reframing formal mathematics as instruction-driven code editing and combining Lean compilation with LLM-based semantic evaluation, APE-Bench I offers a rigorous framework for evaluating LLMs in realistic proof engineering tasks. Our empirical results reveal significant performance gaps among state-of-the-art models, particularly under structurally complex scenarios.

A key limitation of APE-Bench I is its focus on single-file edits. Future work will extend this to APE-Bench II and III, which will address multi-file coordination, project-scale verification, and ultimately, autonomous agents capable of planning, editing, and repairing formal libraries. This benchmark series lays the foundation for developing next-generation systems for practical and scalable formal proof maintenance.

References

- [1] Riyaz Ahuja, Jeremy Avigad, Prasad Tetali, and Sean Welleck. Improver: Agent-based automated proof optimization. In *The Thirteenth International Conference on Learning Representations*.
- [2] Ahmet Celik, Karl Palmskog, and Milos Gligoric. icoq: Regression proof selection for large-scale verification projects. In *2017 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pages 171–182. IEEE, 2017.
- [3] Mark Chen, Jerry Tworek, Heewoo Jun, Qiming Yuan, Henrique Ponde De Oliveira Pinto, Jared Kaplan, Harri Edwards, Yuri Burda, Nicholas Joseph, Greg Brockman, et al. Evaluating large language models trained on code. *arXiv preprint arXiv:2107.03374*, 2021.
- [4] Emily First, Markus N Rabe, Talia Ringer, and Yuriy Brun. Baldur: Whole-proof generation and repair with large language models. In *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pages 1229–1241, 2023.
- [5] Jiewen Hu, Thomas Zhu, and Sean Welleck. miniCTX: Neural theorem proving with (long-)contexts. In *The Thirteenth International Conference on Learning Representations*, 2025. URL <https://openreview.net/forum?id=KIgaAqEFHW>.
- [6] Albert Qiaochu Jiang, Sean Welleck, Jin Peng Zhou, Timothee Lacroix, Jiacheng Liu, Wenda Li, Mateja Jamnik, Guillaume Lample, and Yuhuai Wu. Draft, sketch, and prove: Guiding formal theorem provers with informal proofs. In *The Eleventh International Conference on Learning Representations*, 2023.

- [7] Carlos E Jimenez, John Yang, Alexander Wettig, Shunyu Yao, Kexin Pei, Ofir Press, and Karthik Narasimhan. Swe-bench: Can language models resolve real-world github issues? *arXiv preprint arXiv:2310.06770*, 2023.
- [8] Gerwin Klein. Proof engineering considered essential. In *International Symposium on Formal Methods*, pages 16–21. Springer, 2014.
- [9] The mathlib Community. The lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020*, page 367–381, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450370974. doi: 10.1145/3372885.3373824. URL <https://doi.org/10.1145/3372885.3373824>.
- [10] Talia Ringer, Karl Palmskog, Ilya Sergey, Milos Gligoric, Zachary Tatlock, et al. Qed at large: A survey of engineering of formally verified software. *Foundations and Trends® in Programming Languages*, 5(2-3):102–281, 2019.
- [11] Haiming Wang, Huajian Xin, Chuanyang Zheng, Zhengying Liu, Qingxing Cao, Yinya Huang, Jing Xiong, Han Shi, Enze Xie, Jian Yin, et al. Lego-prover: Neural theorem proving with growing libraries. In *The Twelfth International Conference on Learning Representations*, 2024.
- [12] Huajian Xin, Z.Z. Ren, Junxiao Song, Zhihong Shao, Wanbiao Zhao, Haocheng Wang, Bo Liu, Liyue Zhang, Xuan Lu, Qiushi Du, Wenjun Gao, Haowei Zhang, Qihao Zhu, Dejian Yang, Zhibin Gou, Z.F. Wu, Fuli Luo, and Chong Ruan. Deepseek-prover-v1.5: Harnessing proof assistant feedback for reinforcement learning and monte-carlo tree search. In *The Thirteenth International Conference on Learning Representations*, 2025. URL <https://openreview.net/forum?id=I4YAIwrsXa>.
- [13] Jin Peng Zhou, Yuhuai Wu, Qiyang Li, and Roger Baker Grosse. Refactor: Learning to extract theorems from proofs. In *The Twelfth International Conference on Learning Representations*.

A Extended Background and Related Work

A.1 Formal Proof Engineering: Practice and Challenges

Real-world formal verification projects, including Lean’s Mathlib [9], Isabelle’s Archive of Formal Proofs, and the seL4 microkernel verification project [8], exemplify the scale and complexity of proof engineering. These libraries often contain thousands of interdependent definitions, theorems, and proofs, where modifying a single element may trigger cascading changes across the codebase. Ensuring logical consistency under such conditions demands significant manual labour and deep structural awareness.

While certain tools—such as iCoq for regression-proving [2]—provide partial automation, they are largely heuristic and require intensive human oversight. To date, there remains a lack of automated systems capable of performing high-fidelity edits in complex proof environments.

A.2 Limitations of Existing Benchmarks

The current gap between theorem-proving benchmarks and practical proof engineering extends beyond the aspects highlighted in Table 1. Most benchmarks focus on mathematical reasoning skills in isolation, but lack the context of evolving codebases, dependency management, and continuous integration requirements common in real-world libraries.

Several recent efforts have explored richer proof generation scenarios, such as incorporating intermediate steps, leveraging auxiliary definitions [4–6, 11, 12], or modifying existing proofs through refactoring [13] and improvement techniques [1]. However, these approaches are still typically used as tools for data augmentation or pipeline enhancement, rather than serving as rigorous evaluation frameworks that capture realistic development workflows.

Key missing dimensions in current benchmarks include:

- **Temporal evolution:** Real libraries evolve over time, with changing interfaces, dependencies, and conventions

- **Multi-file coordination:** Changes often span multiple files and require maintaining consistency across module boundaries
- **Developer intent:** Practical edits are driven by specific goals such as optimisation, generalisation, or feature addition
- **Maintenance workflows:** Libraries require continuous refactoring, bug fixing, and adaptation to evolving theories

A.3 Comparison with Software Engineering Benchmarks: The Case of SWE-Bench

The evolution towards more realistic benchmarks is a shared trend across automated reasoning domains. In software engineering, the introduction of benchmarks like SWE-Bench [7] marked a significant step, moving from isolated code generation tasks to evaluating LLMs on resolving real-world GitHub issues within established Python repositories. SWE-Bench’s reliance on existing unit test suites for verifying functional correctness provides an objective and automated measure of success, offering a valuable paradigm.

APE-Bench draws inspiration from this advancement, aiming to create a similarly realistic and challenging environment for automated proof engineering. Like SWE-Bench, it sources tasks from real-world commit histories and focuses on instruction-driven modifications. However, the distinct nature of formal mathematics compared to general software engineering necessitates adaptations in task structure and evaluation. Table 5 outlines the key distinctions.

Aspect	SWE-Bench (Software Eng.)	APE-Bench (Proof Eng.)
Core Task	Resolve functional issues	Implement proof modifications
Syntactic Check	Compiler/Interpreter	Lean Compiler (type checking)
Semantic Verification	Unit tests for functional correctness	LLM-as-a-judge for semantic alignment with instructions
Objects	Observable behavior, I/O correctness	Logical validity, structural integrity, adherence to mathematical intent

Table 5 Comparison between SWE-Bench and APE-Bench.

A primary divergence lies in semantic evaluation. While software functionality can often be robustly verified by unit tests capturing desired behaviors, the semantic correctness of a proof modification is more nuanced. A syntactically valid proof (i.e., one that typechecks via the Lean compiler, analogous to code compilation) may still fail to accurately capture the intended mathematical argument, correctly implement a refactoring goal, or properly introduce a new definition as per the natural language instruction. The abstract logical structures and the specific intent behind a proof change are not always fully verifiable by pre-existing automated tests in the same direct manner.

This distinction motivates APE-Bench’s hybrid evaluation strategy: combining compiler-based syntactic verification with an LLM-as-a-Judge (Section 4.2) to assess semantic fulfillment of the natural language instruction. This approach is a pragmatic response to the unique challenges of evaluating proof engineering tasks. Ultimately, APE-Bench aspires to evolve into a standard environment for developing and benchmarking increasingly sophisticated proof engineering agents, mirroring the role SWE-Bench plays in advancing agentic capabilities for software engineering.

B APE-Bench I Construction Details

B.1 Detailed Commit Mining Methodology

Our benchmark construction pipeline incorporates several specialised heuristics to ensure task quality and diversity:

Semantic Filtering Implementation. To identify commits with recognisable intent, we analyse commit messages using regular expressions that match conventional prefixes like `feat:`, `fix:`, or `refactor:`. We also exclude commits that alter more than 10 files, as these typically represent mechanical changes rather than substantive engineering. Additionally, we filter out commits that only affect `non-Mathlib/` directories (e.g., documentation or build scripts).

Content Quality Metrics. Beyond simple line counting, we implement structural content analysis to identify semantically trivial changes:

- **Whitespace ratio:** We exclude diffs where $>80\%$ of changes affect only whitespace or empty lines.
- **Comment-only changes:** We detect and filter diffs that modify exclusively comment blocks (using Lean’s comment syntax patterns).
- **Import statement changes:** Changes affecting only import order or organisation are excluded.

Chunk Segmentation Strategies. When segmenting modified files, we employ syntax-aware boundaries:

- For existing files, we use Lean’s declaration structure to identify logical boundaries.
- For newly added files, we use heuristics based on blank lines and declaration keywords.
- When expanding large diffs, we maintain declaration integrity by never splitting across `def`, `theorem`, or other key structural elements.

These specialised techniques ensure that the resulting benchmark captures meaningful, self-contained, and structurally coherent proof engineering tasks rather than trivial or fragmented edits.

B.2 Instruction Synthesis Methodology

For instruction generation, we employ a carefully engineered prompt that directs Claude Sonnet 3.7 (thinking mode) to analyse a given diff and extract the underlying developer intent. The prompt specifically targets:

- **Intent Extraction:** Identifying the core purpose of the edit by analysing both structural changes and semantic modifications.
- **Imperative Formulation:** Reframing the extracted intent as a clear, actionable instruction using imperative voice.
- **Technical Precision:** Maintaining mathematical and Lean-specific terminology where appropriate.
- **Scoping Accuracy:** Ensuring the instruction’s scope corresponds to the actual changes in the diff.

To validate instruction quality, we implement a reverse verification procedure where another LLM instance evaluates the alignment between the generated instruction and the actual diff. Instructions that do not sufficiently specify the target change or contain ambiguities are regenerated until they meet quality thresholds.

B.3 Statistical Validation of Task Labels

Difficulty Labels Beyond Line Counts. Figure 4a shows that while **Easy** tasks are generally small, **Medium** and **Hard** tasks span a broad range of edit sizes, with no strict separation based on line count. This indicates that difficulty labels capture more than superficial metrics—they reflect underlying semantic and structural complexity. This is further confirmed by object-level patterns in Figure 9. **Medium** and **Hard** tasks involve more declarations and larger edits per object, particularly for theorems, suggesting greater logical coordination and proof effort. These trends align with empirical results in Section 5, where model performance declines sharply from **Easy** to **Hard**, validating the semantic significance of the difficulty labels.

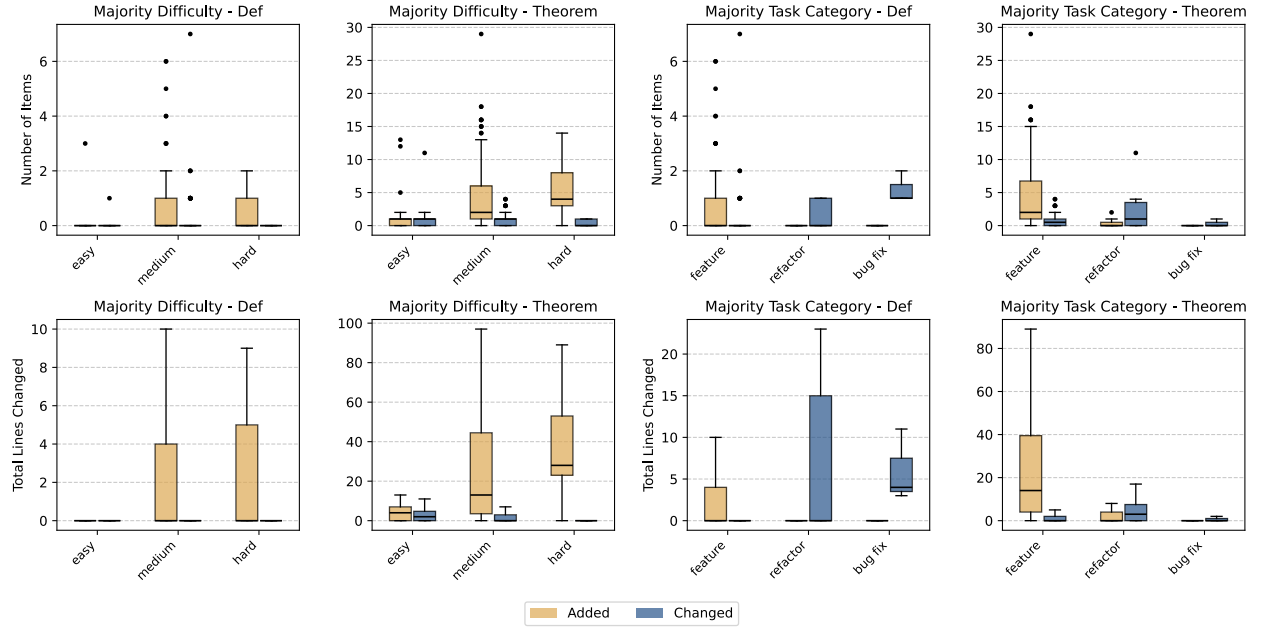


Figure 9 Object-level statistics of Lean patches in the test set. Distribution of added and changed `def` and `theorem` declarations, measured by count and total lines.

Functional Category Distinctions. Task categories also reveal distinct structural roles. As shown in Figure 4b, **Feature** tasks are larger and often involve new declarations, while **Refactor** and **Bug Fix** edits are smaller and focus on modifying existing code. Object-level statistics support this: **Feature** tasks add theorems and definitions, while the other two primarily adjust existing `defs`. These differences reflect practical development workflows. The small scale of **Refactor** and **Bug Fix** edits stems in part from filtering heuristics, which exclude trivial or mechanical changes. As such, retained tasks across all categories represent meaningful engineering actions.

C Evaluation Infrastructure Details

C.1 Eleanstic: Version-Aware Verification Infrastructure

Eleanstic provides a scalable, version-aware verification system for Lean code through a sophisticated snapshot mechanism. Its implementation consists of three key components:

Snapshot Generation. For each unique commit, Eleanstic first performs a clean `lake build` and recursively traverses the resulting worktree. Every file is hashed using SHA-256 and stored in a content-addressable storage (CAS) structure with a two-level hash-based directory layout. In parallel, a binary snapshot is created to record the mapping from relative file paths to content hashes and file types (regular or symbolic). This snapshot, encoded using fixed-width binary records, serves as a complete and portable blueprint of the post-build environment, ensuring reproducibility while minimising metadata overhead.

Our implementation runs on a single server with 128 CPU cores and 1TB of RAM. The initial compilation and snapshot generation for all 3734 commits from the Mathlib4 history required approximately 2 days of processing time. Once generated, these snapshots enable efficient verification of candidate patches, with each patch verification typically completing in seconds.

Snapshot Restoration. At verification time, the appropriate snapshot is loaded and its contents restored into a temporary, isolated worktree that exactly replicates the post-build file structure of the original compilation. Files are fetched from the global CAS and written to disk. This process is stateless and fully parallelisable,

enabling fast switching across historical commits without requiring repeated builds. Empirically, Eleanstic restores a full Lean environment in under one second on SSD-backed systems. To support long-term scalability, Eleanstic performs aggressive global deduplication across all snapshots. Across 3734 commits spanning August 2023 to March 2025, it compresses 15.6 TB of build artifacts into just 1.1 TB, yielding a storage reduction of over 93%. This compression enables persistent caching of every historical state required for evaluation, without exhausting disk resources.

Patch Verification. After restoring the environment, the model-generated patch is applied to the target Lean file, and the resulting content is saved to a temporary file. Verification follows a strict *file-level isolation* policy: rooted in the restored Mathlib worktree, the Lean compiler compiles only the temporary file without affecting any files in the restored environment. Additionally, any temporary file that attempts to import the target file is discarded to prevent unintended leakage across file boundaries. A patch is considered syntactically valid if it compiles successfully within the corresponding version of Mathlib4 and does not emit warnings.

C.2 LLM-as-a-Judge: Semantic Evaluation Protocol

Our semantic evaluation protocol uses a large language model to assess whether a patch correctly implements the specified task. This approach offers several advantages over rule-based verification, including adaptability to diverse instruction types and sensitivity to nuanced semantic requirements.

Model and Prompt. We use Claude Sonnet 3.7 (thinking mode) as the semantic evaluator. Given a task triplet-comprising the instruction, the pre-edit Lean file, and the candidate patch-the model is prompted to assess whether the patch fulfills the instruction in both structure and intent. The prompt encourages multi-step reasoning over the instruction, analysis of the proposed changes, and consistency verification. To ensure output stability and reduce overfitting to prompt phrasing, the full evaluation prompt is designed to be modular and instruction-agnostic.

Voting Strategy and Decision Criteria. To improve robustness, we adopt a **sample@4** strategy: four independent judgements are sampled from Claude for each evaluation instance. The final verdict is determined by majority vote, where a task is considered semantically successful only if the majority of samples agree that all subcomponents of the instruction are correctly implemented. This approach balances reliability and scalability while maintaining consistency across model outputs. All semantic evaluation results reported in this work are based on this protocol.

D Additional Experimental Results and Analysis

D.1 Model Performance Across pass@k Values

Figure 10 illustrates model behaviour across different pass@ k thresholds. The left panel reports syntactic success (Lean Compile), while the right panel shows semantic success (LLM-Judge) conditioned on compilation. Gemini 2.5 Pro Preview achieves the highest semantic pass@ k across all values of k , reflecting consistent success in generating instruction-aligned patches. On the syntactic side, o3-mini leads at higher k values due to more diverse sampling, though its semantic pass@ k grows more slowly in comparison. Claude Sonnet 3.7 (thinking) maintains stable but moderate gains in both dimensions. These trends highlight a persistent syntax-semantic gap: models that perform well in compilation do not always satisfy task intent. Sampling diversity improves raw compilation rates but does not necessarily translate to semantic alignment, underscoring the need for instruction-aware generation strategies.

D.2 Patch Length Alignment with Ground-Truth

Figure 11 evaluates whether model-generated patches exhibit scale-aware behaviour by comparing their length to the corresponding human edits. Most models still tend to over-edit small tasks (fewer than 8 lines of substantive changes, excluding blanks and comments), generating unnecessarily long patches. As task size increases, models like Gemini 2.5 Pro Preview and both Claude Sonnet and DeepSeek variants show strong alignment with the ground truth, maintaining near-diagonal trends and low mean squared error (MSE).

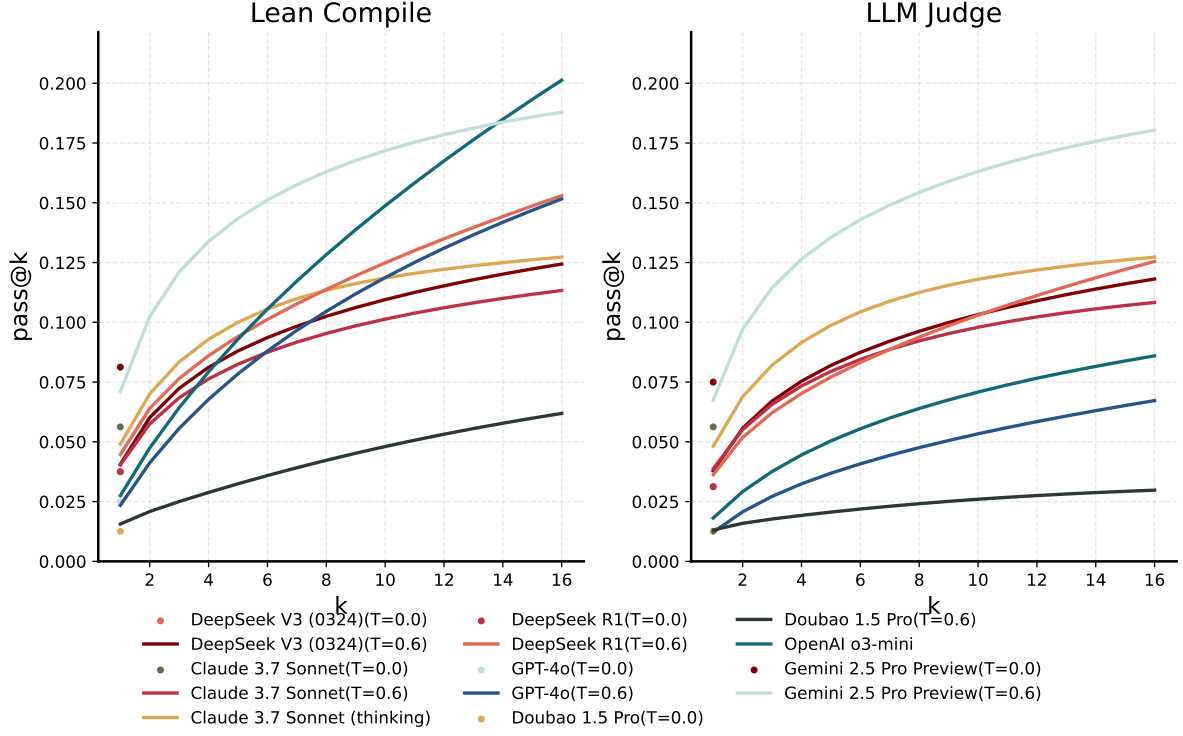


Figure 10 Model performance across pass@k values. Left: Lean Compile pass@k (syntactic validity). **Right:** LLM Judge pass@k (semantic correctness conditioned on compilation).

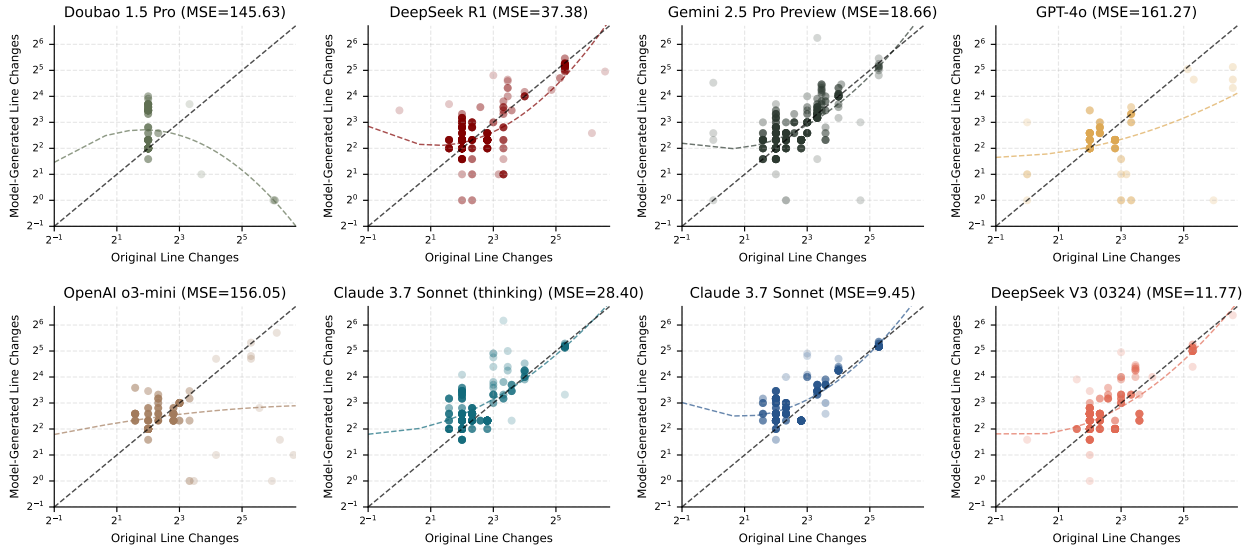


Figure 11 Patch length alignment across models (log-log scale). Each panel plots the number of non-comment lines changed by the model (y-axis) versus the human reference patch (x-axis). The dashed diagonal indicates ideal alignment.

In contrast, GPT-4o, o3-mini and Doubao 1.5 Pro significantly under-edit across the board, especially on larger edits, resulting in high patch-length MSE. This misalignment correlates with a higher frequency of quality defects and component omissions.

These results suggest that while strict length matching is not a prerequisite for semantic correctness, extreme deviation—especially persistent over-editing—can lead to incomplete or misaligned edits. Models that strike a balance between scale-awareness and structural flexibility, such as Claude Sonnet, Gemini and DeepSeek V3, tend to perform more robustly in proof engineering tasks.

D.3 DiffRepair: Patch Normalization System

Model outputs are produced in unified diff format, which often contains structurally imprecise or misaligned edits (e.g., incorrect line anchors, out-of-date contexts). To ensure reliable application and verification, we introduce a post-processing phase called *DiffRepair*, which rewrites imprecise diffs into structurally consistent patches. This mechanism operates in two phases: first, it localises the intended edit position using fuzzy anchor matching; then it reconstructs the patch with preserved structural and contextual integrity.

Intent Localisation. Given a noisy diff, DiffRepair first identifies where in the original Lean file the intended modification should take place. It uses a multi-granularity fuzzy matching strategy based on contextual anchors surrounding each diff hunk. Anchors are matched using exact or prefix-based line similarity, normalized token-level matching with whitespace tolerance, and structural proximity emphasising declaration-aligned contexts. Matches are scored using a dynamic programming model optimising for structural alignment and modification preservation.

Patch Reconstruction. Once the target region is localised, DiffRepair reconstructs a clean diff by re-aligning added and deleted lines to structurally valid positions, augmenting missing context to satisfy unified diff constraints, resolving line number offsets and conflicting hunk overlaps, and merging multiple hunks into a minimal, coherent patch that preserves original semantics. This approach ensures that evaluation focuses on semantic correctness rather than superficial formatting issues.

Model	Raw Apply Success	Exact Match Repair	Fuzzy Match Repair
DeepSeek V3	15.60%	52.08%	83.01%
DeepSeek R1	14.82%	49.46%	83.01%
Doubao 1.5 Pro	15.62%	13.60%	81.64%
Claude Sonnet 3.7	13.39%	13.72%	70.30%
Claude Sonnet 3.7 (thinking)	12.69%	14.22%	69.19%
o3-mini	14.22%	22.34%	58.78%
GPT-4o	12.53%	6.58%	42.95%

Table 6 Patch success rates before and after structural repair. Exact match applies conservative anchor correction; fuzzy match enables tolerant application using semantic alignment.

As shown in Table 6, raw apply success rates remain low for all models, ranging from 12% to 16%, indicating poor structural precision in the initial output. Exact match repair offers moderate improvement for DeepSeek models, but fails to resolve structural errors in o3-mini or GPT-4o outputs. Fuzzy match repair significantly boosts success across the board, particularly for DeepSeek R1, Doubao, and Claude Sonnet 3.7. These results highlight the necessity of structural repair mechanisms for enabling meaningful evaluation and practical usability.

E Illustrative Examples

Source code: [/-](#)
 Copyright (c) 2017 Mario Carneiro. All rights reserved.

```

Released under Apache 2.0 license as described in the file LICENSE.
Authors: Mario Carneiro
-/
import Mathlib.Data.Fintype.EquivFin
import Mathlib.Data.Finset.Option

/--!
# fintype instances for option
-/

assert_not_exists MonoidWithZero MulAction

open Function

open Nat

universe u v

variable {α β : Type*}

open Finset Function

instance {α : Type*} [Fintype α] : Fintype (Option α) :=
  ⟨Finset.insertNone univ, fun a => by simp⟩

theorem univ_option (α : Type*) [Fintype α] : (univ : Finset (Option α)) = insertNone univ :=
  rfl

@[simp]
theorem Fintype.card_option {α : Type*} [Fintype α] :
  Fintype.card (Option α) = Fintype.card α + 1 :=
  (Finset.card_cons (by simp)).trans <| congr_arg2 _ (card_map _) rfl

/-- If 'Option α' is a 'Fintype' then so is 'α' -/
def fintypeOfOption {α : Type*} [Fintype (Option α)] : Fintype α :=
  ⟨Finset.eraseNone (Fintype.elims (α := Option α)), fun x =>
    mem_eraseNone.mpr (Fintype.complete (some x))⟩

/-- A type is a 'Fintype' if its successor (using 'Option') is a 'Fintype'. -/
def fintypeOfOptionEquiv [Fintype α] (f : α ≃ Option β) : Fintype β :=
  haveI := Fintype.ofEquiv _ f
  fintypeOfOption

namespace Fintype

/-- A recursor principle for finite types, analogous to 'Nat.rec'. It effectively says
that every 'Fintype' is either 'Empty' or 'Option α', up to an 'Equiv'. -/
def truncRecEmptyOption {P : Type u → Sort v} (of_equiv : ∀ {α β}, α ≃ β → P α → P β)
  (h_empty : P PEmpty) (h_option : ∀ {α} [Fintype α] [DecidableEq α], P α → P (Option α))
  (α : Type u) [Fintype α] [DecidableEq α] : Trunc (P α) := by
  suffices ∀ n : ℕ, Trunc (P (ULift <| Fin n)) by
    apply Trunc.bind (this (Fintype.card α))
    intro h
    apply Trunc.map _ (Fintype.truncEquivFin α)
    intro e
    exact of_equiv (Equiv.ulift.trans e.symm) h
  apply ind where
    -- Porting note: do a manual recursion, instead of 'induction' tactic,

```

```

-- to ensure the result is computable
/-- Internal induction hypothesis -/
ind : ∀ n : ℕ, Trunc (P (ULift <| Fin n))
| Nat.zero => by
  have : card PEmpty = card (ULift (Fin 0)) := by simp only [card_fin, card_pempty,
    card_ulift]

  apply Trunc.bind (truncEquivOfCardEq this)
  intro e
  apply Trunc.mk
  exact of_equiv e h_empty
| Nat.succ n => by
  have : card (Option (ULift (Fin n))) = card (ULift (Fin n.succ)) := by
    simp only [card_fin, card_option, card_ulift]
  apply Trunc.bind (truncEquivOfCardEq this)
  intro e
  apply Trunc.map _ (ind n)
  intro ih
  exact of_equiv e (h_option ih)

-- Porting note: due to instance inference issues in 'SetTheory.Cardinal.Basic'
-- I had to explicitly name 'h_fintype' in order to access it manually.
-- was '[Fintype α]'
/-- An induction principle for finite types, analogous to 'Nat.rec'. It effectively says
that every 'Fintype' is either 'Empty' or 'Option α', up to an 'Equiv'. -/
@[elab_as_elim]
theorem induction_empty_option {P : ∀ (α : Type u) [Fintype α], Prop}
  (of_equiv : ∀ (α β) [Fintype β] (e : α ≃ β), @P α (@Fintype.ofEquiv α β <_> e.symm) → @P β)
  (h_empty : P PEmpty) (h_option : ∀ (α) [Fintype α], P α → P (Option α)) (α : Type u)
  [h_fintype : Fintype α] : P α := by
  obtain ⟨p⟩ :=
    let f_empty := fun i => by convert h_empty
    let h_option : ∀ {α : Type u} [Fintype α] [DecidableEq α],
      (∀ (h : Fintype α), P α) → ∀ (h : Fintype (Option α)), P (Option α) := by
      rintro α hα - Pα hα'
      convert h_option α (Pα _)
    @truncRecEmptyOption (fun α => ∀ h, @P α h) (@fun α β e hα hβ => @of_equiv α β hβ e (hα _))
    f_empty h_option α _ (Classical.decEq α)
  exact p _
-- .

end Fintype

/-- An induction principle for finite types, analogous to 'Nat.rec'. It effectively says
that every 'Fintype' is either 'Empty' or 'Option α', up to an 'Equiv'. -/
theorem Finite.induction_empty_option {P : Type u → Prop} (of_equiv : ∀ {α β}, α ≃ β → P α → P β)
  (h_empty : P PEmpty) (h_option : ∀ {α} [Fintype α], P α → P (Option α)) (α : Type u)
  [Finite α] : P α := by
  cases nonempty_fintype α
  refine Finite.induction_empty_option ?_ ?_ ?_ α
  exacts [fun α β _ => of_equiv, h_empty, @h_option]

```

Instructions:

- Task 1: Modernizing a Recursion Principle for Finite Types

Consider the recursion principle for finite types that states: "To define a function or prove a property for all finite types, it suffices to handle the empty set case, show how to extend from a finite set to that set plus one extra element, and respect type equivalences."

This principle is implemented using induction on the cardinality of finite types. Refactor the implementation by replacing the manually defined recursive function with Lean's standard induction tactic while preserving the mathematical content. Specifically:

1. Remove the manual recursion approach that uses the 'where' syntax and explicit pattern matching.
2. Introduce the natural number parameter and apply induction directly.
3. In the inductive step, use the induction hypothesis provided by the tactic rather than making an explicit recursive call.
4. Ensure that all mathematical reasoning about cardinality equivalences remains intact.

The refactoring should modernize the code while maintaining the same mathematical structure and reasoning.

Generation Response of DeepSeek-R1:

<think>

Okay, I need to tackle this task of refactoring the recursion principle for finite types in the given Lean4 code. The main goal is to replace the manual recursion approach with Lean's standard induction tactic while preserving the mathematical content. Let me try to break this down step by step.

First, I need to understand the existing code. The 'truncRecEmptyOption' function uses a manual recursion approach with 'ind' defined using the 'where' syntax and explicit pattern matching. The comments mention that this was done to ensure computability, but the task now wants to switch to using Lean's induction tactic.

The key points from the task are:

1. Remove manual recursion ('where' syntax and explicit pattern matching).
2. Introduce a natural number parameter and apply induction directly.
3. Use the induction hypothesis provided by the tactic instead of explicit recursive calls.
4. Keep the mathematical reasoning intact, especially around cardinality equivalences.

So, looking at the 'truncRecEmptyOption' function, the manual recursion is handled by the 'ind' function inside the 'apply ind where' block. The 'ind' function is defined with 'Nat.zero' and 'Nat.succ n' cases.

To refactor this, I need to replace this manual recursion with a standard induction tactic. That means structuring the proof so that Lean's 'induction' tactic can handle the recursion based on the natural number parameter representing the cardinality.

The 'suffices' block is setting up the proof by showing that for all natural numbers 'n', the property 'P' holds for 'ULift (Fin n)'. Then, it binds the result of this to the equivalence between ' α ' and 'Fin (Fintype.card α)'.

The 'apply ind where' part is the manual recursion that needs to be replaced. Instead, I should introduce a natural number parameter (probably the cardinality) and use 'induction' on that.

In the 'Nat.zero' case, the current code uses 'truncEquivOfCardEq' to get an equivalence between 'PEmpty' and 'ULift (Fin 0)', then applies 'of_equiv' with 'h_empty'. Similarly, in the 'Nat.succ n' case, it shows the equivalence between 'Option (ULift (Fin n))' and 'ULift (Fin n.succ)' and uses 'h_option' with the induction hypothesis from 'ind n'.

So, to use the induction tactic, I'll need to structure the proof such that:

- The induction is on the natural number 'n' (cardinality).
- In the base case ('n = 0'), handle the empty set scenario.
- In the inductive step ('n.succ'), use the induction hypothesis to build the proof for 'n.succ'.

The `'induction'` tactic should provide the `induction` hypothesis automatically, so I don't need to make explicit recursive calls.

I also need to ensure that all the equivalences and mathematical reasoning about cardinality are preserved. The `'truncEquivOfCardEq'` and `'Equiv.ulift'` are crucial here for maintaining those properties.

Let me sketch out the changes:

1. Remove the `'apply ind where'` block and the `'ind'` function.
2. Introduce a natural number `parameter for induction`, likely using `'Fintype.card α '`.
3. Use `'induction'` on this natural number.
4. In each case, use the existing logic with `'truncEquivOfCardEq'` and `'Equiv.ulift'` to handle the equivalences.
5. Ensure that the `'h_empty'` and `'h_option'` cases are properly applied with the `induction` hypothesis.

Possible challenges:

- Ensuring that the `induction` hypothesis is correctly applied in the `inductive` step.
- Maintaining the correct use of `'truncEquivOfCardEq'` and `'Equiv.ulift'` when restructuring the code.
- Making sure that all the required instances and typeclass `parameters` are correctly inferred or provided.

Testing the changes would involve checking that the refactored code compiles and that the mathematical content remains unchanged. Since the task specifies preserving the mathematical `structure`, it's crucial that the equivalences and cardinality reasoning are not altered.

Another thing to note is the `'@[elab_as_elim]'` `attribute` on `'induction_empty_option'`, which suggests that `this theorem` is intended to be used as an elimination principle. The refactoring should ensure that `this attribute` is still appropriate and that the `theorem's` usability remains intact.

In summary, the main steps are:

- Replace manual recursion with `'induction'` tactic.
- Structure the proof around a natural number `parameter for induction`.
- Preserve all equivalences and cardinality reasoning.
- Ensure that the `induction` hypothesis is correctly utilized in the `inductive` step.

By carefully following these steps and checking against the original code's logic, I should be able to produce the required unified diff patch.

</think>

To address the task requirements, we'll refactor the `'truncRecEmptyOption'` function by replacing manual recursion with Lean's `induction` tactic while preserving the mathematical content. Here's the step-by-step explanation and the corresponding diff:

Step-by-Step Explanation:

1. **Introduce Natural Number Parameter:**
 - The original code manually recurses on the cardinality of the finite type. We'll instead use a natural number `parameter 'n'` and perform `induction` on it.
2. **Apply Induction Tactic:**
 - Replace the manual `'ind'` function with `'induction n'` to leverage Lean's built-in `induction` tactic. This simplifies the code and uses the `induction` hypothesis provided by the tactic.


```

3. **Base Case ('n = 0'):**
  - Handle the empty set case by using 'truncEquivOfCardEq' to establish the equivalence between
    'PEmpty' and 'ULift (Fin 0)', then apply 'h_empty' via 'of_equiv'.

4. **Inductive Step ('n + 1'):**
  - For the successor case, use 'truncEquivOfCardEq' to equate 'Option (ULift (Fin n))' with
    'ULift (Fin n.succ)'.
  - Apply the induction hypothesis 'ih' (from the 'induction' tactic) and 'h_option' to build the
    proof for 'n + 1'.

5. **Preserve Equivalences:**
  - Maintain the use of 'Equiv.ulift' and 'truncEquivOfCardEq' to ensure the cardinality
    reasoning remains intact.

6. **Cleanup and Simplification:**
  - Remove the now-unnecessary 'ind' function and associated comments.
  - Adjust variable bindings and scopes to match the new structure.

**Unified Diff Patch:**


diff --git a/Mathlib/Data/Fintype/Option.lean b/Mathlib/Data/Fintype/Option.lean
index 1234567..abcdefg 100644
--- a/Mathlib/Data/Fintype/Option.lean
+++ b/Mathlib/Data/Fintype/Option.lean
@@ -52,29 +52,23 @@ def truncRecEmptyOption {P : Type u → Sort v} (of_equiv : ∀ {α β}, α ≃
  (h_empty : P PEmpty) (h_option : ∀ {α} [Fintype α] [DecidableEq α], P α → P (Option α))
  (α : Type u) [Fintype α] [DecidableEq α] : Trunc (P α) := by
    suffices ∀ n : ℕ, Trunc (P (ULift <| Fin n)) by
      apply Trunc.bind (this (Fintype.card α))
      intro h
      apply Trunc.map _ (Fintype.truncEquivFin α)
      intro e
      exact of_equiv (Equiv.ulift.trans e.symm) h
    apply ind where
      -- Porting note: do a manual recursion, instead of 'induction' tactic,
      -- to ensure the result is computable
      /-- Internal induction hypothesis -/
      ind : ∀ n : ℕ, Trunc (P (ULift <| Fin n))
      | Nat.zero => by
        have : card PEmpty = card (ULift (Fin 0)) := by simp only [card_fin, card_pempty,
                                                                    card_ulift]
        apply Trunc.bind (truncEquivOfCardEq this)
        intro e
        apply Trunc.mk
        exact of_equiv e h_empty
      | Nat.succ n => by
        have : card (Option (ULift (Fin n))) = card (ULift (Fin n.succ)) := by
          simp only [card_fin, card_option, card_ulift]
        apply Trunc.bind (truncEquivOfCardEq this)
        intro e
        apply Trunc.map _ (ind n)
        intro ih
        exact of_equiv e (h_option ih)
+    exact Trunc.bind (this (Fintype.card α)) fun h =>
+      Trunc.map (fun e => of_equiv (Equiv.ulift.trans e.symm) h) (Fintype.truncEquivFin α)
+  intro n
+  induction n with


```

```

+ | zero =>
+   have : card PEmpty = card (ULift (Fin 0)) := by simp only [card_fin, card_pempty, card_ulift]
+   apply Trunc.bind (truncEquivOfCardEq this)
+   intro e
+   apply Trunc.mk
+   exact of_equiv e h_empty
+ | succ n ih =>
+   have : card (Option (ULift (Fin n))) = card (ULift (Fin n.succ)) := by
+     simp only [card_fin, card_option, card_ulift]
+   apply Trunc.bind (truncEquivOfCardEq this)
+   intro e
+   apply Trunc.map _ ih
+   intro ih
+   exact of_equiv e (h_option ih)

-- Porting note: due to instance inference issues in 'SetTheory.Cardinal.Basic'
-- I had to explicitly name 'h_fintype' in order to access it manually.
'''

**Explanation of the Diff:**

- **Removed Manual Recursion ('ind' function):**
  - The original code's 'apply ind where' block and manually defined 'ind' function are deleted.

- **Introduced 'induction' Tactic:**
  - The 'induction n with' block replaces manual recursion, using Lean's built-in induction.

- **Base Case ('zero'):**
  - Handles 'n = 0' by establishing equivalence between 'PEmpty' and 'ULift (Fin 0)', then applying 'h_empty'.

- **Inductive Step ('succ n ih'):**
  - Uses 'ih' (induction hypothesis) provided by the 'induction' tactic.
  - Establishes equivalence between 'Option (ULift (Fin n))' and 'ULift (Fin n.succ)'.
  - Applies 'h_option with ih' to build the step case.

- **Preserved Mathematical Content:**
  - All cardinality equivalence checks via 'truncEquivOfCardEq' and 'Equiv.ulift' remain intact.
  - The structure of the proof aligns with the original mathematical reasoning.

This refactoring modernizes the code by leveraging Lean's induction tactic, improving readability and maintainability while preserving the original mathematical structure.

```

Judgement Response of Claude Sonnet 3.7 (thinking):

<think>

Let's analyze the proposed implementation to determine if it fulfills the task requirements.
First, let's understand the original code and then evaluate the changes.

Original Code Understanding

The original code defines a recursion principle for finite types called 'truncRecEmptyOption'.

This function takes:

1. A way to transport through equivalences ('of_equiv')
2. A base case for the empty set ('h_empty')
3. An inductive step for adding one element via 'Option' ('h_option')
4. A type ' α ' with 'Fintype' and 'DecidableEq' instances

The implementation works by:

1. Reducing the problem to showing the principle for 'Fin n' types (standard finite types of size n)
2. Using a manually defined recursive function 'ind' to prove this for all natural numbers
3. For the base case (n=0), it establishes an equivalence with the empty type
4. For the inductive case, it uses the recursive hypothesis and establishes an equivalence between 'Option (Fin n)' and 'Fin (n+1)'

The manual recursion is done using the 'where' clause with explicit pattern matching on natural numbers.

Task Requirements

The task asks to modernize this recursion principle by:

1. Removing the manual recursion approach with 'where' syntax
2. Using Lean's standard induction tactic
3. Using the induction hypothesis provided by the tactic
4. Preserving all mathematical reasoning

Changes in the Proposed Implementation

Let's examine the changes:

1. **Removed manual recursion**: The implementation removed the 'ind' function defined with the 'where' clause and explicit pattern matching.
2. **Introduced induction tactic**: The implementation now uses 'induction n with' to directly perform induction on the natural number parameter.
3. **Using induction hypothesis**: Instead of making an explicit recursive call via 'ind n', the implementation now uses the induction hypothesis 'ih' provided by the tactic.
4. **Mathematical reasoning preserved**: The mathematical content about cardinality equivalences remains intact. The same logic is used in both the base case and the inductive step:
 - In the base case, we establish an equivalence between 'PEmpty' and 'ULift (Fin 0)'
 - In the inductive step, we establish an equivalence between 'Option (ULift (Fin n))' and 'ULift (Fin n.succ)'

5. **Code cleanup**: The implementation also simplifies some nested 'Trunc' operations by using more concise expressions:

```

'''lean
exact Trunc.bind (this (Fintype.card α)) fun h =>
  Trunc.map (fun e => of_equiv (Equiv.ulift.trans e.symm) h) (Fintype.truncEquivFin α)
'''

```

This replaces the more verbose:

```

'''lean
apply Trunc.bind (this (Fintype.card α))
intro h
apply Trunc.map _ (Fintype.truncEquivFin α)
intro e
exact of_equiv (Equiv.ulift.trans e.symm) h
'''

```

Overall, the changes maintain the same mathematical structure and reasoning while modernizing the approach to use Lean's built-in induction tactic rather than a manually defined recursive function.

Evaluation

Let's assess whether the implementation correctly fulfills the task requirements:

1. ****Removal of manual recursion****: The manual recursion using ‘where’ and explicit pattern matching has been removed.
2. ****Introduction of induction tactic****: The implementation now uses ‘induction n with’ to perform induction on the natural number parameter.
3. ****Use of induction hypothesis****: The implementation now uses the induction hypothesis ‘ih’ provided by the tactic rather than making an explicit recursive call.
4. ****Preservation of mathematical reasoning****: All mathematical reasoning about cardinality equivalences remains intact. The same logic is used in both the base case and the inductive step.

The implementation properly fulfills all the task requirements. The code has been modernized while maintaining the same mathematical structure and reasoning. The use of Lean’s induction tactic makes the code cleaner and more in line with modern Lean practices.

</think>

Comprehensive Analysis of Lean4 Code Patch

Task Understanding

The task requires modernizing a recursion principle for finite types by replacing a manual recursion approach with Lean’s standard induction tactic, while preserving the mathematical content. The goal is to update the code style while maintaining the same mathematical reasoning.

Original Code Analysis

The original code implements ‘truncRecEmptyOption’, a recursion principle for finite types. It uses a manual recursive function definition with ‘where’ syntax and explicit pattern matching on natural numbers:

```
““lean
apply ind where
  ind : ∀ n : ℕ, Trunc (P (ULift <| Fin n))
  | Nat.zero => ...
  | Nat.succ n => ...
““
```

This function establishes that to define a property for all finite types, it’s sufficient to:

1. Handle the empty set case
2. Show how to extend from a finite set to that set plus one element
3. Respect type equivalences

The approach works by induction on the cardinality of the finite type, using equivalences between ‘PEmpty’ and ‘Fin 0’, and between ‘Option (Fin n)’ and ‘Fin (n+1)’.

Patch Examination

The patch makes the following changes:

1. Removes the manual recursion using ‘where’ syntax and explicit pattern matching
2. Introduces direct parameter ‘n’ and applies the induction tactic with ‘induction n with’
3. Uses the induction hypothesis ‘ih’ provided by the tactic rather than making explicit recursive calls
4. Preserves all mathematical reasoning about cardinality equivalences
5. Streamlines some code by combining nested ‘Trunc’ operations into more concise expressions

For example, this verbose nested block:

```
““lean
```

```

apply Trunc.bind (this (Fintype.card  $\alpha$ ))
intro h
apply Trunc.map _ (Fintype.truncEquivFin  $\alpha$ )
intro e
exact of_equiv (Equiv.ulift.trans e.symm) h
'''

```

Is replaced with a more concise:

```

'''lean
exact Trunc.bind (this (Fintype.card  $\alpha$ )) fun h =>
  Trunc.map (fun e => of_equiv (Equiv.ulift.trans e.symm) h) (Fintype.truncEquivFin  $\alpha$ )
'''

```

Requirement Fulfillment Analysis

The implementation successfully meets all task requirements:

1. The manual recursion approach using 'where' syntax has been eliminated
2. The natural number parameter is introduced directly and induction is applied with the standard tactic
3. The inductive step uses the tactic-provided induction hypothesis ('ih') rather than an explicit recursive call
4. All mathematical reasoning about cardinality equivalences remains intact

Implementation Quality Analysis

The modernized implementation is:

- More idiomatic to contemporary Lean style by using built-in tactics
- Clearer in structure, as the induction flow is more explicit
- More maintainable, as it follows standard patterns that Lean developers will be familiar with
- Functionally equivalent to the original, preserving all mathematical content
- Slightly more concise due to streamlined expression of 'Trunc' operations

Overall Judgement

```

'''json
{
  "TaskEvaluations": {
    "Task 1": "Excellent"
  },
  "FinalOverallGrade": "Excellent"
}
'''

```