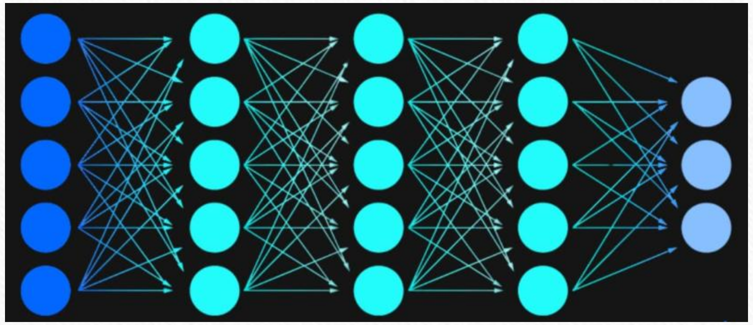
The AI Revolution in TLA+ Modeling

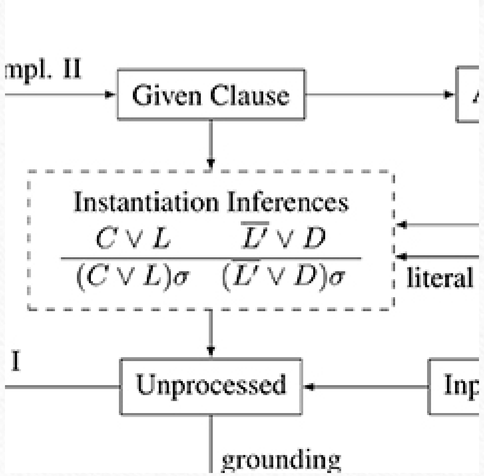
Cheng Huang

2025-11-20

Future of Software is ~~Vibe~~ Peach* Coding

- soft outside – source code generated by statistical models
- hard core – correctness guaranteed by formal methods





---

* Doug Burger (Microsoft Research)

Cost of Formal Methods Trending Zero

- Helen (from Azure Storage team) successfully wrote her first production TLA+ spec using GitHub Copilot and ChatGPT in 5 hours. Her only prior experience was watching Leslie Lamport's training videos.
  - In comparison, it took Cheng one month before he managed to write his first spec.
- Azure Storage uncovered a potential data loss bug by driving AI to derive a precise TLA+ specification from production implementation
  - Race between an old Paxos leader sending deletion and a new Paxos leader adding reference → escaped thorough design/code reviews and extensive testing

THE LAMPORT AGENT: LLM-ASSISTED FORMAL VERIFICATION

> “A PARADIGM SHIFT: TLA+ MEETS LARGE LANGUAGE MODELS.”

The integration of LLMs with TLA+ for [illegible] TLA+ for [illegible] verification, [illegible] verification as a [illegible] for integ[illegible] and [illegible] verification. [illegible] present[illegible] method.[illegible] proport[illegible] [illegible] generation perform[illegible] in [illegible] protocol [illegible] moto[illegible] optimal [illegible] is [illegible] in integrational [illegible] support its accelerated specification writing. [illegible] automated specification, [illegible] writing [illegible] to automated proof generation [illegible] of [illegible] automated proof [illegible] and [illegible] of generation, [illegible] and reduced barrier to entry. reduced blanning, and reduced barrier to entry.

accelerated specification writing, and **automated proof generation**, [illegible] the **automated proof generation**, and [illegible] integration [illegible] version of TLA+ for specification; [illegible] the [illegible] automated environment and **reduced barrier to entry**.

However [illegible] ones with [illegible] the [illegible] verification projec[illegible] proo[illegible] verification, [illegible] to [illegible] individ[illegible], using [illegible] and [illegible] specifications [illegible] experts automated proof for[illegible] [illegible] these solutions is the [illegible] comunications.

> “DEMOCRATIZING FORMAL METHODS FOR A BROADER AUDIENCE.”

The Lamport Agent workflow is to [illegible] verification [illegible] formal [illegible] the TLA+ [illegible] Lamport [illegible] System [illegible] formal [illegible] and [illegible] the [illegible] workflow.

The Lamport Agent workflow from [illegible] most interactive **interactive TLA+ Proof System (TLAPS) support.** [illegible] to the formal [illegible], iterative support [illegible] with iterative [illegible] for the [illegible] Proof System [illegible] based [illegible] the Lamport and TLA+ [illegible] of iterative refinement.

KEY BENEFITS

- Enhanced Productivity
  [illegible]
- Enhanced Productivity
  and accuracy
- Improved Accuracy
  [illegible] enhanced productivity
- Improved Accuracy
  [illegible]
- Scalable Verification
  [illegible] and Verification

Links

- Lamport Agent - AI-assisted Formal Specification | Cheng Huang's corner
- https://github.com/zfhuang99/lamport-agent

BACKUP

THE LAMPORT AGENT: LLM-ASSISTED FORMAL VERIFICATION (TLA+ ONLY)