2025: The Year Reasoning and Agents Became Real

2025 marked the moment LLMs stopped just predicting the next token and started *thinking*. Simon Willison's comprehensive review of the year identifies "reasoning" as the defining trend, driven by a technique known as Reinforcement Learning from Verifiable Rewards (RLVR). This shift has fundamentally changed how we interact with these systems, moving us from chat interfaces to asynchronous agentic workflows.

The "Reasoning" Unlock: RLVR

For a mathematician, the shift to RLVR is the most significant architectural change. By training models against automatically verifiable environments—such as math puzzles or code execution—labs like OpenAI (with o1/o3) and DeepSeek (with R1) taught models to develop problem-solving strategies. As Andrej Karpathy noted, these models learn to break down problems and "backtrack" when they hit a dead end. This isn't just about better conversation; it's about allocating compute to *inference time* rather than just pre-training. Willison points out that this capability is what finally made AI-assisted search and complex debugging reliable: the model can reason about its own errors.

The Era of Coding Agents and "YOLO Mode"

The practical application of this reasoning is the "coding agent." The release of Claude Code defined the year, moving developers away from copy-pasting code snippets to using **asynchronous agents** that run in the background. These tools can plan multi-step tasks, execute code, inspect the results, and iterate. However, Willison highlights a critical security trade-off: the "Normalization of Deviance." To make these agents useful, developers are increasingly running them in "YOLO mode" (bypassing approval prompts), granting autonomous AI systems read/write access to their local environments—a practice that feels efficient until it inevitably isn't.

Conformance Suites as Prompts

Perhaps the most exciting development for those of us who value formal rigor is the rise of **conformance suites**. Willison observed that the most effective way to drive a 2025-era agent isn't a text prompt, but a rigorous test suite. If you provide a model with a comprehensive set of tests (like the html5lib tests or a WebAssembly spec), it can iterate independently until the implementation passes. This aligns perfectly with formal verification methods: the "spec" becomes the instruction, and the agent becomes the implementation engine.

The Open Weight Geopolitics

Finally, the monopoly on intelligence fractured in 2025. Chinese labs released open-weight models (like DeepSeek V3 and Qwen 2.5) that didn't just catch up to US models—they occasionally beat them, causing temporary panic in US markets (specifically impacting NVIDIA). Alongside Google's custom TPU-driven Gemini ecosystem, this has created a diverse, highly competitive field where "state-of-the-art" changes monthly.

Contributor: Alessandro Linzi