

# NormCode: A Semi-Formal Language for Context-Isolated AI Planning

Xin Guan

PsylensAI / Center for Long-Term AI

garguan2001@outlook.com / psylensai.com

## Abstract

Multi-step workflows that chain large language model (LLM) calls suffer from *context pollution*: as information accumulates across steps, models hallucinate, confuse intermediate outputs, and lose track of task constraints. We present **NormCode**, a semi-formal language for constructing *plans of inferences*—structured decompositions where each step operates in data isolation, receiving only explicitly passed inputs. This eliminates cross-step contamination by construction. NormCode enforces a strict separation between *semantic operations* (LLM-driven reasoning, non-deterministic) and *syntactic operations* (deterministic data restructuring), enabling precise cost and reliability tracing. The language exists in three isomorphic formats: .ncds for human authoring, .ncd for machine execution, and .ncn for human verification—supporting progressive formalization from sketch to production. We validate NormCode through two demonstrations: (1) a base-X addition algorithm achieving 100% accuracy on arbitrary-length inputs, and (2) self-hosted execution of NormCode’s own five-phase compiler pipeline. The working orchestrator provides dependency-driven scheduling, SQLite-backed checkpointing, and loop management. By making AI workflows auditable by construction, NormCode addresses a critical need for transparency in high-stakes domains such as legal reasoning, medical decision-making, and financial analysis.

## 1 Introduction

Large language models have enabled AI systems that reason, plan, and act across complex multi-step workflows. Frameworks like LangChain, AutoGPT, and AutoGen demonstrate how agents can decompose problems and coordinate actions through sequences of LLM calls. However, as these workflows grow more ambitious—chaining dozens of outputs, invoking tools, branching on intermediate

results—a critical failure mode emerges: **context pollution**.

### 1.1 The Problem: Context Pollution in Multi-Step Reasoning

Context pollution occurs when accumulated information across reasoning steps causes models to hallucinate, confuse intermediate outputs with inputs, and lose track of original task constraints. Empirical studies show that LLMs “forget” earlier facts in long conversations, leading to contradictory decisions on lengthy tasks (Chang et al., 2025; Modarressi et al., 2024). The compounding error effect is severe: small mistakes in early steps propagate through sequential reasoning, making complex multi-step solutions exponentially more error-prone than simple ones (Research and Fatemi, 2025).

Even state-of-the-art models like GPT-4 struggle to maintain global consistency on complicated plans, often abandoning earlier constraints as context grows. Simply expanding context windows does not solve the problem—research shows that very long prompts can confuse models or cause them to focus on irrelevant details, actually *reducing* correctness despite larger windows (Breunig, 2025).

**Current approaches offer limited defense.** Direct prompting bundles everything into one context window, creating cognitive overload. Chain-of-Thought (CoT) prompting extends interaction step-by-step but does not isolate context between steps—hallucinated thoughts in early reasoning leak forward into later prompts. Agent frameworks like LangChain and AutoGPT provide orchestration but leave data flow implicit (Winland and Noble, 2025; Wang et al., 2024): when step 7 of a 10-step chain fails, developers cannot easily determine what step 7 actually saw. As practitioners note, debugging such agents often happens “in the dark,” requiring reverse-engineering of hidden state to find root

causes (Patel, 2025).

## 1.2 The Solution: Explicit Data Isolation by Construction

NormCode takes a fundamentally different approach: it enforces **explicit data isolation as a language-level constraint**. Rather than letting context bleed implicitly between steps, NormCode defines *plans of inferences*—structured decompositions where each step is a self-contained logical unit with access only to explicitly passed inputs. If an early step processes a raw document and later steps receive only a summarized excerpt, no subsequent inference can accidentally peek at the original—it simply is not in that step’s input by design.

This idea aligns with emerging strategies in advanced agent design. Experts advocate isolating context into separate threads or sub-agents, each handling narrow subtasks with only relevant data, rather than one monolithic agent juggling a combined context (Ruan, 2024). Recent work on execution isolation (e.g., IsolateGPT) proposes sandboxing LLM-based applications to prevent unauthorized data access (Wu et al., 2025). NormCode builds this isolation into the language itself—not as a guideline but as an enforced rule of the programming model.

**The result is full auditability.** Every intermediate state is explicit and inspectable, providing process transparency into how conclusions are reached. For high-stakes domains—legal analysis, medical reasoning, financial decision-making—this transparency is not optional (Sai, 2025). Regulators demand that AI systems provide decision traceability and justification (e.g., EU AI Act requirements for high-impact systems). NormCode produces an audit trail of reasoning that can be verified step-by-step, dramatically improving trust.

## 1.3 Contributions

This paper presents NormCode, a semi-formal language and execution framework for context-isolated AI planning. Our contributions are: (1) **A novel intermediate representation** for AI planning based on *inference decomposition* and *explicit data flow*, bridging natural language intent and machine execution while maintaining auditability; (2) **Semantic/syntactic separation**: A clean architectural distinction between LLM-driven operations (expensive, non-deterministic) and data-restructuring operations (free, determin-

istic), enabling precise cost and reliability tracing; (3) **A three-format ecosystem** (.ncds / .ncd / .ncn) supporting human authoring, machine rigor, and human verification within a single coherent pipeline—enabling progressive formalization from exploratory sketch to production system; and (4) **A working orchestrator** with dependency-driven scheduling, SQLite-backed checkpointing, and loop management, validated through (a) 100% accuracy on base-X addition tasks, and (b) self-hosted execution of NormCode’s own five-phase compiler pipeline.

The rest of this paper is organized as follows: Section 2 reviews related work in AI planning, agent frameworks, and intermediate representations. Sections 3-4 describe the NormCode language and reference system. Section 5 articulates the design philosophy. Sections 6-7 detail the execution model and compiler ecosystem. Section 8 presents case study evaluations. Section 9 discusses limitations and future work, and Section 10 concludes.

## 2 Background and Related Work

NormCode builds on three research traditions: classical AI planning, modern LLM-based agents, and intermediate representations for structured reasoning. This section positions NormCode within this landscape.

### 2.1 Classical Planning and Structured Task Decomposition

NormCode inherits its hierarchical task decomposition from classical AI planning. The seminal STRIPS system introduced representing actions with preconditions and effects for goal-directed problem solving. The Planning Domain Definition Language (PDDL) emerged as a standardized formalism for encoding planning domains—providing structured symbolic blueprints (predicates, actions, goals) that automated planners use to generate valid action sequences.

Hierarchical Task Network (HTN) planning is particularly relevant to NormCode’s design (Erol et al., 1994). HTN represents tasks in a hierarchy where high-level goals are recursively decomposed into lower-level primitive actions. This decomposition mirrors NormCode’s approach of breaking complex inferences into hierarchies of sub-inferences, each with explicit dependencies. However, while HTN planning operates in fully sym-

bolic domains with deterministic actions, NormCode extends this paradigm to handle *probabilistic reasoning* (via LLM calls) within a structured framework.

## 2.2 Modern LLM-Based Agent Frameworks

Recent agent frameworks demonstrate how LLMs can plan and act through iterative reasoning. **ReAct** (Yao et al., 2022) (Yao et al., 2022) interleaves reasoning traces with action outputs, allowing models to “think aloud” while interfacing with tools. **Reflexion** (Shinn et al., 2023) (Shinn et al., 2023) extends this with self-evaluation: after each trial, the agent generates linguistic feedback stored as episodic memory, enabling iterative self-correction without parameter updates.

Frameworks like **LangChain** and **AutoGPT** provide orchestration for multi-step LLM workflows (Winland and Noble, 2025). **LangGraph** (IBM, 2025) explicitly models agent workflows as directed graphs of nodes (decisions, tool uses, conditionals), increasing transparency over linear chains. However, these frameworks leave data flow largely implicit—the system manages prompts and memory behind the scenes, making it difficult to audit what each step actually “sees.”

**NormCode differs in enforcing explicit data isolation.** While LangGraph provides structural transparency (the graph topology is visible), NormCode provides *data-flow transparency*: every input to every step is explicitly declared. When debugging a failure at step 7, NormCode allows precise inspection of step 7’s inputs, not just its position in the workflow graph.

## 2.3 Intermediate Representations and Structured Reasoning

The concept of an intermediate representation (IR) between high-level intent and low-level execution has deep roots in computer science (contributors). In compilers, an IR (e.g., LLVM IR) abstracts away machine details, enabling optimization passes independent of source language. A good IR is accurate (captures all essential information) and modular (supports transformation without loss of meaning).

In LLM research, structured reasoning traces serve analogous purposes. **Chain-of-Thought (CoT)** prompting (Wei et al., 2022) (Wei et al., 2022) encourages models to generate step-by-step reasoning, significantly improving complex problem-solving. **Tree-of-Thought (ToT)** (Yao et al., 2023) (Yao et al., 2023) generalizes this by ex-

ploring branching paths and backtracking. **Graph-of-Thought (GoT)** (Han and Zhao, 2023) allows non-linear exploration of reasoning networks.

NormCode can be viewed as an IR for AI planning that combines these insights: it provides a structured “language of thought” that is simultaneously human-authored (like natural CoT), machine-executable (like compiled code), and inspectable (like a computation graph). Recent work on “Abstractions-of-Thought” (DeLorenzo et al., 2025) (DeLorenzo et al., 2025) and “Blueprint First” approaches (Qiu et al., 2025) uses structured IRs to separate functional decomposition from syntax in LLM-based hardware design—a similar philosophy to NormCode’s separation of reasoning structure from execution details.

Critically, NormCode’s IR supports **progressive formalization**: plans can start as rough sketches and be iteratively refined. This contrasts with traditional IRs (which demand full formalization up-front) and free-form CoT (which lacks enforceable structure).

## 2.4 Semi-Formal Languages and the Formalization Spectrum

NormCode occupies a deliberate position between natural language and formal specification. Pure natural language is expressive but ambiguous; fully formal languages (PDDL, code) are unambiguous but rigid. Semi-formal languages strike a balance, imposing structure to reduce ambiguity while remaining accessible to humans (Silva, 2025).

In requirements engineering, UML provides semi-formal diagrams that allow automated consistency checks while staying understandable to stakeholders. NormCode follows this philosophy for AI planning: the language is strict enough for reliable compilation and execution, but flexible enough that humans can author plans in near-natural language (.ncds format) and verify them as readable narratives (.ncn format).

The name “NormCode” references normative reasoning—the study of obligations, permissions, and prohibitions in deontic logic (Stanford Encyclopedia of Philosophy, 2021). While NormCode does not explicitly encode deontic modalities, the spirit of “norms” suggests rules that agents should follow. Recent work evaluates LLMs’ consistency in handling normative constraints (Sordoni et al., 2025), and NormCode’s design facilitates such evaluation by making every reasoning step explicit and auditable.

**Why semi-formal for LLMs?** Models excel at natural language but struggle with fully formal syntax—small errors break rigid parsers. A semi-formal format provides structural guidance (reducing ambiguity) without unforgiving exactness, allowing LLMs to generate valid plans more reliably. This pragmatic balance enables the progressive formalization lifecycle that NormCode supports.

### 3 The NormCode Language

NormCode is designed around a single fundamental unit: the **inference**. An inference is not merely a function call; it is a structured assertion: “Concept A is obtained by performing Operation B on Inputs C and D.” This structure enforces the data isolation required for reliable AI planning.

#### 3.1 Core Syntax: The Inference Structure

A NormCode plan is a hierarchy of inferences. We define two primary concept markers: `<=` (**Functional Concept**) defines the operation (the “verb”) and triggers an agent sequence, while `<` (**Value Concept**) defines the data (the “noun”) holding the input or output state.

A typical inference looks like this in `.ncds` (NormCode Draft Straightforward):

```
<- summary
  <= summarize the text
  <- raw document
```

This is read bottom-up: “The raw document is used to summarize the text, producing the summary.” The indentation defines the dependency: the parent (`summary`) cannot be resolved until its children (`summarize...`) are complete.

#### 3.2 The Three-Format Ecosystem

NormCode acknowledges that humans, compilers, and reviewers have different needs. The language exists in three isomorphic formats: (1) **.ncds (Draft Straightforward)**: The human authoring format using natural language with minimal structural markers (`<-`, `<=`) to prioritize speed; (2) **.ncd (Draft)**: The formal intermediate representation generated by the compiler, resolving all ambiguities (types, value orders, flow indices) for machine execution; and (3) **.ncn (Natural)**: A compiler-generated narrative translating the formal `.ncd` back into plain English (e.g., “(OUTPUT) The summary (ACTION) is obtained by...”) for verification by non-technical experts.

#### 3.3 Semantic Concept Types (The “Meaning”)

NormCode types are semantic, not just structural. They tell the agent *what* the data represents in the world.

**Entities (Non-Functional)** include: **Objects** `{}` (discrete items, e.g., `{file}`), **Propositions** `<>` (boolean states, e.g., `<file exists>`), **Relations** `[]` (collections or mappings), and **Subjects** `:S:` (active agents, e.g., `:coder_agent:`). **Operations (Functional)** include: **Imperative** `({})` (commands that change state, e.g., `::(calculate sum)`), invoking the **Imperative Sequence**) and **Judgement** `<{}>` (evaluations returning a truth value, invoking the **Judgement Sequence**).

#### 3.4 Syntactic Concept Types (The “Structure”)

While semantic concepts invoke AI reasoning, syntactic concepts manage the plan’s data flow deterministically. These include: **Assigning** (`$=`, `$..`, `$+` to select outputs or carry state); **Grouping** (`&in`, `&across` to structure multiple inputs); **Timing** (`@if`, `@if!`, `@after` to control execution order); and **Looping** (`*every` to process collections item-by-item).

#### 3.5 Plan Addressability

Every step in a NormCode plan is assigned a unique **Flow Index** (e.g., `1.2.3`) based on its indentation depth. This index serves as a permanent address for that inference, enabling **Precise Debugging** (“The error occurred at step `1.4.2`”), **Targeted Intervention** (“Pause execution before step `2.1` starts”), and **Auditing** (“Show me the inputs for step `3.2`”).

#### 3.6 Semi-Formality: Balancing Structure and Flexibility

NormCode’s “semi-formal” nature operates in two complementary ways:

**1. Conceptual Preservation (Progressive Formalization).** NormCode allows natural language content within formal structure. A user can write `::(summarize the text)` without immediately defining implementation details. The structure formalizes *how* the concept relates to others (it is an action with dependencies), while leaving *content* flexible until execution. Plans can start as rough sketches and be iteratively refined into rigorous logic—supporting exploration before commitment.

**2. Strictness Only Where Necessary.** Syntax is strict precisely to the extent required for compilation: to establish unique concept identities, resolve

data flow dependencies, and extract working interpretations (which agent sequence to invoke).

Beyond these requirements, semantic content can remain in natural language. This prevents the brittleness of traditional formal methods (where a single syntax error invalidates the entire specification) while providing sufficient structure for reliable orchestration.

## 4 The Reference System

While concepts define the *meaning* of data, the **Reference System** provides the machinery for storing and manipulating it. In NormCode, every piece of data—from a single file path to a collection of user queries—is encapsulated in a **Reference**, a structure inspired by multi-dimensional tensors.

### 4.1 References as Tensors with Named Axes

Unlike standard lists or dictionaries, a Reference organizes data along named axes (e.g., [’student’, ’assignment’] rather than [0, 1]). This allows operations to be robust to changes in data shape. A collection of documents is not just a list; it is a tensor with a document axis. If we process each document to extract three features, the result is automatically a 2D tensor with [’document’, ’feature’] axes. This explicit structure prevents the “shape mismatch” errors common in ad-hoc prompt chains.

### 4.2 Perceptual Signs: The “Lazy Evaluation” of AI

Carrying large data payloads (e.g., full text of books) through every step of a plan is inefficient and creates context pollution. NormCode solves this with **Perceptual Signs**: lightweight pointers that represent data without loading it.

A sign follows the format `%{Norm}ID(Signifier)`. For example:

```
%{file_location}a1b(data/contract.pdf)
```

This tells the agent: “There is an object here (`ID a1b`). To perceive it, use your `FileSystem` faculty (the `file_location` norm) on the path `data/contract.pdf`.” The actual data is only loaded (“transmuted”) at the exact moment an inference needs to operate on it (the **MVP** step). Until then, the system passes around the lightweight sign, ensuring efficiency.

### 4.3 Semantic vs. Syntactic Operations on References

The distinction between semantic and syntactic operations is implemented at the Reference level through a layered algebra.

#### 1. Syntactic Operations (Data Plumbing):

Operations like **Reshaping** (slice, append) and **Combining** (cross\_product, join) manipulate the *structure* of the tensor without looking at the content. They are instant, deterministic, and cost zero tokens.

#### 2. Semantic Operations (AI Reasoning):

The **Cross-Action** (`cross_action(functions_ref, values_ref)`) is the bridge between structure and meaning, applying an LLM-prepared function to values element-by-element.

By restricting LLMs to `cross_action` and handling all other data movement via syntactic operators, NormCode ensures that AI reasoning is applied only where strictly necessary.

## 5 Design Philosophy

NormCode’s design is guided by three core principles that address a fundamental tension in AI systems: the need for human oversight in processes that are increasingly automated.

### 5.1 Dual-Readability: Bridging Human and Machine

AI planning systems face a dilemma. Humans think in natural language; machines require unambiguous instructions. Most systems resolve this by forcing humans to write in a machine format (tedious, error-prone) or by letting machines interpret natural language (opaque, unauditible).

NormCode sidesteps this dilemma with **three isomorphic formats**: `.ncds`, intended for human authors and used for fast, intuitive authoring in natural language; `.ncd`, designed for the compiler or orchestrator as an unambiguous, machine-executable representation; and `.ncn`, intended for human reviewers as a readable narrative for verification before execution.

The key insight is that **these formats are not translations**—they are the same plan at different levels of explicitness. An author writes `.ncds`, the compiler enriches it to `.ncd` (adding types, bindings, flow indices), and a reviewer reads `.ncn` to verify the logic. No information is lost; no ambiguity is introduced. This allows domain experts (who

may not understand the formal syntax) to audit AI workflows before they run.

## 5.2 Progressive Formalization: From Sketch to Structure

Traditional formal methods demand rigor upfront: you must specify everything before you can execute anything. This is impractical for AI workflows, where the “right” structure often emerges through experimentation.

NormCode supports **Progressive Formalization**—a lifecycle where plans start loose and tighten over time: (1) **Exploration Phase**: Write a rough .ncds sketch with vague concepts; (2) **Refinement Phase**: Run the plan, observe failures, and tighten inferences; (3) **Production Phase**: The plan is rigorous, auditable, and reliable.

This lifecycle is enabled by the semi-formal nature of NormCode (Section 3.6): the formalism only demands what the compiler needs. Everything else can remain flexible until you choose to lock it down.

**Intervenability** is a key feature. Because every step has a unique flow index, a user (or an automated system) can pause execution, inspect inputs, modify a concept’s reference, or fork a run to explore alternative branches.

## 5.3 Semantic vs. Syntactic Separation: Cost and Reliability Tracing

Perhaps the most practically important design decision in NormCode is the clean separation between operations that invoke AI reasoning and operations that simply move data around.

In a typical NormCode plan, the majority of steps are syntactic. They collect inputs, select outputs, iterate over collections, and branch on conditions—all without any AI involvement. Only the “thinking” steps (imperatives and judgements) invoke an LLM.

This separation provides **Cost Visibility** (exact tracking of token usage), **Reliability Mapping** (localizing failures to probabilistic steps), and **Auditability** (generating reports on which steps invoked AI versus deterministic routing).

For high-stakes domains (legal, medical, financial), this transparency is often a regulatory requirement. NormCode makes it structural rather than aspirational.

## 5.4 When to Use NormCode

NormCode adds structure, and structure has costs. The framework is not appropriate for every use case:

**The sweet spot:** Complex, multi-step workflows where you need to know exactly what happened at each step—and where a failure in step 7 should not corrupt the reasoning in step 12.

## 6 The Execution Model

While the NormCode language defines *what* a plan should do, the execution model defines *how* and *when* it happens. This section describes the Orchestrator (the central execution engine), Agent Sequences (execution pipelines for each inference type), and Paradigms (declarative configuration of agent behavior).

### 6.1 The Orchestrator

The Orchestrator is the runtime engine of NormCode. It manages the execution of a plan by tracking dependencies, scheduling inferences, and maintaining state.

**Core Components:** (1) **Waitlist**: A prioritized queue of all inferences in the plan, sorted by flow index, defining the *structural order*; (2) **Blackboard**: A real-time state tracker where every concept/inference has a status (pending, in\_progress, completed, skipped); and (3) **Repositories**: The Concept and Inference Repositories storing data and configuration.

**Execution Cycle:** The Orchestrator runs in cycles. In each cycle, it **scans** the Waitlist for pending inferences whose dependencies are met, **executes** the inference by invoking the appropriate Agent Sequence, and **updates** the Blackboard and Concept Repository with the result.

This **dependency-driven scheduling** ensures that inferences run only when their inputs are ready, and that failures in one branch do not corrupt unrelated branches.

### 6.2 Persistence and Checkpointing

For long-running or resumable workflows, the Orchestrator provides a robust checkpointing system backed by SQLite. Features include: **Run ID** for tracking; **Snapshots** of the full state at each cycle; **Resume** capability with reconciliation modes (PATCH, OVERWRITE, FILL\_GAPS); and **Fork** functionality to branch from a past state.

### 6.3 Agents and the AgentFrame

In NormCode, an **Agent** is not just an abstract actor—it is a concrete container of capability, represented by the **Subject Concept** (`:S:`). When a functional concept executes, it does so *within* an Agent’s context.

The **AgentFrame** class realizes this in the implementation, containing the `**Body**` (the agent’s “toolbox”), `**Sequences**` (pipelines the agent can run), and `**Mode**` (interpretation style). This design enables **multi-agent planning**: different Subjects can have different tool bodies and capabilities.

### 6.4 Agent Sequences: The Execution Pipelines

Each inference type triggers a specific **Agent Sequence**—a standardized pipeline of steps.

#### Semantic Sequences (LLM-Invoking):

The key steps are: `**MFP` (Model Function Perception) resolves the “vertical” input; `**MVP` (Memory Value Perception) prepares “horizontal” inputs; and `**TVA` (Tool Value Actuation) applies the function to values (invoking the LLM).

#### Syntactic Sequences (Deterministic):

These sequences manipulate Reference structures without any AI involvement. They are instant, free, and 100% deterministic.

### 6.5 Paradigms: Configuring Agent Behavior

A **Paradigm** is a declarative JSON specification that configures *how* an agent executes a semantic inference. It bridges the gap between abstract intent (“summarize this document”) and concrete execution (which prompt template, which LLM, which output format).

**The Vertical/Horizontal Split:** Paradigms separate configuration into: (1) **Vertical Steps** (Construction-Time), handled during MFP to resolve tool affordances; and (2) **Horizontal Steps** (Runtime), handled during TVA to pass data values through the function.

#### Mathematical Formalization:

Let  $\mathcal{S}$  be the Agent’s state,  $V_{spec}$  be the vertical specification (paradigm), and  $H_{plan}$  be the horizontal plan. Let  $\mathcal{V}$  be the runtime values.

$$\mathcal{O} = [F_C(F_V(\mathcal{S}, V_{spec}), H_{plan})](\mathcal{V}) \quad (1)$$

Where  $F_V$  is the vertical function (MFP phase) producing tool handles  $\mathcal{T}$ ,  $F_C$  is the composition function compiling  $\mathcal{T}$  and  $H_{plan}$  into function  $\Phi$ ,

and  $\Phi(\mathcal{V})$  is the horizontal execution (TVA phase) producing output  $\mathcal{O}$ .

This clean separation allows paradigms to be reused across different inferences and agents.

### 6.6 Tooling

NormCode provides two primary interfaces for running and monitoring orchestrations: a **CLI** (`cli_orchestrator.py`) supporting ‘run’, ‘resume’, ‘fork’, and ‘list-runs’; and a **Streamlit App** for visualizing the plan hierarchy and real-time status.

## 7 The Compiler Ecosystem

The NormCode compiler transforms human-authored plans into executable artifacts through a multi-stage pipeline. Each stage progressively adds rigor while preserving opportunities for human review.

### 7.1 The Five-Phase Pipeline (Abstract)

The current implementation follows a five-phase pipeline that transforms a natural language instruction into an executable NormCode plan. Notably, **this pipeline is itself implemented as a NormCode plan**—a form of self-hosting that validates the framework’s expressive power.

Each phase includes an opportunity for **manual review**, enabling human intervention before the next stage proceeds. This supports the Progressive Formalization philosophy: the plan tightens incrementally, not all at once.

### 7.2 Deconstruction: Natural Language to Structure

The deconstruction phase is the most LLM-intensive. It uses a recursive decomposition algorithm: (1) **Initialize**: Wrap the entire instruction as a top-level concept; (2) **Loop**: Identify undecomposed concepts, formulate questions, classify types, construct concepts, and distribute source text; and (3) **Terminate**: When no annotations remain.

This process is guided by a taxonomy of question types that map to specific NormCode operators (e.g., “Methodology Declaration” → `@by`, “Conditional Dependency” → `@if`).

### 7.3 Formalization: Adding Rigor

Once the structure is established, formalization adds precision: **Serialization** reframes steps as

Sequence	Steps	Purpose
imperative judgement	IWI → IR → MFP → MVP → TVA → OR → OWI IWI → IR → MFP → MVP → TVA → TIA → OR → OWI	Execute commands/actions Evaluate conditions

Table 1: Semantic Agent Sequences (LLM-invoking).

Sequence	Key Step	Purpose
assigning	AR	Select/specify values
grouping	GR	Collect inputs
timing	T	Check conditions
looping	LR	Iterate over collections

Table 2: Syntactic Agent Sequences (Deterministic).

output-effect relationships; **Redirection** links abstract references to concrete implementations; and **Flow Index Generation** assigns unique addresses. The result is a .ncd file with explicit inputs, outputs, and identity.

#### 7.4 Activation Compilation: .ncd → JSON Repositories

The final compilation stage transforms the formalized .ncd into executable JSON repositories: the **Concept Repository** (fields: ‘concept\_name’, ‘type’, ‘reference\_data’, ‘reference\_axis\_names’) and the **Inference Repository** (fields: ‘flow\_index’, ‘inference\_sequence’, and the critical ‘working\_interpretation’ encoding implicit syntax).

#### 7.5 Translation: .ncd → .ncn

For human verification, the system can generate a **Natural Language NormCode** (.ncn) file. This strips the formal markers and presents the plan as readable prose:

##### .ncd input:

```
<- {Phase 1: Confirmation of Instruction}
  <= &across
  <- {step 1.1: Automated Instruction Distillation}
  <- {step 1.2: Automated Context Registration}
```

##### .ncn output:

```
The first phase is Confirmation of Instruction.
<= This phase is specified as a series of steps.
  <- The first step is Instruction Distillation.
  <- The second step is Context Registration.
```

This enables domain experts (who may not understand the formal syntax) to verify the plan’s logic before execution.

#### 7.6 Current Status and Limitations

The compiler ecosystem is functional but still maturing: it is **Working** (validated on the self-hosted pipeline), **In Progress** (optimizing NL deconstruction prompts), and targeting **Future Work** in automated prompt generation and robust error recovery.

### 8 Evaluation

We validate NormCode through two complementary demonstrations: a **self-hosted compiler pipeline** (demonstrating expressive completeness) and a **base-X addition algorithm** (demonstrating correctness and debuggability).

#### 8.1 Case Study 1: The Self-Hosted Derivation Pipeline

The most significant validation of NormCode is that **its own compiler pipeline is implemented as a NormCode plan**.

The task was to transform a high-level natural language instruction into an executable NormCode plan. The plan used a five-phase, ~50-inference NormCode structure. The orchestrator successfully executed this plan, producing the JSON repositories and runner scripts.

This self-hosting demonstrates: (1) **Expressive Completeness** (handling loops, conditionals, human-in-the-loop); (2) **Practical Viability** of the orchestrator/checkpointing system; and (3) **Recursive Validation** (testing NormCode by running its own pipeline).

#### 8.2 Case Study 2: Base-X Addition (Correctness Validation)

To validate correctness, we implemented a base-X addition algorithm.

The task was adding two arbitrary-base numbers digit-by-digit. The NormCode plan decomposed into ~25 inferences organized around three nested loops (outer loop over number pairs, inner loops for unit-place extraction and appending). The Concept Repository covered 50+ ground and intermediate concepts. Key mechanisms demonstrated in-

Phase	Input	Output	Purpose
<b>1. Confirmation</b>	Raw prompt	Instruction Block + Context Manifest	Distill intent; register context
<b>2. Deconstruction</b>	Instruction Block	.ncd Draft + .ncn Translation	Parse into hierarchical inferences
<b>3. Formalization</b>	.ncd Draft	Serialized + Redirected .ncd	Add flow indices, explicit data flow
<b>4. Contextualization</b>	Formalized .ncd + Context	Prompt files + Context Manifest	Distribute context to each step
<b>5. Materialization</b>	Final .ncd + Context	JSON Repos + Runner Script	Generate executable artifacts

Table 3: The Five-Phase NormCode Compiler Pipeline.

Dimension	Observation
<b>Debuggability</b>	Flow indices enable precise localization of failures (e.g., “Step 1.3.2 failed because input X was empty”).
<b>Token Efficiency</b>	Perceptual signs reduce token cost by passing pointers instead of full data. Syntactic operations are free.
<b>Resumability</b>	Checkpointing allows runs to be paused and resumed, or forked for experimentation.
<b>Auditability</b>	Every inference’s inputs and outputs are logged, enabling post-hoc analysis of AI decisions.

Table 4: Qualitative observations from case studies.

### clude Loop Quantification, Conditional Branching, Grouping, and Timing Dependencies.

**The Result:** The orchestrator achieves \*\*100% accuracy\*\* on the addition task across test suites of varying digit lengths.

Because NormCode ultimately generates code (via paradigms), the final output is deterministic. NormCode structures the *derivation* of that code. Full repository files are in **Appendix A**.

### 8.3 Quantitative Observations

Formal experiments are pending, but qualitative observations include:

Comparative evaluation against direct prompting and other frameworks (LangChain, etc.) is planned for future work.

## 9 Discussion

### 9.1 When to Use NormCode

NormCode is designed for scenarios where explicit auditability and data isolation justify the overhead. \*\*Strong fit\*\* scenarios include: high-stakes decisions (traceability required), complex multi-step reasoning (debugging needed), long-running workflows (checkpointing), and human-AI collaboration. \*\*Poor fit\*\* scenarios include: simple Q&A (direct prompting suffices), rapid prototyping (overhead costs), and real-time applications (latency).

The “sweet spot” is workflows where reliability and transparency outweigh the cost of explicit structure.

### 9.2 Limitations and Tradeoffs

**Syntax density.** The .ncd format’s markers (<=, <-, <\${{...}}%>) create visual clutter. While the .ncds format mitigates this for authoring, debugging compiled plans requires parsing dense notation. IDE support (syntax highlighting, structure visualization) would significantly improve usability.

**Verbosity.** Simple operations expand to multiple lines. A three-step workflow that could be a 10-line Python script becomes a 30-line NormCode plan. This verbosity is the price of explicit data flow—but for complex workflows, the marginal cost decreases (a 20-step workflow is not 10× more verbose).

**Brittleness of manual editing.** The .ncd format is indentation-sensitive and tightly coupled to flow indices. Manual edits risk breaking dependencies. The compiler should be the primary way to modify plans, but this creates a barrier for quick fixes.

**Tooling dependency.** NormCode requires the

orchestrator, compiler, and reference system. This “batteries included” approach limits portability compared to plain Python or LangChain. However, the integrated toolchain is necessary for the guarantees NormCode provides.

**Compiler maturity.** The  $\text{NL} \rightarrow .\text{ncd}$  deconstruction phase relies on carefully designed prompts and is sensitive to instruction complexity. Robust error recovery and automated prompt generation remain open challenges.

### 9.3 Broader Implications

NormCode demonstrates that **structured intermediate representations can bridge human intuition and machine rigor in AI workflows**. The three-format ecosystem (author, execute, verify) suggests a general pattern for transparent AI systems: provide multiple views of the same underlying logic, each optimized for a different stakeholder.

The semantic/syntactic separation has implications beyond NormCode. As LLM-based systems move into production, operators will need precise cost attribution (“which steps burned tokens?”) and reliability mapping (“which failures were probabilistic vs. deterministic?”). NormCode’s architectural separation makes these questions answerable by construction.

## 10 Future Work

**Compiler robustness.** The  $\text{NL} \rightarrow .\text{ncd}$  deconstruction phase remains the most fragile component. Future work should explore fine-tuned models for NormCode generation, iterative refinement loops, and hybrid human-AI sketching.

**Tooling and IDE support.** NormCode would benefit from syntax-aware editors, visual debuggers showing data flow, and “time-travel” debugging using checkpoints.

**Multi-agent planning.** The current implementation supports multiple Subjects (`:S:`) with different tool bodies, but real multi-agent coordination (negotiation, delegation, conflict resolution) remains unexplored. NormCode’s isolation guarantees could enable safe agent-to-agent communication.

**Domain-specific extensions.** High-stakes domains may require specialized semantic types (e.g., `{legal precedent}`), domain-specific verification rules (e.g., “all medical diagnoses must cite evidence”), and compliance reporting.

**Empirical evaluation.** Comparative studies against baseline approaches (direct prompting, LangChain, AutoGPT) on benchmarks like HumanEval or GAIA would quantify NormCode’s cost-accuracy tradeoffs. User studies with domain experts would assess the pragmatic value of the three-format ecosystem.

## 11 Conclusion

As large language models enable increasingly sophisticated multi-step reasoning, the problem of context pollution threatens to undermine their reliability. When information accumulates implicitly across reasoning steps, models hallucinate, confuse intermediate outputs, and lose track of constraints—making complex workflows paradoxically more brittle than simple ones.

NormCode addresses this through **enforced data isolation**: each inference operates in a sealed environment with only explicitly passed inputs. This is not a convention but a language-level constraint. Combined with a clean semantic/syntactic separation (probabilistic reasoning vs. deterministic data flow), NormCode makes AI workflows auditable by construction.

The three-format ecosystem (`.ncds` for authoring, `.ncd` for execution, `.ncn` for verification) embodies a broader principle: transparent AI systems should provide multiple views of the same underlying logic, each optimized for different stakeholders. Domain experts can verify plans in natural language; machines execute with formal rigor; auditors trace decisions with precision.

We validate the approach through self-hosted execution (NormCode’s compiler runs as a NormCode plan) and algorithmic correctness (100% accuracy on base-X addition). These demonstrations confirm that structured intermediate representations can bridge human intuition and machine execution without sacrificing either.

NormCode is not appropriate for every use case—simple tasks don’t justify the overhead. But for high-stakes domains where failures have consequences (legal, medical, financial), the ability to answer “What did step 7 actually see?” is not optional. By making context isolation structural rather than aspirational, NormCode provides a foundation for AI systems that are reliable, transparent, and auditable—requirements that will only intensify as LLMs move into production.

## References

- D. Breunig. 2025. How long contexts fail. dbreunig.com Blog. Accessed: 2025.
- E. Chang et al. 2025. SagaLLM: Context management, validation, and transaction guarantees for multi-agent LLM planning. Technical report, Stanford University.
- Wikipedia contributors. Intermediate representation. Wikipedia. Accessed: 2025.
- M. DeLorenzo et al. 2025. Abstractions-of-thought: Intermediate representations for LLM reasoning in hardware design. *arXiv preprint arXiv:2505.15873*.
- K. Erol, J. Hender, and D. S. Nau. 1994. HTN planning: Complexity and expressivity. In *Proceedings of the 12th National Conference on Artificial Intelligence (AAAI-94)*, pages 1123–1128.
- X. Han and D. Zhao. 2023. Beyond chain-of-thought: Effective graph-of-thought reasoning in language models. *arXiv preprint arXiv:2305.16582*.
- IBM. 2025. What is LangGraph? IBM Think. Retrieved December 2025.
- A. Modarressi, G. Xiao, et al. 2024. SagaLLM reference. Cited in Chang (2025).
- M. Patel. 2025. Why LangChain fails in production: 7 hidden problems. LinkedIn post. Accessed: 2025.
- L. Qiu et al. 2025. Blueprint first, model second: A framework for deterministic LLM workflow. *arXiv preprint arXiv:2508.02721*.
- Wand AI Research and M. Fatemi. 2025. Compounding error effect in large language models: A growing challenge. Wand AI Blog. Accessed: 2025.
- J. Ruan. 2024. Context engineering in LLM-based agents. Medium. Accessed: 2025.
- P. Sai. 2025. Evaluating AI transparency: What do users really need to understand? AI/UI Medium Publication. Accessed: 2025.
- N. Shinn, A. Labash, E. Liu, B. Prystawski, C. H. Park, and C. Raffel. 2023. Reflexion: Language agents with verbal reinforcement learning. *arXiv preprint arXiv:2303.11366*.
- A. R. Silva. 2025. A sea of description languages. In *Software Engineering Companion: Requirements Engineering*. Accessed: 2025.
- A. Sordoni, J. Proulx, M. Gupta, J. Maillard, and J. Pineau. 2025. Are language models deontologically aligned? In *ACL 2025*.
- Stanford Encyclopedia of Philosophy. 2021. Deontic logic. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*, fall 2021 edition.
- P. Wang et al. 2024. AutoGen: Enabling next-gen LLM applications via multi-agent conversation. In *COLING 2024*.
- J. Wei, X. Wang, D. Schuurmans, M. Bosma, B. Ichter, F. Xia, others, and Q. Le. 2022. Chain-of-thought prompting elicits reasoning in large language models. In *ICLR 2023*.
- V. Winland and J. Noble. 2025. What is LLM orchestration? IBM Think Blog. Accessed: 2025.
- Y. Wu et al. 2025. IsolateGPT: An execution isolation architecture for LLM-based agentic systems. In *NDSS Symposium 2025*.
- S. Yao, J. Zhao, D. Yu, K. Narasimhan, D. Zhao, and Y. Cao. 2022. ReAct: Synergizing reasoning and acting in language models. *arXiv preprint arXiv:2210.03629*.
- S. Yao, J. Zhao, D. Yu, K. Narasimhan, D. Zhao, and Y. Cao. 2023. Tree of thoughts: Deliberate problem solving with large language models. *arXiv preprint arXiv:2305.10601*.

## A Appendix A: Base-X Addition Repository

This appendix provides the complete NormCode repository for the base-X addition case study described in Section 8.2.

### A.1 Input Specification

The input to the addition plan is a simple JSON structure:

```
{  
  "{number pair}": {  
    "data": [["%(123)", "%(98)"]],  
    "axes": ["number pair", "number"]  
  }  
}
```

The %() syntax wraps raw values as perceptual signs, deferring their interpretation until needed.

### A.2 NormCode Plan (.ncds Format)

The human-readable plan structure (formal syntax):

#### A.2.1 Natural Language Translation (.ncn Format)

For verification by domain experts, the same plan translates to:

```
[1] (OUTPUT) The new number pair  
  (ACTION) is obtained by iterating through every number pair in the collection.  
  (MECHANISM) Each iteration carries forward the current carry-over number.  
  
[1.1] (OUTPUT) The result of each iteration  
  (ACTION) is assigned from the remainder.  
  
[1.1.2] (OUTPUT) The digit sum  
  (ACTION) is computed by summing the unit place values of all numbers  
    together with the current carry-over number.  
  (INPUT 1) All unit place values of the numbers in the current pair.  
  (INPUT 2) The current carry-over number (initially 0).  
  (YIELDS) The sum.  
  
[1.1.2.4] (OUTPUT) All unit place values of numbers  
  (ACTION) is collected by grouping across the current number pair.  
  
[1.1.2.4.2] (OUTPUT) Each unit place value  
  (ACTION) is obtained by iterating through each number in the current pair.  
  
[1.1.2.4.2.1] (OUTPUT) The loop result  
  (ACTION) is assigned from the single unit place value.  
  
[1.1.2.4.2.1.2] (OUTPUT) The single unit place value  
  (ACTION) is extracted by getting the unit place digit of the number.  
  (INPUT) The current number from the pair.  
  (YIELDS) The extracted digit.  
  
[1.1.3] (OUTPUT) The number pair collection  
  (ACTION) is updated by appending a new number pair.  
  (CONDITION) This append happens ONLY IF NOT all numbers are zero,  
    AND IF the carry-over number is zero.  
  
[1.1.3.2] (OUTPUT) The number pair to append  
  (ACTION) is constructed by iterating through each number in the current pair.  
  
[1.1.3.2.1] (OUTPUT) The loop result  
  (ACTION) is assigned from the number with last digit removed.  
  
[1.1.3.2.1.2] (OUTPUT) The number with last digit removed  
  (ACTION) is computed by: if the number is less than 10, output 0;  
    otherwise, remove the unit place digit.  
  (INPUT) The current number.
```

(YIELDS) The shifted number.

[1.1.3.3] (OUTPUT) The proposition "all numbers are 0"  
(ACTION) is evaluated by checking if each number in the pair to append is 0.  
(TIMING) This check occurs after the number pair to append is ready.  
(CONDITION) True if ALL numbers satisfy: the number is 0.

[1.1.3.4] (OUTPUT) The proposition "carry-over number is 0"  
(ACTION) is evaluated by checking if the carry-over number is 0.  
(TIMING) This check occurs after the number pair to append is ready.

[1.1.3.4.2] (OUTPUT) The updated carry-over number  
(ACTION) is computed from the previous carry-over and new quotient.

[1.1.3.4.2.2] (OUTPUT) The new carry-over value  
(ACTION) is found by computing the quotient of the digit sum divided by 10.  
(TIMING) This occurs after the digit sum is available.  
(INPUT) The digit sum.  
(YIELDS) The quotient (new carry).

[1.1.4] (OUTPUT) The remainder  
(ACTION) is computed by getting the remainder of the digit sum divided by 10.  
(TIMING) This occurs after the digit sum is available.  
(INPUT) The digit sum.  
(YIELDS) The remainder (the digit to output).

(INPUT) The initial number pair collection.

### Reading Guide:

- **(OUTPUT)** = What this step produces
- **(ACTION)** = How it's produced
- **(INPUT)** = What data flows in
- **(YIELDS)** = The specific result extracted
- **(TIMING)** = Dependency on prior steps
- **(CONDITION)** = When the action is executed
- **[X.Y.Z]** = Flow index (unique address for debugging)

### A.2.2 Formal Syntax (.ncd Format)

```
{new number pair} | 1. quantifying
  <= *every({number pair})%:[{number pair}]@(1)^[{carry-over number}<*1}] | 1.1. assigning
    <= ${.{remainder}}
```

  

```
<- {digit sum} | 1.1.2. imperative
<= ::(sum {1}<$([all {unit place value} of numbers])%_> and {2}<$({carry-over number}*1)%_> to get {3}?<$({sum})%_>
  <- {sum}?<:{3}>
  <- {carry-over number}*1<:{2}>
  <- [all {unit place value} of numbers]<:{1}> | 1.1.2.4. grouping
    <= &across({unit place value}:{number pair}*1)
    <- {unit place value} | 1.1.2.4.2. quantifying
      <= *every({number pair}*1)%:[{number}]@{(2)} | 1.1.2.4.2.1. assigning
        <= ${.{single unit place value}}
        <- {single unit place value} | 1.1.2.4.2.1.2. imperative
          <= ::(get {2})?<$({unit place value})%_> of {1}<$({number})%_>
          <- {unit place digit}?<:{2}>
          <- {number pair}*1*2
        <- {number pair}*1
```

  

```
<- {number pair}<${={1}}> | 1.1.3. assigning
  <= ${+({number pair to append}:{number pair})%:[{number pair}]} | 1.1.3.1. timing
    <= @if!(<all number is 0>) | 1.1.3.1.1. timing
      <= @if(<carry-over number is 0>)
```

```

<- {number pair to append}<${1}> | 1.1.3.2. quantifying
  <= *every({number pair}*1)%:[{number}]@(3) | 1.1.3.2.1. assigning
    <= ${.({number with last digit removed})}
      <- {number with last digit removed} | 1.1.3.2.1.2. imperative
        <= ::(output 0 if {1}<${{number}}%_> is less than 10, otherwise remove {2}?<${{unit place digit}}%_> from
          <- {unit place digit}?<:{2}>
          <- {number pair}*1*3<:{1}>
        <- {number pair}*1

<- <all number is 0> | 1.1.3.3. judgement
  <= :%{True}:<{1}<${{number}}%_> is 0> | 1.1.3.3.1. timing
    <= @after({number pair to append}<${1}>)
  <- {number pair to append}<${1}><:{1}>

<- <carry-over number is 0> | 1.1.3.4. judgement
  <= :%{True}:<{1}<${{carry-over number}}%_> is 0> | 1.1.3.4.1. timing
    <= @after({number pair to append}<${1}>)
  <- {carry-over number}*1 | 1.1.3.4.2. grouping
    <= &across({carry-over number}*1:{carry-over number}*1<--!_>)
  <- {carry-over number}*1 | 1.1.3.4.2.2. imperative
    <= ::(find the {1}?<${{quotient}}%_> of {2}<${{digit sum}}%_> divided by 10) | 1.1.3.4.2.2.1. timing
      <= @after({digit sum})
    <- {quotient}?<:{1}>
    <- {digit sum}<:{2}>

<- {remainder} | 1.1.4. imperative
  <= ::(get the {1}?<${{remainder}}%_> of {2}<${{digit sum}}%_> divided by 10) | 1.1.4.1. timing
    <= @after({digit sum})
  <- {remainder}?<:{1}>
  <- {digit sum}<:{2}>

<- {number pair}<${1}>

```

### A.3 Concept Repository (Selected Entries)

The concept repository defines 50+ concepts. Representative examples:

**Ground Concepts** (with pre-populated references):

Concept Name	Type	Reference Data
{number pair}	{}	[["%(123)", "%(98)"]]
{carry-over number}*1	{}	["%(0)"]
{unit place digit}?<:{1}>	{}	"1 digit counting from the right"

Table 5: Selected Ground Concepts.

**Functional Concepts** (operations):

Concept Name	Type	Description
*every({number pair})...<:{1}>	*every	Outer loop with carry state
&across({unit place})...<:{1}>	&across	Group digits across numbers
::(sum {1})...<:{1}>	::({})	Imperative: digit summation
:%{True}:<:{1}>	<{ }>	Judgement: check if zero

Table 6: Selected Functional Concepts.

### A.4 Inference Repository (Selected Entries)

The inference repository contains 23 inference entries. Key examples:

**Outer Loop (flow\_index: 1):**

```
{
  "inference_sequence": "quantifying",
  "concept_to_infer": "{new number pair}",
  "function_concept": "*every({number pair})%:[{number pair}]@(1)^[{carry-over number}<*1>]",
  "value_concepts": ["{number pair}"],
  "context_concepts": ["{number pair}*1", "{carry-over number}*1"],
  "working_interpretation": {
    "syntax": {
      "marker": "every",
      "quantifier_index": 1,
      "LoopBaseConcept": "{number pair}",
      "CurrentLoopBaseConcept": "{number pair}*1",
      "group_base": "number pair",
      "InLoopConcept": "{$carry-over number}*1": 1},
      "ConceptToInfer": ["{new number pair}"]
    }
  }
}
```

#### **Digit Summation (flow\_index: 1.1.2):**

```
{
  "inference_sequence": "imperative_python",
  "concept_to_infer": "{digit sum}",
  "function_concept": "::(sum {1}<...> and {2}<...> to get {3}?<...>)",
  "value_concepts": "[[all {unit place value} of numbers]", "{$carry-over number}*1", "{$sum}?"],
  "working_interpretation": {
    "is_relation_output": false,
    "with_thinking": true,
    "value_order": {
      "[all {unit place value} of numbers]": 1,
      "{$carry-over number}*1": 2,
      "{$sum}?": 3
    }
  }
}
```

#### **Conditional Termination (flow\_index: 1.1.3.1.1):**

```
{
  "inference_sequence": "timing",
  "concept_to_infer": "@if!(<all number is 0>)",
  "function_concept": "@if(<carry-over number is 0>)",
  "working_interpretation": {
    "syntax": {
      "marker": "if",
      "condition": "<carry-over number is 0>"
    }
  }
}
```