Agent / Agentic AI

Fujiao Ji | Advisor: Dr. Doowon Kim

Based on Andrew Ng's Agentic AI, DeepLearning.AI course

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Overview

1. Agentic Workflows
2. Reflection
3. Tool Use
4. Planning
5. Skills
6. Evals + Error Analysis

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Overview

1. Agentic Workflows
2. Reflection
3. Tool Use
4. Planning
5. Skills
6. Evals + Error Analysis

THE UNIVERSITY OF TENNESSEE KNOXVILLE

What Are Agentic Workflows?

LLM-powered systems that execute multi-step workflows

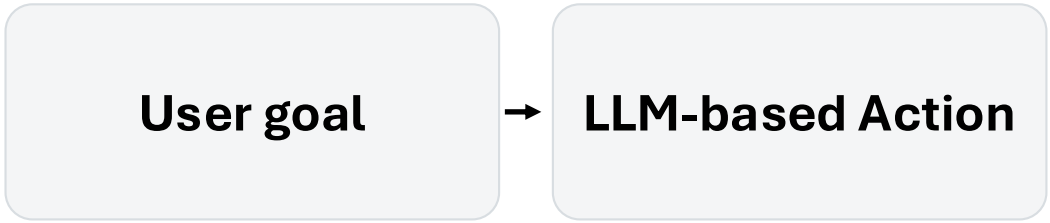
What Are Agentic Workflows?

LLM-powered systems that execute multi-step workflows

User goal

What Are Agentic Workflows?

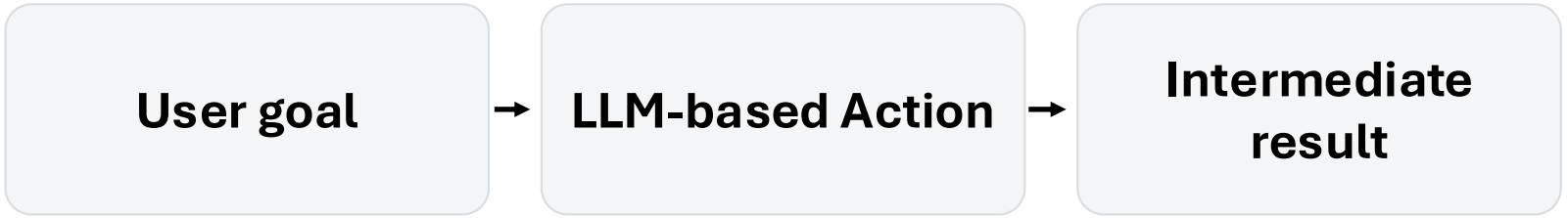
LLM-powered systems that execute multi-step workflows



THE UNIVERSITY OF TENNESSEE KNOXVILLE

What Are Agentic Workflows?

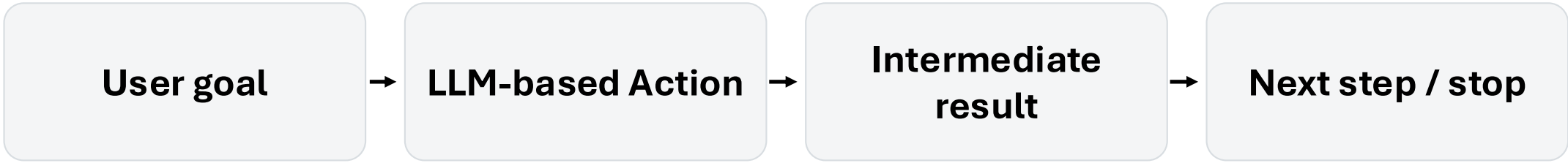
LLM-powered systems that execute multi-step workflows



THE UNIVERSITY OF TENNESSEE KNOXVILLE

What Are Agentic Workflows?

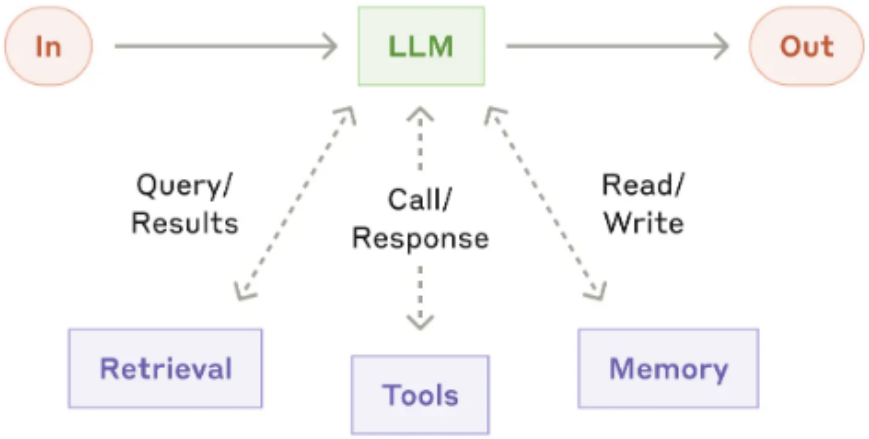
LLM-powered systems that execute multi-step workflows



THE UNIVERSITY OF TENNESSEE KNOXVILLE

Single LLM Call vs. Agentic Workflows

Traditional: Prompt → LLM → Answer



Agentic: Multi-step workflow



Repeat until a stopping condition is satisfied

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Degrees of Autonomy

Fixed workflow

All steps and tools are predetermined.

LOW

Semi-autonomous

LLM selects among available actions.

MEDIUM

Highly autonomous

LLM makes many decisions; may develop new actions.

HIGH



More autonomous decision-making

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Example: Responding to customer email

From: Fujiao Ji
Subject: Wrong item shipped

I ordered a blue Mini13 Instax (Order #8847) but received a red one instead.

I need the item for my friend birthday party this weekend. Can you help?

Fujiao

THE UNIVERSITY OF TENNESSEE KNOXVILLE

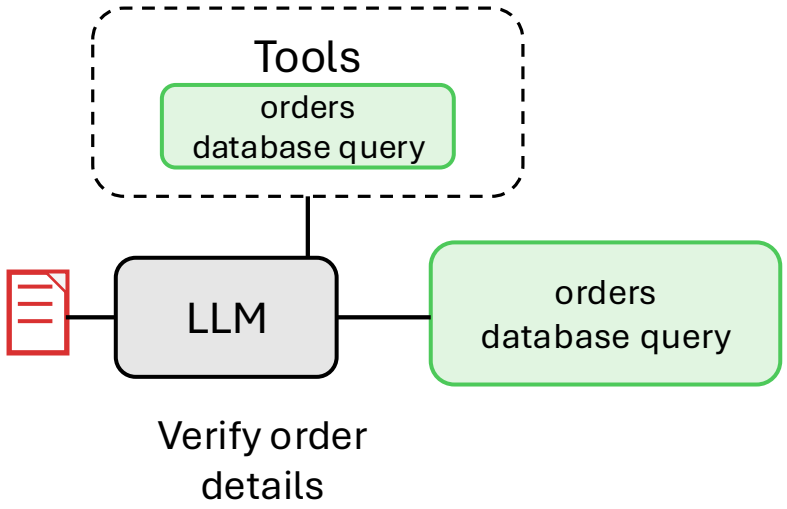
Example: Responding to customer email

From: Fujiao Ji
Subject: Wrong item shipped

I ordered a blue Mini13 Instax (Order #8847) but received a red one instead.

I need the item for my friend birthday party this weekend. Can you help?

Fujiao



Read email → **Query order records**

THE UNIVERSITY OF TENNESSEE KNOXVILLE

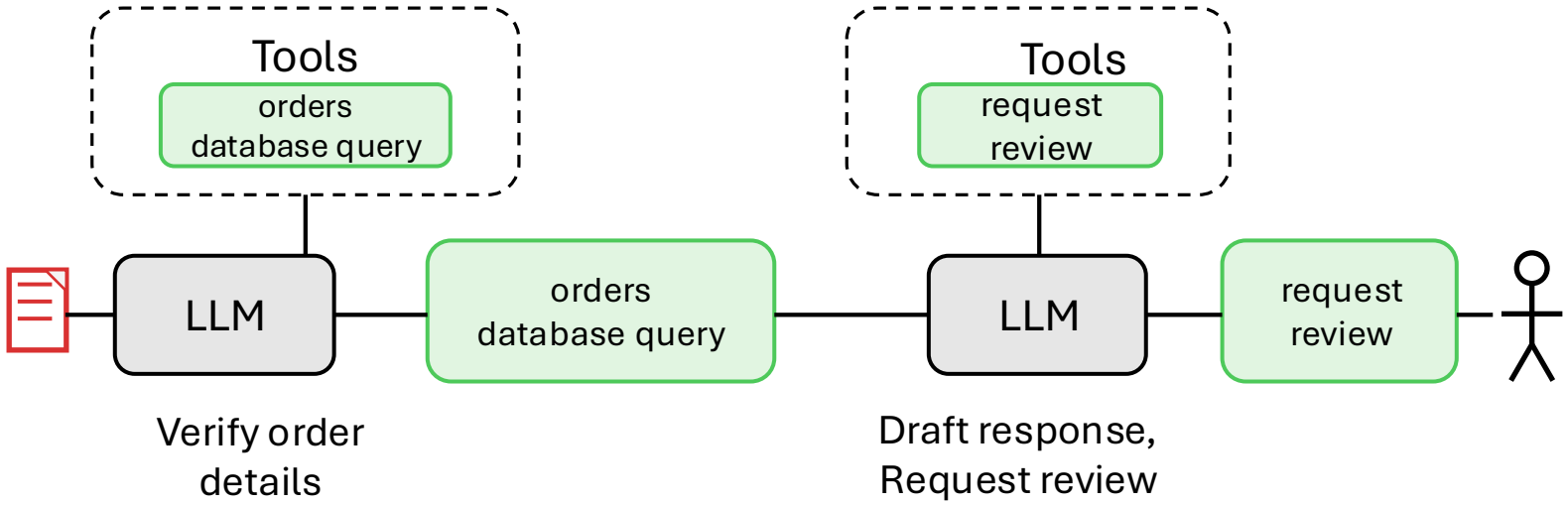
Example: Responding to customer email

From: Fujiao Ji
Subject: Wrong item shipped

I ordered a blue Mini13 Instax (Order #8847) but received a red one instead.

I need the item for my friend birthday party this weekend. Can you help?

Fujiao



Read email → **Query order records** → **Draft a response** → **Human approval**

THE UNIVERSITY OF TENNESSEE KNOXVILLE

What tasks is agentic AI suited to?

Easier → Harder

Clear, step-by-step process	Steps not known ahead of time
Standard procedures to follow	Plan/solve as you go
Text assets only	

Design Technique: Task Decomposition

Task: Write a research paper on Agentic AI Security for the USENIX Conference.

1. Focus on agentic AI security
2. Search web
3. Write the essay

Design Technique: Task Decomposition

Task: Write a research paper on Agentic AI Security for the USENIX Conference.

1. Focus on agentic AI security
2. Search web
3. Write the essay

Design Technique: Task Decomposition

~~3. Write the essay~~

Introduction

- Background: Two sentences introducing the research context;
- Related Work: One paragraph reviewing existing research;
- Challenges: Two sentences highlighting key challenges;
- Research Questions: Clearly define the research questions;
- Proposed Methods: One paragraph summarizing our approach;
- Results: One paragraph presenting the key findings;
- Contributions: One paragraph summarizing the main contributions.

Background

Introduce key concepts and provide necessary technical background.

...

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Agentic Design Patterns

Reflection: Is my output good enough?

Review → improve

Tool use: Do I need external capabilities?

Request → execute

Planning: What should I do next?

Decompose → act



Skills: How should this task be done?

Reusable instructions and workflows: Skills guide agent behavior across multiple design patterns.

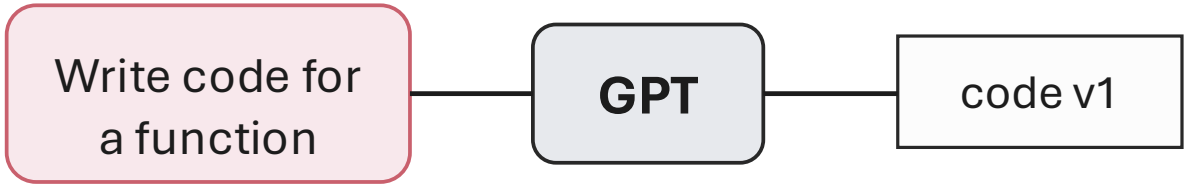
THE UNIVERSITY OF TENNESSEE KNOXVILLE

Overview

1. Agentic Workflows
2. Reflection
3. Tool Use
4. Planning
5. Skills
6. Evals + Error Analysis

THE UNIVERSITY OF TENNESSEE KNOXVILLE

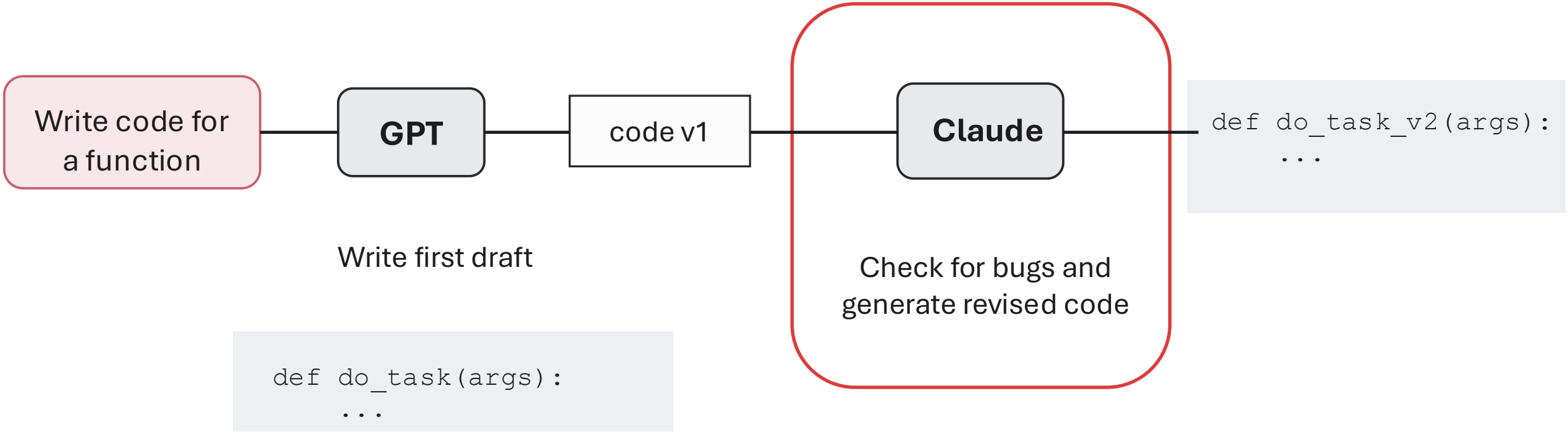
Reflection: using same / other models



Write first draft

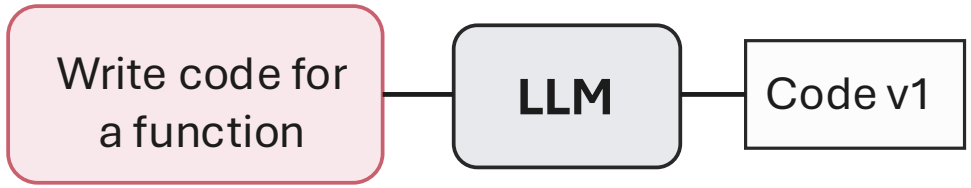
```
def do_task(args):
    ...
```

Reflection: using same / other models



THE UNIVERSITY OF TENNESSEE KNOXVILLE

Reflection: with external feedback



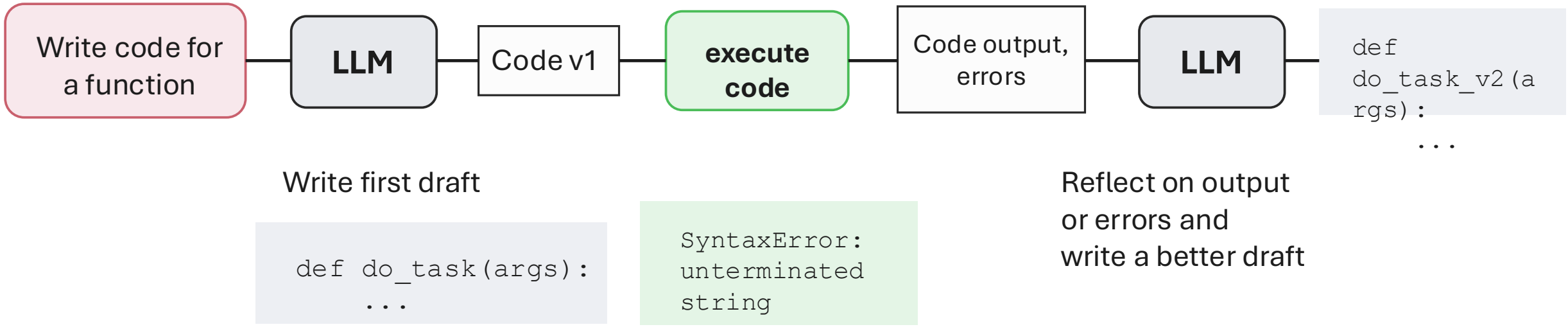
Write first draft

```
def do_task(args):
    ...
```

External feedback can come from running the code, checking outputs, or observing error messages.

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Reflection: with external feedback



External feedback can come from running the code, checking outputs, or observing error messages.

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Overview

1. Agentic Workflows
2. Reflection
3. Tool Use
4. Planning
5. Skills
6. Evals + Error Analysis

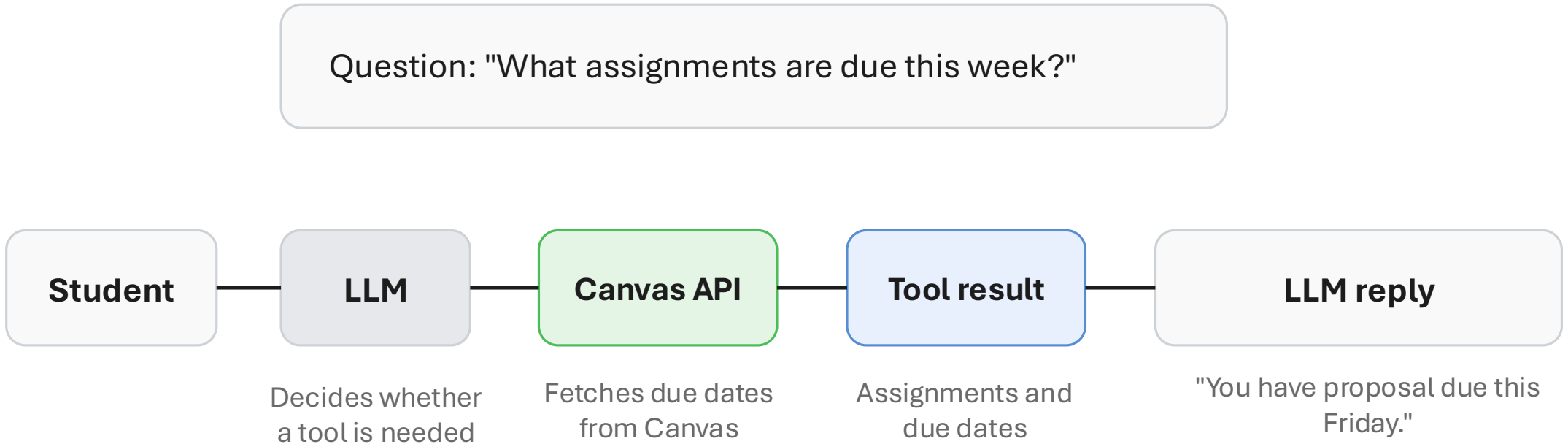
THE UNIVERSITY OF TENNESSEE KNOXVILLE

What are tools?

Tools are external functions or services that an LLM can ask an application to execute.

THE UNIVERSITY OF TENNESSEE KNOXVILLE

What are tools?



THE UNIVERSITY OF TENNESSEE KNOXVILLE

MCP (Model Context Protocol)

MCP is an open-source standard for connecting agents to external services.

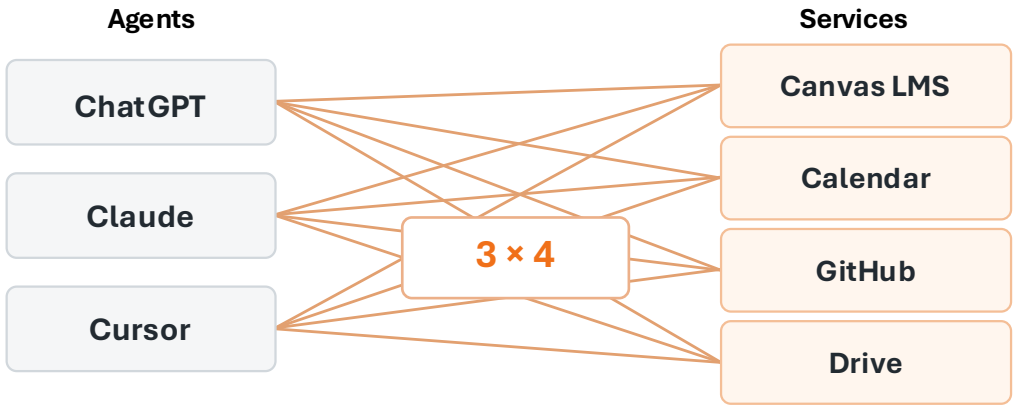
https://modelcontextprotocol.io/docs/2026-07-28/getting-started/intro

THE UNIVERSITY OF TENNESSEE KNOXVILLE

MCP (Model Context Protocol)

WITHOUT MCP

3 agents × 4 services = 12 adapters



Each agent needs a custom adapter to each service.

https://modelcontextprotocol.io/docs/2026-07-28/getting-started/intro

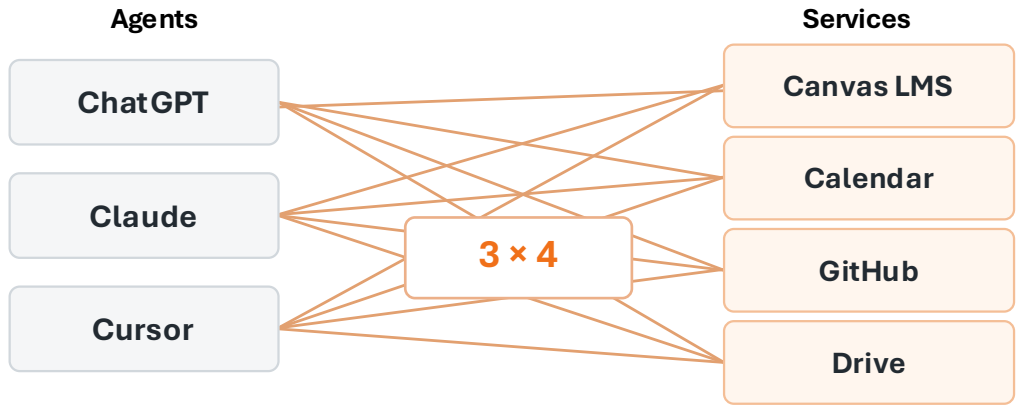
THE UNIVERSITY OF TENNESSEE KNOXVILLE

MCP (Model Context Protocol)

MCP is an open-source standard for connecting agents to external services.

WITHOUT MCP

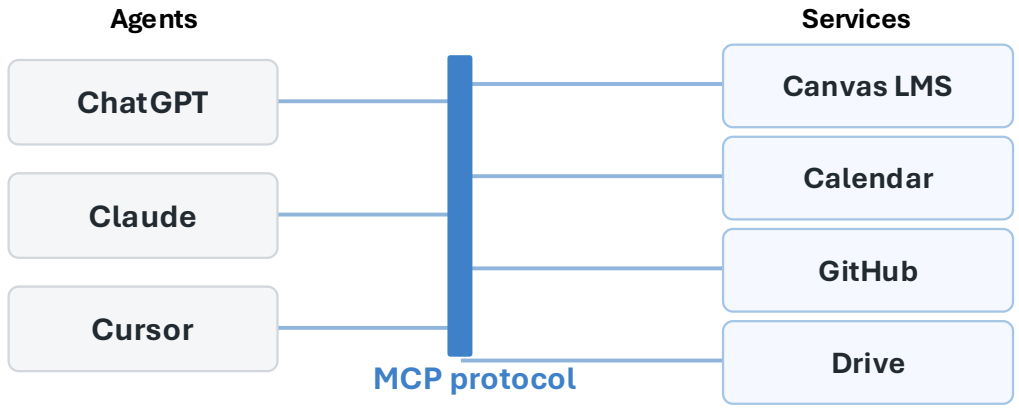
3 agents × 4 services = 12 adapters



Each agent needs a custom adapter to each service.

WITH MCP

3 MCP-ready agents + 4 servers = 7 parts



One reusable standard; compatible agents reuse the servers.

https://modelcontextprotocol.io/docs/2026-07-28/getting-started/intro

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Overview

1. Agentic Workflows
2. Reflection
3. Tool Use
4. Planning
5. Skills
6. Evals + Error Analysis

THE UNIVERSITY OF TENNESSEE KNOXVILLE

What is Agent Planning ?

AI agent planning refers to the process by which an artificial intelligence (AI) agent determines a sequence of actions to achieve a specific goal. It involves decision-making, goal prioritization and action sequencing, often using various planning algorithms and frameworks.

https://www.ibm.com/think/topics/ai-agent-planning

Example

USER REQUEST

Find ergonomic wireless mice under $35, rated 4.3+ with 100+ reviews. Add up to 3 to my Amazon cart.

- get_item_descriptions
- check_inventory
- get_item_price
- check_past_transactions
- process_item_return
- process_item_sale

PLANNING LLM

Generated plan

1. **Find ergonomic wireless mice**
   get_item_descriptions
2. **Check which items are in stock**
   check_inventory
3. **Check prices**
   get_item_price

...

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Overview

1. Agentic Workflows
2. Reflection
3. Tool Use
4. Planning
5. Skills
6. Evals + Error Analysis

THE UNIVERSITY OF TENNESSEE KNOXVILLE

What are Skills ?

Agent Skills are modular capabilities that extend agents' functionality. Each Skill packages instructions, metadata, and optional resources (scripts, templates) that agent uses automatically when relevant.

https://platform.claude.com/docs/en/agents-and-tools/agent-skills/overview

What are Skills ?

instructions, metadata, and

optional resources

WHAT A SKILL CONTAINS

pdf-processing/

- **SKILL.md** — required
- references/ — optional
- scripts/ · templates/

Instructions + metadata + optional resources

```
---
name: pdf-processing
description: Extract text and tables from PDF files, fill forms, merge documents. Use when worki
mentions PDFs, forms, or document extraction.
---

# PDF Processing

## Quick start

Use pdfplumber to extract text from PDFs:

```python
import pdfplumber

with pdfplumber.open("document.pdf") as pdf:
    text = pdf.pages[0].extract_text()
```

For advanced form filling, see FORMS.md.
```

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Why Use Skills?

Without a Skill

Repeat the same detailed instructions across tasks.

With a Skill

Create guidance once; load it automatically when relevant.

KEY BENEFITS

Specialize LLM

Bring domain-specific workflows, context, and best practices.

Reduce Repetition

Create guidance once and reuse it in future requests.

Compose Capabilities

Combine multiple Skills for complex, multistep tasks.

Example: A PDF-Processing Skill

User request: “Extract the text from this PDF and summarize it.”

01

MATCH

Discover pdf-processing from its metadata

→

02

LOAD

Read pdf-processing/SKILL.md

→

03

EXECUTE

Extract text and follow the workflow

→

04

RESPOND

Return a concise PDF summary

THE UNIVERSITY OF TENNESSEE KNOXVILLE

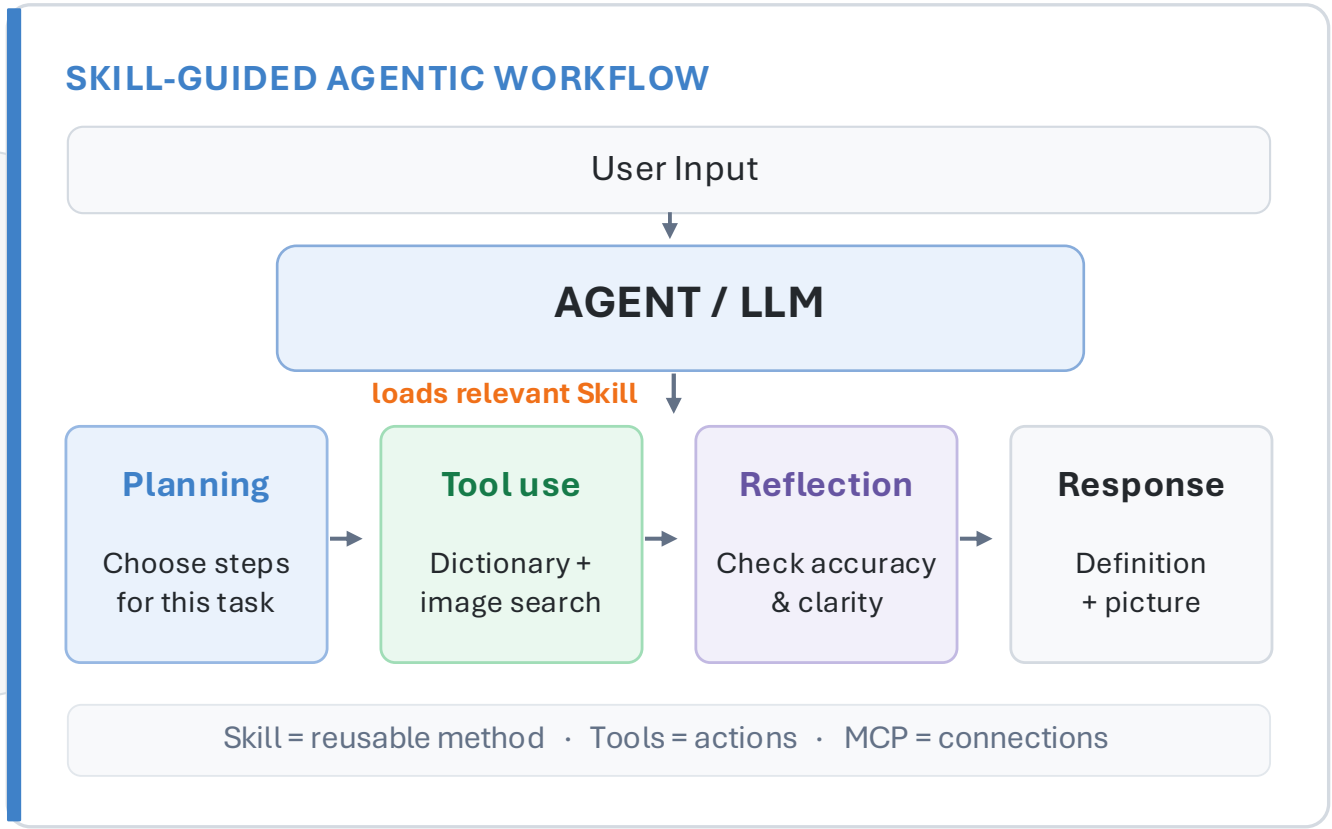
Making Them Together to an Agent

User request: “Extract the text from this PDF and summarize it.”

pdf-processing/

- **SKILL.md** required
- references/ optional
- scripts/ · templates/

Instructions + metadata + optional resources



THE UNIVERSITY OF TENNESSEE KNOXVILLE

Simplest Agent

User request: “Extract the text from this PDF and summarize it.”

pdf-processing/

- **SKILL.md** required

SKILL-GUIDED AGENTIC WORKFLOW

User Input

↓

Codex: guided by Skill

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Overview

1. Agentic Workflows
2. Reflection
3. Tool Use
4. Planning
5. Skills
6. Evals + Error Analysis

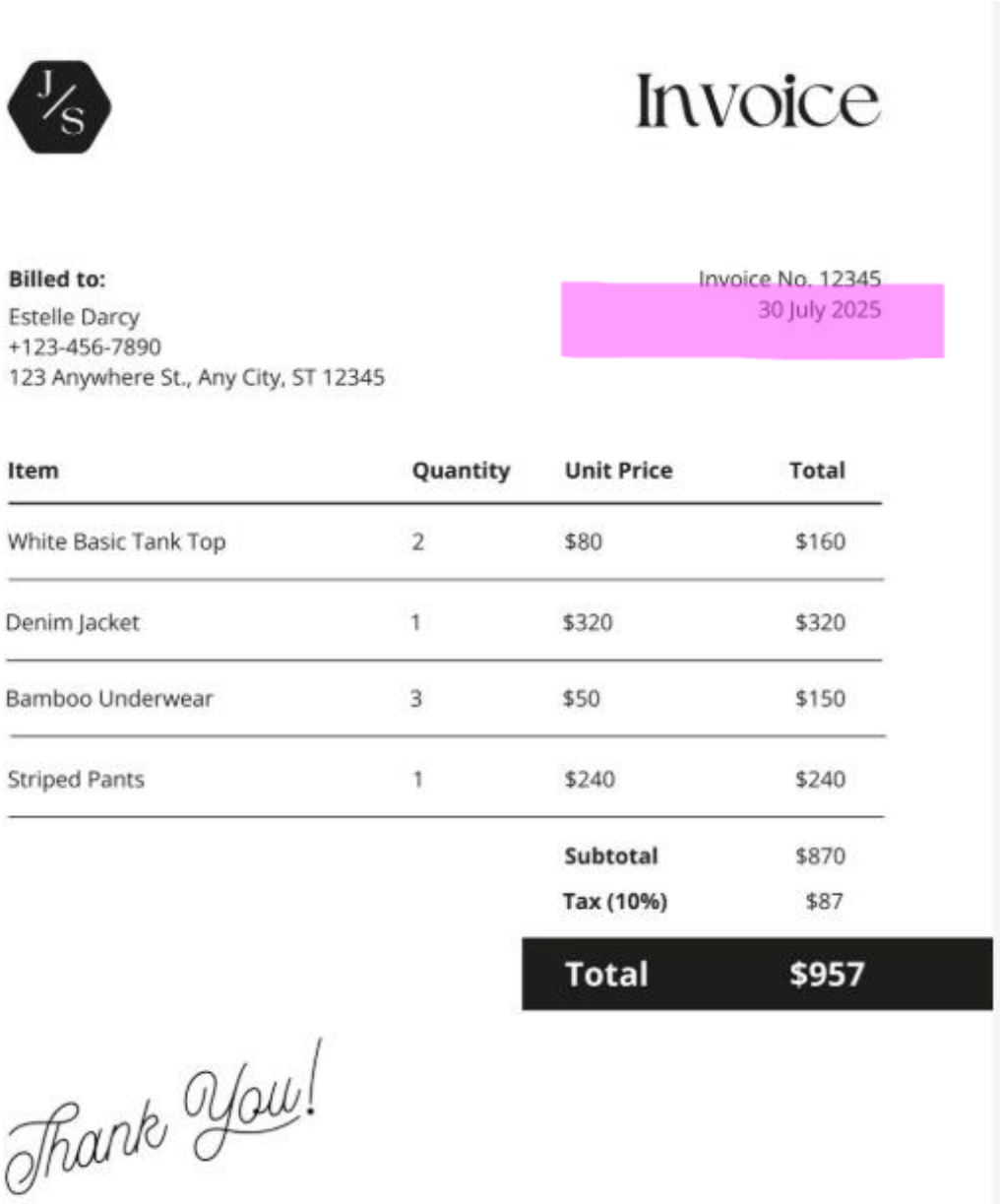
THE UNIVERSITY OF TENNESSEE KNOXVILLE

Eval

1. Manually Check, using code, or LLM-as-a-Judgement
2. Two types of evals: end-to-end and component-level
3. Examine errors

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Building an Eval: Invoice Date Extraction



J/S

Invoice

Billed to:
Estelle Darcy
+123-456-7890
123 Anywhere St., Any City, ST 12345

Invoice No. 12345
30 July 2025

Item	Quantity	Unit Price	Total
White Basic Tank Top	2	$80	$160
Denim Jacket	1	$320	$320
Bamboo Underwear	3	$50	$150
Striped Pants	1	$240	$240
		Subtotal	$870
		Tax (10%)	$87
		Total	**$957**

Thank You!

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Building an Eval: Invoice Date Extraction

1 Prepare labeled examples

Start with 10–20 invoices

INVOICE 001

Due: August 20, 2025

Ground truth (human labeled)

2025/08/20

2 Set the output format

Make the answer machine-readable

MODEL INSTRUCTION

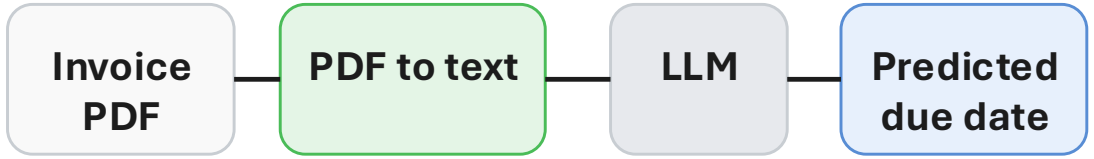
Extract the due date.
Return YYYY/MM/DD only.

Expected format: YYYY/MM/DD

THE UNIVERSITY OF TENNESSEE KNOXVILLE

End-to-end eval vs. component eval

Example: extract the due date from invoices and evaluate the workflow.



1) End-to-end eval

Measure whether the final output is correct.

Ground truth	LLM output	Eval
2025/10/05	2025/05/10	FAIL

Use this when you care about the final user-facing result.

2) Component eval

Measure each step separately to find where errors come from.

- **A. PDF-to-text** — Did the due date appear in the text?
- **B. LLM extraction** — Did the model select the correct date?

Use this when you want to diagnose failures and improve the system faster.

THE UNIVERSITY OF TENNESSEE KNOXVILLE

End-to-end eval tells you if the workflow works. Component eval tells you which step to fix.

Basic Understanding of Agents

Reflection： Is my output good enough?

Review → improve

Tool use： Do I need external capabilities?

Request → execute

Planning： What should I do next?

Decompose → act

Skills： How should this task be done?

Reusable instructions and workflows: Skills guide agent behavior across multiple design patterns.

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Three Examples for agents

1. Paper Review Agents
    1. Codex
2. Item Selection Agents for Amazon
    1. source /Users/fji1/Documents/agent_web/env_agent/bin/activate
    2. Using GPT API key
    3. Check /Users/fji1/Documents/language-agent-execution-planner/read.md
3. Language Learning Agents
    1. source /Users/fji1/Documents/.venv/bin/activate
    2. Using GPT API key
    3. python -m streamlit run app.py --server.address 127.0.0.1

THE UNIVERSITY OF TENNESSEE KNOXVILLE