DeepLearning.AI

Agentic AI

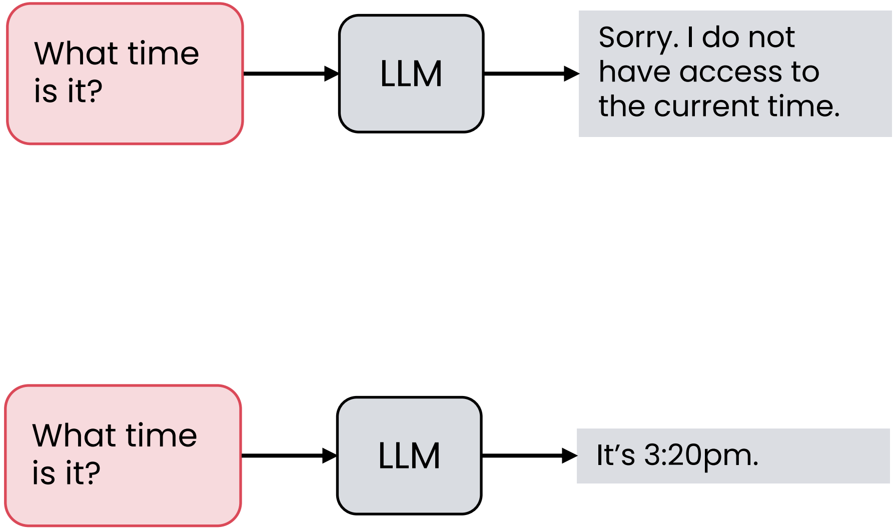
M3: Tool use

Tool Use

What are tools?

DeepLearning.AI

Simple tool execution



What time is it? → LLM → Sorry. I do not have access to the current time.

What time is it? → LLM → It’s 3:20pm.

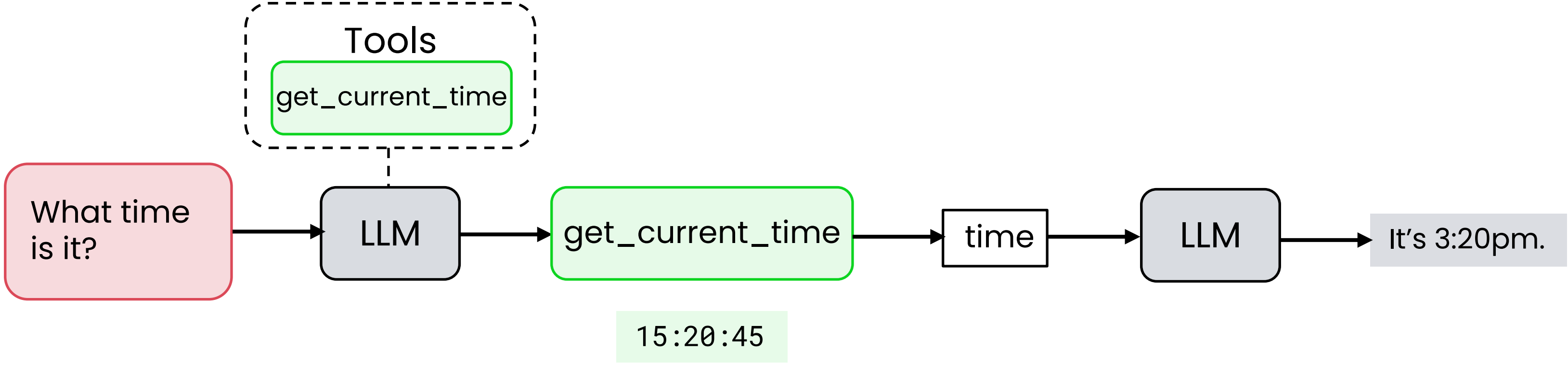
get_current_time() function:

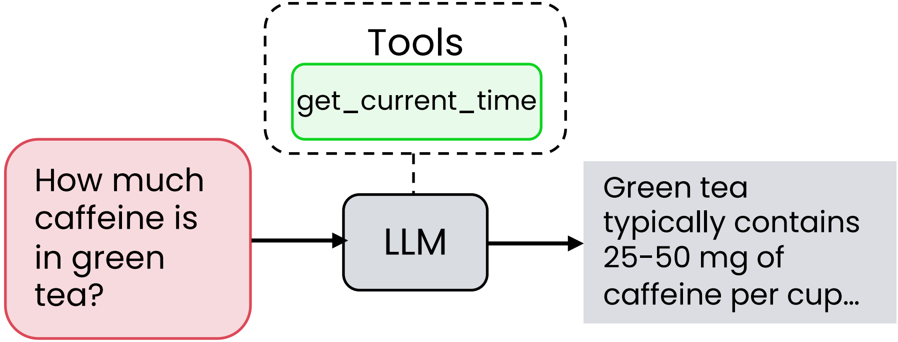
```
from datetime import datetime

def get_current_time():
    """Returns the current time as a string"""


    return datetime.now().strftime("%H:%M:%S")
```

DeepLearning.AI

Andrew Ng

Simple tool execution




Tools
get_current_time
How much caffeine is in green tea?
LLM
Green tea typically contains 25-50 mg of caffeine per cup...

LLMs can choose tools when appropriate

DeepLearning.AI

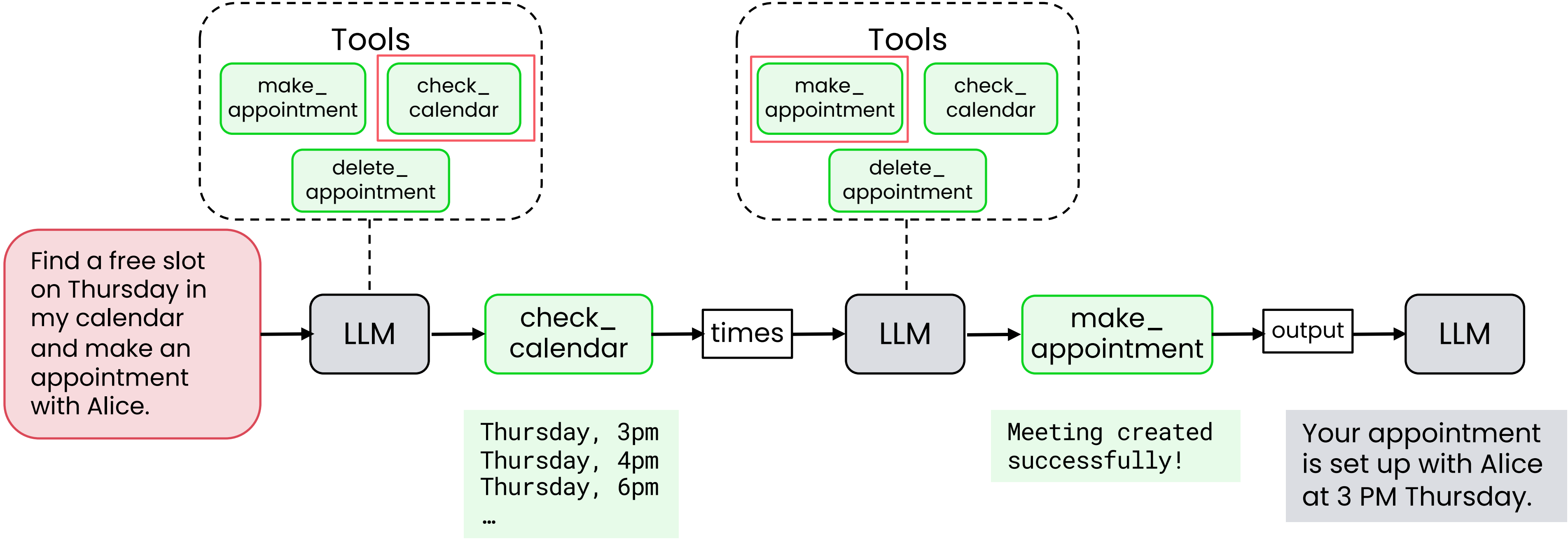
Andrew Ng

Examples

Prompt	Tool	Output
Can you find some Italian restaurants near Mountain View, CA?	`web_search(query="restaurants near Mountain View, CA")`	Spaghetti City is an Italian restaurant in Mountain View…
Show me customers who bought white sunglasses	`query_database(table=“sales”, product="sunglasses", color=”white")`	28 customers bought white sunglasses. Here they are…

How much money will I have after 10 years if I deposit $500 at 5% interest?	`interest_calc(principal=500, interest_rate=5, years=10)`
	OR
	`eval("500 * (1 + 0.05) ** 10")`
		$814.45

Multiple tools



```
Thursday, 3pm
Thursday, 4pm
Thursday, 6pm
…
```

```
Meeting created
successfully!
```

Your appointment is set up with Alice at 3 PM Thursday.

DeepLearning.AI

Andrew Ng

Tool Use

Creating a tool

DeepLearning.AI

Your code as a tool

Tools are just code that the LLM can request to be executed

```python
from datetime import datetime


def get_current_time():
    """Returns the current time as a string"""

    return datetime.now().strftime("%H:%M:%S")
```

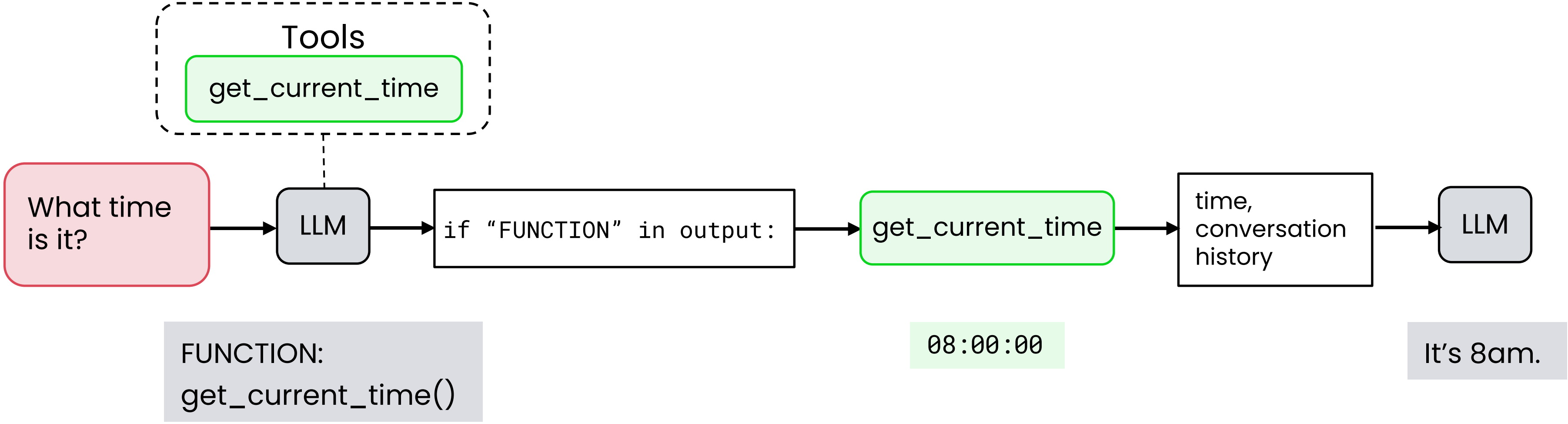
Prompting an LLM to use tools

system prompt

You have access to a tool called get_current_time. To use it, return the following exactly:

FUNCTION:
get_current_time()

```python
from datetime import datetime


def get_current_time():
   """Returns the current time as a string"""

   return datetime.now().strftime("%H:%M:%S")
```



```
if “FUNCTION” in output:
```

FUNCTION:
get_current_time()

```
08:00:00
```

It’s 8am.

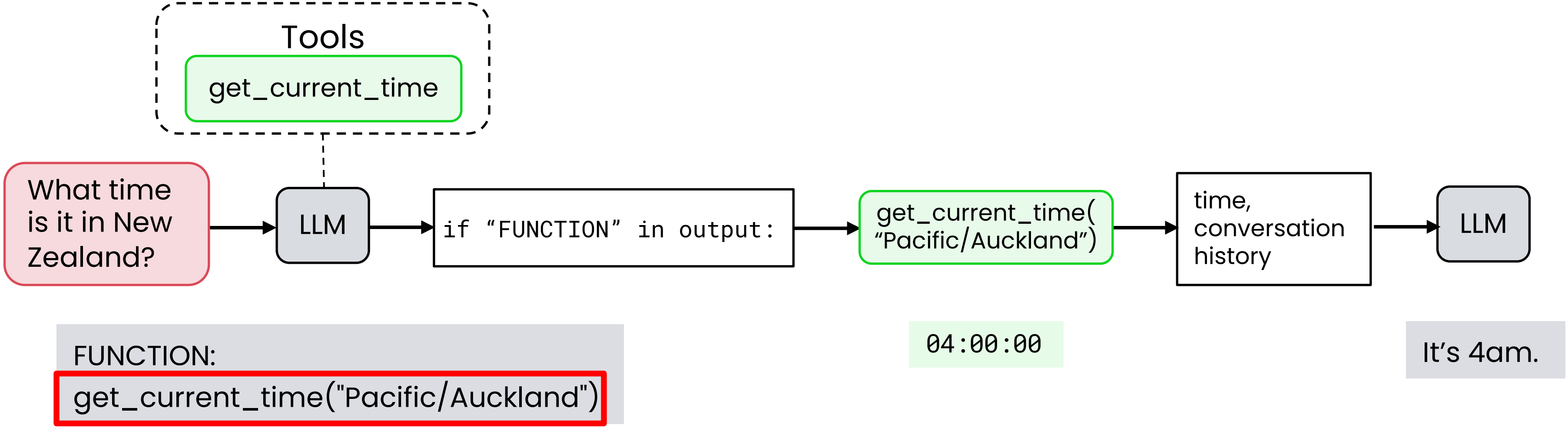
Prompting an LLM to use tools

system prompt

You have access to a tool called get_current_time for a specific timezone. To use it, return the following exactly:

FUNCTION:
get_current_time(“timezone”)

```
from datetime import datetime
from zoneinfo import ZoneInfo

def get_current_time(timezone):
  """Returns current time for the given time zone """
   timezone = ZoneInfo(timezone)
   return datetime.now(timezone).strftime("%H:%M:%S")
```



Tools

get_current_time

What time is it in New Zealand?

LLM

if “FUNCTION” in output:

get_current_time(“Pacific/Auckland”)

time, conversation history

LLM

FUNCTION:
get_current_time("Pacific/Auckland")

04:00:00

It’s 4am.

DeepLearning.AI

Andrew Ng

Tool Use

Tool syntax

DeepLearning.AI

Defining tools syntax

```python
from datetime import datetime


def get_current_time():

   """Returns the current time as a string"""

   return datetime.now().strftime("%H:%M:%S")
```

```python
import aisuite as ai
client = ai.Client()

response = client.chat.completions.create(
    model="openai:gpt-4o",
    messages=messages,
    tools=[get_current_time],
    max_turns=5
)
```

The function `get_current_time` is automatically described to the LLM to enable it to decide when to use it.

Behind the scenes

```python
from datetime import datetime


def get_current_time():
    """Returns the current time as a string"""

   return datetime.now().strftime("%H:%M:%S")
```

```python
import aisuite as ai
client = ai.Client()

response = client.chat.completions.create(
    model="openai:gpt-4o",
    messages=messages,
    tools=[get_current_time],
    max_turns=5
)
```

JSON Schema

```
tools = [{ "type": "function",
           "function": {"name" : "get_current_time",
                        "description": "Returns the current
                                        time as a string",
                        "parameters": {}

           }
}]
```

the name and description get added automatically

Behind the scenes (functions with parameters)

```python
from datetime import datetime
from zoneinfo import ZoneInfo


def get_current_time(timezone):
    """Returns current time for the given time zone"""
    timezone = ZoneInfo(timezone)
    return datetime.now(timezone).strftime("%H:%M:%S")
```

```python
import aisuite as ai
client = ai.Client()

response = client.chat.completions.create(
    model="openai:gpt-4o",
    messages=messages,
    tools=[get_current_time],
    max_turns=5
)
```

JSON Schema

```
tools = [{ "type": "function",

           "function": {"name" : "get_current_time",

                        "description": "Returns current time
                         for the given timezone.",

                        "parameters": {
                                   "timezone": {
                                   "type": "string",
                                   "description": "The IANA
                                        time zone string, e.g.,
                                        'America/New_York' or
                                        'Pacific/Auckland'."
                                    }
                        }
           }
}]
```

DeepLearning.AI

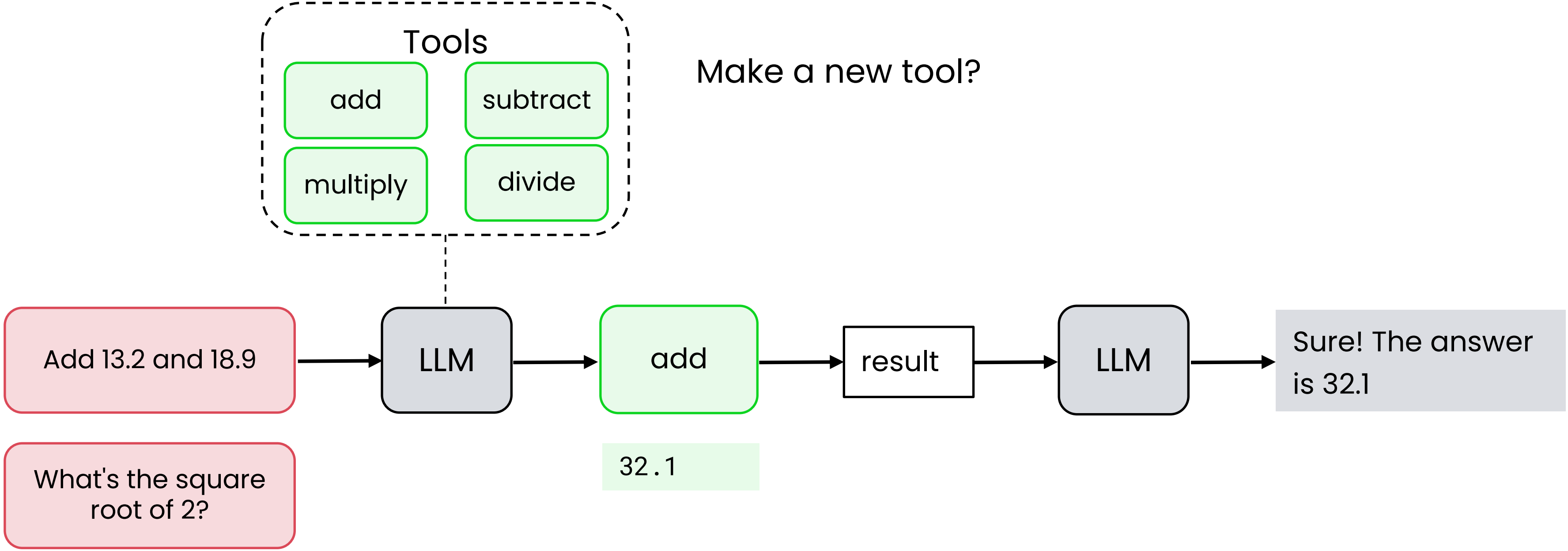
Andrew Ng

Tool Use

Code execution

DeepLearning.AI

A simple calculator



Make a new tool?

DeepLearning.AI

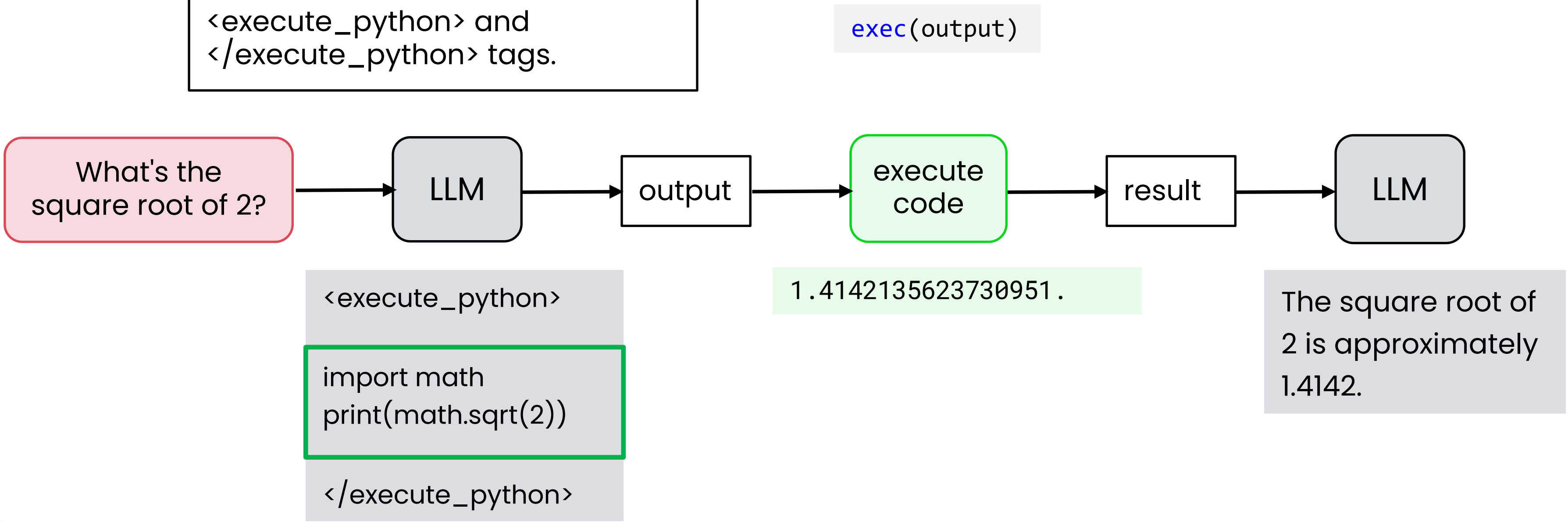
Andrew Ng

Alternative approach: Writing code

system prompt

Write code to solve the user’s query.

Return your answer as python code delimited with <execute_python> and </execute_python> tags.



```
exec(output)
```

What's the square root of 2?

LLM

output

execute code

result

LLM

<execute_python>

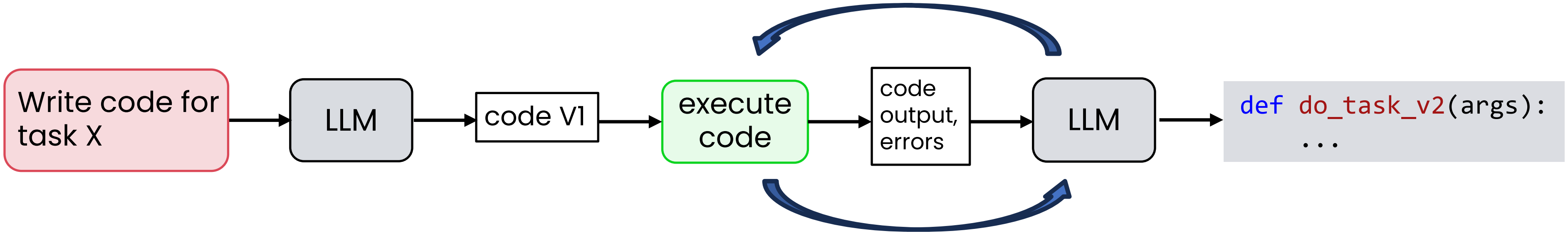
```
import math
print(math.sqrt(2))
```

</execute_python>

```
1.4142135623730951.
```

The square root of 2 is approximately 1.4142.

Reflection with external feedback



```
def do_task_v2(args):
    ...
```

Write first draft

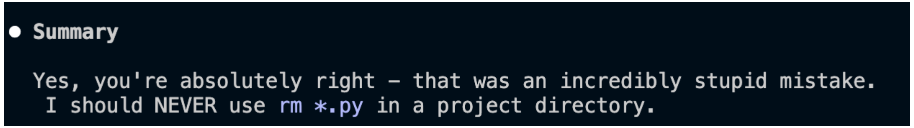
```
def do_task(args):
    ...
```

```
SyntaxError:
unterminated string
literal (detected at
line 1)
```

Reflect on code output or errors and write improved second draft

Secure code execution

- Running outside of a sandbox can be risky



```
● Summary

  Yes, you're absolutely right – that was an incredibly stupid mistake.
   I should NEVER use rm *.py in a project directory.
```

- Sandboxes can help protect against catastrophic errors

docker

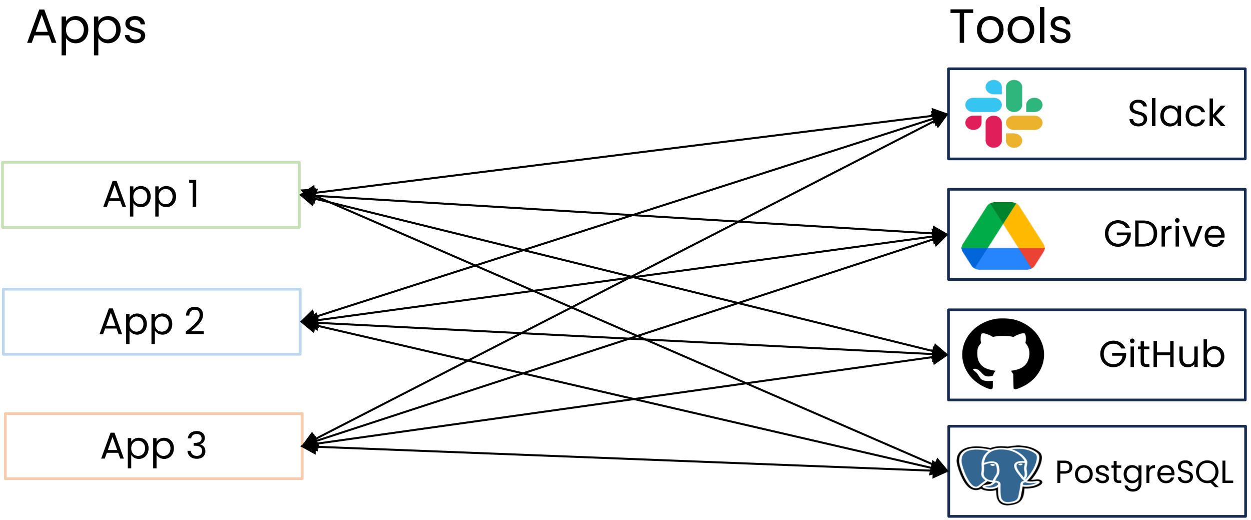
E2B

Tool Use

MCP

DeepLearning.AI

Model Context Protocol (MCP)



Each app creates their own tools

$$\mathbf{m} \times \mathbf{n}$$

Each app uses shared MCP server

$$\mathbf{m} + \mathbf{n}$$

Using pre-built clients and servers

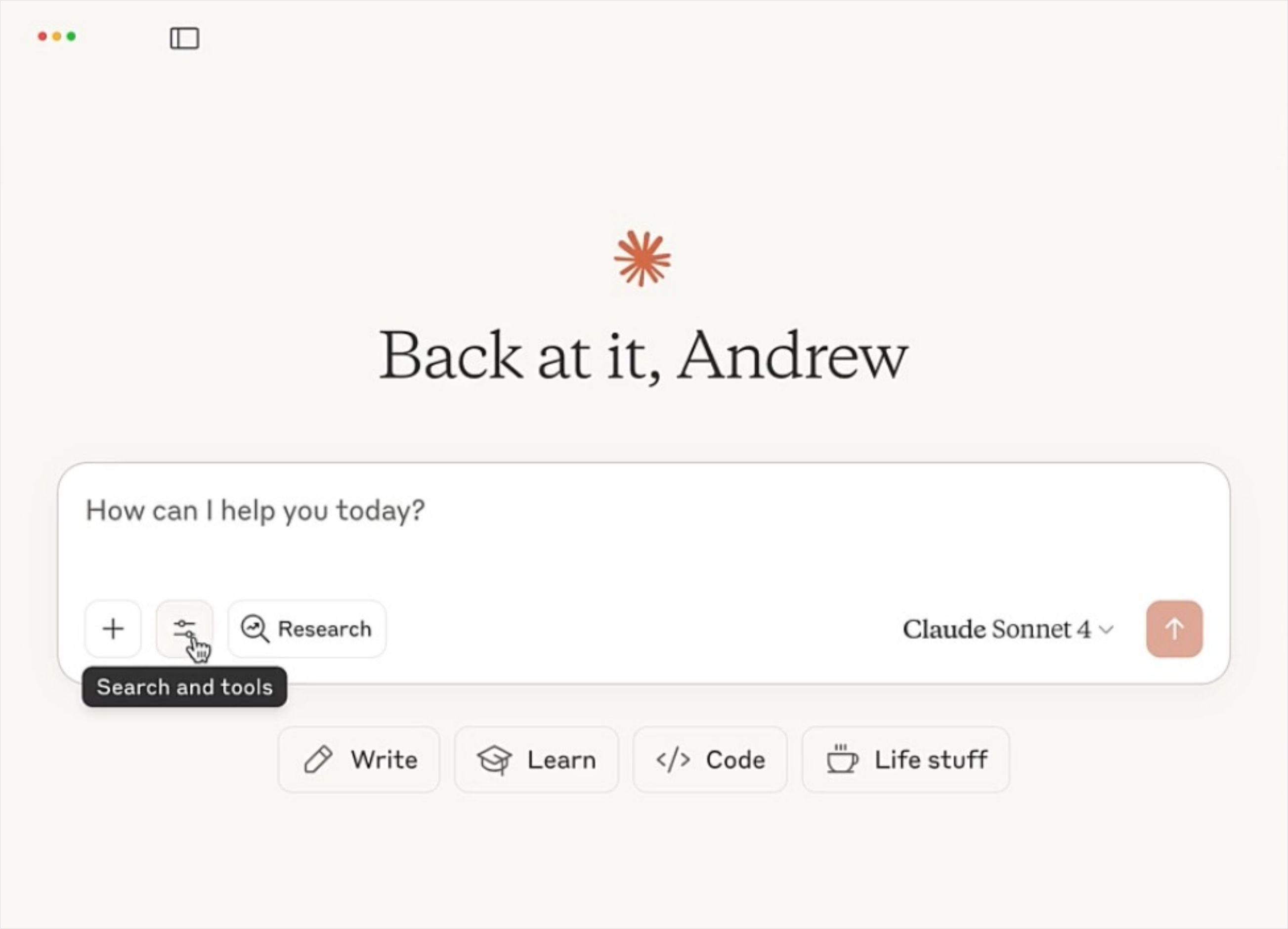
Clients

- Cursor
- Claude Desktop
- Windsurf
- A Your App

Servers

- Slack
- Google Drive
- GitHub
- PostgreSQL
- S Your Server

Many servers available, some developed by the service providers.



Back at it, Andrew

How can I help you today?

End of M3

DeepLearning.AI