ToolCall - Mô hình ngôn ngữ gọi đến một công cụ

Trong LangChain, `ToolCall` đại diện cho việc **mô hình ngôn ngữ gọi đến một công cụ (function)** để thực hiện một hành động cụ thể.

> Nói cách khác, khi bạn dạy AI cách gọi các hàm Python, thì `ToolCall` là cách mô hình nói: *"Tôi muốn dùng hàm `add(5, 3)` nhé."*

Tại sao cần `ToolCall`?

Mô hình ngôn ngữ rất giỏi hiểu và tạo ra văn bản, nhưng lại **không giỏi tính toán, truy vấn API, hoặc thao tác với dữ liệu phức tạp**.
Khi cần làm những việc như vậy, mô hình sẽ **gọi một "tool"** (được định nghĩa trước bằng Python), thông qua một `ToolCall`.

Cấu trúc cơ bản của `ToolCall`

```
from langchain_core.messages import ToolCall


tool_call = ToolCall(
    name="multiply",
    args={"a": 5, "b": 3},
    id="call_123"
)
```

Các thành phần:

- `name`: tên hàm (tool) mà AI muốn gọi (giống với tên bạn đăng ký khi dùng `bind_tools`).
- `args`: tham số truyền vào cho hàm đó.
- `id`: mã định danh của tool call (thường là tự sinh).

Ví dụ đầy đủ: Sử dụng `ToolCall` với LLM

Bước 1: Định nghĩa công cụ

```
def add(a: int, b: int) -> int:
    return a + b
```

Bước 2: Bind tool vào LLM

```
from langchain_openai import ChatOpenAI

llm = ChatOpenAI(model="gpt-4o")
llm_with_tools = llm.bind_tools([add])
```

Bước 3: Gửi tin nhắn có yêu cầu tính toán

```
from langchain_core.messages import HumanMessage

messages = [HumanMessage(content="Hãy cộng 4 và 7 giúp tôi")]
response = llm_with_tools.invoke(messages)

print(response.tool_calls)  # Đây chính là danh sách ToolCall
```

Output mẫu:

```
[
    ToolCall(
        name='add',
        args={'a': 4, 'b': 7},
        id='toolu_abc123'
    )
]
```

Tức là mô hình quyết định gọi hàm `add` với a=4, b=7 thông qua ToolCall.

Tương tác hoàn chỉnh: Gọi Tool và trả lại kết quả

```
from langchain_core.messages import AIMessage, ToolMessage

# Gọi hàm add
tool_result = add(4, 7)
```

```
# Trả kết quả lại cho AI thông qua ToolMessage
final_response = llm_with_tools.invoke([
    HumanMessage(content="Hãy cộng 4 và 7"),
    AIMessage(tool_calls=[ToolCall(name="add", args={"a": 4, "b": 7}, id="call_1")]),
    ToolMessage(tool_call_id="call_1", content=str(tool_result))
])

print(final_response.content)
```

Output

```
Kết quả là 11!
```

Tóm tắt so sánh

Thành phần	Vai trò
`ToolCall`	Yêu cầu gọi hàm từ mô hình LLM
`ToolMessage`	Trả kết quả từ tool về để LLM tiếp tục xử lý
`bind_tools`	Cho LLM biết có thể gọi những hàm nào

Khi nào cần dùng `ToolCall`?

- Khi mô hình phải tính toán, xử lý logic cụ thể, hoặc truy vấn dữ liệu thật.
- Khi xây dựng chatbot có khả năng "hành động", như đặt lịch, gọi API, v.v.

Tác giả: Đỗ Ngọc Tú

Công Ty Phần Mềm VHTSoft

Phiên bản #1
Được tạo 22 tháng 4 2025 03:20:38 bởi Đỗ Ngọc Tú
Được cập nhật 22 tháng 4 2025 03:31:49 bởi Đỗ Ngọc Tú