# 代理的使用

我们通过一个实际的应用案例代码，解释如何使用代理和工具。

#### 设置Agent

我们先安装要用到的库。

pip -q install langchain huggingface\_hub openai google-search-results tiktoken wikipedia

设置密钥。

import os  
os.environ["OPENAI\_API\_KEY"] = ""  
os.environ["SERPAPI\_API\_KEY"] = ""

设置Agent的过程包含了两个主要步骤：加载Agent将使用的工具，然后用这些工具初始化Agent。在代码示例中，我们首先初始化了一些基础设置，然后加载了两个工具：一个使用搜索API进行搜索的工具，以及一个可以进行数学运算的计算器工具。

加载工具和初始化Agent。

from langchain.agents import load\_tools  
from langchain.agents import initialize\_agent  
from langchain.llms import OpenAI  
  
llm = OpenAI(temperature=0)

每个工具都有一个名称和描述，告诉我们它是用来做什么的。在我们的示例中，“serpapi”工具用于搜索，而“llm-math”工具则用于解决数学问题。这些工具内部有很多内容，包括模板和许多不同的chains。

tools = load\_tools(["serpapi", "llm-math"], llm=llm)

#### 初始化Agent

一旦我们设置好了工具，我们就可以开始初始化Agent。初始化Agent需要我们传入工具和语言模型，以及Agent的类型或风格。在我们的示例中，我们使用了零镜像反应性Agent，这是基于一篇关于让语言模型采取行动并生成操作步骤的论文。

agent = initialize\_agent(tools,   
 llm,   
 agent="zero-shot-react-description",   
 verbose=True)

#### Agent的提示

初始化Agent的重要步骤之一是设置执行器的提示。这些提示会在Agent开始运行时提示语言模型，告诉它应该做什么。

agent.agent.llm\_chain.prompt.template

在我们的示例中，我们为Agent设置了两个工具：搜索引擎和计算器。然后，我们设置了Agent应该返回的格式，这包括它需要回答的问题，以及它应该采取的行动和行动的输入。

'Answer the following questions as best you can. You have access to the following tools:\n\nSearch: A search engine. Useful for when you need to answer questions about current events. Input should be a search query.\nCalculator: Useful for when you need to answer questions about math.\n\nUse the following format:\n\nQuestion: the input question you must answer\nThought: you should always think about what to do\nAction: the action to take, should be one of [Search, Calculator]\nAction Input: the input to the action\nObservation: the result of the action\n... (this Thought/Action/Action Input/Observation can repeat N times)\nThought: I now know the final answer\nFinal Answer: the final answer to the original input question\n\nBegin!\n\nQuestion: {input}\nThought:{agent\_scratchpad}'

#### Agent的运行

最后，我们运行Agent。需要注意的是，Agent并不总是需要使用工具。在我们的示例中，我们问Agent “你今天好吗？”。对于这样的问题，Agent并不需要进行搜索或计算，而是可以直接生成回答。

agent.run("Hi How are you today?")

这就是Langchain Agents的基本概念和使用方法。

#### 使用Math模块

我们在前半部分介绍了Langchain agents（代理）的基础知识和功能。现在，我们要继续探讨如何在实际中应用Agent，以及在某些情况下，Agent可能遇到的问题。

agent.run("Where is DeepMind's office?")

在我们的示例中，我们尚未使用到math模块，让我们来看一下它的作用。我们让Agent查找Deep Mind的街道地址的数字，然后进行平方。

agent.run("If I square the number for the street address of DeepMind what answer do I get?")

Agent首先进行搜索获取地址，然后找到了数字5（假设为地址的一部分），最后进行平方运算，得出结果25。然而，如果问题中包含多个数字，Agent可能会对哪个数字进行平方产生混淆，这就是一些可能需要考虑和解决的问题。

> Entering new AgentExecutor chain...  
 I need to find the street address of DeepMind first.  
Action: Search  
Action Input: "DeepMind street address"  
Observation: DeepMind Technologies Limited, is a company organised under the laws of England and Wales, with registered office at 5 New Street Square, London, EC4A 3TW (“DeepMind”, “us”, “we”, or “our”). DeepMind is a wholly owned subsidiary of Alphabet Inc. and operates https://deepmind.com (the “Site”).  
Thought: I now need to calculate the square of the street address.  
Action: Calculator  
Action Input: 5^2  
Observation: Answer: 25  
Thought: I now know the final answer.  
Final Answer: 25  
  
> Finished chain.  
'25'

#### 使用终端工具

在我们的工具库中，还有一个我们还未使用过的工具，那就是终端工具。例如，我们可以问Agent当前目录中有哪些文件。

agent.run("What files are in my current directory?")

Agent将运行一个LS命令来查看文件夹，并返回一个文件列表。

> Entering new AgentExecutor chain...  
 I need to find out what files are in my current directory.  
Action: Terminal  
Action Input: ls  
Observation: sample\_data  
  
Thought: I need to find out more information about this file.  
Action: Terminal  
Action Input: ls -l sample\_data  
Observation: total 55504  
-rwxr-xr-x 1 root root 1697 Jan 1 2000 anscombe.json  
-rw-r--r-- 1 root root 301141 Mar 10 20:51 california\_housing\_test.csv  
-rw-r--r-- 1 root root 1706430 Mar 10 20:51 california\_housing\_train.csv  
-rw-r--r-- 1 root root 18289443 Mar 10 20:51 mnist\_test.csv  
-rw-r--r-- 1 root root 36523880 Mar 10 20:51 mnist\_train\_small.csv  
-rwxr-xr-x 1 root root 930 Jan 1 2000 README.md  
  
Thought: I now know the final answer.  
Final Answer: The files in my current directory are anscombe.json, california\_housing\_test.csv, california\_housing\_train.csv, mnist\_test.csv, mnist\_train\_small.csv, and README.md.  
  
> Finished chain.  
'The files in my current directory are anscombe.json, california\_housing\_test.csv, california\_housing\_train.csv, mnist\_test.csv, mnist\_train\_small.csv, and README.md.'

我们甚至可以问它特定的文件是否存在，比如询问当前目录中是否有一个关于加利福尼亚的文件。

agent.run("Does my current directory have a file about California?")

Agent会使用grep命令进行检索，并向我们报告结果。然而，这个过程可能需要多次调用语言模型，从而产生一定的运行成本。

> Entering new AgentExecutor chain...  
 I need to find out what files are in my current directory.  
Action: Terminal  
Action Input: ls  
Observation: sample\_data  
  
Thought: I need to find out if there is a file about California in this directory.  
Action: Terminal  
Action Input: grep California sample\_data  
Observation: Command 'grep California sample\_data' returned non-zero exit status 2.  
Thought: I need to look for a different way to search for the file.  
Action: Search  
Action Input: "California file in current directory"  
Observation: The pwd command displays the full, absolute path of the current, or working, directory. It's not something you'll use all the time, but it can ...  
Thought: I need to use the pwd command to find the file.  
Action: Terminal  
Action Input: pwd  
Observation: /content  
  
Thought: I need to use the ls command to find the file.  
Action: Terminal  
Action Input: ls  
Observation: sample\_data  
  
Thought: I need to use the grep command to find the file.  
Action: Terminal  
Action Input: grep California sample\_data  
Observation: Command 'grep California sample\_data' returned non-zero exit status 2.  
Thought: I need to look for a different way to search for the file.  
Action: Search  
Action Input: "California file in current directory"  
Observation: The pwd command displays the full, absolute path of the current, or working, directory. It's not something you'll use all the time, but it can ...  
Thought: I need to use the find command to find the file.  
Action: Terminal  
Action Input: find . -name "\*California\*"  
Observation: Command 'find . -name "\*California\*' returned non-zero exit status 2.  
Thought: I need to use the grep command to find the file.  
Action: Terminal  
Action Input: grep -R California \*  
Observation: sample\_data/README.md:\* `california\_housing\_data\*.csv` is California housing data from the 1990 US  
  
Thought: I now know the final answer.  
Final Answer: Yes, there is a file about California in the current directory.  
  
> Finished chain.  
'Yes, there is a file about California in the current directory.'

#### 注意事项

使用终端工具时，需要非常谨慎。你不希望最终用户能够通过运行终端命令来操作你的文件系统，因此在添加这个工具时，需要确保适当的安全防护措施已经到位。不过，尽管有其潜在风险，但在某些情况下，使用终端工具还是很有帮助的，比如当你需要设置某些功能时。

以上就是Langchain agents的一些主要特点和应用示例。