AI Agent 학습 1주차 노트 정리
작성자 문영식
작성일 24년 11월 5일
참고자료 : youtube 모두의AI AI 에이전트의 원리와 단일, 멀티 에이전트

AI Agent 원리
에이전트 시스템은 LLM 또는 LMM이 중심으로 추론 엔진 역할을 한다.
다양한 도구 또는 기억에 따라 사용자 요청에 더 완성도 높은 답변을 할 수 있도록 만들어주는 하나의 시스템이라 볼 수 있다.
LLM이 어떤 작업을 해야 하는지에 대해서 스스로 계획을 짜고 이것을 수행하는 계획과 행동 모듈에 있어서 핵심적 이라고 할 수있다.
어떤 식으로 작업 계획을 세우냐에 따라 완성도가 높아지기 때문에 이 부분에 초점을 두는게 좋다.
에이전트 시스템 구현 완성 후 답변을 받기까지 과정을 보면 LLM이 계획을 세우고 행동하는 과정이 여러 번 반복이 되면서 답변이 고도화 되는 측면을 볼 수 있다.
관리자가 지켜봐야 할 부분은 LLM이 작업을 계획을 잘 세우고 있는지 그리고 이것들을 잘 수행하고 있는지에 초점을 두도록 해야 함.

에이전트의 시작
구글 브레인에서 2022년도에 냈던 논문 ReAct라는 프롬프팅 기법으로부터 시작이 됐다.
실험 1. Hotspot QA (위키피디아에 수집된 질문 답변 데이터 세트)에 의한 답변
1a) 기본
결과 : 잘못된 답변
1b) CoT(Chain-of-Thought, 생각의 사슬) 기법 : 생각 -> 답변
결과 : 잘못된 답변
1c) Act-Only (LLM이 갖고 있지 않는 지식에 대해 다른 도구를 활용해 얻음) 기법 : 행동 -> 관찰 -> 행동 -> 관찰 ... 완료
결과 : 잘못된 답변
예시로 웹 검색 도구를 활용했으나, 웹에 정확한 정보가 없어 잘못된 답변을 함.
1d) ReAct (Reason + Act) 기법 : CoT와 Act-Only의 장점을 합침. 생각 -> 행동 -> 관찰 -> 생각 -> 행동 -> 관찰 ... 답

단일 에이전트
논문 이후 ReAct를 가지고 만들어낸 서비스가 유행을 하게 됐는데 그 중 AutoGPT가 있다.
AutoGPT에 이름 역할 목표를 주면 수행하는데 과정을 보면 ReAct가 적용 된 것을 볼 수 있다.
생각+이유+계획+비판 이렇게 세트로 사용자의 질문 목표에 대해서 어떤 작업을할지 스스로 찾아가 답을 얻는다.
이렇게 ReAct기법을 활용해 LLM이 모든 역할을 하게 만드는 것이 단일 에이전트라고 할 수 있다.

단일 에이전트 한계점.
실무 보고서 같은 작업을 GPT에게 얻은 한 건의 문서로 대체하기엔 결과물이 매우 단순하다는 한계점을 갖고있다.

멀티 에이전트
단일 에이전트의 단점을 보완.
여러 개의 에이전트가 각 전문성있는 역할을 갖고 서로 협업을 해서 작업을 완성하도록 하는 것이 멀티 에이전트
에이전트 상호간 여러 번의 대화를 통해 더 고도화 된 답을 얻을 수 있다.

멀티 에이전트 3가지 유형
협업형 멀티 에이전트 유형 : 주로 CrewAI, AutoGen, langGraph 라는 것들이 있다. 에이전트 각각이 맡은 전문 영역(Tool)을 가지고 협업함.
감독형 멀티 에이전트 유형 : 에이전트들이 평등한 관계를 가지고 작업을 수행하는 것이 아니라 하나의 감독자 에이전트에게 보고하고 피드백 받아 작업을 진행하는 유형이다.
위계형 멀티 에이전트 유형 : 감독형과 큰 의미로는 동일하지만 좀 더 고도화되고 복잡한 구조로 되어있다. 조직규모가 더 커졌다고 보면 되겠다. 아키텍쳐를 보면 스타트업과 대기업의 조직규모 차이 처럼 보인다.