AI 8-9 문제

<8 주차>

1. 다음 중 Pre-training(사전 학습)의 특징으로 올바르지 않은 것은?
① Self-supervised learning을 사용한다.
② 다음 단어를 예측하며 언어 패턴을 학습한다.
③ 인간의 피드백을 통해 보상함수를 학습한다.
④ 방대한 인터넷 텍스트 데이터를 이용한다.

✅ 정답: ③
📘 해설: 인간 피드백 기반 학습은 Post-training의 RLHF 단계에 해당한다.

2. RLHF(Reinforcement Learning from Human Feedback)의 개념과 등장 배경을 설명하시오.

✅ 예시답안:
Instruction-tuning은 정답이 존재하는 지도학습 방식으로, 창의적 과제나 인간 선호를 반영하기 어렵다는 한계가 있다.
이를 보완하기 위해 RLHF가 등장하였으며, 이는 사람이 직접 점수를 매기지 않고 여러 모델 응답을 비교하여 '인간이 선호하는 답변'을 학습하는 보상모델(Reward Model)을 만들고, 이를 통해 언어모델을 강화학습으로 최적화하는 방식이다.
이 과정은 인간의 선호도를 반영해 모델의 안전성과 유용성을 높인다.

3. 아래의 설명 중 DPO(Direct Preference Optimization)에 대한 설명으로 올바른 것을 고르시오.

① RLHF의 보상함수를 강화학습으로 최적화한다.
② 인간의 선호 데이터를 직접 비교하여 강화학습 없이 최적화한다.
③ Self-supervised 방식으로 다음 단어를 예측한다.
④ 인간의 점수 대신 정답 레이블을 사용한다.

✅ 정답: ②

4. RAG(검색 증강 생성)에서 '검색 가능한 항목들을 체계적으로 정리해 더 쉽게 찾을 수 있도록 하는' 역할을 하며, 각 정보 검색 메서드가 활용하여 쿼리와 관련 있는 정보를 식별하게 하는 구성요소는 무엇입니까?

✅ **정답:** Index (또는 인덱스)

5. 다음 중 **Sparse Retriever(희소 검색기)**의 특징으로 가장 거리가 먼 것은 무엇입니까?

1. TF-IDF나 BM-25와 같은 특정 단어의 중요도를 나타내는 가중치 방식을 활용한다.
2. 문서 간의 정확한 용어 일치(어휘적 유사도)에 기반하여 검색을 수행한다.
3. 'bad guy'와 'villain'처럼 의미는 같지만 사용된 단어가 다른 경우에도 의미적 이해를 바탕으로 높은 관련성을 매칭시킨다.
4. 구현의 단순성과 높은 처리 효율성이 장점으로 꼽힌다.

✅ **정답:** 3번

해설: Sparse Retriever는 어휘적 유사도(정확한 용어 일치)에 기반하므로, 의미는 같으나 단어가 다른 경우(예: bad guy, villain)에는 매치가 어렵다는 단점이 있습니다. 이는 **Dense Retriever**의 특징에 해당합니다.

6. 거대 언어 모델(LLM)이 있음에도 불구하고 Retrieval-augmented Generation(RAG) 프레임워크를 사용하는 근본적인 이유를 제시된 내용에서 3가지 이상 서술하고, 이와 관련하여 DataStore의 역할이 기존 LLM의 한계를 어떻게 보완해 주는지 설명하시오.

✅ **핵심 서술 내용:**

1. **지식 저장 한계:** 거대 언어 모델은 모든 지식을 자신의 파라미터에 저장하지 못하며, 특히 자주 등장하지 않는 정보에 대해 큰 효과를 발휘하기 어렵다.
2. **정보의 최신성/갱신 문제:** 거대 언어 모델이 보유한 지식은 학습 시점 이후 금세 시대에 뒤처지며 갱신이 어렵다.
3. **해석 및 검증의 어려움/보안 문제:** 거대 언어 모델의 답변은 해석과 검증이 어려우며, 기업 내부 정보와 같은 보안 정보는 학습에 활용되지 못한다.

✅ **DataStore 역할:**

- DataStore는 가공되지 않은 대규모 텍스트 코퍼스로 구성되어 **쉽게 업데이트가 가능**하고 **확장성**을 만족한다.
- 이를 통해 LLM이 학습하지 못한 **최신 정보**나 **보안/내부 정보**를 검색하여 활용할 수 있게 해, LLM의 지식 한계를 보완하고 **더 정확하고 최신의 답변**을 생성할 수 있도록 돕는다.

7. Dense Retriever(DR) 아키텍처 중, 두 개의 텍스트를 하나의 시퀀스로 결합하여 self-attention을 통해 모든 쿼리와 문서 토큰이 완전히 상호 작용할 수 있어 높은 정확도를 가지지만, 모든 쿼리-문서 쌍을 개별적으로 모

델에 입력해야 해 계산 비용이 크고 처리 속도가 느리다는 단점이 있는 방식은 무엇입니까?

✅ **정답:** Cross-encoder (또는 크로스 인코더)

8. 다음 중 RAG(검색 증강 생성) 프레임워크의 도전 과제 및 한계점과 이를 극복하기 위한 능력으로 가장 적절하게 짝지어진 것은 무엇입니까?

1. 낮은 정확도 $\rightarrow$ Bi-encoder 아키텍처 사용
2. LLM 사전지식과의 충돌 $\rightarrow$ Negative Rejection 학습
3. **검색 노이즈에 취약함 (Hallucination)** $\rightarrow$ **Noise Robustness (노이즈 강건성)**
4. 높은 연산 비용 $\rightarrow$ Cross-encoder 아키텍처 사용

✅ **정답:** 3번

해설: RAG의 결과는 검색 노이즈에 취약하여 환각(Hallucination) 현상이 발생할 수 있습니다. 이를 극복하기 위해 외부 문서에 노이즈가 포함되어 있어도 올바른 답을 찾아내는 능력인 **Noise Robustness(노이즈 강건성)**를 강화해야 합니다.

9. 정보 검색(Information Retrieval)의 두 가지 주요 종류인 **Sparse Retriever**와 **Dense Retriever**의 핵심적인 검색 기반(유사도 기반)과 각각의 장점 및 단점 한 가지씩을 비교하여 서술하시오.

✅ **예시 모범 답안:**

- **Sparse Retriever**
  - **핵심 검색 기반:** 어휘적 유사도 (정확한 용어 일치, TF-IDF/BM-25 등)
  - **장점:** 구현의 단순성과 **효율성**이 높음.
  - **단점:** **제한된 의미 이해**로 인해 동의어나 의미 기반 검색이 어려움.
- **Dense Retriever**
  - **핵심 검색 기반:** 의미적 유사도 (Dense Vector/Embedding 활용)
  - **장점:** 단어가 달라도 문맥을 파악하는 **의미적 이해**가 가능.
  - **단점:** 모든 임베딩 비교로 인해 **높은 연산 비용**이 발생함.

10. 다음 중 **LLM Agent**에 대한 설명으로 옳지 않은 것은?

A. LLM Agent는 거대언어모델을 중심으로 환경을 이해하고 행동을 수행하는 인공지능이다.

B. LLM Agent는 반드시 로봇 형태로 구현되어야 하며 물리적 센서와 액추에이터가 필요하다.

C. LLM Agent는 텍스트 기반 환경에서도 동작할 수 있다.

D. LLM Agent는 언어를 통해 추론, 계획, 상호작용이 가능하다.

✅ 정답: B

🔷 설명: 로봇 형태일 수도 있지만 필수는 아님. 텍스트 환경에서도 충분히 에이전트로 작동함 (예: ChatGPT, Code Agent).

11. 다음 중 Tool Learning 방식에 해당하지 않는 것은?

A. 모방학습 (Imitation Learning)

B. 지도학습 (Supervised fine-tuning)

C. 강화학습 (Reinforcement Learning)

D. 비지도 군집화 (Unsupervised Clustering)

✅ 정답: D

🔷 설명: Tool Learning은 주로 모방, 지도, 강화학습을 활용하며, 비지도 군집화는 사용되지 않음.

12. 다음 문장을 완성하시오.

“WebGPT는 (_____) 학습을 기반으로 사람의 검색 행동을 모방하며,

(_____) 학습을 통해 답변 품질을 개선한다.”

✅ 정답:

“**모방(Imitation)** 학습”, “**강화(Reinforcement)** 학습”

🔷 WebGPT는 모방학습으로 웹 검색 행동을 배우고, RLHF로 성능을 향상시킴.

13. MCP (Model Context Protocol)**의 구조와 장점을 서술하시오.

✅ 예시 답안:

MCP는 언어모델이 외부 툴과 상호작용하기 위한 **표준화된 프로토콜**이다.

구조:

- **MCP Host:** 여러 클라이언트를 관리하는 AI 애플리케이션
- **MCP Client:** 서버와 연결하여 컨텍스트를 전달
- **MCP Server:** 클라이언트에게 컨텍스트를 제공

계층:

- **데이터 계층:** JSON-RPC 기반으로 툴, 리소스, 프롬프트 관리
- **전송 계층:** 메시지 전송, 연결, 인증 관리

장점: 표준화, 확장성, 호환성, 재사용성, 투명성 확보로 다양한 모델이 동일한 도구를 사용할 수 있다.

14. 다음 중 LLM 에이전트가 복잡한 환경에 대한 이해를 높이기 위한 방법론이 아닌 것은?

a) 환경 탐색 (Environment Exploration)을 통해 보상(reward)을 부여하여 학습을 유도한다. b) 탐색 기반 궤적 기억 (Exploration-based Trajectory Memorization)을 사용하여 지시를 재정제한다. c) 모든 필요한 지식을 LLM 파라미터 안에 포함시켜 이해를 완료한다. d) 실시간으로 환경과의 상호작용을 통해 새로운 지식을 발견한다.

✅ 정답: c)해설: 모델은 자신이 상호 작용하는 환경에 대해 모든 것을 알고 있지 않으며 , 일부 지식은 LLM 파라미터에 포함되어 있지만 , 다른 지식은 실시간으로 환경과의 상호 작용을 통해 발견해야 합니다. 따라서 모든 지식을 파라미터 안에 포함한다는 것은 현실적으로 어렵고 에이전트의 학습 방향과도 맞지 않습니다.

15. Plan-and-Solve Prompting (Wang et al, 2023)과 관련이 있으며 , 실행 가능한 전체 계획 경로(planning path)를 한 번에 생성하지만 복잡한 환경에서 실패할 가능성이 있는 계획 종류는?

a) 국소적 계획 (Local Planning) b) 탐색 기반 궤적 기억 (Exploration-based Trajectory Memorization) c) 전역적 계획 (Global Planning) d) 오류 식별과 회복 (Error identification and Recovery)

✅ 정답: c)

해설: **전역적 계획 (Global Planning)**은 실행 가능한 전체 계획 경로를 한 번에 생성하고 , 여러 개의 툴을 조합하여 시퀀스 형태로 결정하는 방식입니다. 효율적이지만 복잡한 환경에서는 실패할 가능성이 있습니다.

16. Langchain에 대한 설명으로 옳지 않은 것은?

a) LLM 기반 애플리케이션을 빠르게 개발할 수 있도록 돕는 오픈 소스 프레임워크이다. b) LLM을 다양한 데이터 및 툴과 연결하여 강력한 애플리케이션 개발을 가능하게 한다. c) 특정 모델만을 지원하며, 다른 LLM Provider와는 독립된 인터페이스로 관리한다. d) Prompt, Memory, Tools와 같은 컴포넌트들이 모듈화 되어 재사용성과 확장성을 확보한다.

✅ 정답: c)해설: Langchain은 다양한 LLM provider(OpenAI, Anthropic, Google 등)와 통합하여 모델/회사별 API 차이를 공통 인터페이스로 관리할 수 있습니다. 특정 회사 모델만 지원하는 것이 아닙니다.

17. Langchain의 주요 컴포넌트 중, 사용자 요청을 수행하기 위해 필요한 툴(Tool)을 동적으로 선택 및 실행하는 역할을 담당하는 것은?

a) Memory b) Agents c) Prompt Templates d) Chains

✅ 정답: b)해설: Agents는 동적으로 툴을 선택하고 실행하는 역할을 하며 , Chains는 여러 단계를 연결한 워크플로우를 의미합니다. Memory는 대화 히스토리와 상태를 유지합니다.

<9 주차>

1. 다음 중 2의 보수 표현 방식에 대한 설명으로 *옳지 않은 것*은 무엇인가?

① 음수를 표현할 때 절댓값을 이진수로 쓰고, 모든 비트를 반전한 뒤 1을 더한다.② 부호 비트는 최상위 비트(MSB)이며, 0은 양수, 1은 음수를 의미한다.③ 2의 보수를 사용하면 기존 덧셈 연산기가 정상적으로 작동하지 않는다.④ 가장 큰 4비트 수는 0111(=+7), 가장 작은 4비트 수는 1000(=-8)이다.

✅ **정답:** ③

2. 다음 설명을 보고 해당하는 개념을 서술하시오.

“부동소수점 수에서 지수를 항상 양수로 표현하기 위해,실제 지수에 일정한 상수값을 더해 저장하는 방식이다.이렇게 하면 음수 지수를 없애고 지수 비교를 단순화할 수 있다.”

✅ **정답 예시:** 바이어스 지수 (Biased Exponent)

3. 다음 중 IEEE 754 단정밀도 부동소수점 포맷에 대한 설명으로 옳은 것을 고르시오.

① 총 32비트로 구성되며, 1비트는 지수, 8비트는 가수, 23비트는 부호이다.② 지수는 bias=255를 적용하며, E=0은 무한대(∞)를 의미한다.③ 가수는 항상 0.xxx 형태로 저장하며, hidden bit를 사용하지 않는다.④ E=255일 때 f=0이면 ±∞, f≠0이면 NaN(Not a Number)이다.

✅ **정답:** ④

4. 양자화(Quantization) 기법 중, 학습 단계에서부터 forward pass quantization을 함께 수행하여 동일 정확도 기준 더 높은 압축률을 얻을

수 있지만, 모델과 학습 데이터가 너무 클 경우에는 적용이 어렵고 학습 복잡도가 크게 상승하는 방식은 무엇입니까?

✅ **정답:** QAT (Quantization-Aware Training)

5. 다음 모델 경량화 기법 중 제공된 자료에서 **'GPU와 궁합이 좋지 않은 기법'**으로 분류되어 전용 가속기(NPU)에서의 효과 극대화가 필요하다고 언급된 것을 모두 고른 것은 무엇입니까?

1. Low-rank adaption (LoRA), Knowledge distillation
2. Quantized low-rank adaption (QLoRA), Structured pruning
3. Knowledge distillation, Structured pruning
4. **Aggressive quantization, Unstructured/partially-structured pruning**

✅ **정답:** 4번

해설: 자료에 따르면 Low-rank adaption (LoRA), QLoRA, Structured pruning, Knowledge distillation 등은 GPU와 궁합이 좋은 기법으로 분류되거나 GPU와 직접적인 호환성 문제보다는 학습 방법에 중점을 둡니다. 반면, Aggressive quantization(극단적인 양자화)이나 Unstructured pruning(비구조적 가지치기)은 GPU가 감당하기 어려운 패턴을 형성하여 전용 가속기가 필요합니다.

6. 양자화(Quantization) 기법 중 **QAT(Quantization-aware training)**와 **PTQ(Post-training quantization)**를 비교 설명하시오. 특히 두 방식이 모델 경량화 과정에서 **학습 데이터의 필요 여부**와 **대규모 모델(LLM)에 적용될 때의 현실적인 제약** 측면에서 어떤 차이를 보이는지 중심으로 서술하시오.

✅ **예시 모범 답안:**

1. **학습 데이터 필요 여부 및 과정:**
   - **QAT**는 모델의 **학습 단계**에서 forward pass quantization을 함께 수행하므로 **학습 데이터**가 반드시 필요하다.
   - **PTQ**는 **사전 학습된 모델**을 바탕으로 양자화를 바로 수행하며, 전체 학습 데이터 대신 양자화 효율을 높이기 위한 **적절한 calibration 데이터**만을 사용한다.
2. **대규모 모델(LLM) 적용 시 제약:**
   - **QAT**는 학습 복잡도가 엄청나게 상승하기 때문에 모델 및 학습 데이터가 너무 큰 LLM에는 **사용이 현실적으로 불가**하다.

- **PTQ**는 사전 학습 모델에 바로 적용할 수 있어, LLM과 같이 학습 데이터 크기가 방대한 모델의 경량화를 위한 **현실적인 옵션**으로 고려된다.

7. 모델 경량화의 세 가지 주요 기법인 양자화(Quantization), 가지치기(Pruning), 지식 증류(Knowledge Distillation) 각각이 모델의 크기나 효율성을 높이기 위해 수행하는 기본 원리를 한 문장씩 간략하게 설명하시오.

✅ **예시 모범 답안:**

- **양자화(Quantization):** 연산 및 메모리 부하를 줄이기 위해 모델 가중치와 활성화 값의 **정밀도를 축소**합니다.
- **가지치기(Pruning):** 모델의 정확도에 기여도가 적은 **불필요한 가중치(weight)를 제거**하여 모델 크기를 줄입니다.
- **지식 증류(Knowledge Distillation):** 큰 모델(Teacher)의 학습된 지식을 **작은 모델(Student)에게 전수**하여, 작은 모델이 큰 모델과 비슷한 성능을 내도록 만듭니다.

8. Full Fine Tuning을 사용하여 대규모 언어 모델(LLM)을 특정 도메인에 특화시킬 때 발생하는 주요 단점으로 가장 거리가 먼 것은 무엇입니까?

1. 원본 모델의 모든 가중치(weight)를 갱신해야 하므로 학습 비용과 메모리 사용량이 매우 높다.
2. 원본 모델의 가중치 자체가 변화하는 과정에서 기존에 학습했던 일반적인 정보가 망각될 수 있다.
3. 파라미터 효율적 파인 튜닝(PEFT)에 비해 도메인 특화 관점에서 Accuracy 이득을 기대하기 어렵다.
4. 사실상 처음부터 새로 학습하는 것에 준하는 컴퓨팅 리소스가 요구될 수 있다.

✅ **정답:** 3번

해설: Full Fine Tuning은 처음부터 새로 학습하는 것에 비해 **적은 데이터만 활용해도** 도메인에 특화될 수 있으며, 도메인 특화 관점에서는 **Accuracy 이득을 기대할 수 있다**는 것이 장점으로 제시됩니다. 따라서 Accuracy 이득을 기대하기 어렵다는 것은 사실과 다릅니다.

9. 대규모 언어 모델(LLM)을 도메인 특화시키는 과정에서 **파라미터 효율적 파인 튜닝(PEFT)**이 등장하게 된 근본적인 배경이 된 Full Fine Tuning의 단점 2가지 이상을 제시하고, PEFT 기법 중 하나인 **LoRA(Low-Rank Adaptation)**가 모델을 특화시키기 위해 어떤 방식으로 학습을 수행하는지 그 원리를 간략히 설명하시오.

✅ **예시 모범 답안:**

1. Full Fine Tuning의 단점 (2가지 이상):

- 원본 모델의 크기가 크기 때문에 모든 가중치(weight)를 갱신하는 데 필요한 **학습 비용**이 매우 부담됩니다.
- 모든 가중치를 갱신해야 하므로 **메모리 사용량** 관점에서 사실상 처음부터 학습하는 수준이 요구됩니다.
- 원본 모델의 가중치 자체가 변화하는 과정에서 이전에 학습했던 **기존 학습 정보의 망각**이 일어날 수 있습니다.

2. LoRA의 원리:

- LoRA는 원본 모델의 **전체 가중치를 전부 갱신하지 않기 위해** 등장했습니다.
- LoRA는 원본 모델의 **특정 가중치 매트릭스**를 고정하고, 해당 매트릭스에 **low-rank update를 위한 추가 가중치**만을 추가합니다.
- 이후 도메인 특화 데이터로 **추가된 low-rank weight만 학습**하여 튜닝 작업을 지원함으로써, Full Fine Tuning보다 훨씬 적은 비용으로 높은 표현력을 달성합니다.