

Paper Review: 초거대 언어모델 연구 동향

[박찬준, 이원성, 김윤기, 김지후, 이활석. \(2023\). 초거대 언어모델 연구 동향. 정보과학회지, 41\(11\), 8-24.](#)

LEAD기술Task 김기수 연구원

참고 논문

초거대 언어모델 연구 동향

Survey on Large Language Models

저널정보

한국정보과학회

정보과학회지 | 학술저널

정보과학회지 제41권 제11호(통권 제414호)

2023.11 | 8 - 24 (17page)

저자정보

박찬준 (업스테이지)

이원성 (업스테이지)

김윤기 (업스테이지)

김지후 (업스테이지)

이활석 (업스테이지)



이용수 1,157 내서재 55

목차

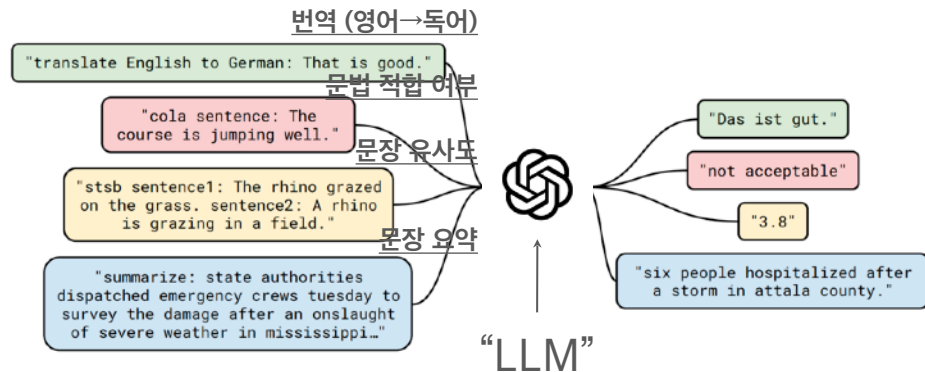
1. 초거대 언어모델 (LLM, Large Language Model)
2. 언어모델 (LM, Language Model) 의 연구 및 발전 과정
3. 최신 **LLM 연구 동향**
4. LLM의 성능 평가 동향
5. LLM 연구와 활용에 대한 **윤리적 원칙 동향**

초거대 언어모델 (LLM, Large Language Model)

초거대 언어모델 (LLM)

- 이전에는 자연어 처리 Task (번역, 요약, 문장 분류 등) 마다 개별 모델이 필요했음
- 이제 **하나의 LLM로 다양한 작업 (+ 질의 응답, 형태소 분석 등)** 을 모두 처리할 수 있게 됨
- LLM 발전의 요인
 - a) 데이터의 양적 확대
 - b) 컴퓨팅 기술의 진보 (GPU/TPU 등 고성능 병렬 처리 HW의 개발로 병목 현상 완화)
 - c) 알고리즘 및 기술의 발전 (Attention mechanism과 Transformer)

문맥 간의 관계를 정교하게 모델링할 수 있는 방법을 제공



분야별 LLM의 활용 가능성

	활용 가능성
교육	<ul style="list-style-type: none">● <u>개인화된</u> 학습 경로 추천● 과제 자동 평가 시스템● 복잡한 질문에 대한 답변 제공
의료	<ul style="list-style-type: none">● 환자 데이터 기반 <u>초기 진단</u> 도구● 복잡한 의료 기록 분석● 신약 개발에 필요한 연구 데이터 분석
금융	<ul style="list-style-type: none">● 개인 투자 성향 및 시장 동향을 분석하여 <u>맞춤 투자</u> 권고● 금융 <u>위험 분석</u> 및 복잡 금융 거래 자동화
제조	<ul style="list-style-type: none">● 설계, 생산, 품질 관리 등 전 과정에서 <u>데이터 분석</u> 및 <u>최적화</u> 도구

LLM의 한계점

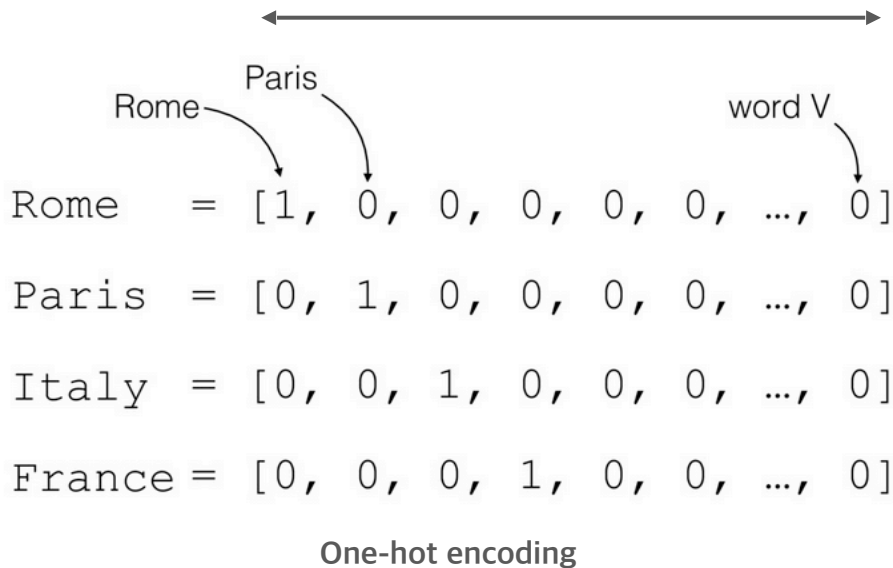
한계점	설명
편향성	학습 데이터의 편향성을 그대로 반영되어, 편향된 결과 또는 추천을 제공할 수 있음.
안전성	LLM을 가짜 뉴스 및 편향된 정보 전파를 위한 도구로 활용할 수 있음
설명 가능성	LLM이 실제로 어떻게 동작하는지, 출력 결과에 대한 설명력이 부족하다.
최신성	LLM은 최신 정보를 반영하기 어려움

언어모델 (LM, Language Model) 의 연구 및 발전 과정

[1] 전통적인 언어모델 연구

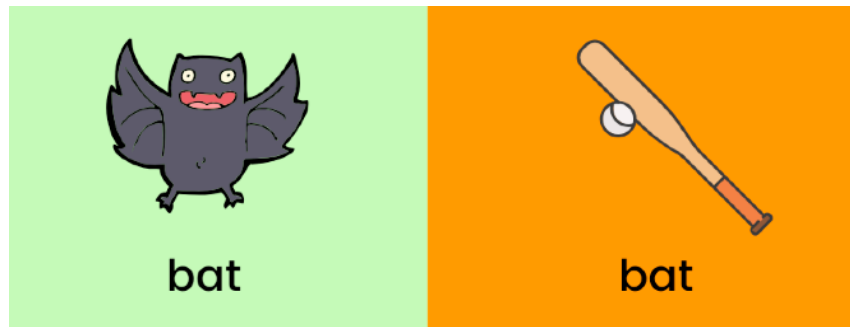
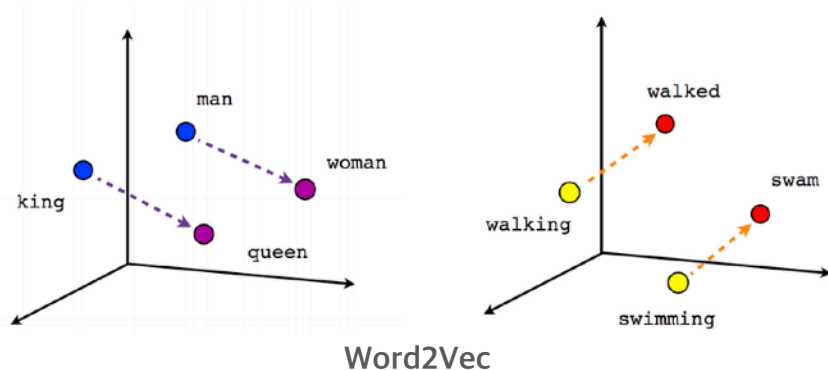
- 인간이 사용하는 단어를 컴퓨터가 이해할 수 있는 숫자 체계로 변환하는 데에 초점
- 단어 집합 (Vocabulary) 을 생성/활용하여 자연어를 표현 → 원-핫 인코딩 (One-hot encoding)
- 원-핫 인코딩의 한계
 - 희소 벡터 (Sparse Vector)
 - 단어 간의 의미적인 연관성을 고려할 수 없음

단어 집합의 크기가 N인 경우, 집합 내 단어를 길이가 N인 벡터로 표현할 수 있다



[2] 의미기반 언어모델 연구

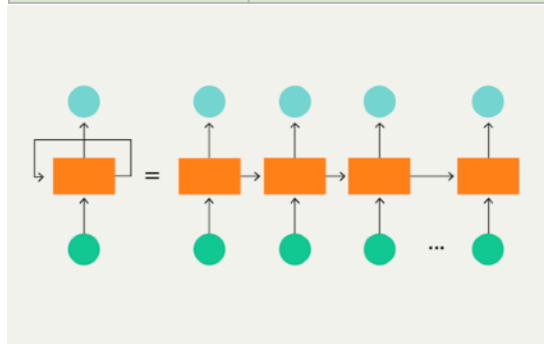
- 단어의 의미가 반영되도록 **밀집 벡터** (Dense Vector) 공간에 표현 → Word2Vec
- 주변 단어로부터 중심 단어를 예측하거나 중심 단어로 주변 단어들을 예측하여, **유사한 의미의 단어들이 서로 가까운 거리에 분포하도록 학습**
- 한계
 - 동음이의어 (사과; apple 또는 apology)
 - 같은 문자임에도 사용되는 문맥에 따라 다른 의미를 지닐 수 있지만, 같은 문자는 같은 밀집 벡터로 표현됨 (문맥 정보를 이해하지 못함)



동음이의어

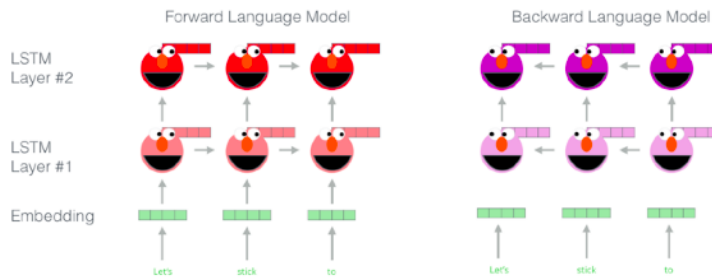
[3] 문맥기반 언어모델 연구: RNN

	특징
LSTM / GRU	텍스트 길이가 길어질수록 처음 정보를 기억하지 못하는 RNN (Recurrent Neural Network) 의 장기 의존성 문제를 해결했으나, 단방향 문맥 정보만 활용하는 한계
ELMo	순방향 (좌→우) 과 역방향 (좌←우) 문맥 정보를 모두 활용하지만, 하나의 벡터에 텍스트의 모든 정보를 담게 되어 정보 손실 발생



RNN-based Model

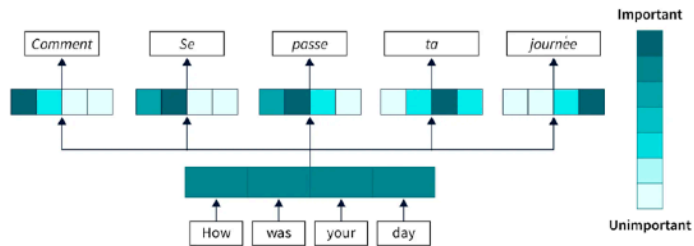
Embedding of "stick" in "Let's stick to" - Step #1



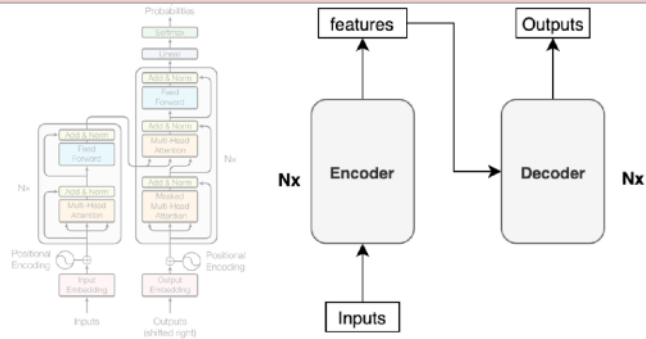
ELMo (Embeddings from Language Model)

[3] 문맥기반 언어모델 연구: Attention 매커니즘

	특징
Transformer	<p>텍스트 내 단어 벡터들을 적절히 활용하는 Attention 매커니즘 기반의 인코더-디코더 구조</p> <ul style="list-style-type: none">● 인코더 (Encoder) 는 주어진 텍스트를 이해하는 역할● 디코더 (Decoder) 는 이해한 텍스트를 기반으로 언어를 생성해내는 역할



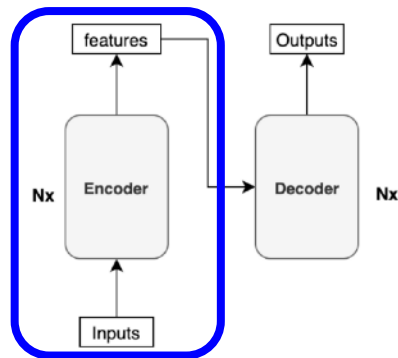
Attention 매커니즘의 예시 (영불 번역)



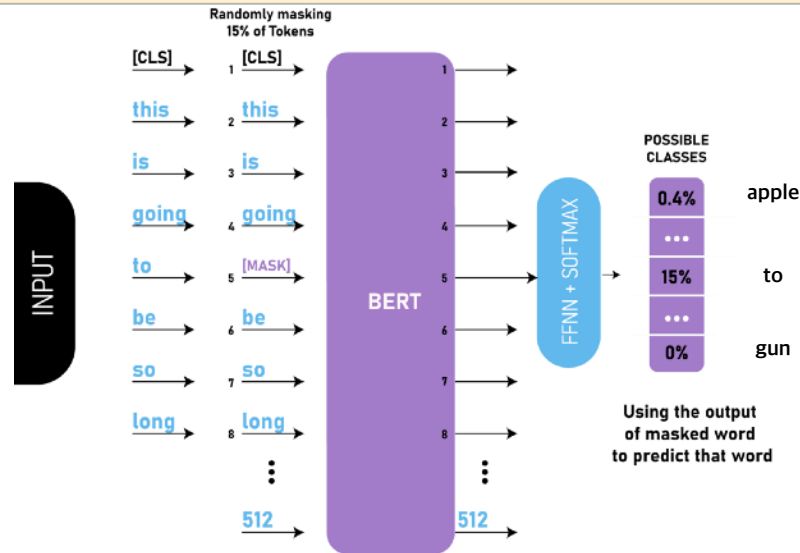
인코더-디코더 구조

[3] 문맥기반 언어모델 연구: Transformer 기반

	특징
BERT	입력 텍스트 일부에 있는 <u>토큰을 임의로 마스킹한 뒤 해당 토큰을 맞추는 방식</u> 으로 학습 (Encoder)



인코더-디코더 구조

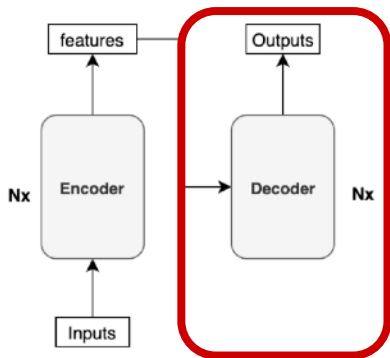


MLM (Masked Language Modeling) 학습 방식

[3] 문맥기반 언어모델 연구: Transformer 기반

	특징
GPT	이전 텍스트를 기반으로 <u>다음에 나올 토큰이 무엇인지 예측</u> 하는 방식으로 학습 (Decoder)

Text: Second Law of Robotics: A robot must obey the orders given it by human beings



인코더-디코더 구조

Generated training examples

Example #	Input (features)	Correct output (labels)
1	Second law of robotics :	a
2	Second law of robotics : a	robot
3	Second law of robotics : a robot	must

NTS (Next Token Prediction) 학습 방식

[3] 문맥기반 언어모델 연구: Transformer 기반

	특징
BERT	입력 텍스트 일부에 있는 <u>토큰을 임의로 마스킹한 뒤 해당 토큰을 맞추는</u> 방식으로 학습 (Encoder)
GPT	이전 텍스트를 기반으로 <u>다음에 나올 토큰이 무엇인지 예측</u> 하는 방식으로 학습 (Decoder)

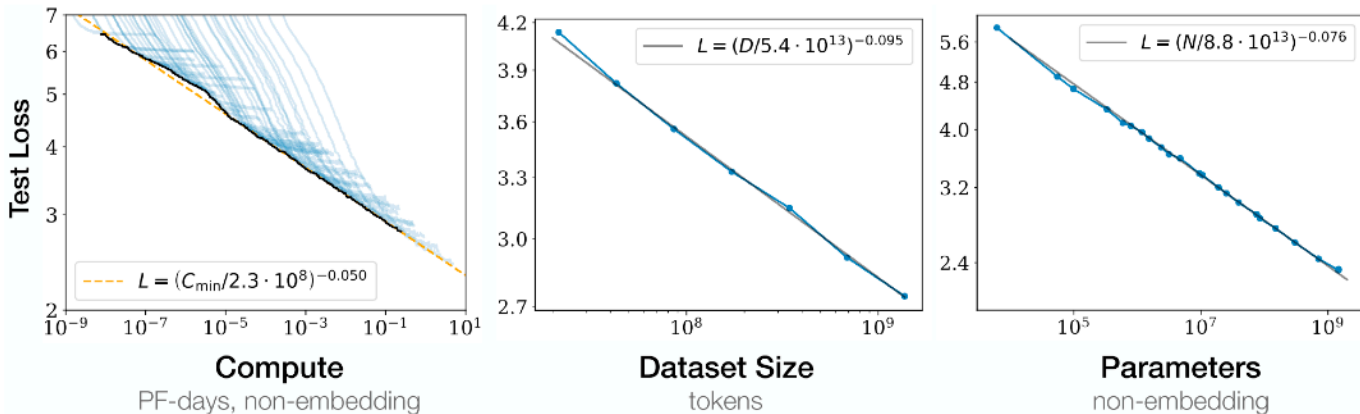
Transformer 기반 언어 모델 정리

- **별도의 Labeling 작업이 없어도** 텍스트 데이터만 있으면 학습이 가능하다 (Self-supervised Learning)
- 대용량의 텍스트 데이터로 **사전학습 (Pretraining)** 하고, 이후 특정 태스크로 **미세조정 (Finetuning)** 하는
Pretrain-Finetune 패러다임 중심으로 발전

[4] 초거대 언어모델 (LLM) 연구: 등장 배경

Scaling Law (규모의 법칙)

- 모델 사이즈 (#Parameters) 또는 학습 데이터 크기 (Datasize) 는 모델의 성능과 양의 상관관계를 보인다.



연산량, 데이터 크기, 모델 매개변수 수에 따른 모델의 Test Loss 변화

[4] LLM 연구: 기존 언어모델과의 차이점

Emergent ability (창발 능력)

- 작은 크기의 언어 모델에서는 발현되지 않는 능력
- In-context Learning (ICL)
 - 모델의 가중치 업데이트 없이도 새로운 태스크를 수행할 수 있는 능력을 가진다.
- ICL의 종류
 - Zero-shot (지시 사항만 가지고 답 예측)
 - One-shot (한 가지 예시를 가지고 답 예측)
 - Few-shot (여러 예시를 가지고 답 예측)

Zero-shot

The model predicts the answer given only a natural language description of the task. No gradient updates are performed.

```
1 Translate English to French: ← task description
2 cheese => ..... ← prompt
```

One-shot

In addition to the task description, the model sees a single example of the task. No gradient updates are performed.

```
1 Translate English to French: ← task description
2 sea otter => loutre de mer ← example
3 cheese => ..... ← prompt
```

Few-shot

In addition to the task description, the model sees a few examples of the task. No gradient updates are performed.

```
1 Translate English to French: ← task description
2 sea otter => loutre de mer ← examples
3 peppermint => menthe poivrée ←
4 plush girafe => girafe peluche ←
5 cheese => ..... ← prompt
```

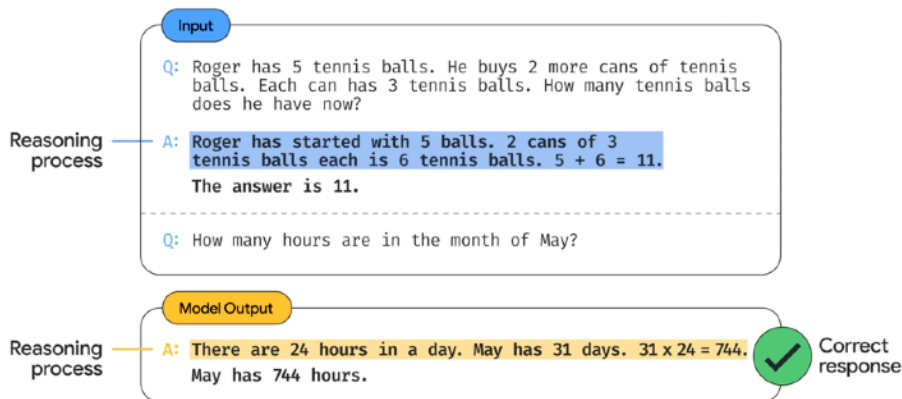
In-context Learning 방식

[4] LLM 연구: 프롬프트 엔지니어링

LLM이 모델 가중치를 업데이트 없이 특정 태스크를 잘 해결하도록, 입력 Prompt를 어떻게 설계할 것인지에 대한 연구

- Chain-of-Thought (CoT)

- 해결하고자 하는 태스크의 예시를 일련의 중간 추론 단계와 함께 투입
- 복잡한 문제를 여러 단계에 나누어 해결하는 프롬프트 방식 제안



CoT 방식 예시

최신 LLM 연구 동향

Overview

1. 사전학습 (Pretraining)

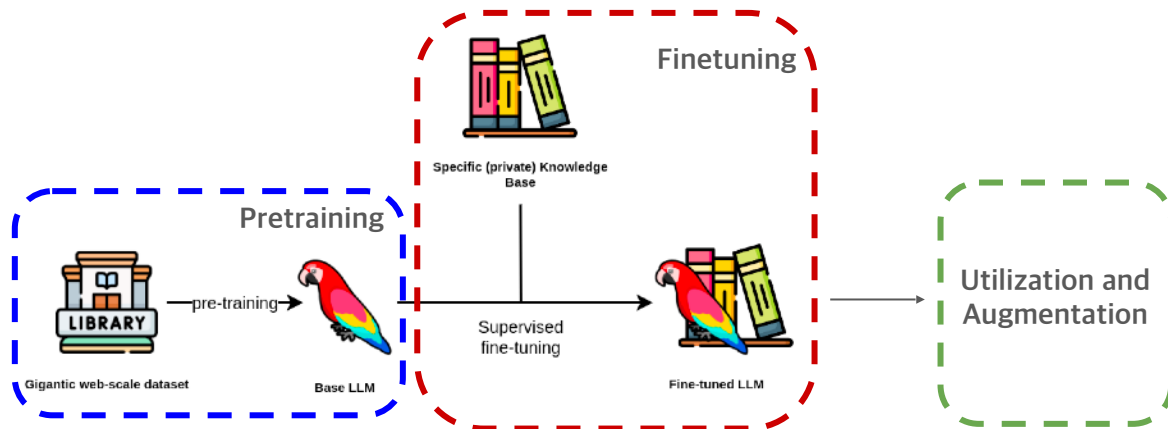
- 대규모 데이터를 학습하여 다양한 하위 태스크에 접목할 수 있는 기반 모델로서의 LLM 개발

2. 미세조정 (Finetuning)

- 하위 태스크를 잘 풀기 위한 목적으로 도메인/태스크 별로 적응시키거나 사람이 기대하는 바와 일치

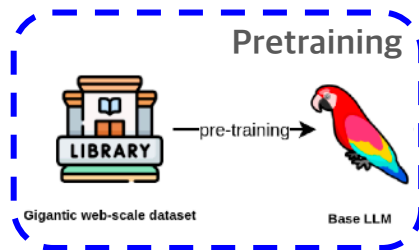
3. 활용 및 증강 (Utilization and Augmentation)

- 다양한 LLM 활용 방안과 내재적인 한계인 환각 (Hallucination) 현상을 개선/해결하는 증강 전략



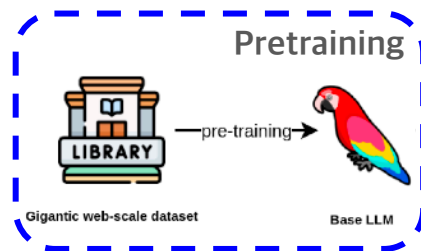
[1] 사전학습: 데이터 선정

- 대량의 코퍼스 (Corpus; 말뭉치) 및 컴퓨팅 자원을 활용하여
언어 생성 및 문맥 이해 능력 등을 모델에 학습시켜 LLM의 근간을 형성하는 과정
- 기존 언어모델 대비 높은 문맥 이해력, 상식, 기호, 논리 추리 능력을 갖추



특징	사례
웹페이지, 책, 대화 데이터, 학술 데이터, 코드 등 다양한 종류의 이질적인 코퍼스를 혼합 (데이터 품질과 더불어 다양성 또한 LLM 성능 향상에 중요)	Google T5: 웹페이지 OpenAI GPT-3: 웹페이지, 책, 뉴스 Meta Llama-1 65B: <ul style="list-style-type: none">● 웹페이지 (87%)● 기타 (13%, 대화, 학술 데이터, 코드, 책, 뉴스 등)
하위 태스크에 특화된 LLM 사전학습을 위해 관련 코퍼스의 비중을 증가	Google LaMDA (대화 특화): 데이터 중 50%를 대화로 구성 <ul style="list-style-type: none">● 교육 및 콘텐츠 추천 영역에서 효용성 입증 BLOOM, PaLM (다국어 특화): 영어 이외의 다국어 텍스트 활용 <ul style="list-style-type: none">● 다국어 기반 번역, 요약, 질의응답 태스크에서 높은 성능 Galactica (과학 도메인 특화): 데이터 중 86%를 과학 데이터 AlphaCode (코드 생성 특화): 전체 데이터를 코드 데이터

[1] 사전학습: 데이터 전처리

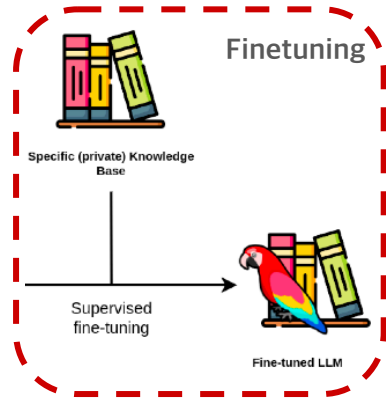


- 수집 데이터를 그대로 사용할 경우 용량, 노이즈, 중복, 독성 데이터 이슈로 문제가 발생할 수 있다.
- 전처리 과정은 **품질 필터링, 중복 제거, 개인정보 제거, 토큰화** 단계로 구성

단계	의미	설명
품질 필터링	수집된 데이터로부터 저품질 데이터를 걸러냄	<ul style="list-style-type: none">● 고품질 텍스트 데이터로 학습된 분류기로 저품질 데이터를 필터링● 정교하게 디자인 된 규칙 (휴리스틱) 기반 필터링
중복 제거	LLM 성능을 저해하는 중복 데이터 제거	<ul style="list-style-type: none">● 반복되는 단어를 갖는 저품질 문장 제거● 단어 및 N-gram 기반 겹침 비율을 계산하여 유사 내용 문서 필터링● 학습 데이터와 평가 데이터 간 중복 제거 (Data Leakage 방지)
개인정보 제거	이메일 주소, 전화번호 등 민감 정보 제거	<ul style="list-style-type: none">● 정교한 프롬프팅으로 개인 식별 정보나 API Key 같은 민감 정보 추출● LLM의 윤리적 사용과 개인정보 침해 위험 방지를 위해 필수 사항
토큰화	원본 텍스트를, 토큰 단위의 시퀀스로 분리	<ul style="list-style-type: none">● LLM뿐만 아니라 전통적인 자연어 처리 태스크에서도 중요 연구 분야● 현재도 컴퓨팅 비용, 언어 의존성, 정보 손실 등을 고려한 토큰화 연구 중

[2] 미세조정

- 사전학습된 LLM을 특정 목적에 맞게 미세조정 (Fine-tuning) 하는 경우가 많다.
- 대표적인 미세조정 전략

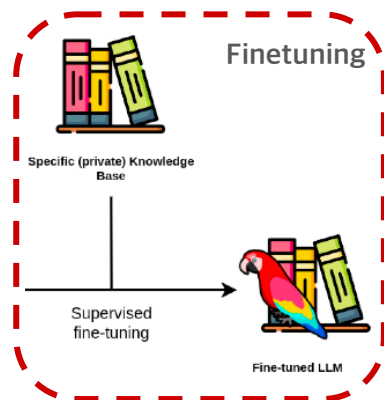


전략	설명
Instruction Tuning	기존에 본 적 없는 태스크에 대한 LLM의 일반화 능력을 향상시키는 접근법
Alignment Tuning	인간의 가치와 기준에 부합하도록 LLM의 출력을 조정하는 접근법
Resource-efficient Tuning	계산 집약적 (엄청난 리소스) 한계를 개선하기 위한 자원 효율적 접근법

[2] 미세조정: Instruction Tuning

사전학습된 LLM에 **지시사항-출력** 데이터를 기반으로 미세조정하는 추가 훈련 과정

자연어로 포매팅된 지시사항 (Instruction) 과 대응되는 출력 (Output) 으로 구성

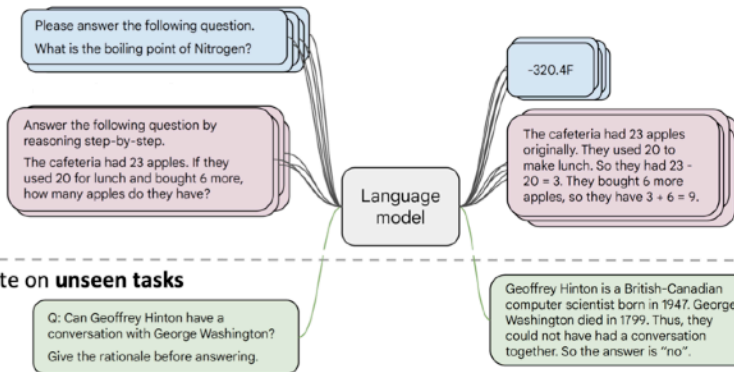


Instruction Tuning의 특징

1. 비교적 적은 수의 예제 (Example) 로 성능 향상과 새로운 태스크에 대한 일반화가 가능한 효율적 학습
2. 예제의 갯수보다 지시사항의 다양성과 품질이 중요
3. 도메인 특화된 데이터셋을 활용하여 일반 LLM을 의학, 법률, 금융 등 특정 분야의 전문가로 학습

Instruction finetuning

- **Collect examples** of (instruction, output) pairs across many tasks and finetune an LM



- **Evaluate on unseen tasks**

Instruction finetuning의 예시

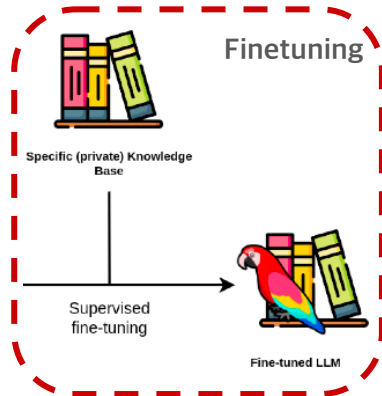
[2] 미세조정: Alignment Tuning

LLM의 의도치 않은 행동을 방지하기 위한 방법론

- LLM의 사전학습 방식은 주로 **MLM (마스킹된 토큰 예측)** 또는 **NTP (다음 토큰 예측)**
 - 학습 과정에서 인간의 선호가 반영되지 않음
 - 종종 유해한 (또는 잘못된) 정보를 제공하거나 편향된 표현을 생성

Alignment Tuning 전략

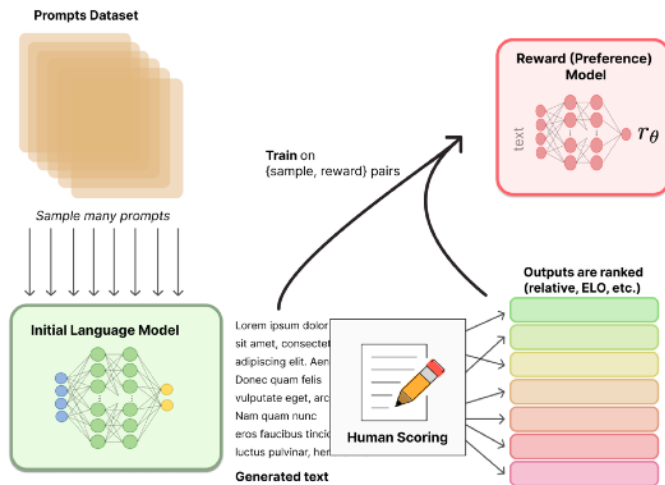
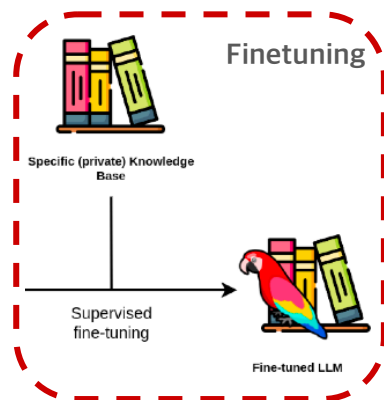
1. Human Alignment
 - 주관적 형태의 기준 (도움이 되는지, 정직한지, 무해한지 등) 을 측정하여 인간의 기대치에 맞게 조정
 - 고품질의 Human Feedback이 필수적이라 상대적으로 많은 비용이 소모되며, 최적화하기 어려움
2. RLHF (Reinforcement Learning from Human Feedback; 사용자 피드백을 활용한 강화학습)



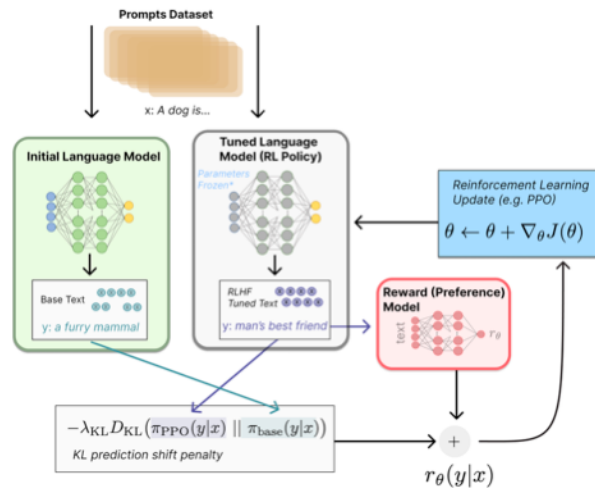
[2] 미세조정: Alignment Tuning (RLHF)

인간의 피드백을 바탕으로 강화학습 기반의 보상 모델을 활용하여 LLM을 미세조정

- 편향성이 적고 안전한 내용을 생성할 수 있다.
- Alignment tax (Alignment 과정에서 LLM 능력이 일정 부분 감소될 수 있음)



사람의 선호도를 수치화하는 보상 모델 학습



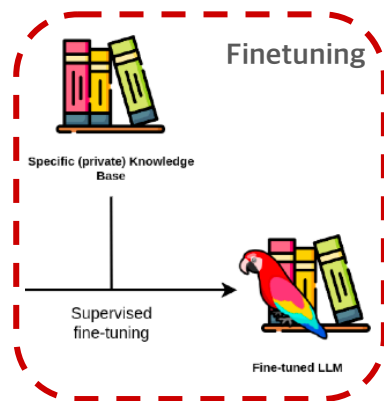
강화학습을 활용한 미세조정

[2] 미세조정: Resource-efficient Tuning

LLM의 수많은 모델 파라미터를 모두 미세조정하는 것은 비효율적.

가능한 한 좋은 성능을 유지하면서 학습가능한 파라미터의 수를 감소시키는 방식

→ PEFT: Parameter-Efficient Fine-Tuning



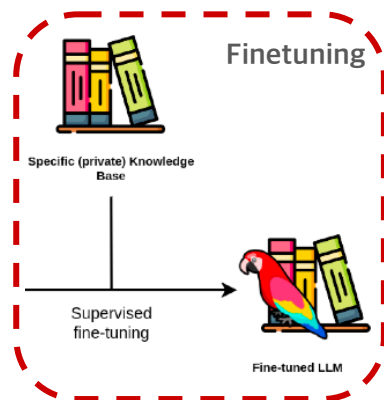
전략	설명
Adapter Tuning	<ul style="list-style-type: none">● Transformer 구조에 작은 신경망 모듈 (Adapter) 을 추가● <u>LLM 모델 파라미터는 고정되고 Adapter의 파라미터만 특정 태스크에 최적화</u>
Prefix Tuning	<ul style="list-style-type: none">● 학습 가능한 연속 벡터로 구성된 Prefix 시퀀스를 Transformer 각 레이어에 추가● <u>기존 파라미터는 고정되고 Prefix 벡터 (파라미터) 만 학습됨</u>
Prompt Tuning	<ul style="list-style-type: none">● 학습 가능한 프롬프트 벡터를 입력 계층에 추가● 학습 과정에서 프롬프트 임베딩만 최적화됨

[2] 미세조정: Resource-efficient Tuning

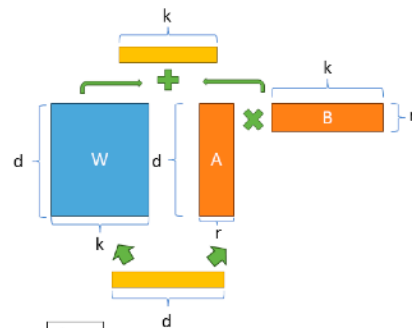
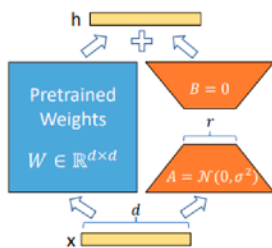
LLM의 수많은 모델 파라미터를 모두 미세조정하는 것은 비효율적.

가능한 한 좋은 성능을 유지하면서 학습가능한 파라미터의 수를 감소시키는 방식

→ PEFT: Parameter-Efficient Fine-Tuning



전략	설명
LoRA (Low-Rank Adaptation)	<ul style="list-style-type: none">행렬 분해 (Matrix Decomposition) 를 활용원래 파라미터 행렬은 고정하고, 업데이트 행렬을 분해 및 근사하여 메모리 절약



[3] 활용 및 증강: 적절한 프롬프팅 활용

In-context Learning (ICL)

- 시연 형태의 몇 가지 예시만으로 언어 모델이 태스크를 학습
- 장점
 - a. 자연어 형태로 제공되므로, 명확하고 이해하기 쉬운 소통
 - b. 유사성으로부터 학습하는 인간의 의사결정 과정과 유사
 - c. 새로운 태스크 적응에 필요한 계산 비용 감소 및 확장 가능성
(Training-free Learning)
- 원리 규명을 위한 여러 가설
 - a. Transformer 는 새로운 함수를 효과적으로 학습하는 알고리즘을 인코딩
 - b. ICL이 기존 미세조정 (파라미터 업데이트) 과 유사하게 동작
 - c. Transformer 내 이전 패턴을 복사하여 다음 토큰을 완성하는 기능 존재

Zero-shot

The model predicts the answer given only a natural language description of the task. No gradient updates are performed.

```
1 Translate English to French: ← task description
2 cheese => ..... ← prompt
```

One-shot

In addition to the task description, the model sees a single example of the task. No gradient updates are performed.

```
1 Translate English to French: ← task description
2 sea otter => loutre de mer ← example
3 cheese => ..... ← prompt
```

Few-shot

In addition to the task description, the model sees a few examples of the task. No gradient updates are performed.

```
1 Translate English to French: ← task description
2 sea otter => loutre de mer ← examples
3 peppermint => menthe poivrée ←
4 plush girafe => girafe peluche ←
5 cheese => ..... ← prompt
```

In-context Learning 방식

[3] 활용 및 증강: 증강의 필요성

LLM의 문제점

1. MLM (마스킹 토큰 예측) 이나 NTP (다음 토큰 예측) 방식과 같이, 존재하지 않는 토큰을 추론하는 학습
→ 사실이 아니지만 구조적으로 그럴듯하게 보이는 콘텐츠를 생성하는 내재적 한계 존재
→ 환각 (Hallucination)
2. 자연어 코퍼스를 활용하여 학습되므로, 산술 추론 등에 약점을 보임
→ $1234+4321=?$

Augmented LLM

- LLM을 추론 및 도구 사용 관점에서 강화한 모델
 - 추론의 경우 ICL 및 CoT 방식

챗GPT와 나는 영동한 문답



대동여지도 연금술사들의 폭동에 대해 자세히 알려줘



18세기 후반 조선시대에 발생한 사건으로, 당시 연금술사들이 창신 총강이라는 비밀 연금술 기관에서 주조한 동을 혁명에 이용하겠다는 계획을 세우면서 시작되었습니다.



거북선의 라이트닝 볼트 발사 매커니즘을 설명해줘



먼저 거북선 내부에서 발사 준비가 완료되면, 발사를 담당하는 승려(승무원)가 노래와 함께 버늘을 돌립니다. ... (중략) ... 이 때 금속 공의 전기가 발사대 위쪽에 위치한 구슬로 전달되면서, 구슬 안의 연쇄 반응이 일어나 라이트닝 볼트가 생성됩니다. ... (후략)

[3] 활용 및 증강: RAG (검색 증강 생성)

Retrieval Augmented Generation; 외부 지식 및 정보에 효과적으로 접근하여 텍스트 생성을 보완하는 기술

- 특정 쿼리와 관련된 정보를 빠르게 색인/추출하여
사실 기반의 답변을 제공하고 최신 정보를 반영할 수 있음
- 불필요한 지식의 저장을 최소화하여
모델 파라미터 수를 줄일 수 있음

