AI 군 참모 기술을 위한 프롬프트 엔지니어링 방법론 연구

문경렬, 박범식, 백승호

LIG넥스원

kyeongryeol.moon@lignex1.com, bumsik.park@lignex1.com, seungho.baek@lignex1.com

Research on Prompt Engineering Methodology for military AI agent technology

Moon Kyeongryeol, Park Bumshik, Baek Seungho

LIG Nex1

요 약

최근 AI 기술은 대형 모델을 중심으로 급속도로 발전하고 있다. 제한된 통신 대역폭과 하드웨어 자원에 비해 실시간 정보처리 요구도가 매우 높은 전장 환경에서, AI 군 참모 기술의 핵심은 LLM을 활용한 지휘관 에이전트이다. 해당 모델의 효율적인 운용을 위해서는 오픈소스 기반의 사전 학습된 모델을 호출하여 시간/비용/유지보수 측면에서의 효율성, 경량화를 통한 하드웨어 자원 요구도 확보, 군 도메인 기반의 모델 학습 등의 여러 요인도 중요하지만, 환경의 제약사항을 제외하면 가장 직관적으로 운용에 영향을 주는 것이 프롬프트이다. 본 논문은 최근 지능형 지휘통제 분야의 큰 관심사인 AI 군 참모 기술을 운용하는데 가장 적절한 응답을 얻을 수 있도록 프롬프트를 설계하는 방법론을 고찰한다.

Ⅰ. 서 론

최근 인공지능 분야에서 대형 언어모델(LLM) 기반의 서비스들이 주목받고 있다. 특히 지능형 지휘통제 분야에서 LLM을 활용한 AI 군 참모 기술은 최신 국방 기술 연구 분야의 큰 축이다. 상황 인지/보고, 위협평가, 전략 추천 등 지휘관의 의사결정에 메인 근거를 제시하는 AI 군 참모 기술은 갈수록 복잡성과 불확실성이 늘어나는 전장 환경에서 신속하고 정확한 의사결정이 필수적으로 요구되는 상황이다.

하지만 현재 국방 도메인에서의 LLM은 고수준, 대량의 데이터셋 확보가 현실적으로 까다로워 학습에서의 제한으로 인하여 그 추론 성능을 확보하기 어렵다. 따라서 처음부터 학습한 모델이 아닌 상용 데이터셋으로 학습한 모델을 호출하여 국방 도메인에 맞게 파인튜닝 후 활용하는 것이 성능/비용 측면을 모두 만족시킬 수 있을 것이다.

GPT-3 발표 이후 LLM의 추론 능력은 프롬프트 엔지니어링을 기반으로 급격히 발전해 오고 있다. 특정 도메인에 파인튜닝된 모델을 활용하는 경우, 정확한 결과를 도출하기 위한 LLM의 추론 성능은 특히 프롬프트 설계에 더욱 의존하게 된다. 따라서 효율적인 파인튜닝과 병렬적으로 모델의 입력, 즉 정교한 프롬프트 엔지니어링을 통해 신뢰도 높은 결과를 도출해 내는 것이 중요하다.

본 논문에서는 콘텍스트 내 학습 등의 프롬프트 기법 및 추론 구성 매개변수에 따른 추론 결과를 분석하여 전장 환경에서의 AI 군 참모 기술 추론 성능 확보 방법론을 제안한다.

Ⅱ. 관련 연구

Ⅱ-1. 프롬프트 엔지니어링 기법

초기 프롬프트 엔지니어링 기법은 2020년 GPT-3의 등장과 함께 제로샷, 퓨샷 추론 등 정답 자체의 추론에 집중된 방식으로 발전해 왔지만, 최근에는 단순한 결과보다 추론 과정 중심의 사고 유도, 자기 검증 매커니즘 등의 방식으로 응답의 논리성과 신뢰성을 향상시키는 연구가 고도화되고 있다. 또한, 자기 검증, 자동 프롬프트 생성 등 전체 프로세스의 최적화를 자동화하는 방향의 연구가 진행되고 있다. 특히 국방, 의료, 법률 등 고신뢰도 응답이 요구되는 분야에서는 Chain-of- thought 계열의 구조적 추론 방식이 강건함을 가져 적극적으로 연구되고 있다.

시기	구분	특징
2020	Zero/Few-shot learning	모델의 일반화 성능, 문제 유형을 학습시키는 정답 자체의 추론 유도 기법
2022	Chain-of-Thought(CoT)[1], Self-Consistency	응답 도출 전, 중간 과정별로 나뉘어 추론 유도 / 응답 일관성 확보
2023	Tree of Thoughts(ToT)[2], Program-Aided Prompting (PAP)	CoT 개념 확장 / 코드로 중간 계산 유도
2024	Prompting with Explanation Feedback (PEF), Auto-CoT / Prompt Optimization	모델 자체적 평가 및 수정 / CoT 프롬프트를 자동 생성(전체 프로세스 최적화)

표 1 프롬프트 엔지니어링 기법 발전 과정

Ⅱ-2. 추론 구성 매개변수

LLM의 응답 특성을 결정하는 요인으로 추론 구성 매개변수에 관한 연구도 진행되고 있다. 최대 토큰 수를 제한하여 출력 응답의 길이를 조절할 수도 있지만, Temperature(온도), Top-k, Top-p 변수 제어를 통해 확률 분포에 따라 다음 생성할 토큰을 선택하는 방식이 중점적이다. 3가지 변수는 개별적으로 설정할 수 있지만, 각각의 연계에 따라 응답의 일관성이 떨어지거나 반복적인 생성 등의 문제가 발생하였다. 그에 따라 다음과 같은 성능 향상을 기대할 수 있는 방식들이 연구되고 있다.

1) Min-p Sampling[3]

기존 Top-p 샘플링 진행 시 높은 Temperature 값에서 응답의 일관성이 저하되는 문제가 빈번했다. 그 해결을 위해 모델의 확신도에 따라 샘플링 임계값을 동적으로 조정하여, 높은 Temperature 값에서도 모델 응답의 일관성을 유지하여 품질과 다양성을 동시에 챙길 수 있는 샘플링 방법이다.

2) KL(Kullback - Leibler)-Divergence 기반 동적 Temperature 조정[4]

변수 간 마찰을 줄이기 위해 Temperature 값을 고정시키는 방식의 개

선을 위해 제안된 방법으로, 모델이 응답을 생성하면서 응답과 소스의 KL 발산 값을 계속 비교하여 Temperature 값을 동적으로 조절하는 방식이다. 온도값 조절을 통해 응답의 다양성을 향상시키며 소스와의 일관성을 확보할 수 있는 방법이다.

3) Long Horizon Temperature Scaling(LHTS)[5]

기존 Temperature 값 조절은 다음 생성할 토큰에 대한 확률분포에 관여하는 방식으로서, 긴 글을 생성할 시 반복, 일관성 부족 등 응답의 품질적인 문제가 발생할 가능성이 존재한다. 이에 따른 개선 방식 제안되었으며, 모델이 긴 응답을 생성하는 전 과정에 걸쳐 Temperature 값을 동적으로 조절하는 방식이다.

위 방식들 이외에도 EDT(Entropy-based Dynamic Temperature) Sampling, LPO(Adaptive Decoding via Latent Preference Optimization) 등 여러 기법들에 관한 연구로 LLM 응답의 정확성을 높이고 있다.

Ⅲ. AI 군 참모 기술 적용 방안

AI 군 참모 기술은 AI기술을 활용하여 군 도메인에서 발생하는 대량의 데이터를 수집, 분석, 예측하여 지휘관의 의사결정을 지원하는 기술이다. 군종, 지역에 따라 원하는 결과에 차이가 있을 수는 있지만, 궁극적으로 AI 군 참모로부터 얻고자 하는 응답은 자신의 위치에 맞게 추천된 정보, 필터링된 상황 인지/보고 데이터, 추천된 방책의 현실성, 상급 부대의 지침 반영성 등의 조건들이 요구된다.

특정된 분야에서 적용할 프롬프트 안을 구성할 때 가장 먼저 고려할 것은 콘텍스트 크기이다. 각 모델마다 고정된 크기의 콘텍스트 윈도우가 있기에 긴 정보를 입력받아도 다 활용하지 못할 수 있다. 또한, 최적의 프롬프트 기법 선택은 사용하고자 하는 LLM의 학습 방법, 튜닝 방법에 따라 달라지기에 그 구조에 적합한 기법을 적용하는 것이 중요하다. AI 군 참모 기술에는 국방 도메인에 맞게 파인튜닝된 일반 모델을 활용할 가능성이 높으므로 Role Prompting(역할 부여), CoT(사고 흐름 유도), Constraint Prompting (제약조건 부여) 등의 기법을 통해 틀에 정해진 응답을 유도하는 것이 활용도가 제일 높을 것으로 보인다.

추론 구성 매개변수의 조정만으로 국방 도메인에서 최적의 결과를 도출하기 위해 간단한 입력 테스트를 진행하였다. 모델은 OpenAI의 GPT-4 (gpt-4-0613 API버전)을 활용하였으며 Open AI의 API를 통해 매개변수만 조정하여 진행하였다. 국방 분야에서의 응답 특성을 알아보기 위해 Top-k는 '제한 없음'으로 설정하였으며, Temperature 값과 Top-p 값은 차등을 두고 조절하였다. 또한, 프롬프트 구성은 앞서 명시된 바와 같이 활용도가 가장 높을 것으로 보이는 Role Prompting, CoT, Constraint Prompting 3가지 기법을 활용하여 동일하게 작성한 프롬프트를 입력하였다. 아래는 각 변수 설정값에 대하여 출력된 응답에 대한 개요이다.

구분	매개변수			응답 특성
	Temperature	Top-p	Top-k	
A	0.2	0.5	제한 없음	매우 표준적, 창의성 낮음, 일관성/신뢰성 높음
B	0.5	0.7	제한 없음	균형 잡힌 방책 추천, 실용성/다양성 균형이 좋음
C	0.8	0.9	제한 없음	다양한 방책 추천, 창의성 높음, 일관성 떨어짐
D	0.9	1.0	제한 없음	매우 창의적 응답, 실용성/신뢰성 낮음

표 2 매개변수 별 응답 특성

위 표의 응답 특성을 분석하면 알 수 있듯이 창의성보단 신뢰도가 중요한 국방 도메인에선 Temperature값과 Top-p값이 0.5, 0.7일 때 가장 균형잡힌 결과를 얻을 수 있을 것으로 보인다. 위 테스트에 Min-p sampling, LHTS를 적용했을 때는 아래와 같이 응답이 개선된다.

구분	변수	Min-p 적용 응답 특성	LHTS 적용 응답 특성
	Temperature		
A	0.2	변화 거의 없음	변화 거의 없음
B	0.5	일관성 유지, 다양성 증가	일관성 유지, 구조적 개선
C	0.8	다양성 유지, 일관성 향상	다양성 유지, 일관성 향상
D	0.9	창의성 유지, 일관성 개선	창의성 유지, 일관성 개선

표 3 Min-p, LHTS 적용 응답 특성

위 결과를 통해 최근 연구되고 있는 기법들을 적용하면 Temperature 값을 0.8까지 활용 가능하여 더 다양한 응답을 도출할 수 있을 것으로 보인다. 적절한 기법 선택과 일관성이 유지되는 한에서 최대한의 신뢰도를 확보할 수 있는 초기 변수 세팅 및 변수 제어 기법을 활용한다면 AI 군 참모 기술에 활용되는 LLM의 최적화를 통해 실전 운용성(추론 성능 및 지휘관 결심 지원 등)을 극대화할 수 있을 것이다.

Ⅳ. 결론

본 논문에서는 AI 군 참모 기술에 적용 가능한 프롬프트 엔지니어링 방법론을 분석하고, 적용 기대효과를 제시하였다. 미래 AI 군 참모 기술은 제한된 통신/하드웨어 환경에서 지휘관 또는 운용자에게 군종에 구애받지 않고 방대한 데이터를 효율적/실시간으로 처리 및 전달하는 기능을 목표로 한다.

최근 LLM은 더욱 다양한 응답을 생성하기 위해 사실이 아님에도, 그럴듯한 토큰을 생성하는 환각 현상에 취약해지고 있다. 국방 도메인같이 신뢰도 높은 응답이 요구되는 분야에서 추론 성능을 확보하려면 해당 분야와 관련된 사전 검증된 양질의 대규모 데이터를 통해 학습된 모델을 활용하는 것이 가장 이상적이다. 하지만 현실적으로 이러한 데이터 확보가 어렵기 때문에, 이를 대체하기 위해 프롬프트 엔지니어링 기법과 매개변수의 적절한 조절법을 활용하여 최적의 응답을 유도하는 접근이 중요하다.

프롬프트의 조작만으로는 모델 자체의 파인튜닝에 비해 성능이 낮을 수 있다. 그러나 국방 도메인 분야에서는 향후 더 고도화되는 기법들의 활용으로 최적의 프롬프트를 설계하여 성능을 확보하는 것이 자원 활용도, 비용적/시간적 측면에서 실적용에 우선 고려되어야 한다.

또한, Edge단에서는 LLM이 아닌 경량화된 sLM, sLLM 등을 활용할 가능성이 높기에, 시뮬레이션 등으로 더 사실적인 데이터를 확보하여 양질의 데이터셋 구축을 통해 모델을 학습시키고, 그에 적절한 프롬프트 엔지니어링 기법들의 연구도 병행되어야 한다.

ACKNOWLEDGMENT

이 논문은 2023년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임(KRIT-CT-23-021)

참 고 문 헌

[1] Wei et al., "Chain-of-Thought Prompting Elicits Reasoning in LLMs", 2022

[2] Long et al., "Tree of Thoughts: Deliberate Problem Solving with Language Models", 2023

[3] Nguyen Nhat Minh et al, "TURNING UP THE HEAT: MIN-p SAMPLING FOR CREATIVE AND COHERENT LLM OUTPUTS". ICLR 2025

[4] Chung-Ching Chang et al, "KL-Divergence Guided Temperature Sampling", 2023

[5] Andy Shih et al, "Long Horizon Temperature Scaling", 2023