

한 문장 핵심 기여 (One-Sentence Contribution)

Toolformer: Language Models Can Teach Themselves to Use Tools

Timo Schick et al. (Meta AI, 2023) • arXiv:2302.04761

핵심 연구 기여 (CORE CLAIM)

“Toolformer 는 인간의 라벨링 없이 , 미래 토큰 예측 손실 (Loss) 감소량을 자율 피드백으로 활용하여 외부 API 도구의 적절한 호출 시점과 방법을 스스로 학습한다 .”

베이스 모델

GPT-J (6.7B)

CCNet 서브셋 파인튜닝

핵심 기법

손실 감소 기반 필터링

손실 감소 조건

$(L^- - L^+ \geq \tau_f)$ 채택

대표 성과

GPT-3 (175B) 압도

25 배 큰 모델 대비

수학 / 검색 우세

문제 제기 및 연구 동기 : 순수 LLM 의 한계와 연구 목표

1. 순수 LLM 의 한계

- 정확한 연산 한계
- 환각 현상
- 최신 지식 결여
- 저자원 언어 약세
- 시간 인지 부재

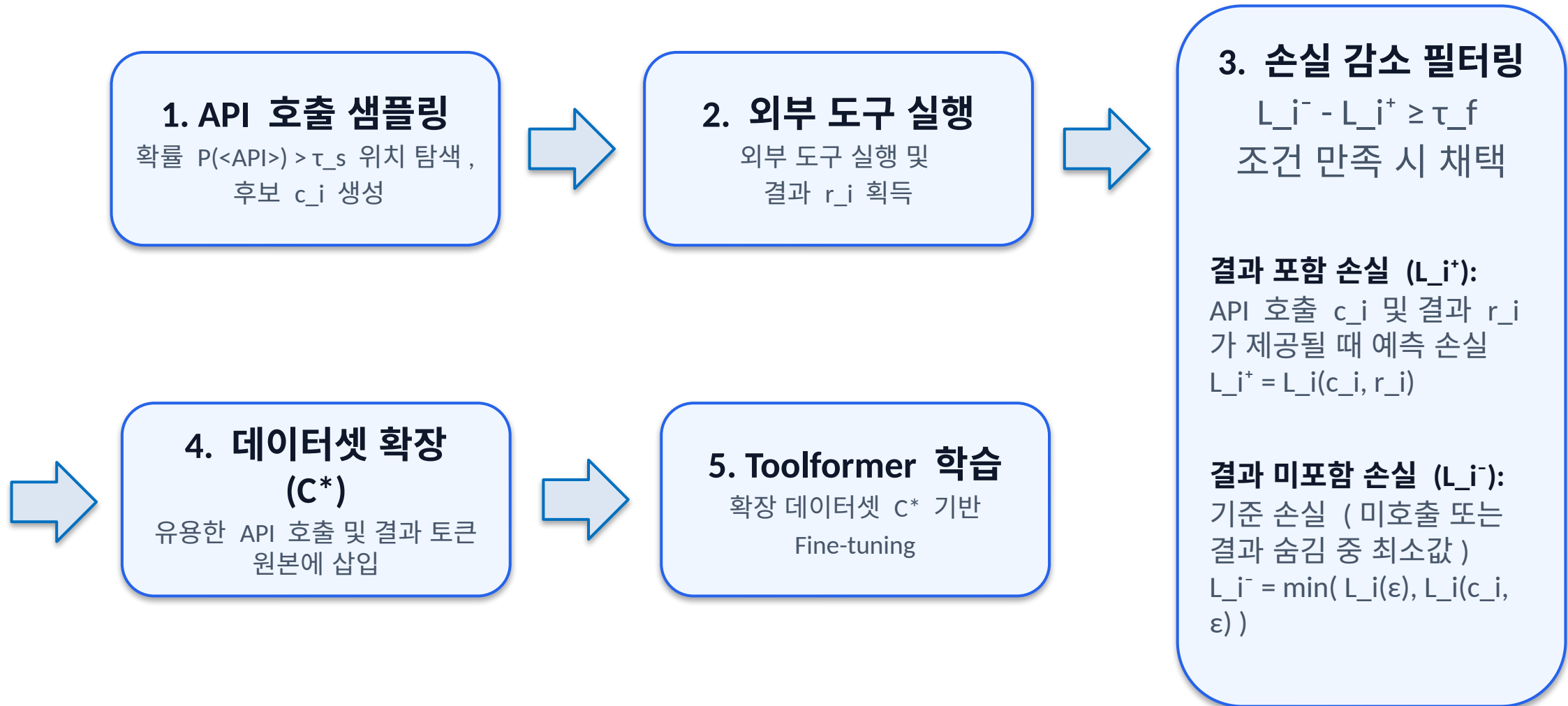
2. 기존 도구 연동의 한계

- 수동 라벨링 비용
- 태스크 전용 프롬프팅
- 자율 판단 능력 부재

3. Toolformer 의 해결책

- ✓ **Self-Supervised 학습**
사람 라벨 없이
자율적으로 도구 활용법
발굴
- ✓ **손실 기반 동적 결정**
미래 토큰 예측 손실 감소
시 도구 트리거
- ✓ **범용 외부 API 통합**
계산기, QA, 검색, 번역,
달력 자율 연동

핵심 메커니즘 : 자기지도학습형 API 샘플링 및 필터링



핵심 성과 : 수학 연산 벤치마크 성능 비교

모델명	파라미터	ASDiv	SVAMP	MAWPS
GPT-J (기본)	6.7B	7.5	5.2	9.9
GPT-J + CC	6.7B	9.6	5.0	9.3
Toolformer (비활성)	6.7B	14.8	6.3	15.0
Toolformer (활성)	6.7B	40.4	29.4	44.0
OPT 베이스라인	66B	6.0	4.9	7.9
GPT-3 베이스라인	175B	14.0	10.0	19.8

- **97.9% 연산기 호출**

수학 벤치마크 문제에서
자율적으로 Calculator 선택

- **25 배 대형 모델 압도**

6.7B + 연산기 조합이 175B
GPT-3 성능 대폭 상회

- **Zero-Prompt 실행**

프롬프트 없이 문맥상
필요성을 판단하여 수행

- **일반 QA 예외**

175B GPT-3 가 우세 유지

약점 및 치명적 한계점 분석

치명적 한계 : 도구 연속 사용 (Tool Chaining) 불가능

- 단일 단계 구조 : 질문 → 도구 A 실행 → 결과 반영 → 최종 생성 (가능)
- 다단계 연결 실패 : 질문 → 도구 A 실행 → 결과 A 로 도구 B 실행 → 최종 생성 (불가능)
- 원인 : 각 토큰 위치에서 독립적 샘플링이 수행되며 , 학습 데이터에 체이닝 예시 부재

1. 인터랙티브 탐색 불가

검색 결과 불충분 시 재검색이나 다단계 탐색 수행 불가

2. 입력 표현 민감성

문장 미세 표현 (Wording) 변화 시 도구 호출 판단 변동

3. 낮은 샘플 효율성

100 만 개 이상 문서 필터링 시 수천 개 샘플 확보 불가

4. 비용 미고려 필터링

손실 감소만 평가하며 API 실행 시간 및 과금 비용 미반영

현대 AI Agent 로의 연계 및 향후 발전 방향

정리

- Toolformer (2023)

셀프 자기지도학습형 도구 호출 제시

- 한계

단일 단계 도구 사용에 집중

- 학술적 유산

LLM 을 수동적 생성기에서 능동적 에이전트로 전환

저자가 제시한 향후 연구 방향

- ✓ 강화학습 (RL) 기반 동적 도구 활용

정적 필터링을 넘어 RL 기반 다단계 에이전트로 확장

- ✓ 비용 인식 도구 최적화 (Cost-Aware)

정확도와 API 실행 시간 / 비용 간의 통합 최적화

- ✓ 다중 모듈 및 샌드박스 연동

Python 실행기, DB, 브라우저 환경과의 결합