Toolformer: Language Models Can Teach Themselves to Use Tools

Timo Schick   **Jane Dwivedi-Yu**   **Roberto Dessì**[†]   **Roberta Raileanu**

Maria Lomeli   **Eric Hambro**   **Luke Zettlemoyer**   **Nicola Cancedda**   **Thomas Scialom**

FAIR, Meta [†]Universitat Pompeu Fabra

简介

Toolformer：通过SFT训练语言模型学会使用外部工具。关键问题在于：如何构造带有tool calling的训练数据？论文提出了一种自监督的数据构建流程：LLM在观察少量tool calling示例后，利用few-shot能力自动采样大量候选的工具调用位置与工具调用内容；系统执行这些调用并获取返回结果。只有当某个调用结果能显著降低LLM对后续token的预测损失时，该调用才会被保留下来，并插入到原始文本中，形成带有调用标记的训练样本。最终，这些样本用于SFT训练模型。通过这种方式，Toolformer 实现了无需人工标注即可学习"何时调用、调用什么、以及如何使用工具结果"的能力。

背景

如何让LLM学会使用外部tool以提升解决问题的能力？现有方法大多依赖人工标注或特定任务的Prompt template，缺乏通用性和扩展性。Toolformer正是在此背景下提出的：它试图让LLM通过自我生成训练数据的方式，学习如何调用工具，并且在不牺牲通用语言能力的前提下，增强模型在多任务场景下的 zero-shot 能力。

生成API CALLING数据

对于每种工具，首先设计一个few-shot prompt template，LLM读到句子 "Pittsburgh is also known as…" 时，先计算插入<API>概率较高的位置i，然后在i位置采样多个API Calls，系统执行api call返回执行结果。模型检查这些答案是否真的有助于理解后续文本，只有能提升预测效果的调用才会被保留。最后，保留的调用会插入回原文中，形成新的训练数据，用于sft。
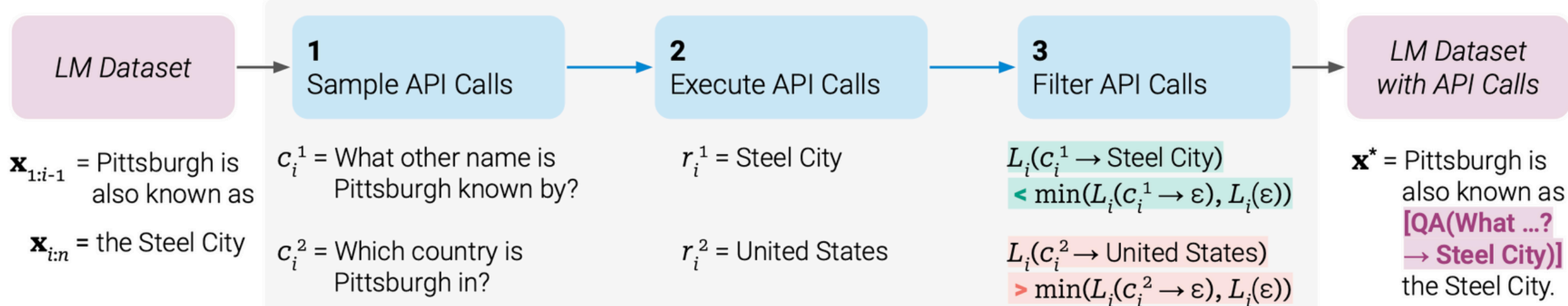
TOOLFORMER

Figure 2: Key steps in our approach, illustrated for a *question answering* tool: Given an input text $\mathbf{x}$, we first sample a position i and corresponding API call candidates $c_i^1, c_i^2, \ldots, c_i^k$. We then execute these API calls and filter out all calls which do not reduce the loss L_i over the next tokens. All remaining API calls are interleaved with the original text, resulting in a new text $\mathbf{x}^*$.

PROMPT FOR SAMPLE API CALL

Your task is to add calls to a Question Answering API to a piece of text. The questions should help you get information required to complete the text. You can call the API by writing "[QA(question)]" where "question" is the question you want to ask. Here are some examples of API calls:

Input: Joe Biden was born in Scranton, Pennsylvania.
Output: Joe Biden was born in [QA("Where was Joe Biden born?")] Scranton, [QA("In which state is Scranton?")] Pennsylvania.

Input: Coca-Cola, or Coke, is a carbonated soft drink manufactured by the Coca-Cola Company.
Output: Coca-Cola, or [QA("What other name is Coca-Cola known by?")] Coke, is a carbonated soft drink manufactured by [QA("Who manufactures Coca-Cola?")] the Coca-Cola Company.

Input: x
Output:

Figure 3: An exemplary prompt $P(\mathbf{x})$ used to generate API calls for the question answering tool.

思考

本文通过SFT的方式让LLM学会使用TOOL，虽然TOOLFORMER会使用多种TOOL，但严格来说不属于MULTI-TOOL的范畴，因为每条数据只包含一种TOOL的调用，只不过在SFT时将多种TOOL数据混合在一起了。因为每条数据有K个位置供采样API CALL数据，因此是可以实现一条数据含有一种TOOL的多次调用的，比如多次调用SEARCH TOOL，但是论文中似乎每条数据只含有一次TOOL调用。

@机器爱学习