

THÔNG TIN CHUNG CỦA NHÓM

- Link YouTube video của báo cáo: <https://youtu.be/9sGxZXRlei0>
- Link slides:
<https://github.com/Ceci-june/CS2205.CH201---Phuongphapnghiencuukhoaahoc/blob/main/%5BSlide%5D%20Try%20then%20Eval.pdf>
- *Mỗi thành viên của nhóm điền thông tin vào một dòng theo mẫu bên dưới*
- *Sau đó điền vào Đề cương nghiên cứu (tối đa 5 trang), rồi chọn Turn in*
- *Lớp Cao học, mỗi nhóm một thành viên*

- Họ và Tên: Lê Thị Phương Vy
- MSSV: 250101078



- Lớp: CS2205.CH201
- Tự đánh giá (điểm tổng kết môn): 8.5/10
- Số buổi vắng: 0
- Số câu hỏi QT cá nhân: 3
- Số câu hỏi QT của cả nhóm: 0
- Link Github:
<https://github.com/Ceci-june/CS2205.CH201---Phuongphapnghiencuukhoaahoc>

ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

XÂY DỰNG TÁC TỬ TỰ ĐỘNG HÓA TÁC VỤ WEB DỰA TRÊN MÔ HÌNH NGÔN NGỮ LỚN VỚI CƠ CHẾ HAI GIAI ĐOẠN THỬ NGHIỆM - ĐÁNH GIÁ (TRY-THEN-EVAL)

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

BUILDING AN LLM-BASED AGENT FOR WEB TASK AUTOMATION USING A TWO-PHASE TRY-THEN-EVAL MECHANISM

TÓM TẮT

Tự động hóa các tác vụ trên giao diện web từ mô tả ngôn ngữ tự nhiên là một hướng nghiên cứu quan trọng, với nhiều ứng dụng trong kiểm thử phần mềm, trợ lý ảo và tối ưu hóa quy trình làm việc. Tuy nhiên, nhiều phương pháp hiện tại vẫn phụ thuộc vào các minh họa thao tác do con người xây dựng thủ công, làm giảm khả năng mở rộng và thích nghi với các tác vụ mới.

Trong đề tài này, chúng tôi đề xuất xây dựng một tác tử thông minh dựa trên mô hình ngôn ngữ lớn (Large Language Model – LLM) có khả năng thực hiện các tác vụ web mà không cần minh họa của con người. Phương pháp được xây dựng dựa trên cơ chế hai giai đoạn Try-Then-Eval, cho phép tác tử học từ các lần thử nghiệm thành công và thất bại thông qua bộ nhớ ngắn hạn và dài hạn.

Tác tử được thiết kế để quan sát trạng thái giao diện web thông qua biểu diễn DOM rút gọn, lập kế hoạch hành động theo từng bước và cải thiện hiệu suất bằng cách lưu trữ các quỹ đạo thành công và trích xuất quy tắc từ các lần thất bại. Đề tài tập trung nghiên cứu kiến trúc tác tử, cơ chế học từ kinh nghiệm và phương pháp đánh giá trên bộ dữ liệu chuẩn MiniWoB++ [1].

Kết quả kỳ vọng của đề tài là xây dựng được một tác tử tự động hóa web có tính khả

thi, dựa trên cơ chế học từ kinh nghiệm Try-Then-Eval.

GIỚI THIỆU

Trong những năm gần đây, các mô hình ngôn ngữ lớn (Large Language Models – LLMs) đã đạt được nhiều tiến bộ trong khả năng hiểu và sinh ngôn ngữ tự nhiên. Từ các tác vụ xử lý ngôn ngữ truyền thống như dịch máy hay tóm tắt văn bản, LLMs dần được mở rộng sang các bài toán yêu cầu suy luận, lập kế hoạch và ra quyết định, qua đó được nghiên cứu như các tác tử thông minh có khả năng tương tác và thực thi hành động trong môi trường phức tạp [2], [3], [4].

Một hướng ứng dụng quan trọng của tác tử dựa trên LLM là tự động hóa các tác vụ trên môi trường web. Các tác vụ này mang tính lặp lại và đa dạng, từ những thao tác đơn giản như nhấp chuột, chọn menu cho đến các quy trình nhiều bước như điền biểu mẫu hoặc điều hướng qua nhiều trang. Việc tự động hóa các tác vụ web có ý nghĩa thực tiễn trong các lĩnh vực như kiểm thử phần mềm, trợ lý ảo và tối ưu hóa quy trình làm việc.

Mặc dù có nhiều tiềm năng ứng dụng, các phương pháp hiện tại trong lĩnh vực tự động hóa web vẫn tồn tại những hạn chế đáng kể, đặc biệt là sự phụ thuộc vào các minh họa thao tác do con người xây dựng thủ công. Việc thu thập các minh họa này tốn kém về thời gian và công sức, đồng thời khó bao phủ được sự đa dạng của các tác vụ web trong thực tế. Ngoài ra, các hệ thống này thường gặp hạn chế khi phải thích nghi với các tác vụ mới hoặc môi trường thay đổi [5], [6], [7].

Trước những hạn chế đó, đề tài này tập trung nghiên cứu xây dựng một tác tử tự động hóa web dựa trên mô hình ngôn ngữ lớn với cơ chế hai giai đoạn Try-Then-Eval. Thay vì học từ minh họa của con người, tác tử được thiết kế để học từ chính các lần thử nghiệm của mình thông qua việc thực hiện hành động, đánh giá kết quả, lưu trữ các quỹ đạo thành công và trích xuất quy tắc từ các lần thất bại. Cách tiếp cận này nhằm giảm sự phụ thuộc vào minh họa thủ công, đồng thời nâng cao tính tự chủ và

khả năng thích nghi của tác tử khi giải quyết các tác vụ web khác nhau, qua đó làm rõ tiềm năng của mô hình ngôn ngữ lớn trong vai trò tác tử thông minh [8], [9].

MỤC TIÊU (Viết trong vòng 3 mục tiêu)

Mục tiêu tổng quát của đề tài là nghiên cứu và xây dựng một tác tử tự động hóa tác vụ web dựa trên mô hình ngôn ngữ lớn, có khả năng thực hiện các thao tác trên giao diện web từ mô tả ngôn ngữ tự nhiên mà không cần sử dụng các minh họa thao tác do con người xây dựng thủ công.

Cụ thể, đề tài hướng tới các mục tiêu sau:

- 1. Nghiên cứu và phân tích bài toán tự động hóa tác vụ web bằng mô hình ngôn ngữ lớn**, bao gồm việc khảo sát các phương pháp hiện có, làm rõ vai trò của LLM trong lập kế hoạch và ra quyết định, đồng thời chỉ ra những hạn chế của các hướng tiếp cận phụ thuộc vào minh họa thao tác của con người.
- 2. Thiết kế và triển khai kiến trúc tác tử tự động hóa web dựa trên LLM**, trong đó tác tử có khả năng quan sát trạng thái giao diện web, lập kế hoạch hành động theo từng bước và sử dụng bộ nhớ ngắn hạn, dài hạn để hỗ trợ quá trình ra quyết định từ mô tả ngôn ngữ tự nhiên.
- 3. Đề xuất và đánh giá cơ chế hai giai đoạn Try-Then-Eval**, cho phép tác tử học từ các lần thực hiện thành công và thất bại thông qua việc lưu trữ quỹ đạo hành động và trích xuất quy tắc, nhằm đánh giá tính khả thi và hiệu quả của cơ chế này trên bộ dữ liệu chuẩn về tương tác web.

NỘI DUNG VÀ PHƯƠNG PHÁP

Nội dung nghiên cứu

Đề tài tập trung nghiên cứu và xây dựng một tác tử tự động hóa tác vụ web dựa trên mô hình ngôn ngữ lớn, với trọng tâm là cơ chế học từ kinh nghiệm thay vì minh họa

thủ công. Nội dung nghiên cứu chính của đề tài bao gồm các phần sau:

Thứ nhất, nghiên cứu tổng quan các công trình liên quan đến việc sử dụng mô hình ngôn ngữ lớn và tác tử thông minh cho bài toán tự động hóa tác vụ web, qua đó phân tích các hướng tiếp cận phổ biến, đặc biệt là các phương pháp phụ thuộc vào minh họa thao tác của con người và những hạn chế của chúng.

Thứ hai, nghiên cứu cách biểu diễn trạng thái giao diện web phù hợp với mô hình ngôn ngữ lớn, tập trung vào việc rút gọn thông tin từ DOM để chỉ giữ lại các phần tử tương tác cần thiết, nhằm giảm nhiễu và tăng hiệu quả suy luận của tác tử.

Thứ ba, thiết kế kiến trúc tổng thể của tác tử tự động hóa web, bao gồm cơ chế lập kế hoạch hành động theo từng bước, bộ nhớ ngắn hạn để lưu trữ quỹ đạo hành động và bộ nhớ dài hạn để lưu trữ kinh nghiệm thu được trong quá trình thực hiện tác vụ.

Thứ tư, nghiên cứu và đề xuất cơ chế hai giai đoạn Try-Then-Eval, cho phép tác tử học từ các lần thực hiện thành công và thất bại thông qua việc lưu trữ quỹ đạo hành động và trích xuất các quy tắc hỗ trợ cho các lần thực hiện tiếp theo.

Phương pháp thực hiện

Đề tài được thực hiện theo phương pháp nghiên cứu thực nghiệm kết hợp với phân tích và mô phỏng hệ thống. Các bước thực hiện chính bao gồm:

Trước hết, tác tử được xây dựng dựa trên mô hình ngôn ngữ lớn để sinh hành động từ mô tả ngôn ngữ tự nhiên của tác vụ và trạng thái hiện tại của giao diện web. Trạng thái giao diện được biểu diễn dưới dạng DOM rút gọn, chỉ bao gồm các phần tử hiển thị và có thể tương tác.

Tiếp theo, tác tử lập kế hoạch hành động theo cơ chế lặp, trong đó mô hình ngôn ngữ lớn sử dụng thông tin về mục tiêu, trạng thái hiện tại và quỹ đạo hành động trước đó để lựa chọn hành động phù hợp. Các hành động được thực thi trực tiếp trên môi

trường web thông qua công cụ tự động hóa.

Trong giai đoạn Try, tác tử thực hiện nhiều lần thử nghiệm để thu thập quỹ đạo hành động, trong đó các quỹ đạo thành công được lưu trữ và các quỹ đạo thất bại được phân tích nhằm trích xuất các quy tắc hỗ trợ. Trong giai đoạn Eval, tác tử sử dụng các quỹ đạo và quy tắc đã học để hỗ trợ ra quyết định khi thực hiện các tác vụ mới. Hiệu quả của tác tử được đánh giá trên bộ dữ liệu chuẩn về tương tác web bằng độ đo Success Rate [4], [6], [10].

KẾT QUẢ MONG ĐỢI

Đề tài kỳ vọng đạt được các kết quả sau:

Thứ nhất, xây dựng được một mô hình tác tử tự động hóa tác vụ web dựa trên mô hình ngôn ngữ lớn, có khả năng thực hiện các thao tác trên giao diện web từ mô tả ngôn ngữ tự nhiên mà không cần sử dụng các minh họa thao tác do con người xây dựng thủ công.

Thứ hai, đề xuất và triển khai cơ chế hai giai đoạn Try-Then-Eval, cho phép tác tử học từ các lần thực hiện thành công và thất bại thông qua việc lưu trữ quỹ đạo hành động và trích xuất quy tắc, qua đó cải thiện khả năng ra quyết định theo thời gian.

Thứ ba, đánh giá được tính khả thi của hướng tiếp cận đề xuất thông qua các thí nghiệm trên bộ dữ liệu chuẩn về tương tác web, từ đó phân tích ưu điểm, hạn chế và tiềm năng mở rộng của tác tử trong các kịch bản tự động hóa thực tế.

Thứ tư, cung cấp một nền tảng nghiên cứu ban đầu cho việc phát triển các tác tử thông minh dựa trên mô hình ngôn ngữ lớn, góp phần làm rõ vai trò của học từ kinh nghiệm trong bài toán tự động hóa tác vụ web.

Kết quả của đề tài góp phần làm rõ tiềm năng của các tác tử dựa trên mô hình ngôn ngữ lớn trong việc tự cải thiện thông qua kinh nghiệm, thay vì phụ thuộc vào dữ liệu

gán nhãn hoặc minh họa chuyên gia [3], [11]. Đồng thời, đề tài cũng kỳ vọng xác định được các hạn chế của hướng tiếp cận đề xuất, làm cơ sở cho các nghiên cứu tiếp theo.

TÀI LIỆU THAM KHẢO

- [1]. E. Z. Liu, K. Guu, P. Pasupat, T. Shi, and P. Liang, “Reinforcement learning on web interfaces using workflow-guided exploration,” in International Conference on Learning Representations (ICLR), 2018.
- [2]. T. Sumers, S. Yao, K. Narasimhan, and T. Griffiths, “Cognitive architectures for language agents,” Transactions on Machine Learning Research, 2023.
- [3]. L. Wang, C. Ma, X. Feng, Z. Zhang, H. Yang, J. Zhang, Z. Chen, J. Tang, X. Chen, Y. Lin et al., “A survey on large language model based autonomous agents,” Frontiers of Computer Science, vol. 18, no. 6, pp. 1–26, 2024.
- [4] X. Deng, Y. Gu, B. Zheng, S. Chen, S. Stevens, B. Wang, H. Sun, and Y. Su, “Mind2web: Towards a generalist agent for the web,” Advances in Neural Information Processing Systems, vol. 36, 2024.
- [5] L. Zheng, R. Wang, X. Wang, and B. An, “Synapse: Trajectory-as-exemplar prompting with memory for computer control,” in The Twelfth International Conference on Learning Representations, 2023.
- [6] H. Sun, Y. Zhuang, L. Kong, B. Dai, and C. Zhang, “Adaplanner: Adaptive planning from feedback with language models,” Advances in Neural Information Processing Systems, vol. 36, 2024.
- [7] G. Kim, P. Baldi, and S. McAleer, “Language models can solve computer tasks,” Advances in Neural Information Processing Systems, vol. 36, 2024.
- [8]. N. Shinn, F. Cassano, A. Gopinath, K. Narasimhan, and S. Yao, “Reflexion: Language agents with verbal reinforcement learning,” Advances in Neural Information Processing Systems, vol. 36, 2024.
- [9] T. Li, G. Li, Z. Deng, B. Wang, and Y. Li, “A zero-shot language agent for computer control with structured reflection,” in The 2023 Conference on Empirical Methods in Natural Language Processing, 2023.
- [10] T. Shi, A. Karpathy, L. Fan, J. Hernandez, and P. Liang, “World of bits: An

open-domain platform for web-based agents,” in International Conference on Machine Learning. PMLR, 2017, pp. 3135–3144.

- [11] P. Ethape, R. Kane, G. Gadekar, and S. Chimane, “Smart automation using llm,” International Research Journal of Innovations in Engineering and Technology, vol. 7, no. 11, p. 603, 2023.