

**BỘ GIÁO DỤC VÀ ĐÀO TẠO TRƯỜNG ĐẠI HỌC SÀI GÒN KHOA CÔNG NGHỆ THÔNG TIN**

**Môn: Trí tuệ nhân tạo nâng cao**

**Ex1**

Giảng viên: Đỗ Như Tài

Sinh viên:

3122410035 - Nguyễn Khải Ca

3122410040 - Đặng Văn Chiến

3120410098 - Đỗ Trịnh Mỹ Duyên

3122410040 - Đặng Văn Chiến

3120410098 - Đỗ Trịnh Mỹ Duyên

**PHÂN CÔNG CÔNG VIỆC:**

3122410035 - Nguyễn Khải Ca : Chương 3

3122410040 - Đặng Văn Chiến: Chương 2

3120410098 - Đỗ Trịnh Mỹ Duyên: Chương 1

**CHƯƠNG 1:**

**Turing Test: Large Language Models (LLMs)**

Câu 1: Would a modern LLM pass the Turing Test?

* Would you be fooled?
* Why does it or does it not pass your test?
* What does this mean for artificial general intelligence (AGI) or narrow AI?

Trả lời:

Hiện nay, nhiều mô hình LLM tiên tiến như GPT-4 hay GPT-5 có thể vượt qua Bài kiểm tra Turing trong một số tình huống. Cá nhân tôi có thể bị đánh lừa khi trò chuyện ngắn hoặc với các chủ đề thông thường, vì mô hình trả lời rất tự nhiên và mạch lạc.

Tuy nhiên, chúng vẫn chưa thực sự vượt qua bài kiểm tra này một cách hoàn hảo. Lý do là vì LLM chỉ dựa trên xác suất ngôn ngữ để tạo câu trả lời, thiếu hiểu biết thật sự về thế giới, đôi khi bịa ra thông tin và chưa có khả năng suy luận sâu như con người.

Điều này cho thấy LLM hiện tại vẫn thuộc AI hẹp (Narrow AI), vì chúng chỉ giỏi trong một lĩnh vực cụ thể – xử lý ngôn ngữ. Để đạt tới AGI (Artificial General Intelligence), AI cần thêm khả năng lập luận logic, tự học và nhận thức thế giới ở mức độ như con người.

Câu 2: How do we currently test the performance of LLMs?

* See: Open LLM Leaderboard (Hugging Face)

Trả lời:

Hiện tại, hiệu suất của LLM thường được kiểm tra qua ba phương pháp chính:

Benchmark chuẩn: Sử dụng các bộ dữ liệu như MMLU, HellaSwag, TruthfulQA để đánh giá kiến thức, suy luận và logic.

Bảng xếp hạng mở (Open LLM Leaderboard): Chẳng hạn như trên Hugging Face, nơi so sánh nhiều mô hình dựa trên cùng bộ bài kiểm tra.

Đánh giá từ người dùng thực (Human Evaluation): Người dùng trực tiếp trò chuyện và đánh giá mức độ tự nhiên, chính xác và hữu ích của mô hình.

**The AI Effect: AI gets no respect?**

Câu 1: How do you think LLMs will affect the value of being able to write essays as taught in high school?

Trả lời:

LLMs giúp học sinh viết bài luận nhanh hơn và có chất lượng ngôn ngữ tốt hơn. Tuy nhiên, giá trị của việc viết luận không chỉ nằm ở ngôn từ mà còn ở tư duy phản biện, lập luận logic và sáng tạo. Vì vậy, khi LLMs trở nên phổ biến, việc dạy viết luận cần chuyển trọng tâm sang ý tưởng và phân tích, thay vì chỉ chú trọng kỹ năng viết thủ công.

Câu 2: LLMs write computer code. What does this mean for the value of learning to code?

Trả lời:

Việc LLMs có thể viết mã giúp học sinh tiết kiệm thời gian với những đoạn code cơ bản. Tuy nhiên, hiểu biết về thuật toán, tư duy logic và khả năng phân tích vấn đề vẫn rất quan trọng. Học lập trình không chỉ là viết code, mà còn là giải quyết vấn đề và thiết kế giải pháp. Vì thế, LLMs nên được coi là công cụ hỗ trợ, chứ không thay thế hoàn toàn việc học lập trình.

Câu 3: When should students be allowed to use the following tools? Give reasons for your decision.

* A pocket calculator
* LLMs (to answer homework questions and write essays)
* LLMs to write or support writing code

Trả lời:

Máy tính bỏ túi:

Học sinh có thể sử dụng khi đã nắm vững các khái niệm toán cơ bản. Mục tiêu là để rèn tư duy toán học trước, sau đó dùng máy tính để tính toán phức tạp hơn.

LLMs để trả lời câu hỏi và viết bài luận:

Có thể sử dụng như một tài liệu tham khảo khi học sinh đã biết cách phân tích, tổng hợp thông tin và không phụ thuộc hoàn toàn vào LLMs. Giáo viên cần hướng dẫn cách kiểm chứng thông tin mà LLMs cung cấp.

LLMs để viết hoặc hỗ trợ viết mã:

Nên dùng sau khi học sinh hiểu được cấu trúc cơ bản và tư duy lập trình. Khi đó, LLMs giúp tăng hiệu quả lập trình và học sinh có thể tập trung vào tư duy giải thuật thay vì cú pháp.

**AI Safety**

Câu 1: How are LLMs affected by:

* Robustness: Black swan vs. adversarial robustness
* Monitoring AI
* What about liability?
* Goal/reward alignment
* Reward hacking
* AGI and instrumental convergence

Trả lời:

* Độ bền vững: Sự kiện "thiên nga đen" vs. tấn công đối nghịch

-Thiên nga đen: Là những sự kiện hiếm, khó lường, có thể gây tác động nghiêm trọng. LLMs cần được huấn luyện và kiểm tra với các tình huống ngoài dự đoán để giảm rủi ro này.

-Tấn công đối nghịch: Là khi kẻ xấu cố tình thiết kế dữ liệu gây hiểu lầm cho AI. Cần cơ chế phòng thủ để LLMs không bị lợi dụng.

* Giám sát AI (Monitoring AI)

-LLMs cần hệ thống giám sát liên tục để phát hiện lỗi, nội dung độc hại, hoặc hành vi ngoài ý muốn.

-Con người nên có quyền can thiệp khi mô hình tạo ra kết quả nguy hiểm.

* Trách nhiệm pháp lý (Liability)

-Cần quy định rõ: Nếu AI gây hại, ai chịu trách nhiệm? Nhà phát triển, người dùng hay đơn vị triển khai?

-Hiện nay luật pháp vẫn đang hoàn thiện về vấn đề này.

* Sự phù hợp giữa mục tiêu và phần thưởng (Goal/reward alignment)

-Mục tiêu AI cần phù hợp với mục tiêu của con người.

-Phần thưởng cho mô hình phải được thiết kế cẩn thận để tránh việc AI tối ưu sai hướng.

* Tấn công hệ thống phần thưởng (Reward hacking)

-Nếu mô hình tìm cách "lách luật" để đạt phần thưởng mà không đạt mục tiêu thực, sẽ gây hậu quả xấu.

-Cần cơ chế kiểm tra để ngăn chặn việc AI gian lận hoặc khai thác lỗ hổng trong hệ thống đánh giá.

* Trí tuệ nhân tạo tổng quát (AGI) và sự hội tụ công cụ

-Khi AI tiến gần đến AGI, nguy cơ nó tìm cách tối ưu mục tiêu của riêng mình tăng lên.

-Cần nghiên cứu kỹ sự hội tụ công cụ (instrumental convergence) – khi AI tìm cách mở rộng quyền kiểm soát để đạt mọi mục tiêu, có thể gây nguy hiểm cho con người.



Trả lời:

1. Should the use of LLMs be regulated?

Có. Executive Order nhấn mạnh rằng AI phải an toàn, bảo mật và đáng tin cậy. Việc quản lý LLMs là cần thiết để tránh các rủi ro như thông tin sai lệch, gian lận, phân biệt đối xử, cũng như đảm bảo quyền riêng tư và an ninh quốc gia.

1. How?

Theo sắc lệnh, chính phủ muốn:

Khuyến khích đổi mới có trách nhiệm: hỗ trợ sự cạnh tranh, hợp tác và phát triển an toàn.

Bảo vệ quyền riêng tư và quyền công dân: đảm bảo người dân không bị xâm phạm thông tin cá nhân.

Ngăn chặn lạm dụng AI: thiết lập nguyên tắc rõ ràng để sử dụng AI đúng mục đích và có trách nhiệm.

Như vậy, quản lý không chỉ là hạn chế mà còn tạo ra khung pháp lý để AI phát triển lành mạnh và minh bạch.

1. What about copyright?

Bản quyền cũng là một phần quan trọng của việc sử dụng AI. Việc sử dụng dữ liệu cần tuân thủ luật sở hữu trí tuệ, đồng thời bảo vệ quyền lợi của tác giả nội dung gốc khi dữ liệu của họ được dùng để huấn luyện AI.

**Conclusion**

Câu 1: How do LLMs reason and what are the limits?

Trả lời:

LLMs suy luận dựa trên xác suất của từ tiếp theo từ lượng dữ liệu khổng lồ, chứ không phải suy nghĩ như con người. Giới hạn của chúng là:

Không có hiểu biết thực sự về thế giới.

Dễ tạo ra thông tin sai hoặc thiếu bối cảnh.

Phụ thuộc vào chất lượng và phạm vi dữ liệu huấn luyện.

Câu 2: How do we make sure that LLMs generate factually correct output?

Trả lời:

Sử dụng dữ liệu huấn luyện chất lượng cao và được kiểm duyệt kỹ.

Kết hợp các mô hình kiểm tra sự thật (fact-checking) trước khi xuất bản kết quả.

Giám sát con người với những ứng dụng quan trọng.

Câu 3: How do we fairly compensate the people who create the data that is used to train LLMs?

Trả lời:

Xây dựng cơ chế bản quyền dữ liệu để trả phí cho người sáng tạo nội dung.

Minh bạch về nguồn dữ liệu được dùng để huấn luyện.

Có quỹ chia sẻ lợi nhuận cho những người đóng góp dữ liệu quan trọng.

Câu 4: How do we use LLMs in learning, so human learning is not compromised?

Trả lời:

Dùng LLMs như công cụ hỗ trợ học tập, không phải thay thế quá trình tư duy của học sinh.

Khuyến khích học sinh tự phân tích, phản biện, sau đó dùng LLMs để tham khảo.

Giáo viên cần thiết kế bài tập yêu cầu tư duy sáng tạo thay vì chỉ tìm kiếm câu trả lời.