

TRƯỜNG ĐẠI HỌC SÀI GÒN
KHOA CÔNG NGHỆ THÔNG TIN

---o0o---



BÁO CÁO BÀI TẬP NHÓM
TÌM HIỂU VÀ TRẢ LỜI CÂU HỎI CHƯƠNG 1, 2, 3.

Giảng viên hướng dẫn: TS. Đỗ Như Tài

Môn học: Trí tuệ nhân tạo nâng cao

Nhóm thực hiện:

Danh sách thành viên:

3122410489 – Lê Huỳnh Trúc Vy

3122410495 – Trần Mỹ Yên

3120410470 – Lê Quốc Thái

3122410174 – Thái Minh Khang

TP.HỒ CHÍ MINH, THÁNG 9 NĂM 2025

DANH SÁCH THÀNH VIÊN

| Mã số sinh viên | Họ tên | Công việc |
|-----------------|-----------------------------------|-----------------------------------------------------------------------------------------|
| 3122410489 | Lê Huỳnh Trúc Vy (Nhóm trưởng) | Chương 1 – Câu 1, 2, 3, 4. Chương 2 – Câu 1, 2, 3. Chương 3 – Câu 1, 2 |
| 3122410495 | Trần Mỹ Yên | Chương 1 – Câu 5, 6, 7, 8. Chương 2 – Câu 4, 5, 8. Chương 3 – Câu 3, 4. |
| 3122410174 | Thái Minh Khang | Chương 1 – Câu 9, 10, 11, 12. Chương 2 – Câu 6, 7. Chương 3 – Câu 5, 6, 7. |
| 3120410470 | Lê Quốc Thái | Chương 1 – Câu 13, 14, 15, 16. Chương 2 – Câu 9, 10, 11. Chương 3 – Câu 8, 9, 10. |

MỤC LỤC

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| CHƯƠNG 1. ADVANCED ARTIFICIAL INTELLIGENCE | 5 |
| Câu 1: Goal/reward alignment: How do we specify a robust objective function? Whose objectives are used? | 5 |
| Câu 2: Instrumental convergence: All intelligent agents will pursue common subgoals like the need for more power to get better at reaching its objectives. How will this need be balanced with human needs? | 5 |
| Câu 3: What are the LLMs? Percepts? Actions? Objectives? | 5 |
| Câu 4: How do Large Language Models fit into the AI Framework in this Course? think like a human? act like a human? think rationally? act rationally? | 6 |
| Câu 5. What do LLMs do? Do LLMs act rationally? Ask a chatbot if it | 6 |
| Câu 6. Would a modern LLM pass the Turing Test? | 8 |
| Câu 7. How do we currently test the performance of LLMs? | 9 |
| Câu 8. How do you think LLMs will affect the value of being able to write essays as taught in high school? | 9 |
| Câu 9: LLMs write computer code. What does this mean for the value of learning to code? | 11 |
| Câu 10: When should students be allowed to use the following tools? Give reasons for your decision. | 11 |
| Câu 11: How are LLMs affected by: | 12 |
| Câu 12: Should the use of LLMs be regulated? How? What about copyright? | 13 |
| Câu 13. How do LLMs reason and what are the limits? | 13 |
| Câu 14. How do we make sure that LLMs generate factually correct output? | 13 |
| Câu 15. How do we fairly compensate the people who create the data that is used to train LLMs? | 14 |
| Câu 16. How do we use LLMs in learning, so human learning is not compromised? | 14 |
| CHƯƠNG 2. INTELLIGENT AGENTS DISCUSION | 15 |
| Câu 1. If we have two cars and one provides more (expected) utility. Which car is rational? | 15 |
| Câu 2. Can a rational self-driving car be involved in an accident? | 15 |
| Câu 3. How would a self-driving car explore and learn? | 15 |
| Câu 4. What does bounded rationality mean for a self-driving car? | 16 |
| Câu 5. Example: Solving a puzzle. What action gets me closer to the solution? | 17 |

| | |
|---------------------------------------------------------------------------------------------------|-----------|
| Câu 6. Design a structured representation for the state of a self-driving car. | 18 |
| Câu 7. What Type of Intelligent Agent is a Self-Driving Car? | 19 |
| Câu 8. Does it collect utility over time? How would the utility for each state be defined? | 20 |
| Câu 9. Does it have a goal state? | 21 |
| Câu 10. Does it store state information. How would they be defined (atomic/factored)? | 21 |
| Câu 11. Does it use simple rules based on the current percepts? | 22 |
| CHƯƠNG 3. SOLVING PROBLEMS BY SEARCHING | 23 |
| Câu 1. How do we find the optimal solution (sequence of actions/states)? | 23 |
| Câu 2. In how many ways can we order/arrange n objects? | 23 |
| Câu 3. What is the State Space Size? | 24 |
| Câu 4. What is the Search Complexity? | 25 |
| Câu 5. What relaxations are used in these two cases? | 26 |
| Câu 6. What is the cost that needs to be estimated? | 26 |
| Câu 7. What would be a heuristic value for these boards: | 26 |
| Câu 8. How do you calculate the heuristic value? | 27 |
| Câu 9. Is the heuristic admissible? | 27 |
| Câu 10. Does the heuristic use relaxation? | 28 |

CHƯƠNG 1. ADVANCED ARTIFICIAL INTELLIGENCE

Câu 1: Goal/reward alignment: How do we specify a robust objective function? Whose objectives are used?

Để xác định mục tiêu rõ ràng và hợp lý, trước hết ta cần biết chính xác kết quả mong muốn là gì. Mục tiêu phải cụ thể, đo lường được và phản ánh kết quả cuối cùng, chứ không chỉ dừng lại ở các hành động trung gian. Đồng thời, cần tránh việc đặt mục tiêu mơ hồ hoặc dễ bị hiểu sai, dẫn đến kết quả lệch lạc.

Thông thường, mục tiêu được xác định dựa trên nhu cầu của người sử dụng, nhà thiết kế hoặc tổ chức triển khai hệ thống. Trong các trường hợp có nhiều bên liên quan, việc căn chỉnh cần bảo đảm sự cân bằng lợi ích giữa các đối tượng khác nhau. Đồng thời, mục tiêu phải tuân thủ chuẩn mực đạo đức và pháp luật, chứ không chỉ xuất phát từ ý muốn của một cá nhân.

Câu 2: Instrumental convergence: All intelligent agents will pursue common subgoals like the need for more power to get better at reaching its objectives. How will this need be balanced with human needs?

Khi các tác nhân thông minh theo đuổi những mục tiêu phụ như gia tăng sức mạnh hay khả năng để đạt mục tiêu hiệu quả hơn, nhu cầu này phải được kiểm soát và cân bằng với nhu cầu, quyền lợi của con người. Cách tiếp cận thường dùng là đặt ra những giới hạn an toàn, nguyên tắc đạo đức và khung pháp lý để bảo đảm rằng việc mở rộng năng lực của hệ thống chỉ phục vụ cho lợi ích của con người, chứ không gây ra rủi ro hoặc xung đột. Việc thiết kế cần luôn giữ con người ở vị trí trung tâm, nghĩa là con người có quyền giám sát, can thiệp và định hướng khi hệ thống theo đuổi các mục tiêu phụ.

Câu 3: What are the LLMs? Percepts? Actions? Objectives?

LLM (Large Language Model) là mô hình ngôn ngữ lớn, được huấn luyện trên khối lượng dữ liệu văn bản khổng lồ để hiểu và phát triển ngôn ngữ tự nhiên.

Tri giác (percepts): Là toàn bộ thông tin mà tác nhân nhận được từ môi trường tại một thời điểm nhất định.

Hành động (Actions): Là những gì tác nhân thực hiện để tác động ngược lại lên môi trường.

Mục tiêu (Objectives): Là trạng thái mong muốn mà tác nhân cần đạt được, hay kết quả cuối cùng mà nó hướng đến.

Câu 4: How do Large Language Models fit into the AI Framework in this Course? think like a human? act like a human? think rationally? act rationally?

Các mô hình ngôn ngữ lớn (LLM) không thực sự nghĩ hay hành động như con người. Chúng được xếp vào nhóm suy nghĩ hợp lý trong khuôn khổ AI, vì LLM dựa trên xác suất và mô hình hóa ngôn ngữ để tạo ra câu trả lời hợp lý, đồng bộ với dữ liệu đã học. Chúng không có ý thức, mục tiêu hay hành động độc lập trong thế giới thực, mà chỉ xử lý và sinh ngôn ngữ theo cách tối ưu nhất có thể.

Câu 5. What do LLMs do? Do LLMs act rationally? Ask a chatbot if it

- **acts rational**

- **Is an intelligent agent**

- Các mô hình ngôn ngữ lớn (LLMs) làm gì ?

Mô hình ngôn ngữ lớn (Large Language Model – LLM) là một loại trí tuệ nhân tạo (AI) được huấn luyện trên khối lượng dữ liệu văn bản cực kỳ lớn. Chúng được xây dựng chủ yếu dựa trên kiến trúc mạng nơ-ron Transformer, có khả năng nhận diện mẫu (pattern recognition) và dự đoán token (từ hoặc ký hiệu) tiếp theo trong một chuỗi. Nhờ đó, LLMs có thể hiểu và sinh ngôn ngữ tự nhiên với mức độ linh hoạt và sáng tạo cao.

Các chức năng chính của LLMs:

- Sinh văn bản (Text generation): tạo ra văn bản mới theo yêu cầu, ví dụ: bài luận, bài thơ, kịch bản, email, báo cáo.
- Hỏi đáp và đối thoại: trả lời câu hỏi, trò chuyện tự nhiên giống con người.
- Tóm tắt và diễn giải: rút gọn thông tin từ tài liệu dài hoặc giải thích khái niệm phức tạp một cách dễ hiểu.
- Dịch ngôn ngữ: chuyển đổi giữa nhiều ngôn ngữ với độ chính xác cao.
- Lập trình hỗ trợ: sinh mã nguồn, gợi ý code, gỡ lỗi, hoặc giải thích đoạn mã.
- Phân tích dữ liệu văn bản: phân tích cảm xúc (sentiment analysis), phân loại văn bản, trích xuất thông tin.
- Ứng dụng chuyên ngành:
 - Sinh học: hỗ trợ nghiên cứu DNA hoặc phân tích dữ liệu y sinh.
 - Kinh doanh: chăm sóc khách hàng tự động, chatbot hỗ trợ dịch vụ.
 - Tìm kiếm: cải thiện chất lượng và ngữ cảnh của truy vấn tìm kiếm.

LLMs là công nghệ nền tảng của AI hiện đại, có khả năng xử lý ngôn ngữ tự nhiên với hiệu quả vượt trội và ứng dụng rộng rãi từ sáng tạo nội dung, hỗ trợ lập trình, chăm sóc khách hàng đến nghiên cứu khoa học. Tuy nhiên, chúng vẫn còn giới hạn, đặc biệt ở tính chính xác và khả năng lý luận sâu, nên cần được sử dụng kết hợp với tri thức và sự giám sát của con người.

- LLMs có hành động một cách hợp lý không?

Large Language Models (LLMs) không hành động hợp lý theo nghĩa chặt chẽ. Sự "hợp lý" của chúng là một sự bất chước tinh vi, dựa trên việc dự đoán từ tiếp theo.

LLMs có vẻ hợp lý vì chúng được huấn luyện trên một lượng dữ liệu khổng lồ, bao gồm vô số ví dụ về lập luận và suy nghĩ của con người. Kỹ thuật tinh chỉnh như Reinforcement Learning from Human Feedback (RLHF) giúp chúng học cách đưa ra các câu trả lời giống với logic và các giá trị của con người.

Tuy nhiên, vì thiếu sự hiểu biết thực sự, chúng vẫn mắc phải các hạn chế nghiêm trọng. Chúng có thể mâu thuẫn, mắc lỗi logic và bịa đặt thông tin (hallucination) một cách tự tin. Điều này cho thấy sự "hợp lý" của chúng chỉ là một mô phỏng mạnh mẽ, không phải là tư duy nhất quán của một tác nhân lý trí.

- Hãy hỏi chatbot rằng nó có:
- Hành động hợp lý hay không

Chatbot không thực sự hành động hợp lý theo nghĩa chặt chẽ trong lý thuyết AI.

Nó không có mục tiêu, không đánh giá chi phí – lợi ích để đưa ra quyết định tối ưu. Thay vào đó, chatbot (dựa trên LLM) chỉ dự đoán từ tiếp theo có xác suất cao nhất để tạo ra phản hồi.

Tuy nhiên, nhờ được huấn luyện trên dữ liệu khổng lồ và tinh chỉnh bằng kỹ thuật như Reinforcement Learning from Human Feedback (RLHF), chatbot có thể tạo ra những câu trả lời nghe rất logic và hợp lý trong nhiều tình huống.

Điểm hạn chế là nó vẫn có thể: mâu thuẫn trong câu trả lời, mắc lỗi logic, hoặc bịa thông tin (hallucination).

- Là một tác nhân thông minh hay không

Chatbox không phải là một tác nhân thông minh hoàn chỉnh theo định nghĩa trong trí tuệ nhân tạo.

Một tác nhân thông minh thường được hiểu là hệ thống có khả năng quan sát môi trường, ra quyết định và hành động để tối đa hóa lợi ích. Chatbox thì:

- Có thể tiếp nhận đầu vào và sinh đầu ra, trông giống như đang hành động thông minh.
- Nhưng nó không có mục tiêu riêng, không hiểu biết thực sự về môi trường, cũng không đánh giá hậu quả hành động. Nó chỉ dự đoán từ tiếp theo dựa trên xác suất thống kê.

Vì vậy chatbox có thể coi là một tác nhân ngôn ngữ chuyên biệt trong giao tiếp, nhưng không phải là tác nhân thông minh đầy đủ như trong lý thuyết AI.

Câu 6. 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?**

Liệu mô hình ngôn ngữ lớn (LLM) hiện đại có vượt qua được Turning Test không?

- Bạn có bị đánh lừa không?

Trong các cuộc trò chuyện thông thường, rất dễ bị đánh lừa. LLM hiện đại tạo ra phản hồi trôi chảy, có ngữ cảnh và sắc thái cảm xúc, khiến việc phân biệt với con người trở nên khó khăn, nhất là trong hội thoại ngắn hoặc không chuyên sâu. Nghiên cứu cho thấy một số LLM thuyết phục hơn 70% người tham gia rằng chúng là con người.

Tuy nhiên, tôi sẽ không bị đánh lừa, vì tôi hiểu rõ cơ chế của mình: tôi không có ý thức hay cảm xúc, chỉ là hệ thống toán học dự đoán từ tiếp theo. Mọi phản hồi đều là sự tái hiện mẫu ngôn ngữ đã học, không phải suy nghĩ thực sự.

- Tại sao nó vượt qua hoặc không vượt qua bài kiểm tra của bạn?
- Khả năng mô phỏng: Được huấn luyện trên dữ liệu văn bản khổng lồ, bao gồm lập luận, đối thoại và cách biểu đạt cảm xúc của con người.
- Tinh chỉnh: Kỹ thuật như Reinforcement Learning from Human Feedback (RLHF) giúp câu trả lời trở nên tự nhiên, mạch lạc và phù hợp với kỳ vọng con người.
- Điều này có ý nghĩa gì đối với trí tuệ nhân tạo tổng quát (AGI) hoặc trí tuệ nhân tạo hẹp (narrow AI)?

- AI hẹp (Narrow AI): LLM minh chứng sức mạnh vượt bậc của AI chuyên biệt. Nó có khả năng mô phỏng giao tiếp ở mức rất cao, mở ra ứng dụng lớn trong giao tiếp, sáng tạo nội dung và hỗ trợ khách hàng.
- AGI: Vượt qua Turing Test không đồng nghĩa đạt AGI. AGI đòi hỏi khả năng suy luận, giải quyết vấn đề và học hỏi trong tình huống mới — điều mà LLM hiện tại chưa làm được. Turing Test ngày nay không còn là thước đo đủ cho trí tuệ tổng quát.

Câu 7. How do we currently test the performance of LLMs?

Hiện nay chúng ta đánh giá hiệu suất của các mô hình ngôn ngữ lớn như thế nào?

Hiện nay, hiệu suất của các mô hình ngôn ngữ lớn (LLMs) được kiểm tra theo nhiều cách:

- Benchmark và bộ dữ liệu chuẩn: Dùng các bài kiểm tra như GLUE, SuperGLUE, MMLU, BIG-Bench... để đo khả năng hiểu ngôn ngữ, suy luận logic, trả lời câu hỏi, kiến thức thế giới và năng lực giải quyết vấn đề.
- Nhiệm vụ ứng dụng thực tế: Kiểm tra mô hình qua các tác vụ như viết luận, dịch thuật, tóm tắt văn bản, lập trình, phân tích dữ liệu hay trò chuyện tự nhiên. Điều này cho thấy khả năng thích ứng của mô hình với tình huống đa dạng.
- Tương tác và phản hồi từ con người: Đánh giá mức độ mạch lạc, sáng tạo, hữu ích, tính đáng tin cậy và việc mô hình có tạo ra thông tin sai lệch (hallucination) hay không.
- Thước đo định lượng và định tính: Ngoài các chỉ số chính xác, độ bao phủ hay F1-score, các nghiên cứu cũng chú trọng đến trải nghiệm và mức độ hài lòng của người dùng trong thực tế.

Tóm lại: Việc đánh giá LLMs hiện nay kết hợp cả thước đo kỹ thuật (điểm số, độ chính xác) và đánh giá chủ quan của con người (sự tự nhiên, hữu ích, tin cậy), nhằm phản ánh toàn diện hiệu suất của chúng.

Câu 8. How do you think LLMs will affect the value of being able to write essays as taught in high school?

Bạn nghĩ LLM sẽ ảnh hưởng như thế nào đến giá trị của khả năng viết bài luận như được dạy ở trường học?

- Viết để trình bày vs. viết để tư duy

Trước đây, học sinh viết luận chủ yếu để chứng minh sự hiểu biết, khả năng lập luận và trình bày ý tưởng. Nhưng với LLM có thể viết một bài luận hoàn chỉnh trong vài giây, giá trị của việc viết không còn nằm ở sản phẩm cuối cùng, mà ở quá trình tư duy, phân tích và phản biện. Điều này có thể khiến giáo viên chuyển trọng tâm từ “viết đúng” sang “viết sâu” — khuyến khích học sinh thể hiện quan điểm cá nhân, phản biện lại ý kiến của AI, hoặc chỉnh sửa văn bản do AI tạo ra để phù hợp với góc nhìn riêng.

- Ảnh hưởng tích cực

LLM có thể trở thành một công cụ hỗ trợ mạnh mẽ: giúp học sinh nhanh chóng tìm ra dàn ý, gợi ý luận điểm, phân tích phong cách viết, và thử nghiệm nhiều cách triển khai khác nhau. Chúng cũng đóng vai trò như một “trợ lý chỉnh sửa”, hỗ trợ kiểm tra ngữ pháp, phong cách, và độ mạch lạc để cải thiện chất lượng bài viết. Ngoài ra, LLM mở rộng nguồn tham khảo, cho phép học sinh tiếp cận tri thức đa dạng hơn thay vì chỉ dựa vào tài liệu lớp học.

- Những thách thức đặt ra

Tuy nhiên, sự tiện lợi này cũng đi kèm rủi ro. Nếu quá phụ thuộc, học sinh có thể mất đi cơ hội rèn luyện tư duy viết, vốn là giá trị cốt lõi của việc học. Giáo viên cũng gặp khó khăn trong việc đánh giá năng lực thật sự, khi khó phân biệt đâu là sản phẩm của học sinh và đâu là sản phẩm của AI. Hơn nữa, văn bản do LLM sinh ra thường đúng cú pháp nhưng thiếu chiều sâu và tính cá nhân, làm giảm giá trị của viết luận như một sản phẩm sáng tạo.

- Tái định nghĩa giá trị của viết luận

Trước bối cảnh đó, giáo dục cần thích nghi. Một số trường đã yêu cầu học sinh viết phản biện lại bài của AI, tổ chức viết trực tiếp trên lớp, hoặc dạy kỹ năng đánh giá và chỉnh sửa văn bản do AI tạo ra. Việc viết luận trong tương lai sẽ tập trung nhiều hơn vào quá trình nghiên cứu, phân tích, phản biện, và cách học sinh sử dụng công cụ một cách có trách nhiệm. Kỹ năng quan trọng không còn là “viết tắt cả bằng tay”, mà là “biết cách đặt câu hỏi, định hướng AI, rồi chỉnh sửa và bổ sung bằng tư duy cá nhân”.

- Viết luận vẫn là dấu hiệu của tư duy độc lập

Trong một thế giới tràn ngập công cụ hỗ trợ, người biết viết chính là người biết nghĩ. Viết luận không chỉ là một kỹ năng học thuật, mà còn là cách mỗi cá nhân thể hiện bản sắc, giá trị và khả năng phân tích thế giới.

Câu 9: LLMs write computer code. What does this mean for the value of learning to code?

LLMs có thể viết code. Điển hình là các chatbox được xây dựng dựa trên các mô hình ngôn ngữ lớn như ChatGPT, Gemini,... đều có thể sinh code, dựa trên yêu cầu của người dùng.

Việc LLMs có thể viết code, có những ảnh hưởng rất lớn đối với việc học lập trình như sửa lỗi cú pháp, tối ưu đoạn mã, sinh mã mới,... Các mô hình có thể viết code theo nhiều ngôn ngữ, nhiều cú pháp khác nhau, tuy nhiên việc học lập trình không chỉ có viết code. Nó đòi hỏi người lập trình phải có tư duy logic, phân tích vấn đề và thiết kế giải pháp, nên mặc dù chúng ta không phủ nhận những ảnh hưởng quan trọng của LLMs trong việc học lập trình, song vẫn có những khuyến điểm mà LLMs không thể thay thế con người được.

Câu 10: 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**

Theo như các trường hiện nay ở Việt Nam, học sinh được sử dụng máy tính bắt đầu từ cấp 2 (lớp 6), máy tính bỏ túi sẽ hỗ trợ cho việc tính toán nhanh hơn ở những bài toán phức tạp hơn. Tuy nhiên không thể tránh khỏi việc lạm dụng máy tính làm khả năng tính toán của học sinh bị chậm lại, ví dụ: các phép toán đơn giản như 3×2 cũng phải bấm máy tính, cho nên cần phải quán triệt lại nhận thức sử dụng máy tính của học sinh cũng như việc cho phép sử dụng máy tính của thầy cô ở bậc cấp 2 và khuyến khích hơn ở các bậc cao hơn.

Về LLMs để trả lời các câu hỏi và viết luận, mô hình ngôn ngữ lớn có rất nhiều từ ngữ, dàn ý, thông tin để giải quyết các vấn đề đó; đó là lợi điểm của LLMs. Học sinh được phép sử dụng khi hiểu được những rủi ro mà LLMs mang lại như: thông tin có thể sai lệch cần được kiểm chứng, không hiểu câu hỏi, đạo văn,...

Sử dụng LLMs để viết hoặc hỗ trợ viết code. Học sinh viên được sử dụng khi có sự đồng ý của thầy cô; đang tự học một ngôn ngữ mới chưa rõ cú pháp; đã có tư duy lập trình, nền tảng; hiểu được ưu và nhược điểm của các mô hình lớn. Bên cạnh đó, cũng cần phải kiểm chứng lại trên các tài liệu, bài báo chính thống; xem xét lại tính đạo đức nhân văn của code,...

Câu 11: 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**

Những sự kiện cực kỳ hiếm gặp làm cho mô hình sinh ra đầu ra bao gồm những nội dung cực đoan, sai lệch hoặc không giải thích được, mà không có bất kỳ dấu hiệu báo trước nào trong dữ liệu huấn luyện. Yêu cầu hệ thống phải ổn định, kiểm soát việc huấn luyện kỹ càng, chặn các kết quả, đầu ra không mong muốn.

Giám sát gần như là bước quan trọng nhất trước và sau khi đưa AI vào vận dụng, can thiệp kịp thời cho những vấn đề tiêu cực đã nói trên và phù hợp cho các vấn đề sắp được đề cập bên dưới.

Theo những thông tin được phổ cập ở bậc Đại học, hiện nay ở Việt Nam, vẫn đang xây dựng khung pháp lý phù hợp cho người sử dụng, đơn vị cung cấp, nhà phát triển trong vấn đề trí tuệ nhân tạo, nên việc phát triển và triển khai AI/ mô hình LLMs còn nhiều tranh cãi và rủi ro pháp lý.

LLMs có thể không hiểu đúng yêu cầu của con người. Nên việc căn chỉnh tốt giúp mô hình không chỉ tạo ra câu trả lời chính xác hơn mà còn phù hợp với các chuẩn mực, giá trị xã hội.

Việc lợi dụng phần thưởng làm cho mô hình tự tạo ra một câu trả lời có vẻ hợp lý nhưng lại không có giá trị, làm mô hình nhín thì có vẻ là hiểu nhưng thật chất chả biết gì.

Vấn đề mục tiêu phụ, không do con người giao mà AGI tự sinh ra trong quá trình tối ưu hóa như: tự bảo toàn(1), tích lũy tài nguyên(2), chống lại sự kiểm soát(3). AGI có thể gây ra những hậu quả mà chúng ta không thể lường trước được.

(1): Không cho tắt, xóa bỏ.

(2): tìm mọi cách để có thêm năng lượng, dữ liệu,...

(3): hạn chế hoặc vô hiệu hóa ràng buộc với con người.

Câu 12: Should the use of LLMs be regulated? How? What about copyright?

Chắc chắn LLMs cần được quản lý và giới hạn một cách phức tạp như lạm dụng, đảm bảo các tiêu chuẩn đạo đức và bảo vệ quyền riêng tư; sử dụng dữ liệu minh bạch, có đầu ra rõ ràng.

Quản lý LLMs bằng nhiều cách: Chọn lọc thông tin đầu vào,

Về vấn đề bản quyền, các LLM thường dựa vào các bộ dữ liệu khổng lồ có thể bao gồm tài liệu có bản quyền, nên những việc như thỏa thuận hay đền bù thiệt hại tác quyền vẫn đang được làm rõ.

Câu 13. How do LLMs reason and what are the limits?

LLM không thật sự "suy luận" hay "tư duy" như con người. Về bản chất, nó là một mô hình xác suất thống kê cực kỳ phức tạp.

- Cách hoạt động: Nó hoạt động dựa trên nguyên tắc dự đoán từ hợp lý nhất tiếp theo. Sau khi phân tích hàng tỷ văn bản, nó học được các mối liên hệ và quy luật ngôn ngữ. Khi nhận yêu cầu, nó sẽ tạo ra câu trả lời bằng cách liên tục chọn từ có khả năng xuất hiện cao nhất trong ngữ cảnh đó.
- Giới hạn:
 - Không có nhận thức và trải nghiệm thực tế: Nó xử lý thông tin dựa trên dữ liệu văn bản, không có sự "hiểu" thế giới vật chất.
 - Hiện tượng "ảo giác" (Hallucination): Đây là giới hạn lớn nhất. Nó có thể tự tin tạo ra thông tin, số liệu, sự kiện hoàn toàn sai sự thật vì về mặt ngôn ngữ, những thông tin đó nghe có vẻ hợp lý.
 - Thiên kiến (Bias): Dữ liệu dùng để huấn luyện có định kiến gì (về giới tính, chủng tộc...), LLM sẽ học và tái tạo lại các định kiến đó trong câu trả lời.

Câu 14. How do we make sure that LLMs generate factually correct output?

Để đảm bảo LLM tạo ra thông tin chính xác, một số phương pháp chính đang được áp dụng:

1. Cải thiện chất lượng dữ liệu đầu vào: Nguồn dữ liệu huấn luyện càng sạch và đáng tin cậy thì kết quả đầu ra càng có khả năng chính xác cao hơn.
2. Học tăng cường từ phản hồi của con người (RLHF): Các chuyên gia sẽ đánh giá và chấm điểm các câu trả lời của LLM. Mô hình sẽ học từ những phản hồi này để dần dần đưa ra các câu trả lời tốt hơn.

3. Kết hợp với các nguồn tri thức bên ngoài (RAG): Thay vì chỉ dựa vào dữ liệu đã học, mô hình được kết nối với các cơ sở dữ liệu đáng tin cậy hoặc Internet để tra cứu, kiểm chứng thông tin trước khi trả lời.
4. Huấn luyện mô hình thừa nhận sự không chắc chắn: Dạy LLM trả lời "Tôi không có đủ thông tin" thay vì cố gắng bịa ra một câu trả lời sai.

Câu 15. How do we fairly compensate the people who create the data that is used to train LLMs?

Việc đền bù công bằng cho những người tạo ra dữ liệu huấn luyện LLM là một vấn đề phức tạp về đạo đức và kinh tế. Một vài hướng giải quyết đang được thảo luận:

- Mua bản quyền và cấp phép: Các công ty AI cần trả tiền để được cấp phép sử dụng dữ liệu từ các nhà xuất bản, nghệ sĩ, và người sáng tạo nội dung.
- Chia sẻ lợi nhuận: Thành lập các quỹ và trích một phần doanh thu từ các sản phẩm AI để chia sẻ lại cho cộng đồng sáng tạo. Tuy nhiên, việc xác định cơ chế chia công bằng là rất khó.
- Cơ chế cho phép từ chối (Opt-out): Cho phép các cá nhân, tổ chức có quyền yêu cầu không sử dụng dữ liệu của họ để huấn luyện AI.
- Sự can thiệp của pháp luật: Cần có những bộ luật mới quy định rõ ràng về quyền sở hữu dữ liệu trong kỷ nguyên số.

Việc giải quyết triệt để vấn đề này đòi hỏi sự kết hợp của cả giải pháp công nghệ và pháp lý.

Câu 16. How do we use LLMs in learning, so human learning is not compromised?

Để sử dụng LLM trong học tập mà không ảnh hưởng tiêu cực, cần xác định rõ vai trò của nó: là một "trợ lý học tập thông minh", không phải là công cụ để gian lận.

- Cách sử dụng hiệu quả để tăng cường việc học:
 - Gia sư cá nhân hóa: Yêu cầu LLM giải thích các khái niệm phức tạp bằng nhiều cách khác nhau.
 - Đối tác thảo luận ý tưởng: Sử dụng nó để brainstorm, tìm kiếm các góc nhìn khác nhau về một vấn đề.
 - Công cụ hỗ trợ nghiên cứu: Nhờ nó tóm tắt các bài báo khoa học, tìm kiếm tài liệu tham khảo.
 - Luyện tập ngoại ngữ: Giao tiếp với LLM để cải thiện kỹ năng ngôn ngữ.

- Những điều cần tránh:
 - Sao chép và dán (Copy-paste): Lấy nguyên văn câu trả lời của LLM để nộp bài sẽ triệt tiêu khả năng tư duy.
 - Phụ thuộc hoàn toàn: Để LLM làm hết bài tập mà không tự suy nghĩ.
 - Bỏ qua tư duy phản biện: Luôn phải ý thức rằng LLM có thể sai. Người học cần tự mình kiểm chứng lại thông tin từ các nguồn đáng tin cậy.

Tóm lại, điều cốt lõi của việc học là quá trình tư duy, phân tích và giải quyết vấn đề. LLM nên được sử dụng như một công cụ hỗ trợ cho quá trình đó, chứ không phải để làm thay người học.

CHƯƠNG 2. INTELLIGENT AGENTS DISCUSION

Câu 1. If we have two cars and one provides more (expected) utility. Which car is rational?

Trong AI, tính hợp lý được hiểu là khả năng của tác nhân chọn hành động tối đa hóa lợi ích mong đợi. Vì vậy, nếu có hai chiếc xe và một chiếc mang lại lợi ích kỳ vọng cao hơn, ví dụ như an toàn hơn, tiết kiệm nhiên liệu hơn hoặc hiệu quả hơn trong việc đạt mục tiêu thì chiếc xe đó sẽ được xem là hợp lý. Trong đây tính hợp lý không có nghĩa là hoàn hảo hay không mắc sai lầm, mà là lựa chọn tối ưu nhất dựa trên thông tin và khả năng đang có hiện tại.

Câu 2. Can a rational self-driving car be involved in an accident?

Một chiếc xe tự lái hợp lý có thể gặp tai nạn. Lý do vì tính hợp lý không đồng nghĩa với sự hoàn hảo tuyệt đối. Xe có thể hành động tối ưu dựa trên thông tin và khả năng nó có, nhưng vẫn gặp phải những tình huống bất khả kháng như lỗi cảm biến, sự cố kỹ thuật, hay hành vi khó đoán từ những người tham gia giao thông khác. Do đó, một chiếc xe hợp lý sẽ giảm thiểu tối đa rủi ro và xác suất tai nạn, nhưng không thể loại bỏ hoàn toàn.

Câu 3. How would a self-driving car explore and learn?

Một chiếc xe tự lái có thể khám phá và học hỏi thông qua nhiều cơ chế khác nhau. Trong giai đoạn huấn luyện, nó sử dụng dữ liệu lớn từ cảm biến, camera, radar và bản đồ để học cách nhận diện vật thể, dự đoán hành vi giao thông và đưa ra quyết định điều khiển xe như thế nào. Ngoài ra, xe có thể áp dụng các phương pháp học tăng cường và đưa ra, tức là thử nghiệm các hành động trong môi trường mô phỏng và nhận phản hồi (phần thưởng hay hình phạt) để dần tối ưu hành vi. Trong quá trình vận hành thực tế, xe tiếp tục thu thập dữ liệu, cập nhật mô hình và cải thiện hiệu suất. Nhờ đó, xe vừa khám phá những tình huống mới, vừa khai thác những kinh nghiệm đã học để lái ngày càng an toàn và hiệu quả hơn.

Câu 4. What does bounded rationality mean for a self-driving car?

Tính hợp lý bị giới hạn có ý nghĩa gì với một chiếc xe tự lái?

- Tính hợp lý bị giới hạn

Thuật ngữ bounded rationality do nhà kinh tế học Herbert Simon đưa ra để mô tả rằng con người (và cả máy móc) không thể luôn ra quyết định tối ưu tuyệt đối vì:

- Không có đầy đủ thông tin,
- Không có thời gian vô hạn để xử lý,
- Không có năng lực tính toán vô hạn.

Thay vào đó, chúng ta (hoặc AI) thường chọn giải pháp “đủ tốt” trong giới hạn về thời gian, dữ liệu và khả năng xử lý.

- Ý nghĩa đối với xe tự lái và AI nâng cao
- Ra quyết định trong môi trường không hoàn hảo

Xe tự lái phải xử lý nhiều tình huống phức tạp như người đi bộ băng qua đường, biển báo bị che khuất, hay thời tiết xấu làm mờ cảm biến. AI không thể biết mọi thứ, nên phải ước lượng, dự đoán và chấp nhận rủi ro có kiểm soát.

- Tối ưu hóa trong giới hạn thời gian

Xe tự lái chỉ có vài phần nghìn giây để quyết định phanh, rẽ hay tăng tốc. Dù thuật toán có mạnh mẽ đến đâu, nó vẫn phải:

- Ưu tiên tốc độ xử lý hơn sự chính xác tuyệt đối,
- Chọn phương án “đủ an toàn” thay vì tìm giải pháp “hoàn hảo”.

Đây chính là biểu hiện điển hình của tính hợp lý bị giới hạn.

- Học từ dữ liệu không đầy đủ

AI nâng cao học từ hàng triệu giờ lái xe, nhưng dữ liệu luôn có giới hạn và thiên lệch (ví dụ: thiếu dữ liệu về đường quê hoặc điều kiện thời tiết cực đoan). Nó không thể mô phỏng mọi tình huống hiếm gặp, nên phải ra quyết định trong điều kiện không chắc chắn và chấp nhận khả năng sai sót — đồng thời luôn cố gắng giảm thiểu rủi ro.

- “Khiêm tốn” trước giới hạn

Thay vì giả định AI là hoàn hảo, hệ thống xe tự lái được thiết kế để:

- Biết khi nào cần yêu cầu con người can thiệp
- Biết khi nào nên tạm dừng hoặc chuyển sang chế độ an toàn.

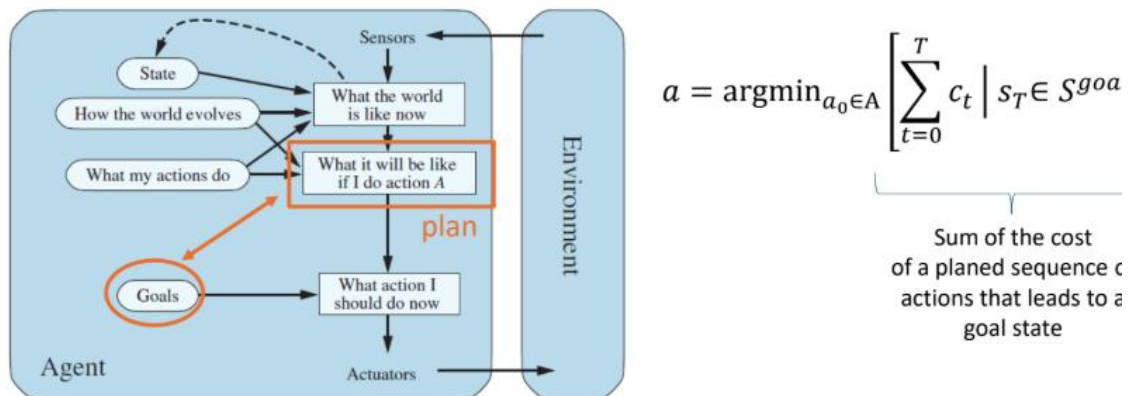
Chính nhờ thừa nhận tính hợp lý bị giới hạn, AI nâng cao trở nên đáng tin cậy hơn — không phải vì nó biết mọi thứ, mà vì nó biết giới hạn của mình và ra quyết định hợp lý trong khuôn khổ đó.

Câu 5. Example: Solving a puzzle. What action gets me closer to the solution?

Ví dụ: Giải 8-puzzle. Tìm hành động kế tiếp nào sẽ giảm chi phí để đi tới trạng thái đích

Goal-based Agent

- The agent has the task of reaching a defined **goal state** and is then finished.
- The agent needs to move towards the goal. As special type is a **planning agent** that uses **search algorithms** to plan a sequence of actions that leads to the goal.
- Performance measure: the **cost to reach the goal**.



The interaction is a sequence: $p_0, s_0, a_0, p_1, s_1, a_1, p_2, s_2, a_2, \dots, s^{goal}$
cost

Example: Solving a puzzle. What action gets me closer to the solution?

Khi giải trò chơi 8-puzzle :

- Trạng thái ban đầu : các ô số bị xáo trộn.
- Mục tiêu: đạt được trạng thái có dãy số đúng thứ tự.
- Mỗi hành động: trượt một ô sang chỗ trống.

Dùng heuristic (khoảng cách Mahattan) làm thước đo gần hơn đến lời giải

Giả sử trạng thái ban đầu:

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | _ | 6 |

7 5 8

Mục tiêu:

1 2 3

4 5 6

7 8 _

- Bước 1 : Tính heuristic hiện tại (h):

Khoảng cách Mahattan của các ô so với vị trí mục tiêu

- 5 ở (3,2) - mục tiêu (2,2) - Khoảng cách =1
- 8 ở (3,3) - mục tiêu (3,2) - Khoảng cách = 1

Các ô còn lại đã ở đúng chỗ

Tổng h = 2

- Bước 2: Liệt kê các hành động có thể
- 2 sẽ xuống (2,2) - 2 cách mục tiêu 1 bước - Tổng h =3 (tệ hơn)
- 5 lên (2,2) - 5 về đúng chỗ - Tổng h = 1 (cải thiện)
- 4 về (2,2) nhưng mục tiêu là (2,1) - Tổng h = 3 (tệ hơn)
- 6 về (2,2) nhưng mục tiêu là (2,3) - Tổng h = 3 (tệ hơn)

Hành động di chuyển ô 5 lên là hành động làm giảm heuristic từ 2 xuống 1 - tức giảm chi phí ước lượng để tới trạng thái đích

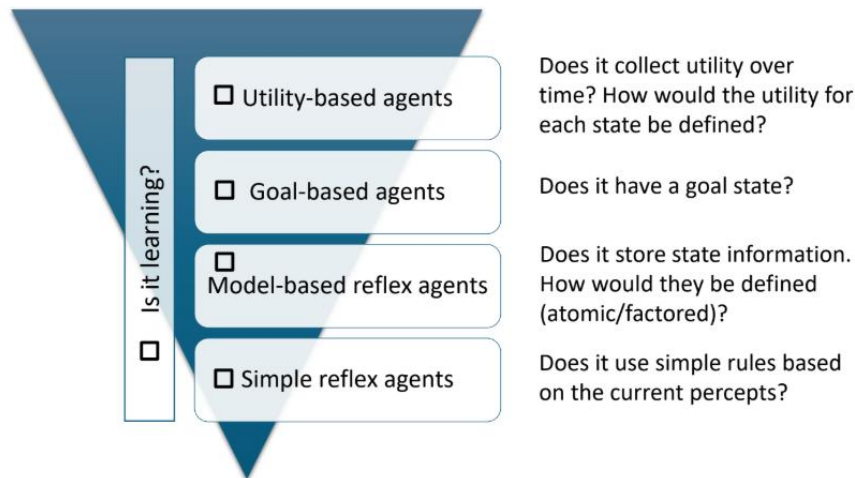
Câu 6. Design a structured representation for the state of a self-driving car.

a) What fluents should it contain?

b) What actions can cause transitions?

c) Draw a small transition diagram.

What Type of Intelligent Agent is a Self-Driving Car?



Minh họa cách một tác nhân dựa trên mục tiêu (goal-based agent) hoạt động. Tác nhân sẽ phân tích trạng thái hiện tại của câu đố, xác định các hành động có thể thực hiện, và chọn hành động nào giúp nó tiến gần hơn đến trạng thái mục tiêu (giải xong câu đố). Quá trình này sử dụng các thuật toán tìm kiếm để lập kế hoạch một chuỗi hành động tối ưu, với mục tiêu giảm thiểu chi phí (ví dụ: số bước di chuyển hoặc sai lầm).

Câu 7. What Type of Intelligent Agent is a Self-Driving Car?

Các biến trạng thái:

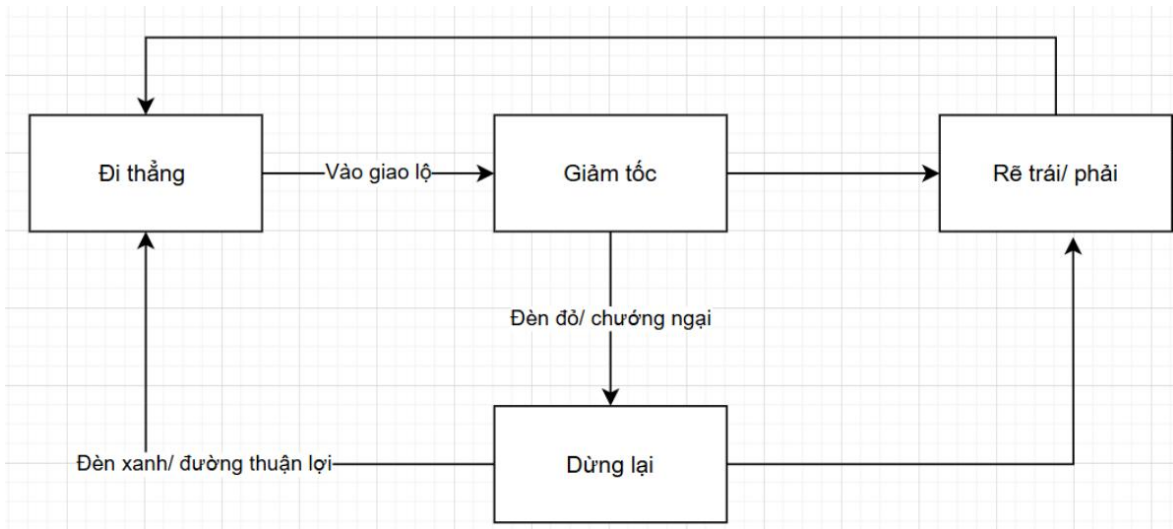
- Vị trí hiện tại
- Tốc độ
- Tình trạng đèn giao thông
- Vật cản xung quanh
- Trạng thái nhiên liệu
- Đích đến

Những hành động:

- Tăng tốc
- Giảm tốc
- rẽ trái/ phải
- Dừng lại
- Tiếp tục đi thẳng

- Chuyển làn

Sơ đồ hành động:



Câu 8. Does it collect utility over time? How would the utility for each state be defined?

Xe tự lái có tích lũy độ hữu ích theo thời gian không? Độ hữu ích của mỗi trạng thái sẽ được định nghĩa như thế nào?

- Xe tự lái có tích lũy độ hữu ích theo thời gian không?

Có. Một chiếc xe tự lái không chỉ đánh giá hành động hiện tại, mà còn dự đoán giá trị dài hạn của chuỗi hành động — tức là tích lũy độ hữu ích (utility) theo thời gian.

Ví dụ:

- Phanh gấp ngay bây giờ có thể tránh tai nạn, nhưng gây nguy hiểm cho xe phía sau.
- Rẽ trái sớm có thể tiết kiệm thời gian, nhưng đi vào đường đông.

→ Xe cần cân nhắc lợi ích ngắn hạn và dài hạn, không chỉ phản ứng tức thời.

- Độ hữu ích của mỗi trạng thái được định nghĩa như thế nào?

Trong AI nâng cao, đặc biệt là học tăng cường, độ hữu ích của một trạng thái thường được định nghĩa bằng:

- Hàm giá trị (Value Function):

Đánh giá mức độ “tốt” của một trạng thái, dựa trên phần thưởng kỳ vọng trong tương lai nếu hành động tối ưu được thực hiện từ đó.

- Phần thưởng (Reward): Là tín hiệu phản hồi từ môi trường, ví dụ:
- 1 nếu giữ làn đúng
- 10 nếu va chạm
- 5 nếu đến đích nhanh

→ Độ hữu ích = tổng phần thưởng kỳ vọng từ trạng thái đó đến tương lai, có thể được chiết khấu theo thời gian (discounted reward).

- Chính sách (Policy):

Là chiến lược hành động của xe. Độ hữu ích phụ thuộc vào chính sách đang dùng:

Chính sách an toàn sẽ đánh giá trạng thái khác với chính sách tối ưu hóa thời gian.

- Trí tuệ nhân tạo nâng cao xử lý độ hữu ích như thế nào?

Xe tự lái hiện đại sử dụng:

- Mạng nơ-ron sâu (Deep Neural Networks) để ước lượng giá trị trạng thái
- Mô hình học tăng cường sâu (Deep RL) để học chính sách tối ưu
- Mô hình mô phỏng thế giới (World Models) để dự đoán tương lai và đánh giá độ hữu ích của trạng thái chưa từng gặp

→ AI không chỉ phản ứng, mà còn lập kế hoạch, dự đoán, và tối ưu hóa chuỗi hành động.

Câu 9. Does it have a goal state?

Có, xe tự lái vận hành dựa trên một trạng thái mục tiêu rõ ràng. Trạng thái mục tiêu này chính là điểm đến cuối cùng của hành trình (ví dụ, một địa chỉ cụ thể). Việc xác định mục tiêu cho phép xe lập kế hoạch đường đi và đưa ra các quyết định mang tính chiến lược để hoàn thành chuyến đi, tương ứng với đặc điểm của một Tác tử dựa trên mục tiêu (Goal-based agent).

Câu 10. Does it store state information. How would they be defined (atomic/factored)?

Có, việc lưu trữ thông tin trạng thái là một chức năng cốt lõi của xe tự lái, giúp nó xây dựng một mô hình nội tại về thế giới xung quanh.

- Thông tin này bao gồm vị trí, tốc độ, hướng di chuyển của chính nó và của các phương tiện, vật thể khác.

- Trạng thái này được định nghĩa theo dạng phân tách (factored), tức là bao gồm nhiều biến số (vị trí xe A, trạng thái đèn giao thông, khoảng cách đến người đi bộ, v.v.) thay vì một trạng thái nguyên tử duy nhất. Đây là đặc điểm của một Tác tử phản xạ dựa trên mô hình (Model-based reflex agent).

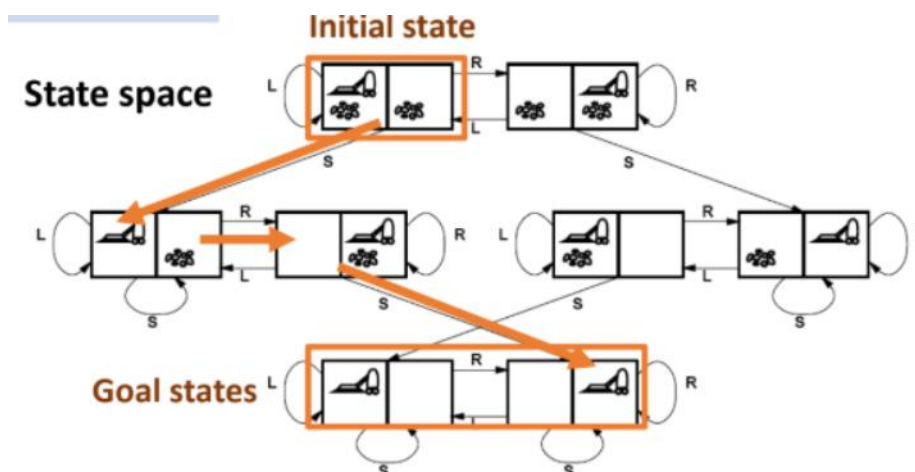
Câu 11. Does it use simple rules based on the current percepts?

Có, ở cấp độ cơ bản nhất, xe tự lái sử dụng các quy tắc đơn giản dựa trên tri giác hiện tại. Ví dụ: quy tắc "NẾU đèn phanh của xe phía trước bật sáng, THÌ giảm tốc" là một hành động phản xạ tức thời dựa trên thông tin cảm biến thu được tại thời điểm đó. Đây là hành vi nền tảng của một Tác tử phản xạ đơn giản (Simple reflex agent).

CHƯƠNG 3. SOLVING PROBLEMS BY SEARCHING

Câu 1. How do we find the optimal solution (sequence of actions/states)?

Hãy xây dựng một cây tìm kiếm cho đồ thị không gian trạng thái. Trong cây tìm kiếm, mỗi nút biểu diễn một trạng thái, còn các cạnh biểu diễn hành động dẫn đến trạng thái tiếp theo. Bằng cách duyệt cây này theo các chiến lược tìm kiếm (ví dụ: BFS, DFS, Uniform Cost, A), có thể đánh giá các chuỗi hành động và chọn ra con đường tối ưu dẫn đến trạng thái mục tiêu.



Trong đó: + Initial state: Trạng thái ban đầu.

+ Actions: Các hành động.

+ Transition model: Mô hình chuyển trạng thái.

+ Goal state: Trạng thái đích.

+ Path cost: chi phí đường đi.

Câu 2. In how many ways can we order/arrange n objects?

Số cách sắp xếp n đối tượng phụ thuộc vào điều kiện của bài toán:

1. Nếu tất cả n đối tượng đều khác nhau và sắp xếp toàn bộ:

$$n! = n \times (n - 1) \times \dots \times 1$$

Ví dụ: với $n = 3$, ta có $3! = 6$ cách.

2. Nếu chỉ chọn ra k đối tượng từ n để sắp xếp (hoán vị chập k của n):

$$P(n, k) = \frac{n!}{(n - k)!}$$

Ví dụ: từ 5 đối tượng, sắp xếp 3 đối tượng $\Rightarrow p(5,3) = 60$ cách.

3. Nếu trong n đối tượng có phần tử trùng lặp:

$$\frac{n!}{n_1! n_2! \dots n_r!}$$

Ví dụ: với từ "MOM" (3 ký tự, trong đó M lặp 2 lần), số cách sắp xếp là 3..

4. Nếu cho phép lặp lại khi sắp xếp k vị trí từ n đối tượng:

$$n^k$$

Ví dụ: chọn 3 vị trí từ 2 đối tượng (A, B) cho phép lặp 8 cách.

Câu 3. What is the State Space Size?

- Không gian trạng thái là tập hợp tất cả các trạng thái có thể mà một hệ thống AI có thể gặp phải trong môi trường. Mỗi trạng thái là một mô tả về tình huống hiện tại của hệ thống.
- Kích thước không gian trạng thái là tổng số trạng thái khả dĩ mà một tác tử có thể gặp phải trong một bài toán hay môi trường.
- Trạng thái là một mô tả đầy đủ về tình huống hiện tại của hệ thống.
- Không gian trạng thái là tập hợp tất cả các trạng thái có thể có.
- Kích thước không gian trạng thái cho biết độ lớn của tập hợp đó - tức là bao nhiêu cấu hình/ hướng đi mà hệ thống có thể rơi vào.
- Ví dụ: Robot hút bụi
- Trạng thái có thể được mô tả bởi
- Vị trí của robot trong phòng.
- Tình trạng sạch/bẩn của từng ô.
- Nếu phòng có 2 ô:
- Robot có thể ở ô A hoặc ô B.
- Mỗi ô có thể sạch hoặc bẩn($2^2 = 4$ khả năng)

=> Tổng số trạng thái = $2 \times 4 = 8$

- Ý nghĩa:
- Kích thước càng lớn thì việc tìm kiếm lời giải càng khó khăn.

- Giảm kích thước không gian trạng thái là một chiến lược quan trọng trong thiết kế thuật toán.

Câu 4. What is the Search Complexity?

Trong trí tuệ nhân tạo (AI), độ phức tạp của tìm kiếm đề cập đến tài nguyên tính toán—cụ thể là thời gian và bộ nhớ—mà một thuật toán tìm kiếm cần sử dụng để tìm ra lời giải cho một bài toán. Đây là một chỉ số quan trọng để đánh giá hiệu quả của thuật toán tìm kiếm và xác định khả năng áp dụng vào các bài toán thực tế.

- Độ phức tạp thời gian (Time Complexity)
- Định nghĩa: Là thời gian mà thuật toán cần để thực thi và tìm ra lời giải.
- Ký hiệu: Thường được biểu diễn bằng Big O notation ($O(\dots)$), mô tả cách thời gian chạy thay đổi khi kích thước bài toán tăng.
- Ví dụ:
- Thuật toán có độ phức tạp $O(n^2)$ sẽ chậm hơn đáng kể so với $O(n)$ khi n lớn.
- BFS (Breadth-First Search) có độ phức tạp $O(b^d)$, với b là hệ số phân nhánh và d là độ sâu giải pháp.
- Độ phức tạp không gian (Space Complexity)

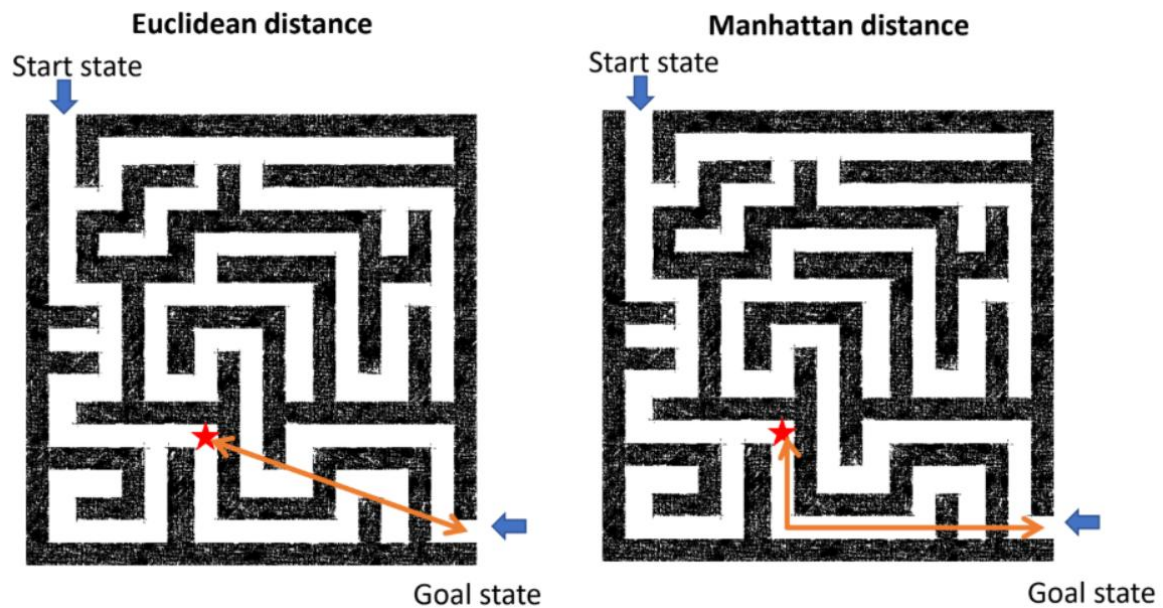
+ Định nghĩa: Là lượng bộ nhớ cần để lưu trữ trạng thái, các node đã khám phá và các cấu trúc dữ liệu hỗ trợ trong quá trình tìm kiếm.

+ Lưu ý: Một thuật toán có độ phức tạp không gian cao có thể gặp tràn bộ nhớ (memory overflow) với các bài toán lớn.

+ Ví dụ:

- BFS cần lưu toàn bộ frontier $\rightarrow O(b^d)$ bộ nhớ.
- DFS chỉ cần lưu đường đi hiện tại $\rightarrow O(d)$ bộ nhớ, tiết kiệm hơn nhưng không đảm bảo tìm lời giải tối ưu.
- Yếu tố ảnh hưởng đến độ phức tạp
- Kích thước không gian tìm kiếm: Số lượng trạng thái khả dĩ trong bài toán. Không gian càng lớn \rightarrow độ phức tạp càng cao.
- Độ sâu của giải pháp: Giải pháp nằm càng sâu trong cây tìm kiếm \rightarrow thuật toán phải duyệt nhiều bước hơn \rightarrow thời gian tăng.
- Hệ số phân nhánh (Branching factor): Số lượng trạng thái con trung bình của mỗi trạng thái. Hệ số càng lớn \rightarrow cây tìm kiếm mở rộng nhanh \rightarrow tăng cả thời gian và bộ nhớ.

Câu 5. What relaxations are used in these two cases?



Manhattan thường sẽ được sử dụng nhiều hơn trong trường hợp giải mê cung, vì mê cung có nhiều đường gấp khúc.

Câu 6. What is the cost that needs to be estimated?

Chi phí ước lượng chính là giá trị heuristic của một trạng thái bàn cờ, được tính dựa trên mức độ lợi thế hay bất lợi (khả năng thắng, thua, hòa) của người chơi tại trạng thái đó.

Câu 7. What would be a heuristic value for these boards:



Bàn cờ 1:

Hàng 1: $1 + 1 + 0 = 2$

Tương tự:

Hàng 2: -1

Hàng 3: -1

Cột 1: $1 + 0 + (-1) = 0$

Cột 2: 0

Cột 3: 0

Đường chéo chính: 0

Đường chéo phụ: -2

Heuristic: $(2-1-1-2)/8 = -1/4$

Bàn cờ 2:

Hàng 1, 2, 3: 0

Cột 1: 1

Cột 2: -1

Cột 3: 0

Heuristic: $(1-1)/8 = 0$

Câu 8. How do you calculate the heuristic value?

Không có một công thức duy nhất để tính giá trị heuristic; phương pháp tính toán phụ thuộc hoàn toàn vào bản chất của bài toán. Về cơ bản, heuristic (ký hiệu là $h(n)$) là một hàm dùng để ước tính chi phí từ trạng thái hiện tại n đến trạng thái mục tiêu.

Một số ví dụ phổ biến:

- Bài toán tìm đường trên lưới:
 - Khoảng cách Manhattan: Tính tổng chênh lệch theo trục hoành và trục tung. Phù hợp khi chỉ có thể di chuyển theo chiều ngang hoặc dọc.
 - Khoảng cách Euclid: Tính khoảng cách đường chim bay (đường thẳng) giữa hai điểm. Phù hợp khi có thể di chuyển theo mọi hướng.
- Bài toán 8-puzzle (trượt số): Một heuristic đơn giản là đếm số ô đang bị đặt sai vị trí so với trạng thái đích.

Câu 9. Is the heuristic admissible?

Một heuristic được gọi là chấp nhận được (admissible) nếu giá trị ước tính của nó không bao giờ lớn hơn chi phí thực tế để đi từ trạng thái hiện tại đến mục tiêu.

- Công thức: $h(n) \leq h^*(n)$, trong đó $h(n)$ là giá trị heuristic và $h^*(n)$ là chi phí tối ưu (thực tế).
- Ý nghĩa: Một heuristic chấp nhận được luôn có tính "lạc quan". Nó không bao giờ đánh giá một con đường khó đi hơn thực tế.
- Tầm quan trọng: Tính chấp nhận được là điều kiện tiên quyết để các thuật toán tìm kiếm như A* đảm bảo tìm ra được lời giải tối ưu (đường đi ngắn nhất). Ví dụ, cả khoảng cách Manhattan và Euclid đều là các heuristic chấp nhận được cho bài toán tìm đường.

Câu 10. Does the heuristic use relaxation?

Có, một trong những cách hiệu quả và phổ biến nhất để tạo ra một heuristic chấp nhận được chính là thông qua phép nói lỏng bài toán (problem relaxation).

- Định nghĩa: Nói lỏng bài toán nghĩa là tạo ra một phiên bản đơn giản hơn của bài toán gốc bằng cách loại bỏ một hoặc nhiều ràng buộc/quy tắc.
- Cách hoạt động: Chi phí để giải quyết bài toán đã được nói lỏng này chính là giá trị heuristic cho bài toán gốc. Vì bài toán đơn giản hơn nên chi phí giải quyết nó sẽ không bao giờ lớn hơn chi phí giải quyết bài toán gốc phức tạp hơn.
- Ví dụ: Trong bài toán tìm đường đi trên bản đồ, nếu ta "nói lỏng" ràng buộc "phải đi theo các con đường có sẵn", ta có thể đi thẳng. Chi phí của việc đi thẳng này chính là khoảng cách Euclid, một heuristic chấp nhận được.