BÁO CÁO EX1 NHÓM 2

Danh sách thành viên và phân công:

|  |  |  |  |
| --- | --- | --- | --- |
| **MSSV** | **Họ tên** | **Phân công** | **Github** |
| 3122410185 | Nguyễn Anh Khoa | Chương 1 | [Link](https://github.com/KhoaNguyenK4/TTNTNC-LABs/tree/main/TTNTNC) |
| 3122410267 | Huỳnh Khôi Nguyên | Chương 2 | [Link](https://github.com/CriinWa/BT-TriTueNhanTaoNangCao-gvDoNhuTai) |
| 3122410274 | Trần Gia Nguyễn (nhóm trưởng) | Chương 3 | [Link](https://github.com/Remilia172112/AAI-CaNhan-TranGiaNguyen-3122410274) |

Github nhóm 2: <https://github.com/Remilia172112/AAI-Nhom-2-GV.DoNhuTai>

# CHƯƠNG 1: Introduction Discussion

Câu hỏi: **What are the LLMs’ Percepts? Actions? Objectives?**

Trả lời:

* **Percepts (nhận thức)**: văn bản đầu vào do người dùng nhập.
* **Actions (hành động)**: sinh ra văn bản phản hồi, câu trả lời hoặc đoạn văn bản mới.
* **Objectives (mục tiêu)**: dự đoán từ tiếp theo chính xác, cung cấp câu trả lời hữu ích dựa trên dữ liệu huấn luyện.

Câu hỏi: **What do LLMs do? Do LLMs act rationally?**

Trả lời:

* **What do LLMs do?** LLMs dự đoán từ tiếp theo để tạo văn bản mới dựa trên dữ liệu huấn luyện, có thể trả lời câu hỏi, viết đoạn văn, dịch…
* **Do LLMs act rationally?** Ở mức độ nào đó có, vì chúng phản hồi dựa trên quy tắc tối ưu xác suất để đạt mục tiêu, nhưng chúng không có “ý định” hay “nhận thức” thực sự, nên hành vi hợp lý chỉ giới hạn trong phạm vi dự đoán thống kê.

Câu hỏi: **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 AGI or Narrow AI?**

Trả lời:

* **Would you be fooled?** Có thể, với những câu hỏi quen thuộc, LLM có thể khiến người dùng tưởng đang nói chuyện với người thật.
* **Why?** Vì LLM có thể tạo câu trả lời tự nhiên, ngữ pháp tốt, giống người. Nhưng khi hỏi sâu hoặc yêu cầu kiến thức thực sự, nó lộ ra giới hạn (sai thực tế, thiếu lý luận).
* **Ý nghĩa:** Điều này cho thấy LLM hiện tại vẫn là Narrow AI (trí tuệ hẹp), chưa đạt mức AGI (trí tuệ tổng quát).

Câu hỏi:

* **How do you think LLMs will affect the value of being able to write assays as taught in high school? ( LLMs sẽ ảnh hưởng đến việc học viết luận ở trường trung học thế nào? )**
  + **LLMs write computer code. What does this mean for the value of learning to code? ( LLMs viết code, vậy còn giá trị học code? )**
* **When should students be allowed to use the following tools? Give reasons for your decision. ( Khi nào nên cho học sinh dùng LLMs? )**

Trả lời:

* **Ảnh hưởng viết luận:** LLM giúp viết nhanh hơn, nhưng có thể làm giảm khả năng tự tư duy và lập luận của học sinh nếu lạm dụng.
* **Viết code:** LLM giúp sinh code nhanh, nhưng hiểu nền tảng lập trình vẫn quan trọng để kiểm tra và chỉnh sửa code.
* **Khi nên cho dùng:** Khi học sinh đã hiểu cơ bản, LLM có thể hỗ trợ tra cứu, gợi ý. Không nên dùng để thay thế hoàn toàn việc học kỹ năng gốc.

Câu hỏi: **How are LLMs affected by: robustness, monitoring AI, liability, goal/reward alignment, reward hacking, AGI & instrumental convergence?**

Trả lời:

* **Robustness:** LLM cần chống chịu trước đầu vào gây nhiễu hoặc tấn công (prompt injection).
* **Monitoring AI:** cần hệ thống giám sát để phát hiện nội dung không phù hợp.
* **Liability:** phải có cơ chế xác định trách nhiệm khi AI gây hại.
* **Goal/reward alignment:** cần thiết kế mục tiêu phù hợp với giá trị con người.
* **Reward hacking:** LLM có thể “lách” mục tiêu nếu không được kiểm soát.
* **AGI & instrumental convergence:** nếu tiến tới AGI, các nguy cơ này càng cao, cần chuẩn bị giải pháp quản trị.

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

Trả lời:

* **Regulated?** Có, để đảm bảo an toàn, bảo mật dữ liệu, ngăn chặn lạm dụng.
* **How?** Đặt tiêu chuẩn kiểm định nội dung, yêu cầu minh bạch dữ liệu huấn luyện, quy định trách nhiệm pháp lý cho nhà cung cấp.
* **Copyright:** cần khung pháp lý rõ ràng về việc sử dụng dữ liệu có bản quyền để huấn luyện và tạo nội dung mới, đồng thời bảo vệ quyền tác giả.

# CHƯƠNG 2: Agents discussin

Ảnh có chứa văn bản, ảnh chụp màn hình, phương tiện, ô tô

Nội dung do AI tạo ra có thể không chính xác.

• If we have two cars and one provides more (expected) utility.

Which car is rational?

- Trường hợp này thì cả 2 đều có sự hợp lý riêng, Xe nào có thể tối đa hóa tiện ích kì vọng (ví dụ nhanh hơn, an toàn hơn, thoải mái,..) thì xe đó hợp lí hơn. Hợp lí thì không có nghĩa là hoàn hảo, mà là dựa trên thông tin hiện có để có thể chọn hành động tốt nhất.

• Can a rational self-driving car be involved in an accident?

- Một chiếc xe tự lái hoàn toàn có thể gặp tai nạn. Vì sự hợp lí chỉ là chọn hành động tốt nhất trong khả năng và thông tin hiện có. nhưng môi trường luôn phức tạp và có các yếu số ngẫu nhiên bất ngờ xảy ra (ví dụ người đi bộ bất ngờ chạy qua đường, hoặc xe lao ra từ góc khuất, các cảm biến bị trục trặc,...) , trong các tình huống bất ngờ đó thì dù agent rational, tai nạn vẫn có thể xảy ra.

• How would a self-driving car explore and learn?

- Thu thập dữ liệu từ các cảm biến (camera, lidar, radar).

- Sử dụng Machine learning (Học tăng cường , học có giám sát)

- Khám phá và thử nghiệm các hành động mô phỏng để đánh giá hiệu quả rồi cập nhật các chiến lược khiển (được thưởng khi lái xe an toàn và bị phạt khi xảy ra va chạm).

- Việc học sẽ chủ yếu diễn ra trong môi trường mô phỏng hoặc dữ liệu đã thu thập trước đó , vì trên đường thực tế sẽ tiềm ẩn nguy cơ tai nạn lớn.

• What does bounded rationality mean for a self-driving car?

* Tính hợp lý bị giới hạn nghĩa là xe không thể :

+ Không tính toán tất cả tình huống tối ưu (do giới hạn thời gian, tài nguyên)

+ Nhận diện hoàn hảo mọi thứ do cảm biến có giới hạn.

+ Không được ra quyết định trong thời gian dài vô hạn (phải xử lý trong thời gian thực).

* Thay vào đó, xe sẽ phải dùng sác xuất, heuristic, mô hinhf đơn giản để đưa ra quyết định đủ tốt trong thời gian ngắn, thay vì đi tìm lời giải hoàn hảo.

Ảnh có chứa văn bản, ảnh chụp màn hình, phương tiện, ô tô

Nội dung do AI tạo ra có thể không chính xác.

* **Performance measure (Thước đo hiệu suất):**
* An toàn: tránh va chạm, bảo vệ hành khách và người đi đường.
* Tuân thủ luật giao thông: tốc độ, tín hiệu đèn, biển báo.
* Thời gian đến đích: nhanh, hiệu quả.
* Sự thoải mái của hành khách: lái mượt, không phanh gấp bất ngờ.
* Tiết kiệm năng lượng/nhiên liệu.
* Tôn trọng các yếu tố xã hội (ưu tiên xe cứu thương, người đi bộ).

**- Environment (Môi trường):**

* Đường (cao tốc, đô thị, nông thôn).
* Các phương tiện khác (xe hơi, xe máy, xe tải, xe buýt).
* Người đi bộ, xe đạp.
* Tín hiệu giao thông, biển báo, vạch kẻ đường.
* Điều kiện thời tiết (mưa, sương mù, tuyết), ánh sáng (ngày/đêm).
* Điều kiện đường (ổ gà, trơn trượt).

**- Actuators (Bộ chấp hành):**

* Bánh lái.
* Ga (tăng tốc).
* Phanh.
* Còi.
* Đèn xi-nhan, đèn pha, đèn phanh.
* Cần gạt mưa.
* Hệ thống truyền động (điện/động cơ).

**- Sensors (Cảm biến):**

* Camera (nhận diện làn đường, biển báo, vật cản).
* Lidar (quét 3D môi trường).
* Radar (đo khoảng cách, vận tốc xe khác).
* GPS (định vị).
* IMU (cảm biến quán tính: gia tốc kế, con quay hồi chuyển).
* Cảm biến tốc độ bánh xe, cảm biến ABS.
* Microphone (âm thanh, ví dụ xe cứu thương).

Ảnh có chứa văn bản, ảnh chụp màn hình, phương tiện, ô tô

Nội dung do AI tạo ra có thể không chính xác.

**1. Fully observable vs Partially observable**

* **Fully observable**: Sai.
  + Xe không bao giờ quan sát được toàn bộ trạng thái môi trường (góc khuất, sương mù, che khuất bởi xe khác).
* **Partially observable**: Đúng.
  + Xe chỉ nhận một phần thông tin từ cảm biến → cần **nhớ (memory)** và **suy luận (inference)** để ước lượng trạng thái còn thiếu.

**2. Deterministic vs Stochastic**

**Deterministic**:

* **a) Percepts are 100% reliable** → Sai.
  + Cảm biến **không đáng tin tuyệt đối**: camera mù trong sương mù, radar nhiễu, GPS sai số.
* **b) Changes in the environment are completely determined by the current state of the environment and the agent’s action** → Sai.
  + Môi trường thay đổi không chỉ do hành động của xe mà còn do **yếu tố ngoài** (xe khác, người đi bộ, động vật, thời tiết).

⟶ **Kết luận: môi trường không deterministic.**

**Stochastic**:

* **a) Percepts are unreliable (noise distribution, sensor failure probability, etc.)** → Đúng.
  + Mô hình cảm biến luôn có **xác suất sai số** (stochastic sensor model).
* **b) The transition function is stochastic leading to transition probabilities and a Markov process** → Đúng.
  + Khi xe chọn hành động (vd: phanh), kết quả có thể khác nhau (trượt trên đường ướt).
  + Ngoài ra, hành vi xe khác/ người đi bộ là **ngẫu nhiên** → cần mô hình xác suất Markov

⟶ **Kết luận: môi trường là stochastic.**

**3. Known vs Unknown**

* **Known**: Đúng một phần.
  + Xe biết: mô hình vật lý cơ bản, luật giao thông, bản đồ, một số đặc điểm của cảm biến.
* **Unknown**: Đúng một phần.
  + Xe **không biết trước** hành vi của người lái xe khác, điều kiện mặt đường, xác suất sự kiện hiếm → cần học từ dữ liệu và kinh nghiệm.

Ảnh có chứa văn bản, phương tiện, Phương tiện đường bộ, ô tô

Nội dung do AI tạo ra có thể không chính xác.

**a) Các fluents (thuộc tính trạng thái) nên có**

Một trạng thái (state) của xe tự lái nên chứa những thông tin quan trọng sau:

* **Vị trí & định hướng**: tọa độ (x,y), heading, tốc độ, gia tốc.
* **Làn đường**: ID làn xe, khoảng cách tới mép làn, có chướng ngại phía trước.
* **Trạng thái giao thông**: đèn đỏ/vàng/xanh, biển báo, vạch kẻ đường.
* **Thông tin phương tiện khác**: vị trí, tốc độ, hướng di chuyển của xe xung quanh.
* **Người đi bộ/xe đạp**: khoảng cách, hướng di chuyển.
* **Điều kiện môi trường**: thời tiết (mưa, sương mù), độ bám đường.
* **Mục tiêu cục bộ**: waypoint tiếp theo, tốc độ mong muốn.
* **Trạng thái xe**: pin/nhiên liệu, cảm biến hoạt động/ lỗi.

**b) Các hành động có thể gây ra chuyển trạng thái**

Xe có thể thay đổi trạng thái bằng những hành động (actuators) sau:

· **Điều khiển động học**: tăng tốc, phanh, giữ tốc độ.

· **Điều khiển hướng**: Rẽ trái/ rẽ phải, chuyển sang làn trái/ phải.

· **Điều khiển dừng/khẩn cấp**: dừng, phanh gấp.

· **Tín hiệu phụ trợ**:xi nhan trái/ phải, bấm còi, bật đèn xe.

**c) Sơ đồ chuyển trạng thái**

**Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

Nội dung do AI tạo ra có thể không chính xác.**

Ảnh có chứa văn bản, ảnh chụp màn hình, phương tiện, ô tô

Nội dung do AI tạo ra có thể không chính xác.

1. **Does it collect utility over time? How would the utility for each state be defined?**
   * Có. Xe tự lái luôn tối ưu **utility theo thời gian**: an toàn, tiết kiệm nhiên liệu, thoải mái, tuân thủ luật, rút ngắn thời gian hành trình.
   * Utility cho mỗi trạng thái có thể được định nghĩa theo **hàm đánh giá**:
     + An toàn (tránh va chạm, giữ khoảng cách).
     + Hành khách thoải mái (không phanh gấp, lái mượt).
     + Tiết kiệm nhiên liệu/ năng lượng.
     + Hoàn thành mục tiêu (đi đến đích đúng giờ).
2. **Does it have a goal state?**
   * Có trạng thái mục tiêu. Mục tiêu (goal) là **đi đến đích** (destination waypoint) trong bản đồ.
3. **Does it store state information? How would they be defined (atomic/factored)?**
   * Có lưu trữ thông tin trạng thái.
   * **Factored representation**: trạng thái được mô tả bằng nhiều **fluents** như:
     + Tốc độ hiện tại, vị trí, làn đường.
     + Khoảng cách với xe trước.
     + Tình trạng đèn giao thông.
     + Thời tiết, độ bám đường.
   * Không phải **atomic state** (chỉ 1 nhãn), vì cần nhiều thuộc tính để mô hình hóa.
4. **Does it use simple rules based on the current percepts?**
   * Không. Chỉ dùng **rule đơn giản** thì không đủ.
   * Xe tự lái có thể dùng một số **rule-based reflex** (vd: “Nếu đèn đỏ → dừng”), nhưng không thể chỉ dựa trên percept hiện tại, mà cần kết hợp **state quá khứ + dự đoán tương lai**.
   * Vì vậy, xe tự lái **không phải chỉ là simple reflex agent**.

# CHƯƠNG 3: Search Discussion

**Case Study: Heuristic cho trò chơi Tic-Tac-Toe**

1. Trạng thái đích (Goal states):

- Một trong hai người chơi (X hoặc O) có được ba ký hiệu liên tiếp trên một hàng, một cột hoặc một đường chéo.  
- Hoặc bàn cờ đã kín (không còn ô trống) mà không ai thắng → trạng thái hòa.

2. Chi phí cần ước lượng:

- Chi phí ước lượng chính là “độ gần” của trạng thái hiện tại đến trạng thái thắng.  
- Nói cách khác, heuristic cần ước lượng số bước (nước đi) tối thiểu để đạt được trạng thái đích (thắng).

3. Giá trị heuristic cho một số bàn cờ:

- Nếu X đã có 2 ký hiệu liên tiếp và còn 1 ô trống để hoàn tất hàng/cột/chéo → heuristic = 1 (chỉ cần 1 bước thắng).  
- Nếu không có hàng nào gần thắng, heuristic có thể cao hơn (ví dụ = 2, nghĩa là cần ít nhất 2 bước mới có thể thắng).  
- Nếu trạng thái là hòa hoặc đối thủ đã thắng → heuristic có thể đặt ở mức vô cùng (∞) hay một giá trị rất lớn để chỉ ra rằng không còn khả năng thắng.

4. Cách tính heuristic:

- Đếm số đường (hàng, cột, chéo) mà người chơi vẫn còn khả năng thắng (chưa bị chặn bởi ký hiệu của đối thủ).  
- Với mỗi đường còn khả năng, heuristic có thể tính theo số ô trống còn lại cần để hoàn tất.  
- Ví dụ: Một hàng có X, X, trống → giá trị = 1; một hàng có X, trống, trống → giá trị = 2.

5. Heuristic có admissible không?

- Nếu heuristic luôn đánh giá số bước cần thêm để thắng mà không bao giờ đánh giá thấp hơn thực tế, nó là admissible.  
- Ví dụ: Nếu nói cần ít nhất 2 bước để thắng thì thực tế không thể thắng nhanh hơn 2 bước → heuristic admissible.

6. Có dùng relaxation không?

- Có. Một dạng relaxation là giả sử đối thủ không ngăn cản ta, và ta chỉ quan tâm đến số bước cần để thắng trong tình huống “thuận lợi nhất”.  
- Điều này đơn giản hóa bài toán và cho ta một heuristic để dẫn hướng tìm kiếm.