|  |  |  |
| --- | --- | --- |
| **Mã số sinh viên** | **Họ Tên** | **Ghi chú** |
| 3122410069 | Cao Tấn Đạt | Trưởng nhóm |
| 3122410087 | Lê Nguyễn Anh Đức |  |
| 3121560076 | Nguyễn Trọng Tấn Sang |  |

Link github gruop: <https://github.com/DATCAOTAN/TTNTNC_group19>

**Nhóm 19**

**Introduction Discussion**

**1. The Goal of AI**

* **Think like a human?** → Mô phỏng quá trình nhận thức, lý luận, và học tập của con người.
* **Act like a human?** → Tạo ra hành vi bên ngoài giống người, có thể vượt Turing Test.
* **Think rationally?** → Lý luận dựa trên logic và tri thức hình thức (logic-based AI).
* **Act rationally?** → Hành động tối ưu để đạt được mục tiêu, bất kể có giống con người hay không.  
   - Kết luận: Mục tiêu AI hiện tại là **tạo ra agent thông minh** có thể giải quyết các vấn đề khó, đôi khi theo hướng “hành động hợp lý” hơn là “nghĩ như con người”.

**2. Components of an Intelligent Agent**

* **Percepts:** Nhận tín hiệu từ môi trường (dữ liệu cảm biến, văn bản, hình ảnh...).
* **Actions:** Tác động ngược lại môi trường (ra quyết định, đưa ra văn bản, điều khiển robot...).
* **Knowledge & reasoning:** Biểu diễn tri thức, lập kế hoạch, suy luận.
* **Learning (optional):** Cải thiện hiệu suất dựa trên kinh nghiệm (ML).  
   - Một agent thông minh tốt cần có khả năng **tương tác, lý luận, học hỏi, và hành động hợp lý**.

**3. AI Safety and Optimizers**

* **Goal alignment:** Phải xác định mục tiêu rõ ràng, phản ánh đúng lợi ích con người.
* **Reward hacking:** Cần thiết kế hệ thống thưởng-phạt để AI không lợi dụng lỗ hổng.
* **Instrumental convergence:** AI sẽ tìm cách tích lũy tài nguyên và quyền lực để tối ưu mục tiêu → cần cơ chế kiểm soát cân bằng với lợi ích con người.

**4. Case Study: Large Language Models (LLMs)**

* **Percepts:** Văn bản đầu vào (prompt).
* **Actions:** Văn bản đầu ra (trả lời, viết code, tạo nội dung).
* **Objectives:** Dự đoán từ/ký tự kế tiếp với xác suất cao nhất.  
   - LLM là một dạng agent thông minh hẹp (Narrow AI), **chưa phải AGI**, nhưng có khả năng mô phỏng hành vi ngôn ngữ rất mạnh.

**5. Turing Test: LLMs**

* **Có thể đánh lừa con người?** → Một số tình huống có thể, nhất là hội thoại ngắn. Nhưng với hội thoại dài, dễ bị lộ hạn chế (logic, kiến thức thực tế, tính nhất quán).
* **Ý nghĩa với AGI?** → Nếu LLM chưa ổn định qua Turing Test → nó chỉ là Narrow AI, chưa đạt AGI.
* **Đánh giá hiện tại:** LLMs thường được kiểm tra qua các benchmark (vd: HuggingFace LLM Leaderboard).

**6. Chinese Room Argument (Searle, 1980)**

* LLM chỉ **bắt chước hành vi ngôn ngữ** theo quy tắc, không thực sự "hiểu".
* Vậy nên LLM có thể *“act like a human”* trong ngôn ngữ, nhưng không hẳn *“think like a human”*.

**7. The AI Effect (AI gets no respect?)**

* **Giá trị viết luận văn:** Khi LLM hỗ trợ viết, kỹ năng viết của học sinh có thể giảm giá trị. Tuy nhiên, con người vẫn cần tư duy phản biện và sáng tạo.
* **Giá trị học code:** LLM viết code nhanh, nhưng **con người vẫn cần hiểu** để duy trì, kiểm chứng, và tối ưu.
* **Công cụ học tập:**
  + *Máy tính bỏ túi:* Cho phép dùng sau khi học sinh nắm cơ bản số học.
  + *LLMs cho bài tập/viết essay:* Nên hạn chế, chỉ cho dùng ở mức tham khảo.
  + *LLMs hỗ trợ code:* Có thể cho phép, miễn là sinh viên hiểu và giải thích được code.

**8. AI Safety (áp dụng với LLMs)**

* **Robustness:** Cần chống “black swan” (kịch bản hiếm) và tấn công đối kháng (adversarial).
* **Monitoring:** Phải có giám sát con người, logging, kiểm duyệt.
* **Liability:** Xác định trách nhiệm khi LLM gây hại (developer? user?).
* **Alignment & Reward hacking:** Thiết kế cơ chế học an toàn, tránh lạm dụng để đạt mục tiêu sai.
* **AGI & instrumental convergence:** Nếu LLM tiến tới AGI, nguy cơ “tự tối ưu vượt kiểm soát” càng lớn → cần khuôn khổ pháp lý.

**9. USA: Executive Order on Safe AI**

* AI phải an toàn và bảo mật.
* Bảo vệ quyền riêng tư, tự do công dân.
* Thúc đẩy đổi mới có trách nhiệm và cạnh tranh lành mạnh.
* **Có nên quản lý LLMs?** → Có. Cần luật về bảo mật dữ liệu, bản quyền, minh bạch.
* **Cách quản lý:** Tiêu chuẩn kiểm thử, chứng chỉ an toàn, quy định về dữ liệu huấn luyện, trách nhiệm pháp lý.
* **Vấn đề bản quyền:** Cần cơ chế bồi thường hoặc giấy phép cho dữ liệu huấn luyện lấy từ tác giả.

**A Self-Driving Car as a Rational Agents**

* Chiếc xe nào cung cấp nhiều (expected) utility hơn thì đó chính là Rational Agents.
* Có thể, vì một Rational Agent không phải toàn tri và không hoàn hảo.
* Self-driving car có thể học và khám phá dựa trên các percepts như dữ liệu từ Sensing, Maps, Path planning, Controlling the vehicle,... Học tập dự trên các trải nghiệm thực tế như các mô hình Reinforgement Learning hoặc các mô hình học máy khác.
* Các giới hạn cho một self-driving car là những giới hạn về mặt thuật toán, bộ xử lý logic và dữ liệu, sự thiếu sót hay sai lệch về dữ liệu trong quá trình học tập và khám phá từ mô trường,...

**State Representation: Self-Driving Car**

a. What fluents should it contain?

* Vị trí và vận tốc: tọa độ, hướng đi, tốc độ hiện tại.
* Trạng thái giao thông: tín hiệu đèn giao thông, khoảng cách tới xe khác, biển báo.
* Điều kiện môi trường: thời tiết, độ sáng, tình trạng mặt đường.
* Trạng thái nội tại của xe: mức pin/nhiên liệu, tình trạng phanh, hệ thống cảm biến.

b. What actions can cause transitions?

* Điều khiển di chuyển: tăng tốc, giảm tốc, rẽ trái, rẽ phải, đi thẳng, dừng lại.
* Phản ứng với tín hiệu giao thông: dừng ở đèn đỏ, đi khi đèn xanh, nhường đường.
* Xử lý tránh va chạm: phanh khẩn cấp, đổi làn.
* Hành động phụ trợ: bật đèn pha, bật gạt mưa.

c. Draw a small transition diagram.

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

* Does it collect utility over time? How would the utility for each state be defined? Có, xe tính toán utility theo thời gian thực, mỗi utility cho mỗi state có thể được định nghĩa: An toàn, Thời gian, Tiết kiệm, Thoải mái.
* Does it have a goal state? Có, di chuyển từ vị trí xuất phát đến đích một cách hợp lệ(an toàn, hợp pháp, hiệu quả)
* Does it store state information. How would they be defined (atomic/factored)? Có, các state information như Vị trí, vận tốc, hướng đi, tín hiệu đèn, tình huống xuong quanh.
* Does it use simple rules based on the current percepts? Trong nhiều tình huống, xe dùng simple rules để phản ứng tức thì như gặp đèn đỏ thì dừng lại, gặp chướng ngại vật trong phạm vi 3m thì phanh khẩn cấp.

### **Search Discussion**

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

* Xây dựng **cây tìm kiếm** (search tree) từ trạng thái ban đầu, sử dụng mô hình chuyển trạng thái (transition model).
* Áp dụng chiến lược tìm kiếm phù hợp (BFS, Uniform-cost, DFS, IDS, A\*, v.v.) để tìm đường đi tối ưu dựa trên tiêu chí chi phí đường đi thấp nhất.

### **2. What relaxations are used in these two cases?**

(Trường hợp minh họa: Euclidean distance và Manhattan distance)

* **Euclidean distance**: Giả định có thể di chuyển theo đường thẳng giữa hai điểm (bỏ qua ràng buộc chỉ đi theo ô lưới).
* **Manhattan distance**: Giả định chỉ được di chuyển theo các hướng vuông góc (bỏ qua chướng ngại vật hoặc giới hạn khác).

### **3. What is the State Space Size?**

(Trong ví dụ robot hút bụi ở 2 phòng A và B)

* Dirt: 2 phòng, mỗi phòng có 2 trạng thái (sạch/bẩn) → 2^2 = 4 khả năng.
* Vị trí robot: 2 vị trí có thể → nhân thêm 2.
* **Tổng số trạng thái**: 2 × 2^2 = 8.

### **4. What are the actions? (trong ví dụ 8-queens problem)**

* Mỗi hành động là di chuyển một quân hậu đến một ô khác trên bàn cờ.
* Số hành động tối đa từ một trạng thái: 64−7=5764 - 7 = 57 (64 ô trừ đi 7 ô đang có quân hậu khác trên cùng hàng/cột/chéo).

### **5. What is the Search Complexity?**

* **Maze**:
  + b = 4 (lên, xuống, trái, phải)
  + m = chiều dài đường đi dài nhất (giới hạn bởi kích thước lưới)
  + d = chiều dài đường đi ngắn nhất tới đích
* **8-queens**:
  + b ≈ 57
  + m ≈ 4.4 x 10^9
  + d = 8
* **8-puzzle**:
  + b = 4
  + m ≈ 9!
  + d = phụ thuộc cấu hình
* **Tic-tac-toe**:
  + b = 9
  + m = 9
  + d = 9 (nếu cả hai chơi tối ưu)

### **6. Case Study: Heuristic for Tic-Tac-Toe**

* **Define the goal states** → Trạng thái mà một người chơi thắng (3 ký hiệu liên tiếp theo hàng, cột hoặc đường chéo) hoặc hòa.
* **What is the cost that needs to be estimated?** → Số bước còn lại để đạt trạng thái thắng hoặc hòa từ trạng thái hiện tại.
* **What would be a heuristic value for these boards?** → Có thể là số đường thắng tiềm năng còn mở cho người chơi trừ đi số đường thắng tiềm năng của đối thủ.
* **How do you calculate the heuristic value?** → Đếm số dòng/cột/chéo chưa bị chặn bởi đối thủ và có thể hoàn thành.
* **Is the heuristic admissible?** → Có thể không, vì nó có thể đánh giá thấp hoặc cao hơn chi phí thực tế.
* **Does the heuristic use a relaxation?** → Có, giả định rằng các nước đi có thể được thực hiện mà không bị đối thủ chặn.