The City College of New York

CSC 59866-E: Senior Project I
AI Agents for Decision Making in the Real World

By Saptarashmi Bandyopadhyay
Email: sbandyopadhyay@ccny.cuny.edu, sbandyopadhyay@gc.cuny.edu
Assistant Professor of Computer Science
City College of New York and Graduate Center at the City University of New York

Research Methods, Metrics, & The "Wild West" of AI Agents

Logistics & Reminders

- **Overtally Deadline:** Today (Wed, Jan 28) by 5:00 PM ET. Email immediately if pending.
- **Google Colab Setup:** Create account, verify it works, and email me the associated email address by **Monday, Feb 2** so I can share Colab notebooks.
- **Office Hours:** Begin Feb 2nd (Mon 4-5 PM, NAC 8/206D).
- **Goal:** By Feb 11, you should be comfortable running fine-tuning Model Tutorials (Torch-tune, Unsloth).

Email:

- sbandyopadhyay@ccny.cuny.edu
- sbandyopadhyay@gc.cuny.edu

Grading Structure (Subject to Change)

- **Programming Assignments (20%)**
  - The sum of all coding assignment scores will be weighted to generate a score out of 20
- **Classroom Participation (10%)**
  - 1% each class, 10 classes max
  - This is a participation grade, not a correctness grade, so please ask questions!
  - Setting up Colab counts as 1 point
- **Group Project (55%)**
  - Abstract (Report in LaTeX code PDF) (17%)
  - Midterm Presentation (12%)
  - Final Presentation (15%)
  - Final Report (21%)
- **Bi-weekly Research Progress Update (10%)**
  - Every two weeks students will submit a brief summary of their research project progress
- **Research Paper Reviews (5%)**
  - 1 page handwritten report on strength, weakness and opportunities of 2 papers
  - Assignments will be individual submissions

How to do Good Research

What is “Research”?

Implications of Research in this Class:

1. **Innovation:** Something entirely new in direction.
2. **Improvement:** Enhancing an existing algorithm, theory, system, model, or dataset.
3. **Benchmarking:** Creating new standards to measure performance.
4. **Application:** Using existing code innovatively.

Policy ((s1, a1), (s2, a2)... (sn,an))

What is “Research”?

The Output: A research paper is an innovation asset.
Target Venues:

- Short-term: ACL, CVPR, and CHI Workshops (2026).
- Long-term: NeurIPS.

How to Read Research Papers

The Rule: Spend **20 minutes maximum** to skim a paper initially.

The "Rabbit Hole" Warning: If you spend 2 hours and don't understand it, stop. Let the instructor know.

How to Read Research Papers

1. **Abstract (5 mins):** Read 200-250 words. Identify the *weakness* of existing methods and the *solution* proposed.
   - *Action:* Scratchpad notes on Strengths/Weaknesses (2 mins).
2. **Conclusion & Future Work (4 mins):** Look for the hard numbers (results) and the author's admitted weaknesses.
   - *Action:* Note down future work suggestions embedded in the text.
3. **Deep Dive (Only if relevant):** Read Methods/Algorithms and Results/Plots (5+ mins).

"Pillar Papers": Identify the 2-3 papers that describe the main system you are improving. Read these thoroughly.

Recommended Reading List (Non-Sequential)

- *Prioritized but exploratory reading:*
    1. **JAXMARL:** Simulated environments for AI Agent capabilities (NeurIPS 2024).
    2. **YETI:** Proactive Agency & Multimodal Efficiency (arXiv 2025).
    3. **Social Intelligence:** Imitation Learning & Population-based Learning.
    4. **Self-Driving Cars:** Multimodal Model Predictive Control.
    5. **AI Agents for K-12:** Interactive Visualization.
    6. **Factored NMT:** Training with less data (Efficiency focus).
    7. **Multi-Agent LLM Debate:** Improving truthfulness via agent argumentation (ICML 2024).
    8. **REINFORCE:** High-variance low-bias RL method, the first policy gradient algorithm.

The Real AI Landscape

- **Dehypifying the Industry:**
  - **5%:** Generative AI (LLMs, Image Gen).
  - **10%:** Tool-based AI Agents (Specific, narrow tasks).
  - **85%:** The "Wild West" of Generalizable AI Agents.
- **The Limitation of GenAI:**
  - LLMs are **Auto-Regressive Transformers**.
  - They lack a controlled learning mechanism for generating probability distributions.
- **The Opportunity:** Scientific discovery, robotics, and complex decision-making live in the 85%.

Evaluation Metrics (How do we measure success?)

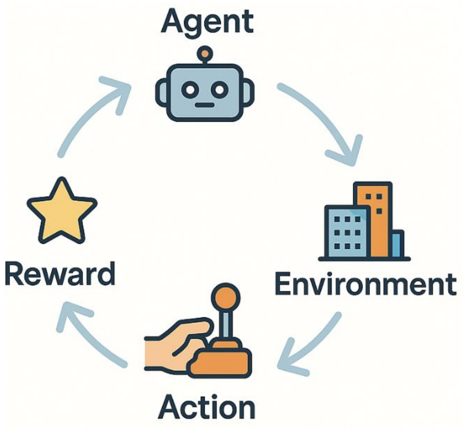
- **Standard Supervised Metrics:**
  - Accuracy, Precision, Recall, F-Measure.
  - **Visuals:** Loss Plots (Training vs. Test), AUC Plots.
- **GenAI/Agent Specific Metrics:**
  - **ROUGE / Meteor:** Text overlap metrics.
  - **BLEU:** Comparing machine translation to human professional translation.
- **The Danger Zone: Overfitting**
  - **Definition:** Memorizing training data (including noise) but failing on unseen data.
  - **Detection:** Superimposing Training Loss vs. Test/Validation Loss plots.

Efficiency & Hardware (Dark Silicon)

- **The Hardware Bottleneck:**
  - Most of a modern chip is unused at any given time to prevent melting ("Dark Silicon").
  - Paper: arXiv:2211.16385.
- **AI Designing AI:**
  - **AlphaChip:** Using RL to design computer chips (Google DeepMind).
  - **Circuit Training:** Open-source RL for chip floorplanning.
- **Relevance:** Your agents must be efficient to run on real hardware (Smart Glasses, Robots), not just massive server farms.
- **Compute Access:** Top US universities have 0.8 GPUs per student, Google Colab Pro access means you de-facto have a GPU loaned just for you!

Tools & Tutorials (Start Soon!)

- **Finetuning LLMs:**
  - **Torch-tune:** PyTorch native library.
  - **Unsloth AI:** Optimized finetuning (faster, less memory).
- **HuggingFace Ecosystem:**
  - **Deep RL Course:** Intro to Reinforcement Learning.
  - **Agents Course:** Tool use and planning.
  - **Robotics Course:** Simulation and control.
- **JAX:**
  - High-performance numerical computing (we will use **JAXMARL** later in the semester).



Designing Your Group Research Project

- **The Inputs & Outputs:**
  - What **Methods/Algorithms** will you use?
  - What **Datasets** are required?
  - What **AI Models** (LLM, VLM, RL policy) are the engine?
  - What is the **Outcome**? (Text, Image, Numerical Decision?)
- **Next Steps:**
  - Start skimming papers using the "20-minute rule."
  - Setup Colab.
  - Pick a tutorial (HuggingFace/Unsloth) and run a "Hello World" experiment.
- **Careers/Internships**: Keep your resumes/CVs up to date, I may ask to share them with industry partners or national labs for jobs/internship opportunities.

Questions?