AIM-5011-1: Natural Language Processing (3 credits)

Adam Faulkner

Falln 2025

E-mail: adam.faulkner@yu.edu
Office Hours: Class Hours: Tuesday 5:30-7:30pm
Office: Classroom: 205 Lexington Avenue Rm. 700

Final Project

For the course-final group project, students are asked to build an NLP application utilizing the concepts and skills learned throughout the course. Students can choose from the predefined list of projects provided below or propose their own project. On the last day of class, students will present a slide deck describing their application as well as a live or pre-recorded demo of their application.

Key Dates

- **Dec 2:** Project teams submit project proposals
- **Dec 23:** Project presentations

Ideas for Final Projects

1. **Language Learning Assistant**
   Create an LLM-based learning assistant that teaches the user the basics of a language of your choice in different settings: ordering in a restaurant, buying a train ticket, or asking for directions. The assistant should be able to determine if the user's response is a grammatical and appropriate response and to correct the user's response.

2. **A RAG-based Tutor**
   Index the text of Jurafsky & Martin's Speech & Language Processing and create a RAG-based tutor that is able to answer student questions regarding the concepts in this text and is able to show the provenance of these answers by also returning the excerpt(s) of the Jurafsky & Martin text that supports these answers. You can also use a different text for

a different subject for this task but must still show excerpts from the original text used to support the answers.

3. **Custom Guardrails for an LLM Deployed in an Educational Setting**
   Suppose a school is interested in internally deploying an LLM to help perform basic tasks such as checking grammar, writing emails, or generating ideas for projects. In order to deploy such a model, guardrails should exist that prevent students looking up answers to exam questions or generating essay content. Using NeMo-Guardrails or a similar framework, create guardrails that prevent students from being able to access content related to two-to-three subjects such as Astronomy, Biology, English Literature, etc. Demonstrate the efficacy of these guardrails using sets of questions designed to prompt the LLM to answer questions regarding these topics. The guardrails should only affect the target topics– students should still be able to check the grammar of text and perform other basic tasks.

4. **Instruction-tune an LLM to Answer xkcd "What if?" Questions**
   Randall Munroe's xkcd site contains a section devoted to answering 150 semi-serious "What if?" questions that touch on math and science such as "Is it possible to build a jetpack using downward firing machine guns?" These questions aren't answered by public-facing LLMs such as Gemini because of guardrails. Create a What If? LLM by instruction-tuning an LLM on these questions and Munroe's answers.Your LLM should be able to answer different variants of the original question (e.g. , "Can I make a jet pack that propels me forward with backward-facing machine guns?") using Munroe's answers.

5. **Agent-based Task Fulfillment Chatbot**
   Create a chatbot that can fulfill tasks on behalf of a customer, such as making a payment to their credit card or ordering clothing. Use the Agent-based framework we'll be learning about later in the semester to create a conversational agent that can interact with the external world via tools. There should be multiple tools each for different tasks such as checking to see if the customer has sufficient funds or subtracting the purchase amount from their existing funds. For example, if the user has $100 and makes a $50 purchase, an update should be made to a backend database via a tool.

1 Project proposal outline format

If you decide to propose your own project, please section your proposal as follows:

- **Names of contributors**

- **Background**
  What problem is your system designed to solve? This could be an open problem in NLP or a particular business problem. For example: "Copywriters who want to generate ad copy (marketing emails, etc.) from an LLM often need to personalize the generated content using customer profile data. This system uses the technique of "RAG-curated prompting" to allow copywriters to personalize their generated ad copy by querying a database of customer demographic and behavioral data ("resident of New York, retired, mostly spends on travel") and add returned results from the database to the prompt context",etc.

- **Implementation details**
  For example, you could write something like, "The proposed system will use Llama2-13b as the base LLM. To index and query the data we will use the FAISS semantic search library."

- **Data**
  For example, you could write something like, "The demographic and behavioral data is drawn from these sources: [add descriptions of data, including URLs]"

- **Demo**
  For example, you could write something like, "In the demo, we will use a gradio to demonstrate a typical session in a basic UI."