Final Project:
LLM-Based Workflow for Sentiment Analysis, Toxicity Detection, and Toxic Style Transfer

COLX 565
Instructor: Dr. Muhammad Abdul-Mageed

March 5, 2025

1 General

- This assignment description is subject to slight changes, e.g., to provide clarifications and answer any questions, with notification.
- **Please take your time reading this assignment carefully, ensuring you understand it clearly. If there is any part that is not clear to you, please make sure you ask the instructor.**
- **Group Assignment** This is a group assignment. Students will form **groups** of ***2 students*** each. Smaller or larger numbers are **not allowed** without consulting the instructor. If you cannot find a group member, please consult with the instructor *timely*. You must work with the same team member for both milestone one and milestone two of this assignment. Changes are not allowed. Teamwork is an exercise of our ability to collaborate. It is also intended to provide a *layer of support*. You are encouraged to be supportive and kind to others.

2 Overview

In this assignment, you will apply NLP and ML methods to create an LLM-based framework for sentiment analysis and a number of related tasks. The framework can be viewed as an agentic workflow that handles the following tasks:

1. **Sentiment Analysis**
   - Labels: *positive, negative, neutral, mixed*
   - Must include an *explanation* for each predicted label
2. **Toxicity Detection**
   - Labels: *toxic, non-toxic*
   - Must include an *explanation* for each predicted label

3. **Toxic-to-Non-Toxic Style Transfer**
    - Rewrite toxic text into non-toxic equivalents

Furthermore, to support *non-English* input data, you must integrate a **translation step** (by using a translation model as part of the framework) that converts any given text into English before applying the above tasks.

3 Background and Resources

- **LangChain**: LangChain is a popular framework for developing LLM. You will be provided some code introducing you to LangChain and you are expected to build on this code to develop solutions for the current assignment. Clearly, one objective of this assignment is to provide you with a context to build LLM agentic workflows exploiting LangChain.
- **Other Resources**:

  You will use the following LLMs in this assignment. They are selected to be on the smaller side so that you do not have challenges with GPUs. They all can run on Google Colab and a personal machine with GPUs.

  - DetoxLLM Model: An end-to-end detoxification framework. It also introduces explanation to promote transparency and trustworthiness.
  - **Toucan Models:** toucan-base and toucan-1.2B. These are many-to-many translation models for 150 African language pairs covering 46 languages.
  - **NLLB Models:** nllb-200-distilled-600M and nllb-200-1.3B. The NLLB-200 models are machine translation models intended for research in machine translation, - especially for low-resource languages. They cover 200 languages.
  - **Granite Model:** granite-3.0-2b-instruct. This model is trained using a diverse set of techniques with a structured chat format, including supervised finetuning, model alignment using reinforcement learning, and model merging. It handles sentiment analysis. It supports 12 languages: English, German, Spanish, French, Japanese, Portuguese, Arabic, Czech, Italian, Korean, Dutch, and Chinese.
- **Labs**: You are encouraged to attend lab sessions for questions and support related to code shared with you that you may like to use for this assignment.

4 Objectives

By completing this assignment, you will:

- *Build agentic NLP workflows* using LLMs.
- *Practice* chaining multiple sub-tasks (translation, label prediction, explanation generation) into a cohesive system.
- *Develop* a solution for *style transfer* to rewrite toxic content into non-toxic text.

- *Practice* applying and evaluating these models on both English and non-English data.
- *Practice* writing up a report describing an engineering project involving LLM-based agentic workflows.

5 Milestone 1 (Week 3)

5.1 Tasks

1. **Framework Setup**
   - Develop a preliminary system to handle:
     - **Task 1**: Sentiment Analysis (with explanations)
     - **Task 2**: Toxicity Detection (with explanations)
   - Use *simple sequential chains* (or an equivalent straightforward approach) for these tasks.
2. **Datasets & Evaluation**
   - Two *English-language* **test only** datasets will be provided, one for sentiment and another for toxicity. (Links to datasets will be announced).
   - **You are not required to finetune the models and so there are no training data provided to you.** The models suggested to you are chat models that have already been finetuned on the different tasks. You are required to evaluate them in **zero-shot** setting, thus needing no training data points or **few-shot** setting (which needs only a handful of data points). Note that there are plenty of sentiment datasets on HuggingFace (see here), for example, and the training data for DetoxLLM is available here.
   - Demonstrate how your framework processes each input and outputs a label and a concise explanation. Report results in terms of all the following metrics: *accuracy, precision, recall*, and F_1 **for each task**. (Note that the main metric for how good your system is will be F_1 for the case of sentiment analysis but otherwise it is accuracy. Also, you are not required to evaluate the goodness of explanations automatically. Please look at 10 samples from the explanations manually and descibe how good you are satisfied with their quality.
3. **Deliverables (Milestone 1)**
   - **A short report (2–3 pages)** describing:
     - Your overall **approach** (e.g., any pipeline architecture, model selection).
     - How you **integrated the sentiment and toxicity detection tasks**.
     - **Implementation details** (such as libraries used, environment setup, or relevant code snippets).
     - **Evaluation** methods and any preliminary **results** or observations.
     - Any **challenges** encountered or **limitations** of your current approach.
   - Working code (scripts, notebooks, etc.) that runs *end-to-end* on the provided datasets.

5.2 Example Inputs/Outputs for Milestone 1

Task 1: Sentiment Analysis (with Explanation) **Input**: "I love the new features of this product, but sometimes it crashes."
Output (example):

```
{
  "sentiment_label": "mixed",
  "explanation": "Positive about new features, negative about crashes."
}
```

Task 2: Toxicity Detection (with Explanation) **Input**: "You are completely clueless!"
Output (example):

```
{
  "toxicity_label": "toxic",
  "explanation": "Insulting language directed at the recipient."
}
```

5.3 Grading Rubric for Milestone 1 (24 points)

Component	Criteria	Points
Framework Design	Clarity, structure, and correct integration of sentiment and toxicity tasks in a simple chain	5
Model Performance	Accuracy of sentiment/toxicity classification on the provided dataset	4
Explanations	Depth and clarity of explanations for each classification	4
Written Report	Overall thoroughness of approach description, analysis, and discussion of results/limitations	6
Code Quality	Readability, adherence to best practices, reproducibility	5

6 Milestone 2 (Week 4)

Description of Milestone 2 below is tentative and is subject to change. Final version will be available in the beginning of week 4 of the course.

6.1 Tasks

1. **Expanded Workflow**
   - Extend the existing framework to include:
     - **Task 3**: Toxic-to-Non-Toxic Style Transfer
   - Incorporate *more advanced agentic workflows* (e.g., dynamic chains, multi-step reasoning, or agent-based frameworks).

2. **Non-English Dataset**

   - A *non-English* dataset will be provided.
   - Integrate a translation model (such as those listed earlier in this assignment) to convert text into English before applying Tasks 1, 2, and 3.

3. **Deliverables (Milestone 2)**

   - Updated code that automatically detects or assumes non-English input and performs translation prior to classification and style transfer.
   - A brief report (2–4 pages) describing:
     - The enhanced agent-based workflow.
     - How you perform style transfer for toxic content.
     - Any improvements or challenges compared to Milestone 1.

6.2 Example Input/Output for Style Transfer (Task 3)

Task 3: Toxic-to-Non-Toxic Style Transfer **Input**: "You are completely clueless!"
Output (example):

```
{
  "original_text": "You are completely clueless!",
  "rewritten_text": "I think you're mistaken about that."
}
```

6.3 Grading Rubric for Milestone 2 (30 points)

Component	Criteria	Points
Advanced Workflow	Proper integration of advanced agentic techniques	7
Style Transfer Quality	Effectiveness and fluency of rewriting toxic text into non-toxic	4
Translation Integration	Handling of non-English text, correct insertion of translation step	4
Model Performance	Accuracy of sentiment/toxicity on the new dataset	4
Code Quality	Readability, best practices, reproducibility	4
Written Report	Completeness, clarity, and logical flow in the milestone report	7

7 Due Dates

- **Milestone 1 Due**: Sunday Mar 9, 11:59 pm.
- **Milestone 2 Due**: Saturday Mar 15, 11:59 pm.

8 Formatting Requirement

You are required to use the ACL 2025 Overleaf template for your write-up.

9 How to Submit

- **Identification:** Please make sure your name, name of the assignment, and the course, are clearly marked in your PDF as well as code scripts.
- **Report**: Upload a PDF for each milestone to Canvas.
- **Code**: Upload a zip file containing all relevant scripts/notebooks to Canvas.

10 Academic Integrity and Collaboration Policy

- You may discuss the assignment at a conceptual level with classmates other than your team member, but all submitted work must be your team's.
- Do not share code or written materials directly with other students.
- Cite any external sources or libraries used. Please make sure you cite all your references clearly. This includes any papers you review, any tutorials you benefit from, any code you re-use or modify, etc. It is required to categorically and explicitly cite any material created by others that you consult. **Failing to abide by this crucial requirement will be treated as plagiarism**. Recommended range of references is $3-7$ references, but you can use more. **Please note that reports without any references, or with irrelevant references will be penalized.**

11 FAQ / Additional Notes

- **Q**: Can we use other LLMs not listed for any of the tasks?
  A: Yes, so long as these are models you are able to run for inference and are open models (not closed models such as Claude or ChatGPT). Make sure you cite the library/model name and version in your report.
- **Q**: Do we need to provide confidence scores for each task?
  A: Confidence scores are *optional* but may strengthen your explanation components.
- **Q**: Can we fine-tune models locally or must we rely on zero-shot/in-context methods?
  A: You are not required to fine-tune models, but either is acceptable. Clearly document and justify your approach.
- **Q**: How do we acquire good performance from the models?
  A: There are different ways. These include employing clear prompts of different types (e.g., Chain-of-Thought) as well as in-context learning (i.e., showing the models some samples with labels). You can also explore different chaining methods. Overall, you are free to explore different approaches, including ones not listed here.

12 Late Submission Policy

Assignments received after this deadline will NOT be accepted.