Live Session 1:
Course Overview and Assessment Brief

Dr Zak Varty

Welcome!

This Session:

1. Course Content
2. Course and Assessment Structure
3. Briefing on Assessments 1 & 2
4. Q & A

Course Content

Course Content - Accountability

Part 3 of MLDS Ethics will focus on the topics of Accountability and Security (40%)

Week 1 Reproducible Workflows

- 1.1 Reproducible pipelines in Python
- 1.2 Reproducibility in ML vs traditional software

Week 2 Robust Workflows

- 2.1 Determinism and Stability
- 2.2 A Champion-Challenger Deployment Pipeline

Course Content - Securtiy

Week 3 - Security by Cyphers

- 3.1 Cryptography Overview
- 3.2 Homomorphic Encryption

Week 4 - Security by Distribution

- 4.1 Federated Learning (part 1)
- 4.2 Federated Learning (part 2)

Week 5 - Security Risks

- 5.1 Adverserial Learning
- 5.2 Evasion Attacks
- 5.3 Privacy Attacks

Reading List

Course Structure

Part 3 as a Capstone

- More technical aspects of MLDS Ethics: conceptually, mathematically and computationally,
- Build on skills developed over the last 18 months.

- Structured as a student-lead capstone
- Weekly videos and readings, use these as starting points for deeper exploration.

- **Workload response:** curated set of aynchronous and asynchronous activities
- you choose which topics to explore independently in greater depth,
- assessments are designed to guide you through this.

Purpose and Benefits

- Can focus on what is most interesting and relevant to you.
- Demonstrate your ability to independently explore and engage with current literateure in MLDS Ethics.
- Construct well-founded and evidence-based arguments with which to positively influence the actions of stakeholders and decision-makers.
- Transition towards reasearch project, but with more structure.

Assessment Details

Weekly Reading Summaries (5%)

- As in previous parts, there will be 1 assigned reading weekly for which you should write a rhetorical precis.
- **Deadlines:** Thursdays and Sundays 23:59.
- Worth 1% each, graded on highest 5 of 6.

Assessments 1 & 2

You have been hired as a consultant by a large energy company, which has recently started a data ethics initiative. The aim of this initiative is to raise awareness and knowledge throughout the company about the ethical approaches to data science that are covered in MLDS Ethics Part III and how they might be relevant to the business.

As their first project, the data ethics initiative plans to create a series of “explainer” documents. The full series will cover the following 8 topics:

Topic Groups

Topic Group A

- Automated and reproducible workflows
- Data pipelines
- Version control for data, code and models

Topic Group B

- Robust estimation procedures in machine learning
- Homomorphic encryption
- Federated learning
- Data privacy attacks
- Adversarial learning.

Assessments 1 & 2

For Assessment 1 you will submit a document outline and literature review for two topics from the series. You will receive feedback on these from a company representative one week after the submission deadline. This feedback will include comments on your two proposals and a decision on which topic you should develop into a full explainer document.

For Assessment 2, you will act on the feedback provided to create the first explainer document in this series.

Further details of each task are given below. Since the company representative will be telling you which of your topics to take forward, **you should not start Assessment 2 until you receive instruction on which proposal to fully develop**.

Assessment 1: Proposal and Literature Review (15%)

`YOUR_CID-ethics-3-assessment-1.pdf`

10 March 2024 at 23:59

- The proposal document should present an outline document structure for two explainer documents, one from topic group A and one from topic group B.
- This should proposal should include a literature review giving a critical summary of several relevant publications, book chapters, videos or other resources that you will draw from when constructing your explainer document.
- The outline document structure should be a paragraph-level plan for proposed explainer document, clearly stating which resources you plan to use to support your arguments and outlining areas for further exploration should you take this topic forward.
- The proposal document should be presented as a single pdf document of at most 5 pages in length. Each outline should be at most 2 pages in length. A fifth page can optionally be used to provide bibliographic references and any additional figures, diagrams or tables.

Assessment 2: Explainer Document (20%)

`YOUR_CID-ethics-3-assessment-2.pdf`

08 April 2024 at 23:59

- A pdf document of at most 8 pages in length.
- The first page of this should be a self-contained information sheet or flyer that explains the importance and main ideas of the selected topic to a general staff member within the company.
- This should be followed by an introductory tutorial on the chosen topic that is suitable for the junior members of the data science team. This tutorial should introduce the reader to the topic in a self-contained way.
- The tutorial should also direct the reader to further resources (such as papers, documentation, code examples or videos) that they might use to explore the topic in more detail.

Tips for Explainer Document (1)

> This section provides general suggestions on how you might structure the tutorial section of your explainer document. You are **encouraged to be creative** in how you approach this task, these guidelines are not prescriptive and do not constitute a marking scheme.

- Begin by introducing the topic and purpose of the literature review. Explain why the topic is important, and how the papers you read contributed to your understanding of the topic;
- Provide a brief overview of the papers you read, including the title, authors, and main ideas or findings, organise the papers by theme;
- Discuss the strengths and weaknesses of the papers you read. Consider the methods used, the quality of the data and analysis, and the implications of the findings;

Tips for Explainer Document (2)

- Summarise the information from the papers to draw conclusions about the topic. Discuss the implications of the findings, identify possible shortcomings, and suggest areas for future research.
- Conclude by summarising the main points of the review and highlighting the contributions of the papers you read. Discuss the importance of the topic and any areas for further exploration.

Obvious but worth repeating:

- Use clear and concise language, and organise your summary into paragraphs (possibly with headings) to make it easy to follow;
- Make sure to cite all sources properly and follow a constistent citation style;
- Proofread your summary carefully to ensure that there are no errors or typos.

Tips for Explainer Document (3)

Important!

> Your explainer document should not simply be repetition of what you have read. It should be a critical analysis and synthesises to provide an introduction to the most relevant aspects of the topic.

Thank you. Questions?