# A.I. LITERACY FUNDAMENTALS

TREVOR YU & CARTER DEMARS

# WHY LEARN ABOUT AI LITERACY?

**Goal:** Equip everyone with the tools to understand, talk about, and evaluate AI systems

**Why?**
- Be able to evaluate and effectively use AI products
- Discern facts from "AI hype" in news and social media
- First steps towards working on AI projects

2

# BY THE END OF THIS WORKSHOP, YOU SHOULD BE ABLE TO...

- Classify scenarios as descriptions of artificial intelligence (AI), machine learning (ML) and data science (DS)
- Explain the difference between AI and ML
- Give examples of AI applications
- Explain why data needs to be processed before being used by ML models
- Suggest appropriate types of models for different problems

# WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence is machines demonstrating "intelligent" capabilities once thought only to be displayed by humans.

- Intelligence includes learning, perception, recognition, decision making, conversation, language understanding, planning, control, knowledge representation, reasoning, etc.
- Today's machines are digital computers
- AI include machine learning, computer vision, automated decision making, robotic control, chatbots, etc.

# WHAT IS MACHINE LEARNING?

**Machine learning** is a computer system that performs a task from data instead of being explicitly programmed.

- ML algorithms are based on the math from linear algebra, calculus and statistics
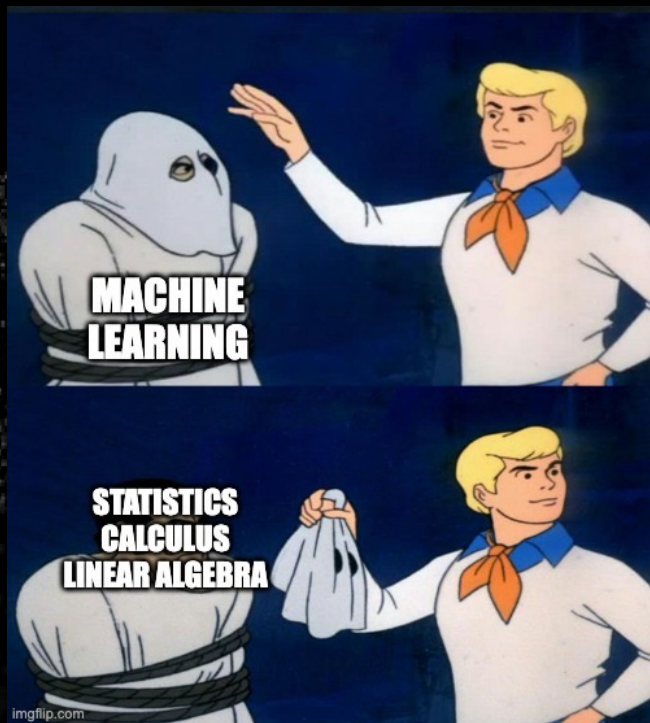
# EXAMPLE: RECOMMENDATION SYSTEM

Explicitly programmed (not ML):
- A users selects a short list of tags they're interested in
- If/then/else rules to filter content based on tags
- The user has to explicitly add tags if their interests change

Learns from data (is ML):
- A user "likes" content from their feed, labelling data points of what they prefer
- An algorithm uses the data to learn what things the user wants to see and what they ignore
- The same algorithm can be applied to different users without programming in their individual preferences

# SOME COMMON ML TERMINOLOGY

**Machine learning** is a computer system that performs a task from data instead of being explicitly programmed.

- **Supervised learning**: The system learns a rule to process inputs based on labelled outputs
- **Classification**: Task to separate input examples into two or more discrete groups
- **Regression**: Task to estimate a continuous output value from input data

# WHAT IS DATA SCIENCE?

Data science is the use of methods in statistics, computing, and science to extract knowledge from data.

- **Data**: Raw observations about the world
- **Knowledge**: Useful information about the world
- ML techniques are often used for data processing in the data science field

# ACTIVITY: DISTINGUISH BETWEEN AI, ML, AND DS

# MACHINE LEARNING IS A SUBSET OF AI

**"Machine learning" is often used interchangeably with AI. But:**
- AI also includes other techniques like optimization, logic, and knowledge representation
- Machine learning can be studied outside the context of building intelligent systems
- Beyond today's session, assume we will be using ML techniques to build AI systems

# AI, ML, AND DS ARE CONNECTED

**Human intelligence is natural data processing**
- We take inputs like sensory information, memories, and goals
- We output movement, speech, and decisions

**Processing and understanding data is fundamental to building intelligent systems**
- A data science mindset helps us understand how to build good AI and ML systems
- AI and ML techniques help data scientists draw better insights from data

# MACHINE LEARNING IN RESEARCH VERSUS IN PRODUCTION

|  | Research | Production |
|---|---|---|
| Requirements | SOTA Performance | Depend on stakeholders |
| Computational Priority | High throughput | Fast inference |
| Data | Static | Constantly shifting |
| Fairness | Generally, not a focus | Must be considered |
| Interpretability | Generally, not a focus | Must be considered |

Adapted from Designing Machine Learning Systems, O'Reilly.

# QUESTION BREAK

What can we clarify about the content so far?

# THREE ASPECTS OF AI LITERACY

- **Data**: What data is being processed
- **Application**: What intelligent capability is being done and for what purpose
- **Model**: What method is being used to represent intelligence

14

# EXAMPLES OF PAST WAT.AI PROJECTS

- The medical imaging processing project used a **convolutional neural network** to **detect prostate cancer** based on **MRI images**.
- The Open Climate Fix project used a **decision tree** to **estimate solar panel output** based on **weather data**.
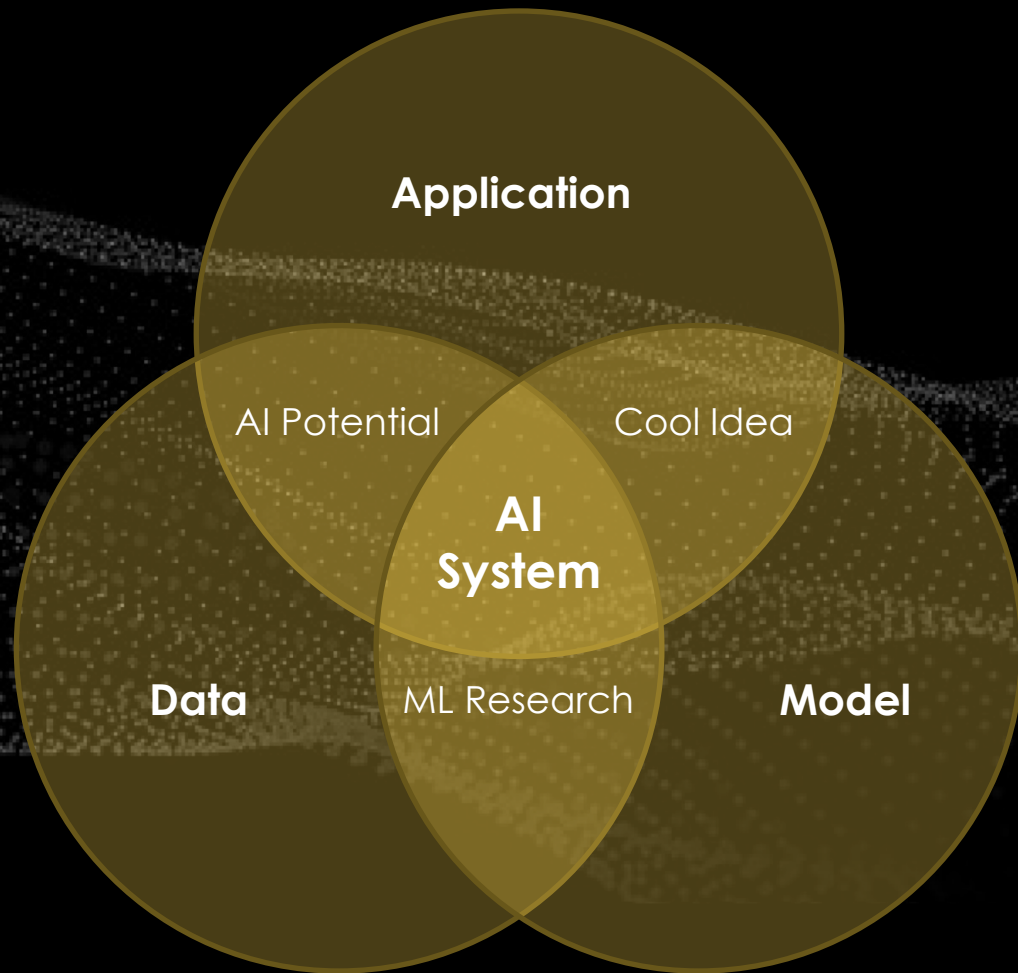
# UNDERSTANDING DATA

- **Data** is a collection of information about the world, such as facts, observations, measurements, and experiments
- Raw data alone is useless, we need to apply some processing to generate useful inferences about the world

# DATA FOR MACHINE LEARNING

- **High quality ML systems require training with a large volume of data**
  - ML models need to learn patterns from many examples
  - Supervised learning also requires labels, which may be hard to collect
  - ML models do better with high quality data
- **Data preprocessing is important because AI models require data to be in specific formats**
  - ML models are based on linear algebra → data should be represented as vectors
  - It takes a lot of time and effort to prepare data for ML

# IMAGE PIXELS AS INPUT VECTORS
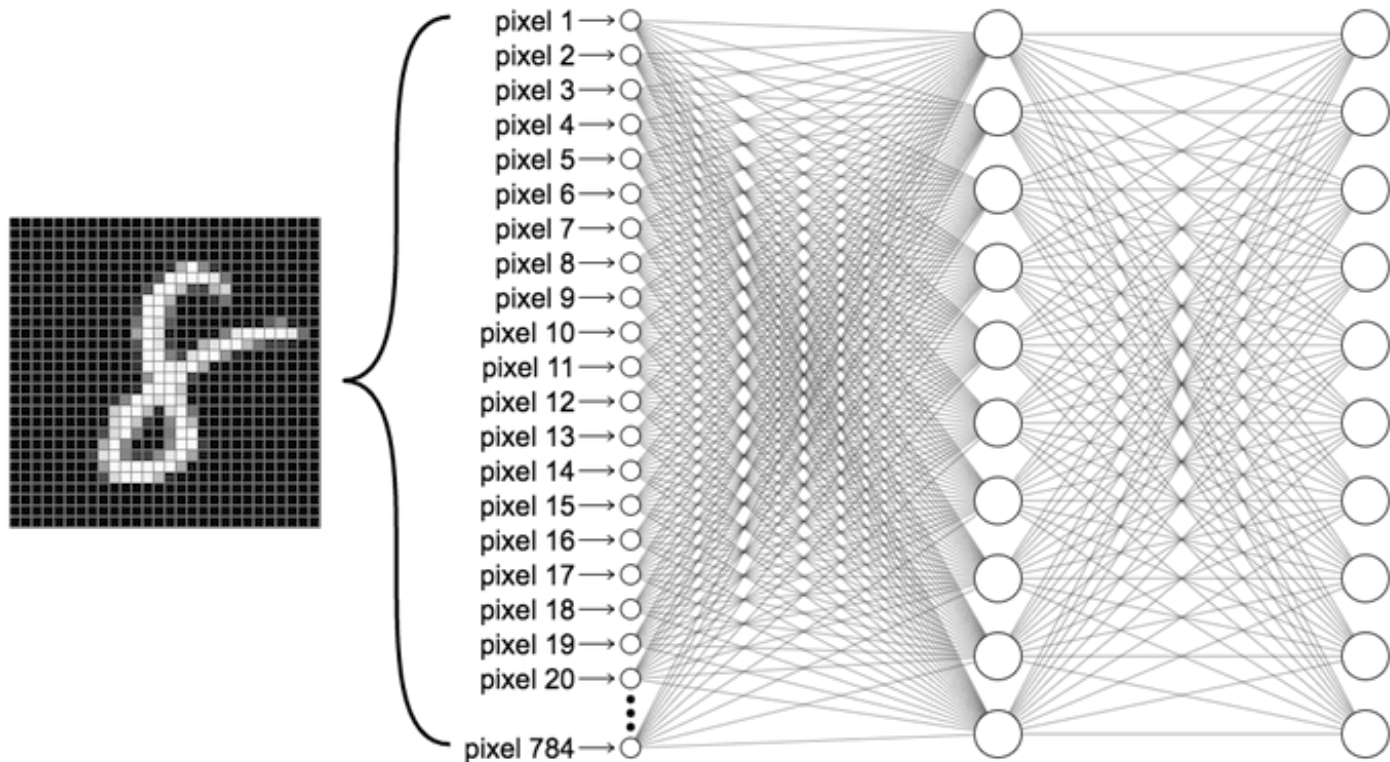
# DATA MODALITIES

- **Images**
  - Natural images, satellite imagery, medical images
- **Tabular**
  - Spreadsheets
- **Text**
  - Books, internet, social media, foreign language
- **Audio**
  - Speech, sonography
- **Time-series**
  - Sensor data, sequences of game actions, video

# AI APPLICATIONS: SOLVING PROBLEMS

- **What problem is the AI system trying to solve?**
    - How is success defined and how do we measure it?
    - Is it necessary to use AI to solve this problem?
    - Can the problem be formulated as classification or regression?

# AI APPLICATION MODALITIES

- **Tabular data**
  - **Identify anomalies, forecast sales**
- **Computer vision**
  - **Object recognition, image classification, pose estimation**
- **Natural language processing**
  - **Text classification, entity extraction, language understanding, translation**
- **Time-series forecasting**
  - **Real-time sensor classification, robotic trajectory estimation**
- **Generative**
  - **Chat bots, image generation**
- **Many industries**
  - **Robotics, healthcare, medical science, finance, business, manufacturing, environmental science, education, etc.**

# LIMITATIONS OF AI SYSTEMS

- **We don't yet have artificial general intelligence that can do everything as well as people can**
  - Most AI systems are developed to perform a specific task very well
- **AI systems still make mistakes**
  - AI practitioners need to investigate how and why mistakes occur to prevent and mitigate them
  - Mistakes influence levels of trust in using AI systems
- **All AI systems have bias**
  - Training data can have bias towards what kind of labels are associated with certain inputs, or there can be gaps in data
  - Assumptions made about the modelling technique can introduce systematic bias towards the way decisions are made
- **Large and complex AI systems are expensive to develop and run**

# AI APPLICATIONS: INTERACTIONS WITH THE WORLD

- **How will the AI system interact with the world?**
    - Consider people, other technology, institutions, laws, conventions, etc.
    - An AI system can perform really well, but if society doesn't use it, it's worthless!

# INAPPROPRIATE USES OF AI

- **Things that cause harm to people**
  - Warfare, scammer bots, hate speech, discriminatory decision making, privacy invasive surveillance, social manipulation, etc.
- **Situations where there is NO human in the system or when AI would completely replace a human's job**
  - Unless the people being affected themselves want to be replaced
- **When the AI system's performance is poor or inadequately tested**
  - Influences trust in adopting AI systems

# ACTIVITY: SUGGEST AI APPLICATIONS

Suggest an application of an existing AI product, or an application of AI that you are excited about

# UNDERSTANDING MODELS

- **A model is a conceptual representation of a system and allow us to represent the system in a precise way, such as using a diagram or mathematical notation**
    - **E.g. modeling the trajectory of a ball using kinematic equations**
- **Models make simplifications and assumptions about the systems they represent**
    - **Models are never completely correct about their representation, but are often good enough to be useful**

**An AI model is a simplified representation of "intelligence". It is not precisely correct about the true nature of intelligence, but it is useful enough to solve problems.**

# EXAMPLES OF ML MODELS

- **Classic ML and statistical methods**
  - Linear regression, support vector machines, decision trees, probabilistic models
- **Neural networks**
  - Multi-layer perceptron, convolutional neural networks, recurrent networks, transformers
- **Large language models**
  - GPT-4, PaLM, LLaMA

# WHEN TO USE WHICH MODELS

| Model Type | Data Modality | # Parameters (model size) | # Examples (dataset size) | Tasks |
|---|---|---|---|---|
| Classical ML | Tabular, time-series, image | 10 – 10,000 | 10 – 10,000 | Classification, regression |
| Small neural networks | Image, time-series, tabular | 100 – 100,000 | 1,000 – 100,000 | Classification, regression |
| Large neural networks | Image, text | 100k – 100M | 100k – 1B | Classification, regression, low-quality generation |
| Large language models | Text, image | 1B+ | 1B – 100T | High-quality generation, classification |

# ACTIVITY: SUGGEST TYPES OF MODELS

# ACTIVITY: CHATGPT CASE STUDY

- **With a group or on your own, analyze the ChatGPT AI system based on the prompts in the shared document. Write your answers in the shared document for everyone to see.**
- [bit.ly/3Lo9qml](bit.ly/3Lo9qml)

# BY THE END OF THIS WORKSHOP, YOU SHOULD BE ABLE TO...

- Classify scenarios as descriptions of artificial intelligence (AI), machine learning (ML) and data science (DS)
- Explain the difference between AI and ML
- Give examples of AI applications
- Explain why data needs to be processed before being used by ML models
- Suggest appropriate types of models for different problems

# FUTURE AI LITERACY TOPICS

- **Designing AI systems for human-AI interaction**
- **Bias in AI systems**
- **Reading AI literature**

# UPCOMING EDUCATION SESSIONS

- **Data Preprocessing**
- **Classical Machine Learning**
- **Neural Networks for Novices**
- **Dive into Deep Learning**

**EXIT SURVEY – ATTENDANCE!**