Lecture 2 - Introduction to IUI (2)

Defining Artificial Intelligence

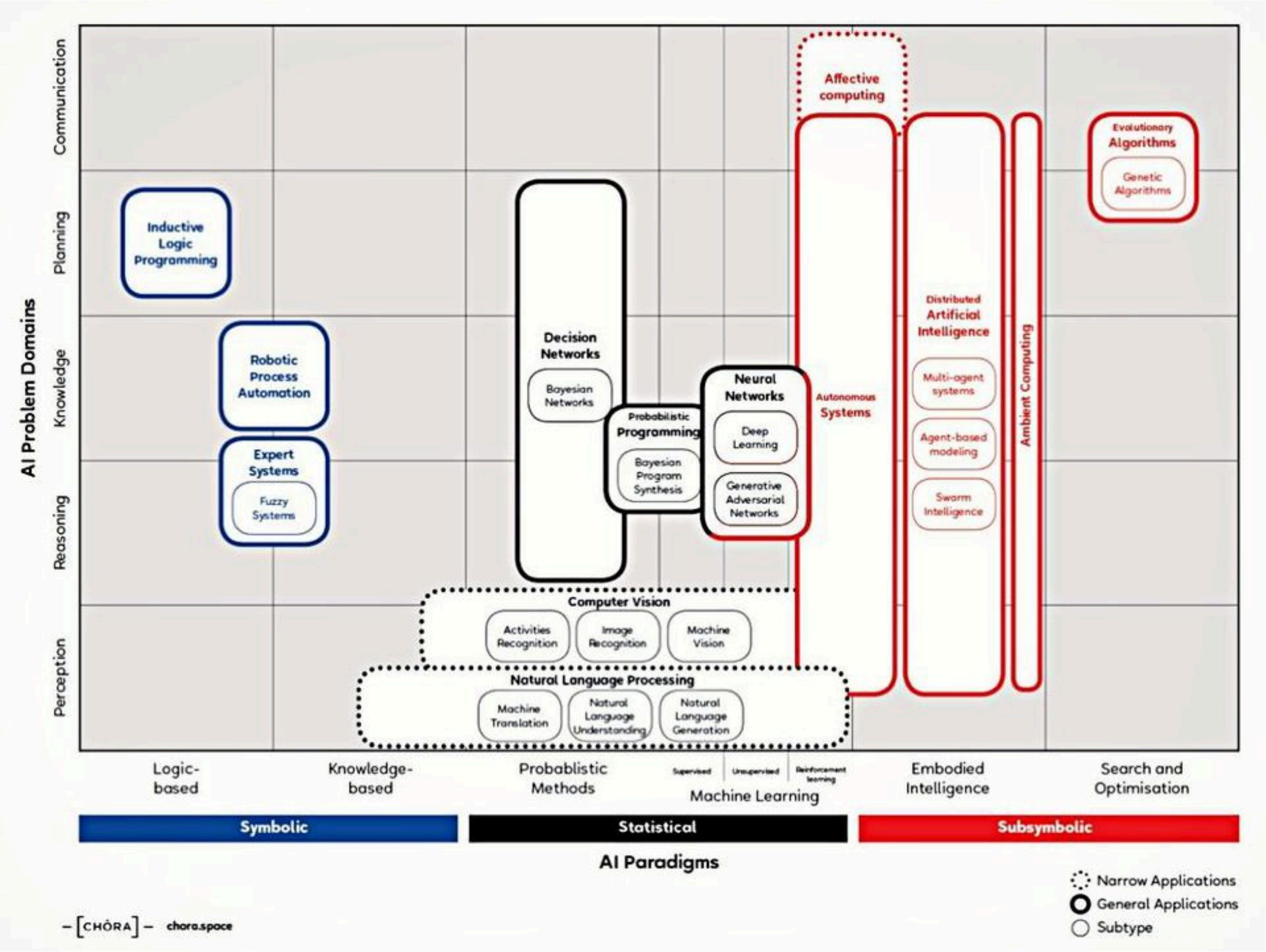
- “What is considered Artificial Intelligence?” and “What is AI?”
    - **Artificial Narrow Intelligence (Weak AI):** Solves very specific, well-defined problems in a particular domain.
        - **Artificial General Intelligence (Strong AI):** Capable of mimicking human intelligence such that its behavior is indistinguishable from that of a human.
        - **Artificial Super Intelligence:** Surpasses human intelligence.

Understanding AI Categories

Distinguishing among narrow, general, and super AI is essential. Current real-world systems largely fall under narrow AI, which are specialized tools rather than all-encompassing thinking machines.

The AI Knowledge Map: Technologies and Domains

- **Technologies**
    - **Logic-based:** Tools for knowledge representation and problem-solving.
    - **Knowledge-based:** Systems using ontologies, databases, and rule sets.
    - **Probabilistic methods:** Approaches that handle uncertainty and incomplete information.
    - **Machine Learning:** Algorithms that learn patterns from data.
    - **Embodied Intelligence:** Systems that incorporate physical or simulated bodies to achieve higher-level intelligence.
    - **Search and Optimization:** Methods to intelligently explore and choose among many possible solutions.
- **Domains**
    - **Reasoning:** Solving problems through logical inference.
    - **Knowledge:** Representing and understanding the world.
    - **Planning:** Setting goals and achieving them.
    - **Communication:** Understanding and generating language.
    - **Perception:** Converting raw sensor data (e.g., images, sounds) into actionable information.

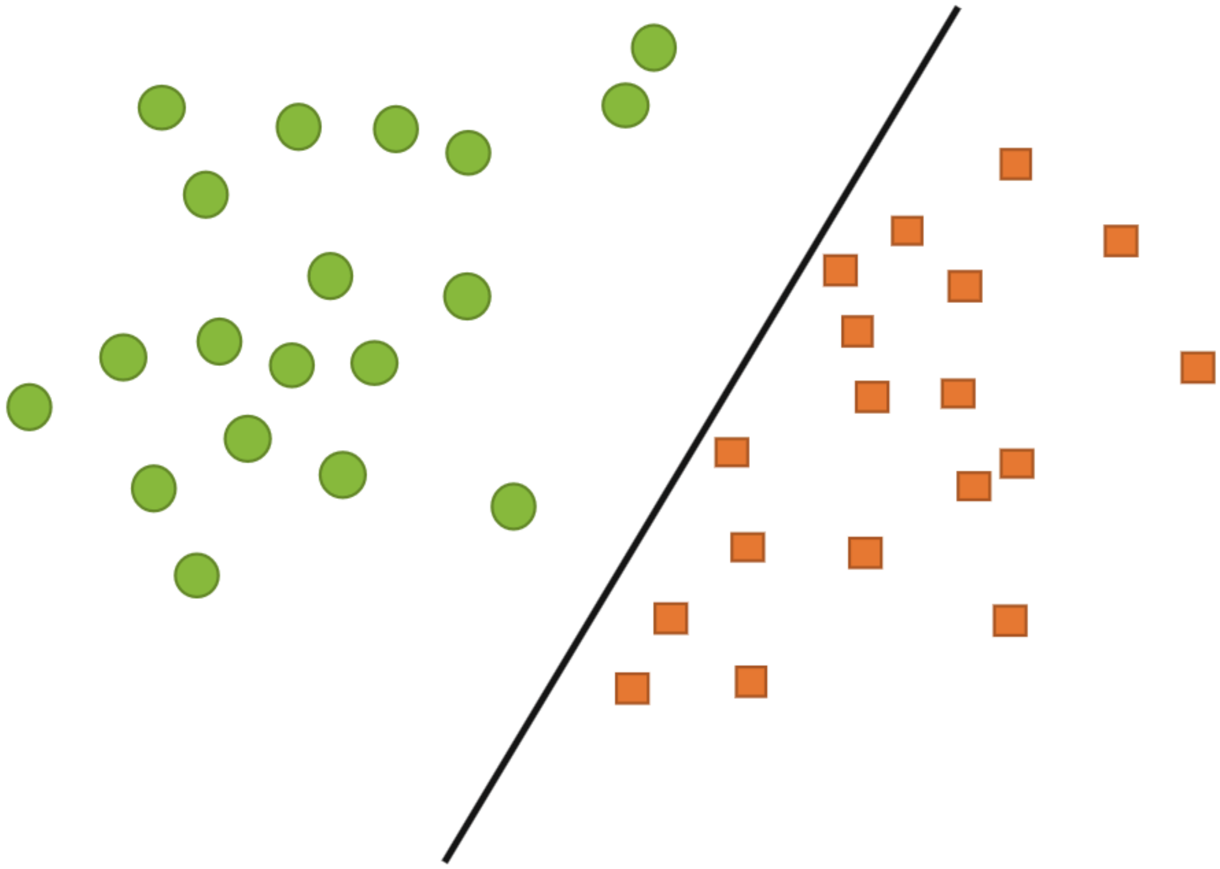


AI Knowledge Map: how to classify AI technologies. A sketch of a new AI technology landscape Francesco Corea

---

Classification in AI

- **Classification** as a fundamental problem in AI: determining a “line” that separates data into different groups (e.g., deciding whether an email is spam or not).
- **Key Points:**
  - Classification requires examples of data where the class (label) is known.
  - The goal is to find a boundary that maximally separates different classes.
  - **Example:** Support Vector Machines (SVM) are mentioned as an approach that finds the optimal boundary between classes.



How can we find a "line" that separates the two groups?

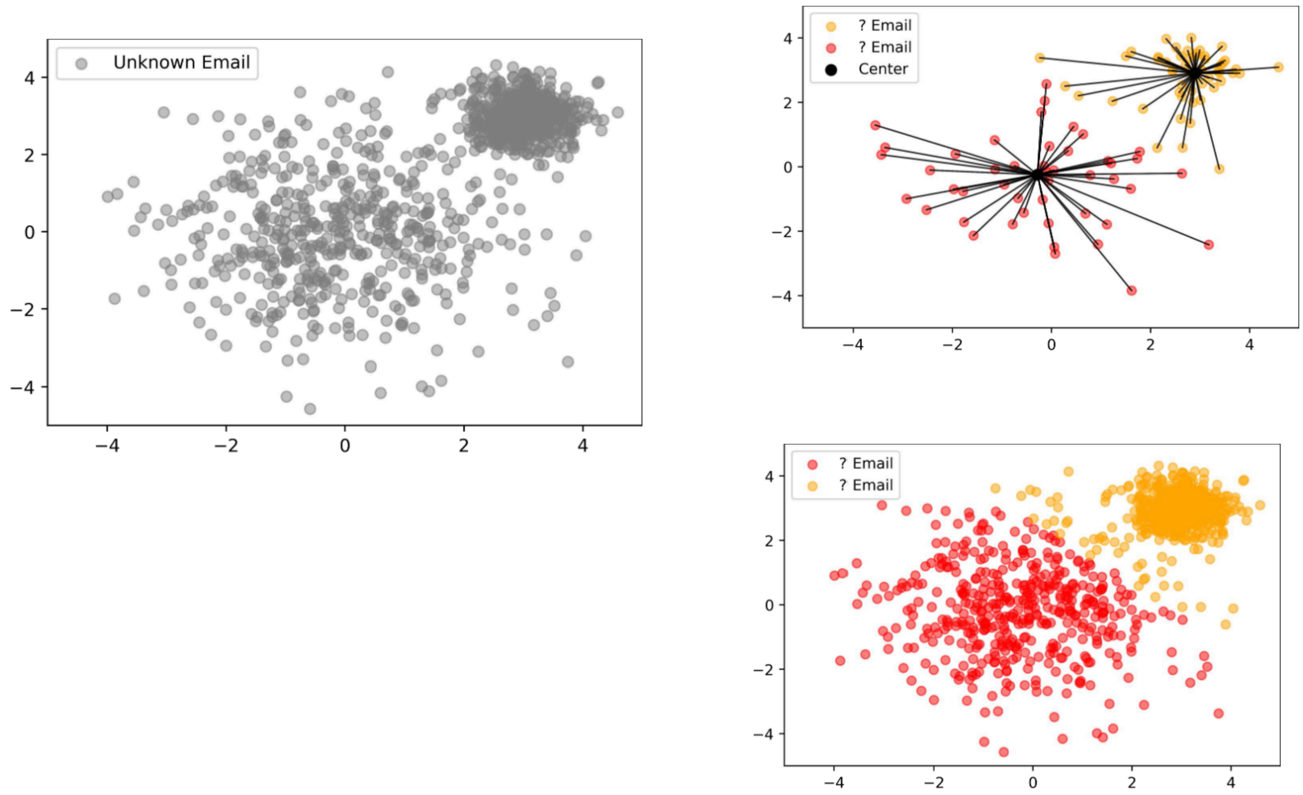
A common approach is to use a linear classifier such as a Support Vector Machine (SVM). The SVM finds the optimal hyperplane—essentially a line in two dimensions—that maximizes the margin between the two classes, thereby minimizing misclassification and providing a robust decision boundary.

Why Classification Matters

Classification is central to many AI applications — from spam detection to image recognition. It lays the groundwork for understanding supervised learning methods.

Supervised vs. Unsupervised Learning

- **Supervised Learning:**
  - Learning from labeled examples.
  - A dataset with known outcomes (labels) is used to train a model.
  - The model is then tested on unseen data to evaluate its performance.
- **Unsupervised Learning:**
  - Learning patterns from data without explicit labels.
  - Clustering, representation learning, and density estimation.
  - Used for exploratory data analysis and dimensionality reduction.

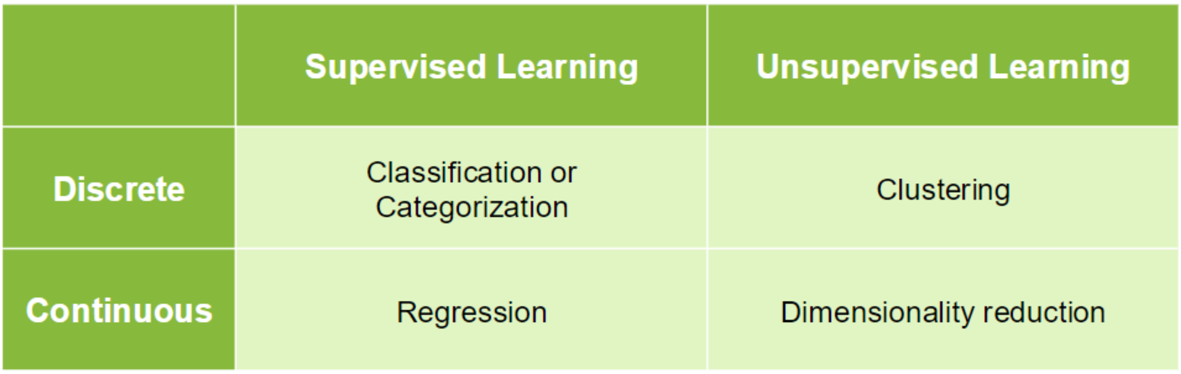


Unknown Data → K-Means Clustering → two clusters with each one center, every newly added points copuld shift the clusters

> **Unsupervised Learning**
>
> “The most common tasks within unsupervised learning are clustering, representation learning, and density estimation...”

> **Supervised vs. Unsupervised**
>
> Supervised learning relies on labeled data to predict outcomes, while unsupervised learning aims to uncover hidden structures in unlabeled data.

Unsupervised Learning and Clustering



	Supervised Learning	Unsupervised Learning
Discrete	Classification or Categorization	Clustering
Continuous	Regression	Dimensionality reduction

- **Learning Strategies:**

    - **Supervised:** Discrete outcomes (classification, regression).
        - **Unsupervised:** Discovering natural groupings (clustering) or reducing dimensionality.
- **Unsupervised Methods:**
    - Techniques such as hierarchical clustering, k-means clustering, Principal Component Analysis (PCA), Singular Value Decomposition (SVD), and Independent Component Analysis
- **Clustering Focus:**
    - Detailed discussion on clustering as a method to uncover structure in data.
    - **K-means clustering** is highlighted with several slides discussing its application and challenges—such as determining the optimal number of clusters

---

Discussion: Usable Security

- **Security Applications:**
    - How to detect when “the wrong user” attempts to log in.
    - Differentiating between a denial-of-service attack and a user’s mistake (e.g., forgetting a password).
    - The potential use of clustering algorithms to identify anomalous behavior.

> **Usable Security Challenges**
>
> Machine learning can enhance security by automating anomaly detection, but careful tuning is required to avoid false positives and ensure user convenience.
