Artificial Intelligence Foundation – JC3001

Lecture 47: Ethics in AI II

Prof. Aladdin Ayesh (aladdin.ayesh@abdn.ac.uk)

Dr. Binod Bhattarai (binod.bhattarai@abdn.ac.uk)

Dr. Gideon Ogunniye, (g.ogunniye@abdn.ac.uk)

October 2025

Material adapted from:
Russell and Norvig (AIMA Book): Chapter 28

UNIVERSITY OF ABERDEEN

Course Progression

- Part 1: Introduction
  1. Introduction to AI ✓
  2. Agents ✓
- Part 2: Problem-solving
  1. Search 1: Uninformed Search ✓
  2. Search 2: Heuristic Search ✓
  3. Search 3: Local Search ✓
  4. Search 4: Adversarial Search ✓
- Part 3: Reasoning and Uncertainty
  1. Reasoning 1: Constraint Satisfaction ✓
  2. Reasoning 2: Logic and Inference ✓
  3. Probabilistic Reasoning 1: BNs ✓
  4. Probabilistic Reasoning 2: HMMs ✓
- Part 4: Planning
  1. Planning 1: Intro and Formalism ✓
  2. Planning 2: Algorithms & Heuristics ✓
  3. Planning 3: Hierarchical Planning ✓
  4. Planning 4: Stochastic Planning ✓
- Part 5: Learning
  1. Learning 1: Intro to ML ✓
  2. Learning 2: Regression ✓
  3. Learning 3: Neural Networks ✓
  4. Learning 4: Reinforcement Learning ✓
- Part 6: Conclusion
  1. **Ethical Issues in AI**
  2. Conclusions and Discussion

Objectives

- Limits of Current and Future AI ✓
- Ethical Issues

Outline

Given that AI is a powerful technology, we have a moral obligation to use it well, to promote the positive aspects and avoid or mitigate the negative ones.

Positive aspects examples

- AI can save lives through improved medical diagnosis, new medical discoveries, better prediction of extreme weather events
- AI can improve lives, Microsoft's AI for Humanitarian Action program applies AI to recovering from natural disaster
- AI applications in crop management and food production help feed the world

Examples of Negative Aspects

Lethal autonomous weapons

The UN defines a lethal autonomous weapon as one that locates, selects, and engages (i.e., kills) human targets without human supervision.

Israel's Harop missile is a "loitering munition" with a ten-foot wingspan and a fifty-pound warhead. It searches for up to six hours in a given geographical region for any target that meets a given criterion and then destroys it.

Autonomous weapons have been called the "third revolution in warfare" after gunpowder and nuclear weapons. Their military potential is obvious.

The debate over autonomous weapons includes **legal, ethical and practical aspects**.

Lethal autonomous weapons

- **Legal:** requires the possibility of discriminating between combatants and non-combatants, the judgment of military necessity for an attack, and the assessment of proportionality between the military value of a target and the possibility of collateral damage.
- **Ethical:** some find it simply morally unacceptable to delegate the decision to kill humans to a machine.
  More than 140 NGOs in over 60 countries are part of the Campaign to Stop Killer Robots, and an open letter organized in 2015 by the Future of Life Institute organized an open letter was signed by over 4,000 AI researchers and 22,000 others.

Lethal autonomous weapons

- **Reliability:** a very serious concern for military commanders, who know well the complexity of battlefield situations. Cyberattacks against autonomous weapons could result in friendly-fire casualties.
- **Practical:** the scale of an attack that can be launched is proportional to the amount of hardware one can afford to deploy.

AI is a **dual use technology**: AI technologies that have peaceful applications can easily be applied to military purposes.

The Ethics of AI

Surveillance, security, and privacy (1)

- As of 2018, there were as many as 350 million surveillance cameras in China and 70 million in the United States.
- As more of our institutions operate online, more vulnerable to cybercrime and cyberterrorism. Attackers can use automation to probe for insecurities and they can apply reinforcement learning for phishing attempts and automated blackmail
- Defenders can use unsupervised learning to detect anomalous incoming traffic patterns and various machine learning techniques to detect fraud

- More data on us is being collected by governments and corporation
- In the U.S., the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA) protect the privacy of medical and student record

- **De-identification:** eliminating personally identifying information (such as name and social security number) so that medical researchers can use the data to advance the common good
  Federated learning
- **Secure aggregation:** central server doesn't need to know the exact parameter value from each distributed user.

Fairness and bias

- Machine learning models can perpetuate societal bias
- Designers of machine learning systems have a moral responsibility to ensure that their systems are fair
- Six of the most commonly-used concepts for fairness:
  - Individual fairness
  - Group fairness
  - Fairness through unawareness
  - Equal outcome
  - Equal opportunity
  - Equal Impact

Fairness and bias

- **COMPAS** is a commercial system for recidivism (re-offence) scoring. It assigns to a defendant in a criminal case a risk score, which is then used by a judge to help make decisions
  - does not achieve equal opportunity: the proportion of those who did not re-offend but were falsely rated as high-risk was 45% for blacks and 23% for whites

Fairness and bias

- Sample size disparity can lead to biased results.
- In most data sets there will be fewer training examples of minority class
- Machine learning algorithms give better accuracy with more training data, so that means that members of minority classes will experience lower accuracy
- A constrained model may not be able to simultaneously fit both the majority and minority class
- Bias can also come into play in the software development process
- De-bias the data: over-sample from minority classes to defend against sample size disparity

Set of best practices

- Software engineers must talk with social scientists and domain experts to understand the issues and perspectives, and consider fairness from the start.
- Create an environment that fosters the development of a diverse pool of software engineers that are representative of society.
- Define what groups your system will support: different language speakers, different age groups, different abilities with sight and hearing, etc.
- Optimize for an objective function that incorporates fairness.

Set of best practices

- Optimize for an objective function that incorporates fairness.
- Examine your data for prejudice and for correlations between protected attributes and other attributes.
- Understand how any human annotation of data is done, design goals for annotation accuracy, and verify that the goals are met.
- Don’t just track overall metrics for your system; make sure you track metrics for subgroups that might be victims of bias.
- Include system tests that reflect the experience of minority group users. Have a feedback loop so that when fairness problems come up, they are dealt with

Trust and transparency

- An AI system that can explain itself is called explainable AI (XAI).
- A good explanation has several properties:
  - Verification means that the product satisfies the specifications
  - Validation means ensuring that the specifications actually meet the needs of the user and other affected parties
- Certification and safe standards, ISO in other industries
- The AI industry is not yet at this level of clarity, although there are some frameworks in progress, such as IEEE P7001, a standard defining ethical design for artificial intelligence and autonomous systems
- **Transparency:** consumers want to know what is going on inside a system, and that the system is not working against them, whether due to intentional malice, an unintentional bug, or pervasive societal bias that is recapitulated by the system

Trust and transparency

- An AI system that can explain itself is called explainable AI (XAI).

- A good explanation has several properties:
  - it should be understandable and convincing to the user
  - it should accurately reflect the reasoning of the system
  - it should be complete,
  - it should be specific in that different users with different conditions or different outcomes should get different explanations.

The future of work

- An immediate reduction in employment when an employer finds a mechanical method to perform work previously done by a person
- More automation with physical robots, first in controlled warehouse environments, then in more uncertain environments, building to a significant portion of the marketplace by around 2030.
- The ratio between workers and retirees changes. In 2015 there were less than 30 retirees per 100 workers; by 2050 there may be over 60 per 100 workers
- Problems due to the pace of change

Robot rights

- If robots can feel pain, if they can dread death, if they are considered “persons,“ then the argument can be made that they have rights and deserve to have their rights recognize
- If robots have rights, then they should not be enslaved, and there is a question of whether reprogramming them would be a kind of enslavement
- Another ethical issue involves voting rights: a rich person could buy thousands of robots and program them to cast thousands of votes—should those votes count?
- Ernie Davis argues for avoiding the dilemmas of robot consciousness by never building robots that could possibly be considered conscious.

AI Safety

- Design a robot to have low impact, instead of just maximizing utility, maximize the utility minus a weighted summary of all changes to the state of the world.
- Victoria Krakovna (2018) has cataloged examples of AI agents that have gamed the system, figuring out how to maximize utility without actually solving the problem that their designers intended them to solve.
- Genetic algorithm operating in a simulated world was supposed to evolve fast-moving creatures but in fact produced creatures that were enormously tall and moved fast by falling over.
- Designers of agents should be aware of these kinds of specification failures and take steps to avoid them.
- Need to be very careful in specifying what we want, because with utility maximizers we get what we actually asked for. The value alignment problem.

AAAI is currently working on a set of “Responsible AI Licences”

- Restrictions on use of AI software defined by their developers
- In the spirit of Open Source Licences

`https://www.licenses.ai/aaai-sss`

Outline

- Philosophers use the term weak AI for the hypothesis that machines could possibly behave intelligently, and strong AI for the hypothesis that such machines would count as having actual minds (as opposed to simulated minds)
- AI is a powerful technology, and as such it poses potential dangers, through lethal autonomous weapons, security and privacy breaches, unintended side effects, unintentional errors, and malignant misuse. Those who work with AI technology have an ethical imperative to responsibly reduce those dangers.
- AI systems must be able to demonstrate they are fair, trustworthy, and transparent
- There are multiple aspects of fairness, and it is impossible to maximize all of them at once. So, a first step is to decide what counts as fair
- Automation is already changing the way people work. As a society, we will have to deal with these changes.

Future of AI Summary

- Limits of AI
- Strong vs. Weak AI and arguments
- Ethical and Safety aspects of AI
  - Positive and Negative aspects of advances in AI
  - Ethical Guidelines
- AI Licenses

Any Questions.