2023 Spring 双教授线上科研项目-外方教授大纲

卡耐基梅隆大学计算机科学终身教授

人工智能，机器学习，深度学习

2023年03月11日-04月15日

课题简介

人工智能正在为人机交互带来巨大的推动作用。目前，人工智能是从感知智能向认知智能发展。例如：机器可以进行自主学习且变得更为智能吗？我们可以输入指令让电脑执行日常任务：比如开车吗？现如今，机器学习无处不在，它正在深刻地改变我们的社会。人工智能与机器学习，即使不使用解决方案逻辑编写明确的程序，也可以解实际生活中的决许多问题。当我们尝试通过互联网使用信用卡购买商品时会发生什么？我们如何确保网上银行系统的安全性？我们可以设计一个不能被破解的密码吗？的确，人工智能在最近两年大出风头，无人驾驶汽车，阿尔法狗战胜人类最强棋手，演唱会人脸识别抓捕逃犯，手机多国语言在线翻译，这一切一切无不给我们带来深深的震撼，可以说人工智能将在不久的未来引来巨大的爆发式增长，对我们每个人的生活带来深刻的影响。
因此，本课题将会系统探索人工智能与机器学习之间的相互作用。在我们的日常生活中，这一领域也起着越来越重要的作用。近些年来，机器学习的应用范围从金融应用程序到军事领域，再到比特币，甚至在保护日常的应用程序（如微信和WhatsApp）的安全方面等。本课题将面向初学者介绍人工智能/机器学习与密码学和区块链等非常热门的主题，且这些领域正在蓬勃发展，并提供了巨大的潜力。

学习目标

- 理解人工智能及机器学习的核心概念
- 探索机器学习与图神经网络的发展历程
- 学习区块链和深度学习等高端技术
- 预测机器学习和计算机科学方向挑战和机遇

课题要求

为了更好参与本课题，请在开课前仔细阅读相关学术材料。若有相关学术问题，请及时与TA老师进行沟通。

阅读材料

1. Introduction to Cryptography
2. From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues
3. An Artificial Intelligence Approach

（具体教学材料报名后将由教务老师进行统一发放）

教授信息

Prof. V G
卡耐基梅隆大学计算机科学终身教授
加州大学洛杉矶分校博士学位
卡耐基梅隆大学计算机理论组、计算机加密技术组主要负责人
曾在微软研究部担任过7年的研发工作、计算机加密技术领域专家，27个国际计算机加密技术峰会项目成员
2016年获得网络安全顶级会议测试奖
荣获JP Morgen教员奖学金，微软研究生奖学金及谷歌杰出研究生奖
研究多次被《麻省理工科技评论》及《自然》等大众科学出版物收录及出版
2013年度福布斯30位30岁以下科学及医疗领域杰出人获奖者之一（30 under 30）

任职大学

卡内基梅隆大学（Carnegie Mellon University），简称CMU，是美国25所新常春藤盟校之一。2020年QS世界大学学科排名中，其计算机与信息系统学排名世界第3。截至2019年3月，该校共培养出了13个图灵奖、17个诺贝尔奖、9个奥斯卡金像奖、114个艾美奖、44个托尼奖得主。长期以来，CMU的计算机系都占据全美第一的位置，学校的软件工程专业全美排名第一，其研究院更是美国国防部的军官研究院。CMU位列CSRankings排名世界第一。U.S. News计算机本科及硕士项目与斯坦福大学，麻省理工学院，加州大学伯克利分校并列全美第一。CMU的量化金融硕士项目（MSCF）也常年位列全美前3。此外，CMU戏剧学院还被好莱坞报道评为全美五大最佳本科戏剧学院之一。CMU的其他理工科专业也名声显赫。梅隆科技学院（Mellong College of Science）培养了10名诺贝尔奖得主；同时该院是全球第一个开设“绿色化学”课程的学院；硅胶、防弹材料、现代主流的塑料制造工艺都是该学院的研究成果。

项目收获

★ 课程证明、教授评价表、科研项目推荐信

★ 出勤及作业达标的优秀学生可获得至多8封外方教授edu网推推荐信和至多8封支持邮寄的中方教授纸质版推荐信

★ 辅导学生在EI/CPCI或同等级别国际会议上以独立一作发表学术论文，鼓励学生实地或远程参加国际学术会议

项目亮点

在地国际化特色

不出国门，就可以跟随海外名校教授进行学术研究，既为学生及其家庭节省了国际旅费又避免了时差等不适应性。

海外名校现职/终身教授全程授课并指导科研

教授均为海外名校现职教授/终身教授，具有丰富的学术和科研经验，教授将根据中国学生特点设计课题，学术性与趣味性兼备，让学员在学术框架下，充分发挥想象力和创造力，从开题、文献检索、科研报告撰写、修改等多个环节进行学习，实现理论与实践的融会贯通。

国家一流大学现职教授全程直播辅助指导

教授均为国家一流大学现职教授，具有丰富的学术和科研经验，教授将根据中国学术发展方向以及中国学生特点设计课题，学术性与趣味性兼备。中方和外方教授带领学生在同一领域探索更多学术内容，同时让学员在学术框架下，充分发挥想象力和创造力，实现理论学习与实践应用的同步发展。

专业TA/RA助教全程辅助

助教将经过严格筛选，择优录取相关专业研究生/博士生，并通过系统化培训及考核后参与进入科研项目组。助教将协助学生进行课题知识的预习和复习，并为学员提供辅助性指导和技术支持。此外，助教将与学生分享自身升学、海外学习和科研等经验，更加贴近学生实际情况，提供辅助性建议。

专业论文老师1V1论文发表辅导

参与项目的每一位论文老师都是经过严格筛选，为学生量身定制国际会议及时间规划。另外在论文选题，论证，语言组织，排版，选会，投稿，录用，见刊和检索等一系列环节上，也为学生提供一对一的论文专业指导，最终助力学生论文写作水平及相关能力的提升。

全面提升多项能力，提高名校录取几率

为来自全球高中生及大学生提供经济便捷的世界顶级学术研讨和实践的参与机会，帮助学培养批判性思维、分析和创造性思维、复杂沟通-口头和书面表达和全球视野，通过深度学习，帮助学生大幅提高申请几率，并向成为国际水平高精尖领域人才和高水平创新人才更近一步。

时间规划

Schedule	Time
Professor 教授	8：00-10：00 AM (Beijing Time) 早上8：00-10：00 （北京时间）
TA 助教	TBA 根据组内学生时间共同商定
Office Hour 答疑	TBA 根据组内学生时间共同商定

学习计划

Schedule	Topics
Professor Warm Up	Course Introduction and Greetings
TA Preview	Course Preview and Introduction
Lecture 1	What is machine learning? What is artificial intelligence? What are their common applications? Why is it such an exciting topic? Supervised and unsupervised learning. Classification and regression. An overview of the course. 什么是机器学习？什么是人工智能？它们常见的应用是什么？为什么这是一个如此令人兴奋的话题？监督学习和非监督学习；分类和回归
Lecture 2	Linear and Polynomial Regression: Linear regression is perhaps the most basic machine learning algorithm. We will see the basics of linear regression, the notion of cost function, and the widely used gradient descent algorithm. We will use our first learning algorithm to solve real world problems. We will also have a small refresher on linear algebra. We will see how to handle multiple features in linear regression and the notion of polynomial regression. We will also see normal equation method to solve linear regression using matrix algebra. 线性回归与多项式回归：线性回归可能是最基本的机器学习算法；我们将系统学习线性回归的基础，代价函数的概念及梯度下降算法；我们将使用第一个学习算法来解决现实世界中的实际问题，进而复习线性代数；学生将看到是如何处理线性回归和多项式回归概念中的多重特性；我们也将看到如何用矩阵代数来解决线性回归的正规方程的相关方法
Lecture 3	Logistics Regression, Neural Networks, Support Vector Machines, K-Means Clustering: We will see Logistic regression, sigmoid function, and logistic regression cost function. We will see basics of neural networks, building and representing neural networks, and training a neural network. We will see the notion of support vector machines (SVMs) at a high level. We will then move to unsupervised learning and learn the popular K-means clustering algorithm. 物流回归分析，神经网络，支持向量机，K-Means Clustering算法：我们将看到物流回归，机器学习之Sigmoid函数，和物流回归成本函数；我们将学习神经网络的基础知识：如何建立和表示神经网络，并训练神经网络；最后我们将从高层次上了解支持向量机(SVMs)的概念，进而将转向无监督学习，并学习流行的K-means聚类算法
	Automated Game Playing: Can computers be smart enough to play games like Chess or Go and even beat expert humans? We will cover the basics of combinatorial games which develops theories and

Lecture 4	algorithms which can be implemented on computers and used to win board games. We will look at many board games which almost all of us have played as children. 全自动玩游戏：机器可以聪明到玩国际象棋或围棋，甚至打败人类高手吗？我们将介绍组合游戏的专业知识，并系统介绍在计算机上实现的理论和算法，并用于赢得棋盘游戏的方法；我们将着眼于许多几乎所有人都在孩童时期玩过的桌面游戏
Lecture 5	Privacy Preserving Machine Learning: Whenever there is big data, there are privacy issues. Can we train models without violating data privacy? This is one of the hottest areas within AI/machine learning. We will learn the basics and cover a few cryptographic techniques to help doing machine learning while preserving privacy. 机器学习：只要有大数据，就会涉及隐私问题；我们能在不侵犯数据隐私的情况下训练模型吗？这是AI/机器学习中最热门的领域之一；我们将学习基础知识，并涵盖一些密码技术，以帮助做机器学习，同时保护数据隐私
Lecture 6	Summary, and Q&A 最终成果展示、课题答疑

大纲原文

Class Topic: Artificial Intelligence & Machine Learning

Prof. V G

Carnegie Mellon University

Course Overview:

This is a first course in machine learning and AI. We will go through the very basics of machine learning and artificial intelligence. This course is designed keeping in mind a high school or a beginner college student. If you have already taken a course or otherwise have significant pre-existing experience in the subject, this course is not right for you. At the end of the course, the students will have a clear idea of the basics of this field and the common techniques which are employed.

Course Description:

This is a first course in machine learning and AI. We will go through the very basics of machine learning and artificial intelligence. This course is designed keeping in mind a high school or a beginner college student. If you have already taken a course or otherwise have significant pre-existing experience in the subject, this course is not right

for you. At the end of the course, the students will have a clear idea of the basics of this field and the common techniques which are employed.
Prerequisites: There are no prerequisites for this course. However, we expect the students to have a basic background in mathematics. To help the students, the course will include a brief refresher on the necessary mathematics concepts.

Course Objectives:

- Understand the core concepts of artificial intelligence and machine learning
- Explore the evolution of machine learning and graph neural networks
- Learn about high-end technologies such as blockchain and deep learning
- Predict challenges and opportunities in machine learning and computer science

Extended Readings:

1. Introduction to Cryptography
2. From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues
3. An Artificial Intelligence Approach

Session Plan:

Lecture 1
What is machine learning? What is artificial intelligence? What are their common applications? Why is it such an exciting topic? Supervised and unsupervised learning. Classification and regression. An overview of the course.
Lecture 2
Linear and Polynomial Regression: Linear regression is perhaps the most basic machine learning algorithm. We will see the basics of linear regression, the notion of cost function, and the widely used gradient descent algorithm. We will use our first learning algorithm to solve real world problems. We will also have a small refresher on linear algebra. We will see how to handle multiple features in linear regression and the notion of polynomial regression. We will also see normal equation method to solve linear regression using matrix algebra.
Lecture 3
Logistics Regression, Neural Networks, Support Vector Machines, K-Means Clustering: We will see Logistic regression, sigmoid function, and logistic regression cost function. We will see basics of neural networks, building and representing neural networks, and training a neural network. We will see the notion of support vector machines (SVMs) at a

high level. We will then move to unsupervised learning and learn the popular K-means clustering algorithm.

Lecture 4

Automated Game Playing: Can computers be smart enough to play games like Chess or Go and even beat expert humans? We will cover the basics of combinatorial games which develops theories and algorithms which can be implemented on computers and used to win board games. We will look at many board games which almost all of us have played as children.

Lecture 5

Privacy Preserving Machine Learning: Whenever there is big data, there are privacy issues. Can we train models without violating data privacy? This is one of the hottest areas within AI/machine learning. We will learn the basics and cover a few cryptographic techniques to help doing machine learning while preserving privacy.

Final Session

Summary, and Q&A

A word for my students:

Dear student! I am keen to see you in my class. In this short, but rather intensive and interactive course you will learn skills, which will help you to feel confident in Machine Learning. I will try to share with you not only the theory (which, I am sure, such a talented student as you can learn from textbooks), but also how it is actually done by practitioners. I hope that this knowledge will give you confidence in your future job interviews. I look forward to introducing you to this exciting topic with broad applications!