机器学习 Machine learning

第一章 绪 论
Introduction

授课人: 周晓飞 zhouxiaofei@iie.ac.cn 2022-9-2

第一章 绪 论

- 1.1 机器学习研究背景:人工智能
- 1.2 机器学习的发展
- 1.3 机器学习研究的问题
- 1.4 课程主要内容
- 1.5 课程安排

第一章 绪 论

- 1.1 机器学习研究背景:人工智能
- 1.2 机器学习的发展
- 1.3 机器学习研究的问题
- 1.4 课程主要内容
- 1.5 课程安排

课程安排

教师团队介绍

首席教师: 周晓飞,研究员

研究方向: 机器学习、人工智能、自然语言处理

zhouxiaofei@iie.ac.cn

教师助教: 董林华,博士研究生

研究方向: 机器学习、知识图谱

donglinhua@iie.ac.cn

课程安排

课程安排

课程编号	课程名称	学时	学分	限选人数	已选人数	教师	开课地点
201M4004H	机器学习	60	3.0	214+212+208	214+212+208	周晓飞	雁栖湖

■ 上课时间(第2-20周,每周3学时)

■ 地点: 一班: 教 1-207 (周五 13:30 - 16:10), 中间休息 2次,每次 5分钟

二班: 教 1-009 (周五 18:10 - 20:50), 中间休息 2 次,每次 5 分钟

三班: 教 1-107 (周六 8:30 - 11:10), 中间休息 2 次,每次 5 分钟

■ 授课方式:课堂讲授

■ 考核方式: 作业+课堂闭卷考试

■ 考试时间: 2022 年 1 月 6 日

课程安排

■课时安排

周	月	_	=	Ξ	四	五	六	日
2	八月/ 九月 /十月	29	30	31	1	2	3	4
3		5	6	7	8	9	10	11
4		12	13	14	15	16	17	18
5		19	20	21	22	23	24	25
6		26	27	28	29	30	1	2
7	十月	3	4	5	6	7	8	9
8		10	11	12	13	14	15	16
9		17	18	19	20	21	22	23
10		24	25	26	27	28	29	30
11	十一月 /十二月	31	1	2	3	4	5	6
12		7	8	9	10	11	12	13
13		14	15	16	17	18	19	20
14	/ 1/1	21	22	23	24	25	26	27
15		28	29	30	1	2	3	4
16	十二月 /一月	5	6	7	8	9	10	11
17		12	13	14	15	16	17	18
18		19	20	21	22	23	24	25
19		26	27	28	29	30	31	1
20		2	3	4	5	6	7	8

考试

第一章 绪 论

- 1.1 机器学习研究背景:人工智能
- 1.2 机器学习的发展
- 1.3 机器学习研究的问题
- 1.4 课程主要内容
- 1.5 课程安排

什么是人工智能?

"人工智能就是让机器来完成那些如果由人来做则需要智能的事情的科学";

"人工智能就是研究如何使计算机去做只有人才能做的智能工作";

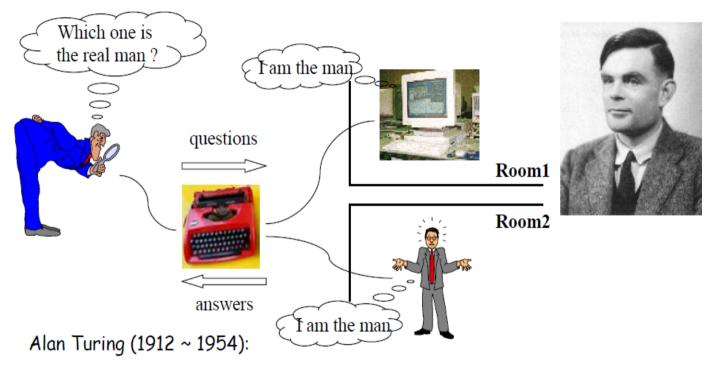
"人工智能是研究使<mark>计算机</mark>来模拟人的某些思维过程和智能行为(如学习、推理、思考、规划等)的学科"。



1956 年 8 月,在美国达特茅斯学院,约翰·麦卡锡(John McCarthy)、马文·闵斯基(Marvin Minsky,人工智能与认知学专家)、克劳德·香农(Claude Shannon,信息论的创始人)、艾伦·纽厄尔(Allen Newell,计算机科学家)、赫伯特·西蒙(Herbert Simon,诺贝尔经济学奖得主)等科学家讨论着一个完全不食人间烟火的主题:用机器来模仿人类学习以及其他方面的智能。会议足足开了两个月的时间,虽然大家没有达成普遍的共识,但是却为会议讨论的内容起了一个名字:人工智能。因此,1956 年也就成为了人工智能元年。

-8- 中国科学院大学网络空间安全学院 2022-2023 学年秋季课程

图灵测试



20世纪最伟大的科学天才之一,他的三大贡献对计算机科学产生了深远的影响。1966年,ACM设立图灵奖。图灵生平见:

"20世纪最伟大的智者之一Alan Turing". 计算机科学, 2000, 27(12)

图灵测试

思考的问题

人的智能非常复杂:例如直觉、顿悟、理解,等等;

人的智能具有"人"性:例如情绪、伪装、狡猾,等等;

人的智能缺陷:不依赖于数学工具,无法实现高难度、大规模的运算;

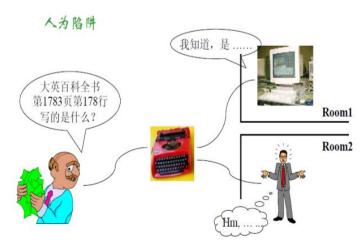
不依赖于词典和存储工具,信息的记忆量、精准性有限;

问题1: 能否从"表现"来评判智能?

思维实验:西尔勒中文屋子



问题2: 能否了解人类的智能水平?



-10- 中国科学院大学网络空间安全学院 2022-2023 学年秋季课程

图灵测试

我们研究的是弱人工智能

强人工智能

科幻电影中





弱人工智能

现实情况中

- AI 与小学生的做题之战, 孰胜孰败?
- DeepMind 称:人工智能在数学领域实现新发现和见解
- 会唱歌、会弹琴,清华大学 AI 学生华智冰火了
- AI 生成的代码可信吗? 编写的代码有 Bug 吗?
- 跟人聊天 VS 跟机器聊天,你更爱哪个?
- AI 盯上了外包司机,看后视镜就被扣分,奖金拜拜!
- AI 天气预报准确度高于气象台,一张 GPU 1秒预测未来 90 分钟天气
- Facebook 正在研究新型 AI 系统,以自我视角与世界进行交互
- 机器人能帮助缝制 T 恤吗? 机器可以取代人力吗?
- 乐高小车竟被装上「生物大脑」,无需算法走出蜂巢迷宫!
- 阿里无人车配送快递突破 100 万单,小蛮驴牵引的自动驾驶战略布局
- 防疫: 英国利兹大学的研究团队开源了 DeepSOCIAL

-11- 中国科学院大学网络空间安全学院 2022-2023 学年秋季课程

人工智能的发展

孕育期 (~1956)

• 1950 年图灵测试

推理期 (1956~1965)

• 1956 年逻辑理论家程序、1960 年 Lisp 语言

知识期 (1965~1983)

• 1965 年分子结构的专家系统 DENDRAL, 1972 年细菌感染专家系统 MYCIN

学习期 (1983~2006)

• 解决知识工程瓶颈,统计机器学习主导

人工智能的发展

黄金期 (2006~)

- 2006年DBN;
- 2012 年 AlexNet;
- 2015年ResNet;
- 2016年创建公益性的人工智能机构 OpenAI;
- 2016年 IBM 发布类脑超级计算机平台; 谷歌量子计算机取得重要的突破;
- 2016年AlphGo;
- 2018 年 AlphaFold; 2020 年 AlphaFold2 夺魁 CASP 大赛,可媲美最先进的实验技术
- 2018-2022 年,以深度学习为代表的人工智能核心技术不断取得新突破, Google 发布预训练语言模型 BERT、OpenAI 开放商用 GPT-3 API 等.

人工智能的发展

对人工智能的期望

- 在人工智能的第一波中, 你必须成为一名程序员;
- 在人工智能的第二次浪潮中,你必须是一名数据科学家;
- 人工智能的第三次浪潮- 你越道德越好。。。

人工智能创新发展对社会的影响

引领新一轮产业变革之势,推动人类社会进入智能化时代

"智能+"模式的普适应用为经济社会发展注入新动能,乐观的看,人工智能有望 引领第四次工业革命,对社会、经济、军事等领域将产生变革性影响,在制造、交通、 教育、医疗、服务等方面可以造福人类。

人工智能创新发展对社会的影响

人工智能成为世界各国竞相战略布局的新高地

- 美、日、德、英、法、俄等国家都制定了发展人工智能的国家战略
- 2017年起工业互联网公司相继成立 AI 研究院
- 2017 年国务院印发《新一代人工智能发展规划》

第一步, 2020年 与世界先进水平同步

第二步,2025年 实现重大突破,部分技术与应用达到世界领先水平

第三步,2030年 达到世界领先水平,成为世界主要人工智能创新中心

- 2018 年国内高校院所相继成立了人工智能学院
- 2020-2021 年国内外 AI 研究机构和公司竞相规划 "元宇宙"蓝图

人工智能创新发展对社会的影响

人工智能成为世界各国竞相战略布局的新高地

- 2021 我国十四个五年规划和 2035 年远景目标纲要
 - ◇ 第二篇 坚持创新驱动发展 全面塑造发展新优势
 - ---科技前沿领域攻关专栏包括: 新一代人工智能、脑科学与类脑研究
 - ◆ 第三篇 加快发展现代产业体系 巩固壮大实体经济根基
 - ---制造业核心竞争力提升专栏包括:智能制造与机器人技术
 - ◆ 第五篇 加快数字化发展 建设数字中国 培育壮大人工智能、大数据、区块链、网络安全等新兴数字产业
 - ---数字经济重点产业专栏 7 个主题:云计算、大数据、物联网、工业互联网、区块链 人工智能、虚拟现实和增强现实
 - ---数字化应用场景专栏 10 个主题:智能+(交通、能源、制造、农业水利、教育、医疗、文旅、社区、家居、政务)

人工智能创新发展对社会的影响

全球人工智能技术现状及竞争格局

• 我国人工智能综合实力不断提升

2021 年全球人工智能创新指数仍呈现明显的梯次分布, 46 个参评国家分为四大梯队:

第一梯队:美国和中国,

第二梯队包括韩国、英国等 9 个国家,

第三梯队包括瑞典、卢森堡等 13 个国家,

第四梯队包括印度、俄罗斯等 22 个国家。

(《2021 全球人工智能创新指数报告》中国科学技术信息研究所)

人工智能创新发展对社会的影响

全球人工智能技术现状及竞争格局

• 美国对华的技术限制

2019 年 8 月、10 月,美国商务部将旷视科技、商汤科技、依图科技等中国知名人工智能服务企业加入贸易管制名单; 把将近 50 家与华为相关联的公司拉入了实体清单。

2020 年 5 月,宣布了一份新的出口管制"实体清单",将中国的 33 家科技公司、科研机构和高校纳入制裁,尤其与 AI 智能、量子计算、互联网服务、光电技术、安全与监控、材料仪器、数据分析等相关的领域。凡是被列到清单上的企业和机构,都必须在涉及美国产品与技术的出口、转口和转让贸易时,事先获得美国相关部门发放的许可证。

2020 年 8 月,美国商务部宣布,严格限制华为使用美国的技术、软件设计和制造半导体芯片,禁止包括台积电、高通、 三星及 SK 海力士、美光等将不再供应芯片给华为,同时将华为在全球 21 个国家的 38 家子公司列入"实体名单"。

人工智能创新发展对社会的影响

人工智能这个机遇与挑战并存的新课题引起了全球范围内的广泛关注和高度重视。虽然人工智能未来的创新发展还存在不确定性,但是大家普遍认可人工智能的蓬勃兴起将带来新的社会文明,将推动产业变革,将深刻改变人们的生产生活方式,将是一场影响深远的科技革命。

党的十八大以来,习近平总书记把创新摆在国家发展全局的核心位置,高度重视人工智能发展,多次谈及人工智能的重要性,为人工智能如何赋能新时代指明了方向。 2018 世界人工智能大会9月17日在上海开幕,习总书记致信祝贺并强调指出人工智能发展应用将有力提高经济社会发展智能化水平,有效增强公共服务和城市管理能力。深入学习领会习总书记关于人工智能的一系列重要论述,务实推进我国《新一代人工智能发展规划》,有效规避人工智能"鸿沟",着力收获人工智能"红利",对建设世界科技强国、实现"两个一百年"的奋斗目标具有重大战略意义。

----- 谭铁牛 十三届全国人大常委会专题讲座第七讲 人工智能的创新发展与社会影响

第一章 绪 论

- 1.1 机器学习研究背景:人工智能
- 1.2 机器学习的发展
- 1.3 机器学习研究的问题
- 1.4 课程主要内容
- 1.5 课程安排

什么是机器学习?

机器学习是一门人工智能的科学

"机器学习是一门人工智能的科学,该领域的主要研究对象是人工智能,特别是如何在经验学习中改善具体算法的性能"。Langley (1996)

"机器学习是对能通过经验自动改进的计算机算法的研究"。Tom Mitchell (1997)

"机器学习是用数据或以往的经验,以此优化计算机程序的性能标准"。Alpaydin (2004)

机器学习发展时期

推理期:

20世纪50-70年代初;认为只要给机器赋予逻辑推理能力,机器就能具有智能。

A. Newell 和 H. Simon 的 "逻辑理论家"程序、"通用问题求解"程序;获得了 1975 年图灵奖。

知识期:

20世纪70年代中期,认为要使机器具有智能,就必须设法使机器拥有知识。

E.A. Feigenbaum 作为"知识工程"之父在 1994 年获得了图灵奖。

学科形成:

20世纪80年代, 机器学习成为一个独立的学科领域, 并开始快速发展;

1980 年美国卡内基梅隆大学举行第一届机器学习研讨会;

1983 年《机器学习:一种人工智能途径》出版;

1986 年《Machine Learning》创刊;

1989 年《Artificial Intelligence》出版了机器学习专辑;

1990年《机器学习:风范与方法》出版。

机器学习发展时期

蓬勃发展期:

20 世纪 90 年代后,统计学习方法占主导,代表 SVM;

• 2006 至今,大数据分析的需求,神经网络又被重视,成为深度学习理论的基础。

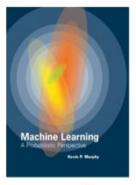
(回顾神经网络发展: 50 年代代表性工作主要有感知机、Adaline; M. Minsky 和 S. Papert, 1969 年指出神经网络只能用于线性分类,此后 15 年停滞期; 1983 年, J.J. Hopfield 利用神经网络求解 TSP 问题获得了成功,连接主义重新受关注,特别是 D.E. Rumelhart、G.E. Hinton 和 R.J. Williams 重新发明了著名的 BP算法,产生了非常大影响。)

学科特点

广泛的应用前景、人工智能的前沿、学科体系趋于成熟



Tom Mitchell 1997



Kevin P. Murphy 2012



周志华, 2016

- Christopher M. Bishop, Pattern Recognition and Machine Learning, 2006
- Andrew ng, machine learning, Stanford Course, 2004-2016.
- · 李航,统计学习方法,2012.

应用领域

- 航空航天、军事、国防
- 机器人、无人车、NASA-JPL 火星机器人
- 互联网应用

搜索引擎: 网页、图片、视频、新闻、学术、地图、。。。

信息推荐:新闻、商品、游戏、书籍、。。。

图片识别:人像、用品、动物、交通工具、。。。

文本信息: 机器翻译、对话系统、。。。

用户分析: 社交网络、影评、大众点评、商品评论、。。。

000



Google的成功,使得Internet 搜索引擎成为一个新兴的产业

不仅有众多专营搜索引擎的公司出现(例 如专门针对中文搜索的就有慧聪、百度 等),而且Microsoff等巨头也开始投入巨 资进行研发



Google掘到的第一桶金,来源于其 创始人Larry Page和Sergey Brin提出 的PageRank算法

机器学习技术正在支撑着各类搜索 引擎(尤其是贝叶斯学习技术)



应用领域

- 信息安全 入侵检测 日志挖掘
- 生物信息学
- 天气预报、地震预警、环境污染检测
- 智能识别图像识别、视频分析语音识别、音频分析可穿戴、虚拟现实、智能家居
- 金融、经贸、管理、公共安全、医学、交通、……

入侵检测:

是否是入侵?是何种入侵?



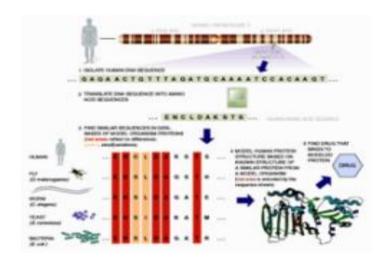
如何检测?

•历史数据:以往的正常 访问模式及其表现、以往 的入侵模式及其表现.....

•对当前访问模式分类

这是一个典型的机器学习问题 常用技术:

神经网络 决策树 支持向量机 贝叶斯分类器 k近邻 序列分析 聚类



-27- 中国科学院大学网络空间安全学院 2022-2023 学年秋季课程

机器学习研究意义

机器学习是人工智能的基石

- 卡内基梅隆大学 2006 年宣布成立"机器学习系"
- 国内许多学会(如 CCF、CAA、CIPS 等)每年都会针对机器学习,开展培训课程和讲座

机器学习引领人工智能的前沿

- 2006 年 Hinton 在 Science 上的论文算起,深度学习为学术创新开启了新思路
- 近年 ResNet、AlphGo、GAN、Bert 等深度学习技术,推动了人工智能的飞速发展,颠覆了语音、图像、自然语言等众多领域。
- 大数据时代的到来,以及 GPU 等各种更加强大的计算设备的发展,深度学习如虎添翼。

机器学习研究意义

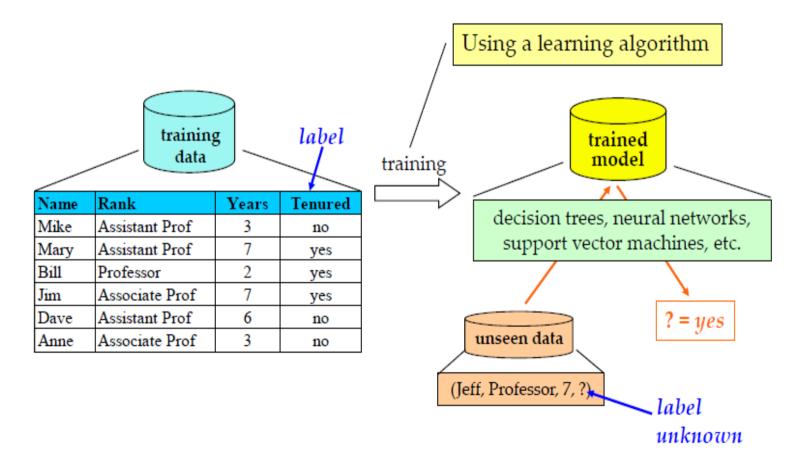
支持宽泛的学科领域

正在逐渐成为基础性、透明化、无处不在的支持技术、服务技术, 在它们真正成功的时候,可能人们已经感受不到它们的存在, 人们感受到的只是更健壮的防火墙、更灵活的机器人、更安全的自动汽车、更好 用的搜索引擎······

第一章 绪 论

- 1.1 机器学习研究背景:人工智能
- 1.2 机器学习的发展
- 1.3 机器学习研究的问题
- 1.4 课程主要内容
- 1.5 课程安排

机器学习的一般过程



机器学习的一般过程

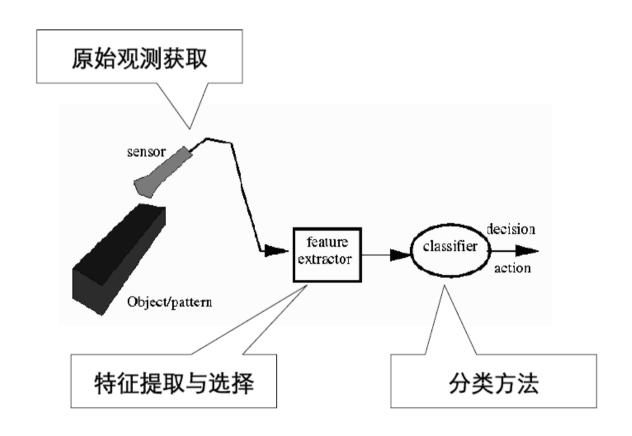


图 2 引自 张学工《模式识别》

机器学习问题

Supervised learning

- Learning mapping between input \mathbf{x} and desired output \mathbf{y}
- Teacher gives me y's for the learning purposes

Unsupervised learning

- Learning relations between data components
- No specific outputs given by a teacher

Reinforcement learning

- Learning mapping between input x and desired output y
- Critic does not give me y's but instead a signal (reinforcement) of how good my answer was

Other types of learning:

- Concept learning, explanation-based learning, etc.

机器学习问题

Supervised learning

Data:
$$D = \{d_1, d_2, ..., d_n\}$$
 a set of n examples $d_i = \langle \mathbf{x}_i, y_i \rangle$

 \mathbf{x}_i is input vector, and y is desired output (given by a teacher)

Objective: learn the mapping
$$f: X \to Y$$

s.t. $y_i \approx f(x_i)$ for all $i = 1,..., n$

Two types of problems:

- Regression: X discrete or continuous →
 - Y is continuous
- Classification: X discrete or continuous →
 - Y is discrete

机器学习问题

Supervised learning example

Classification: Y is discrete

Y: 年轻人(1), 老年人(-1)

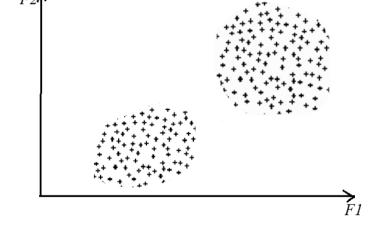
X: x_1 黑头发的比例, 值域(0, 1);

*x*₂ 行走速度, 值域(0, 100)米/每分钟.

Training Data:

 $Y=1: (1, 99), (0.9, 80), (0.80, 100) \dots$

 $Y=-1: (0.2, 30), (0.5, 50), (0.4, 30) \dots$



Test:

X=(0.85, 98), Y=?

机器学习问题

Supervised learning example

Regression: Y is continue

Y: 房屋价钱 (万元), 值域 Y>=0.

X: x₁=房屋面积 m^{2.}

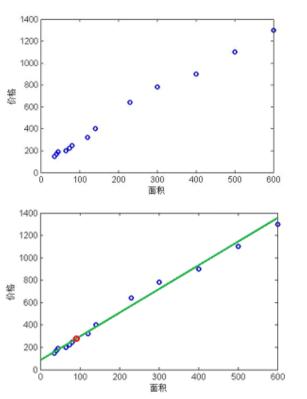
Training Data:

35	150
40	170
45	190
65	200
74	224
80	245
120	320
140	400
230	640
300	780
400	900
500	1100
600	1300



X=90

Test:



y=ax+b

机器学习问题

Unsupervised learning

- **Data:** $D = \{d_1, d_2, ..., d_n\}$ $d_i = \mathbf{x}_i$ vector of values No target value (output) y
- Objective:
 - learn relations between samples, components of samples

Types of problems:

- Clustering
 Group together "similar" examples, e.g. patient cases
- · Density estimation
 - Model probabilistically the population of samples

机器学习问题

Unsupervised learning example

Clustering:

X: (颜色,形状,大小)

Data:





机器学习问题

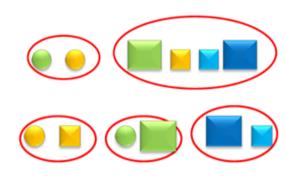
Unsupervised learning example

Clustering:

X: (颜色,形状,大小)

Data:





机器学习问题

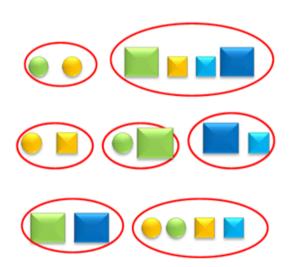
Unsupervised learning example

Clustering:

X: (颜色,形状,大小)

Data:





机器学习问题

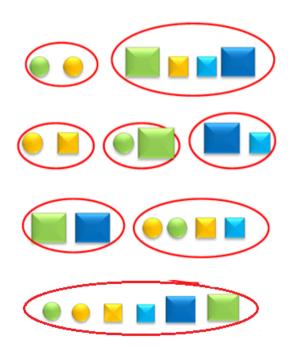
Unsupervised learning example

Clustering:

X: (颜色,形状,大小)

Data:

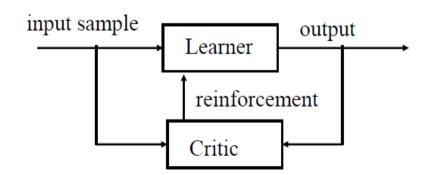




机器学习问题

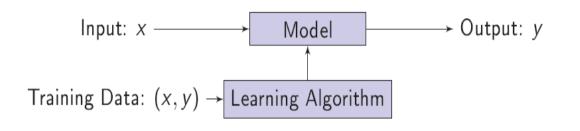
Reinforcement learning

- We want to learn: $f: X \to Y$
- We see samples of \mathbf{x} but not y
- Instead of y we get a feedback (reinforcement) from a critic about how good our output was



The goal is to select outputs that lead to the best reinforcement

建模过程



- **1. Data:** $D = \{d_1, d_2, ..., d_n\}$
- 2. Model selection:
- Select a model or a set of models (with parameters)

E.g.
$$y = ax + b + \varepsilon$$
 $\varepsilon = N(0, \sigma)$

• Select the error function to be optimized

E.g.
$$\frac{1}{n} \sum_{i=1}^{n} (y_i - f(x_i))^2$$

- 3. Learning:
- Find the set of parameters optimizing the error function
 - The model and parameters with the smallest error
- 4. Application:
- Apply the learned model
 - E.g. predict ys for new inputs \mathbf{x} using learned $f(\mathbf{x})$

第一章 绪 论

- 1.1 机器学习研究背景:人工智能
- 1.2 机器学习的发展
- 1.3 机器学习研究的问题
- 1.4 课程主要内容
- 1.5 课程安排

课程目的

了解机器学习研究问题

- 有监督学习: 分类、回归
- 无监督学习:聚类、降维、特征提取等;

掌握基本的统计和优化方法

- 统计学习基础: 最大似然估计、最小均方等;
- 优化基础:梯度下降、随机梯度下降等;

掌握机器学习的基础理论和算法

Bayes、SVM、鉴别分析、logistic、决策树、感知机、多层感知机、Adaboost、 线性回归、k-means、PCA、概率图模型、知识图谱、深度学习及前沿等;

能够针对任务设计机器学习方案

课程内容

大纲

课程内容	3	参考教材: 周志华,《机器学习》, 2016 补充内容
第一章	绪论	第1章
第二章	贝叶斯学习	第7章
第三章	线性分类	第2章、第3章、第5章5.2、
第四章	非线性分类	第4章、第5章、第8章、第6章
第五章	回归分析	第3章
第六章	聚类分析	第9章
第七章	特征降维	第10章、第11章
第八章	信息论模型	补充内容
第九章	概率图模型	第6章、第12章
第十章	神经网络与深度学习	第 14 章

学习资源

研究数据

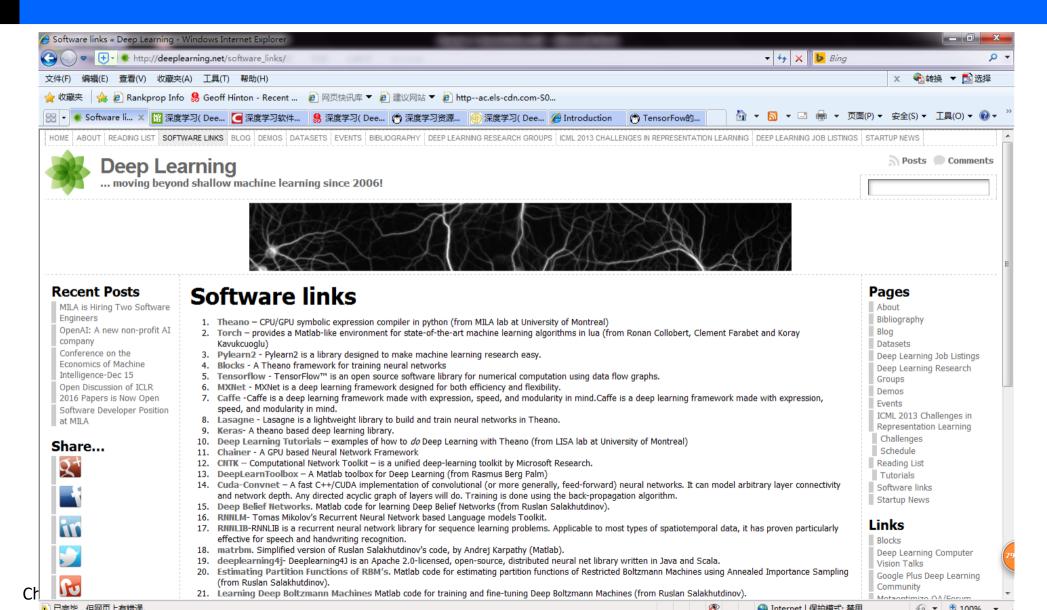
- 不同领域标准数据集(论文中获取)、不同领域会议的评测数据
- UCI Machine Learning Repository: http://archive.ics.uci.edu/ml/
- 数据堂
- 网络爬取
- 微软研究院开发数据集 https://www.microsoft.com/en-us/research/project/microsoft-research-open-data
- VisualData 计算机视觉数据集: https://visualdata.io/discovery
- Kaggle 数据集: https://www.kaggle.com/datasets
- Quandl 金融数据集: https://www.quandl.com/search
- Google 公开数据集: https://cloud.google.com/bigquery/publicdata

. . .

学习资源

工具

- Tensorflow: https://tensorflow.google.cn
- Pytorch: https://pytorch.org
- Python 机器学习工具包 milk: https://github.com/luispedro/milk
- OpenCV: http://opencv.org/
- OpenAl: https://www.openai.com/
- 深度学习开源汇总: http://deeplearning.net/software_links/
- Github: https://github.com/
- Paddle Paddle: https://www.panddlepaddle.org.cn
- NLTK: http://www.nltk.org
- Standford NLP: https://nlp.standford.ed/software
- Paper With Code: https://paperswithcode.com
- 机器学习平台 PAI: https://www.aliyun.com
- Amazon Deep Learning AMI: https://aws.amazon.com



学术会议

ICML、CVPR、NIPS、

IJCAI、AAAI、KDD、

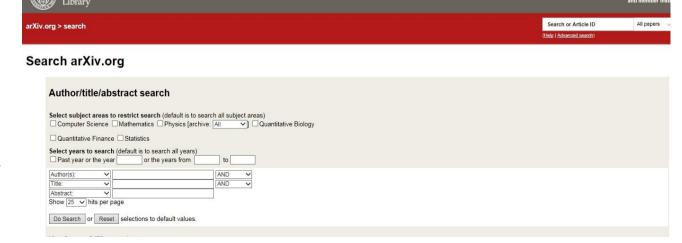
SIGIR, SIGMOD,

COLT, ACL, ECML,

ICDM、WWW、CIKM、IJCNN、

VLDB、ICDE ···

Arxiv 预印论文库: https://arxiv.org/find/



Cornell University

学术刊物

- IEEE-PAMI
- Machine Learning (ML)
- Journal of Machine Learning Research
- IEEE-TKDE
- Artificial Intelligence
- Data Mining and Knowledge Discovery
- Computational Intelligence
- Pattern Recognition
- Neural Computation
- IEEE-NN
- Annals of Statistics
- Journal of Artificial Intelligence Research
- Research, Information and Computation

参考教材和资料

- 课程参考教材: 周志华, 机器学习, 2016.
- 参考资料:
 - -- Chris Bishop. Pattern recognition and Machine Learning. Springer, 2006.
 - --Duda, Hart, Stork. Pattern classification. 2nd edition. J Wiley and Sons, 2000. 模式分类(第二版)中文版.
 - --Pattern Recognition 2nd 模式识别(第二版、第四版).
 Tsinghua 模式识别课程讲义:张学工,模式识别.
 - --统计学习方法,李航,清华大学,2012.
 - -- Simon Haykin, 申富饶等译,神经网络与学习机器,第三版。

本讲参考文献

- 1. 周志华, 机器学习, 清华大学出版社, 2016.
- 2. 周志华, Slides@"机器学习"暑期学校, 2006.