



LiVE Group
视觉智能与学习研究中心

机器学习（第1讲）

主讲：张磊

E-mail: leizhang@cqu.edu.cn
Lab Website: <http://www.leizhang.tk>

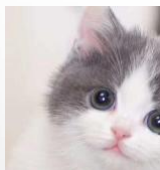
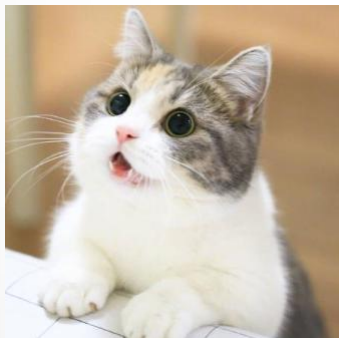




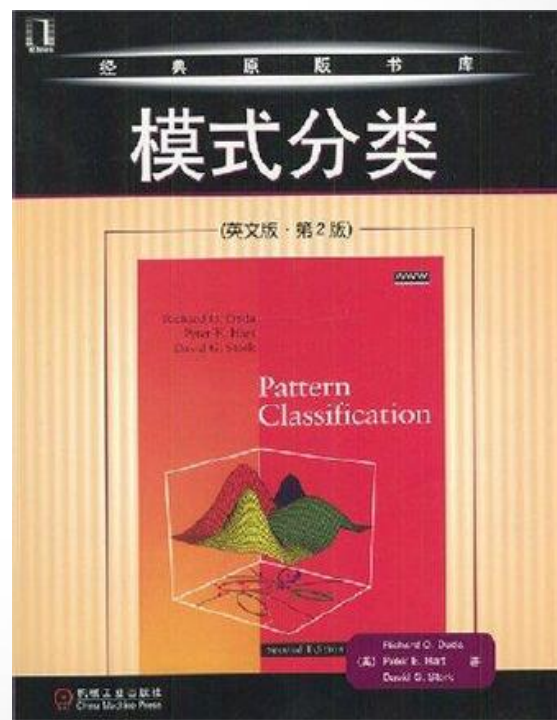
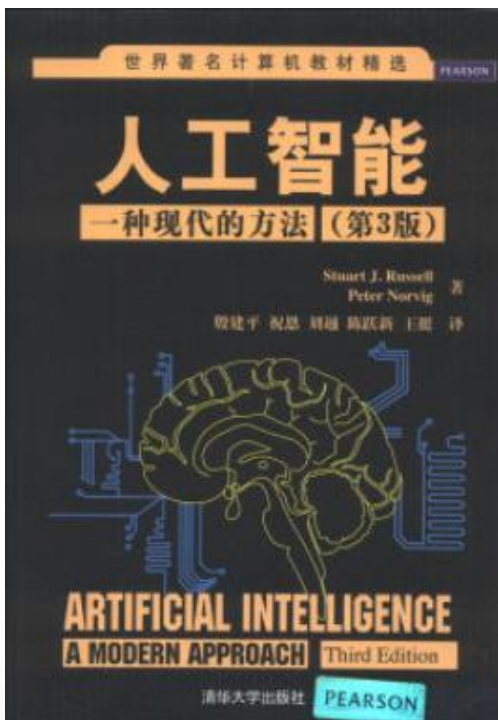
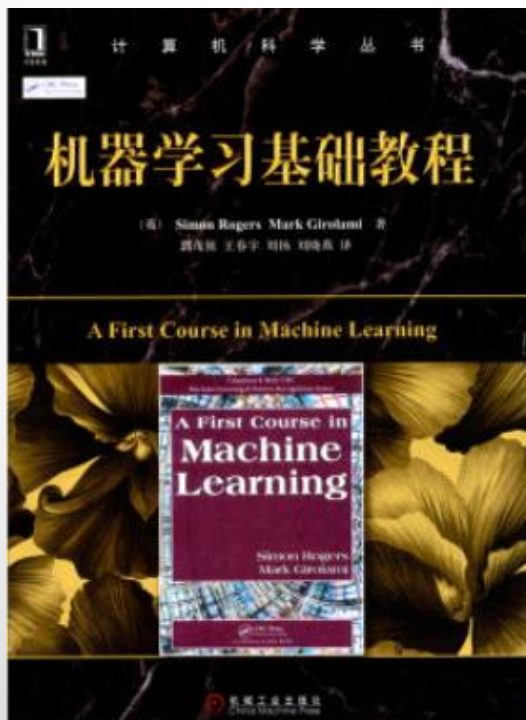
机器学习是什么？

What is Machine Learning?

看图识猫?



教材与参考书目





教材与参考书目

Simon Rogers, Mark Girolami编, 《机器学习基础教程》, 机械工业出版社

Stuart J. Russell, Peter Norvig编 《人工智能——一种现代的方法》第3版, 清华大学出版社,

Richard O. Duda, Peter E. Hart, David G. Stork编 《模式分类》第2版, 机械工业出版社, 中信出版社

Tom M. Mitchell编, 《机器学习》, 机械工业出版社



课时安排

学时：32学时（16次）

考试：理论笔试（闭卷）

学分：2.0

成绩（百分制）：70%考试+30%出勤



课程内容

基础概念：

第一章：绪论—人工智能概念

第二章：智能体

第三章：机器学习中的数学基础

理论方法：

第四章：线性建模（回归）

第五章：正则化学习

第六章：概率建模

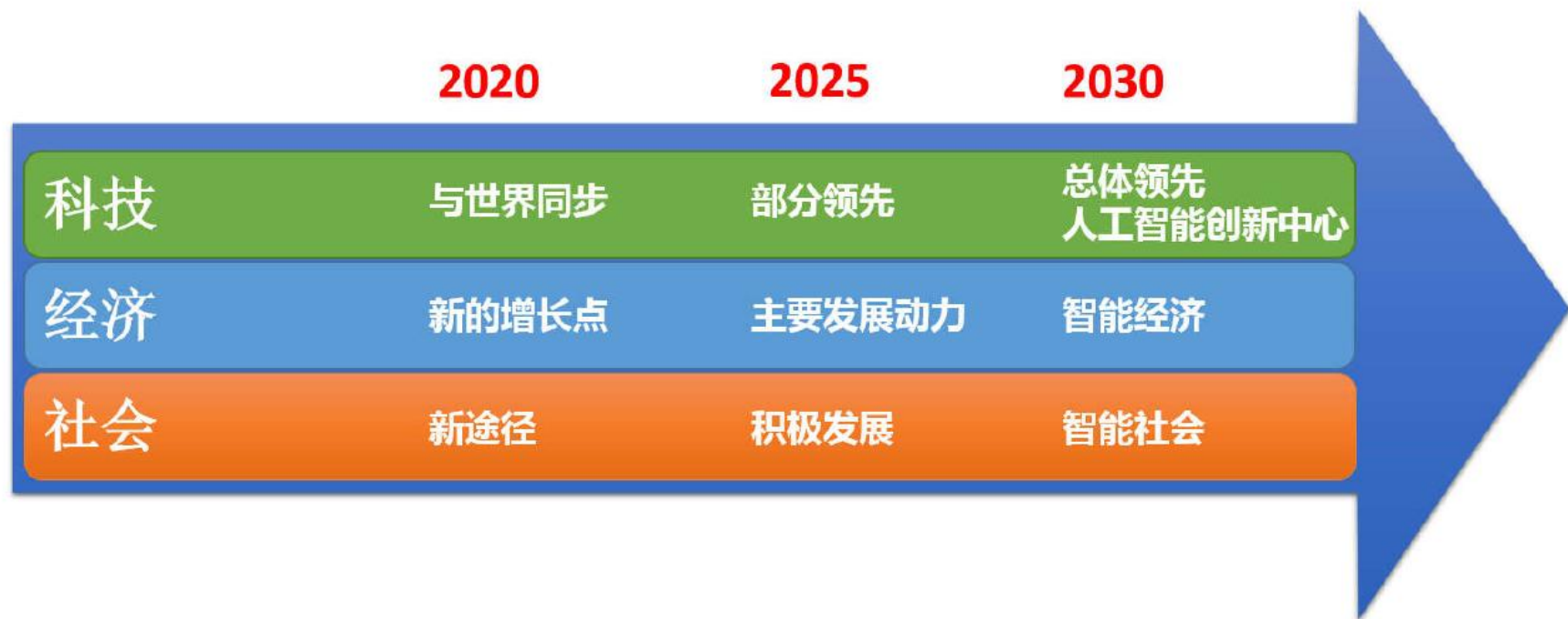
第七章：贝叶斯学习

第八章：分类器学习

第九章：群体智能仿生优化

第十章：神经网络与深度学习

国家人工智能发展规划（国务院2017.7）

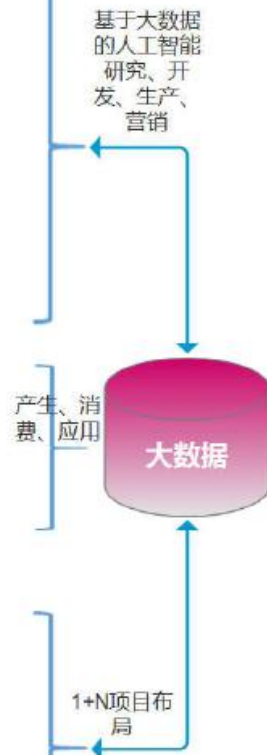
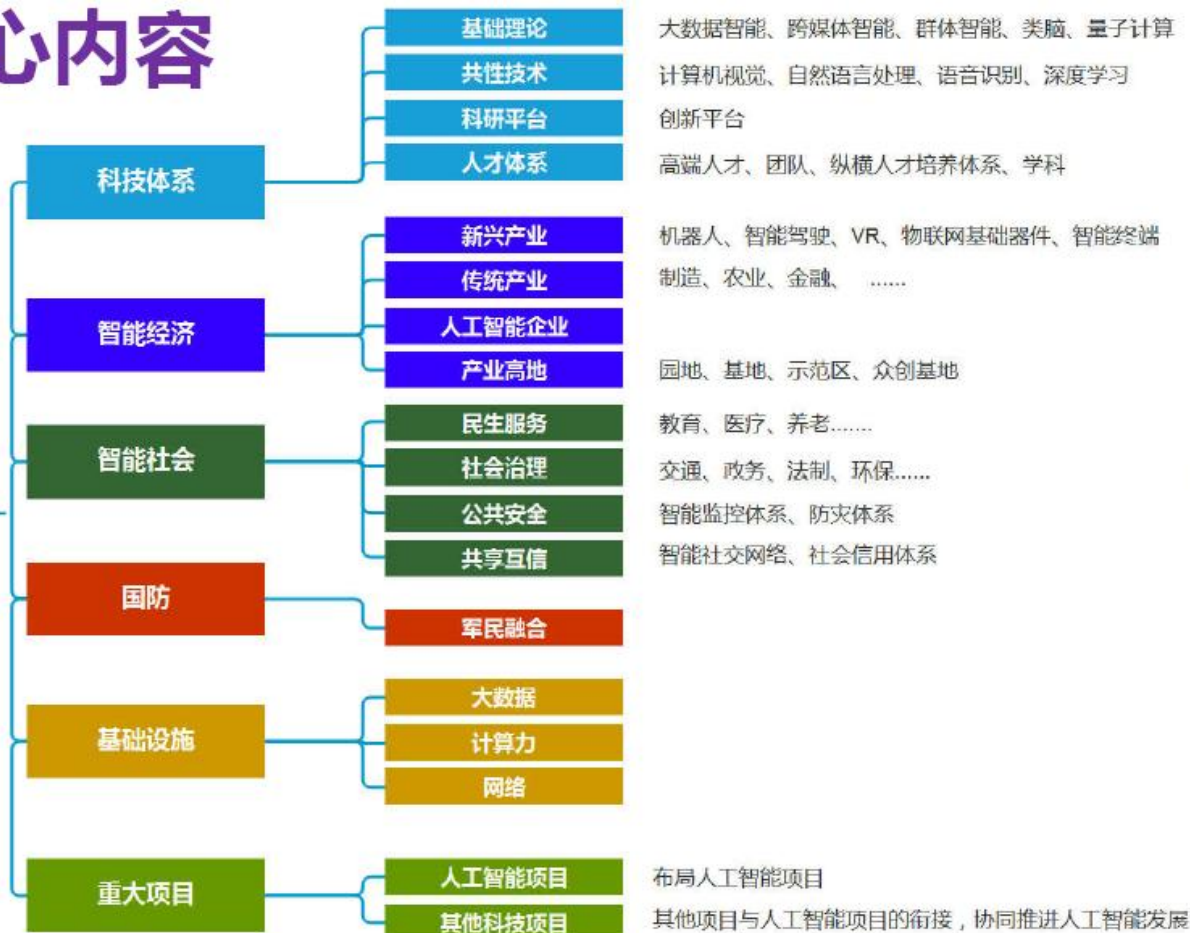


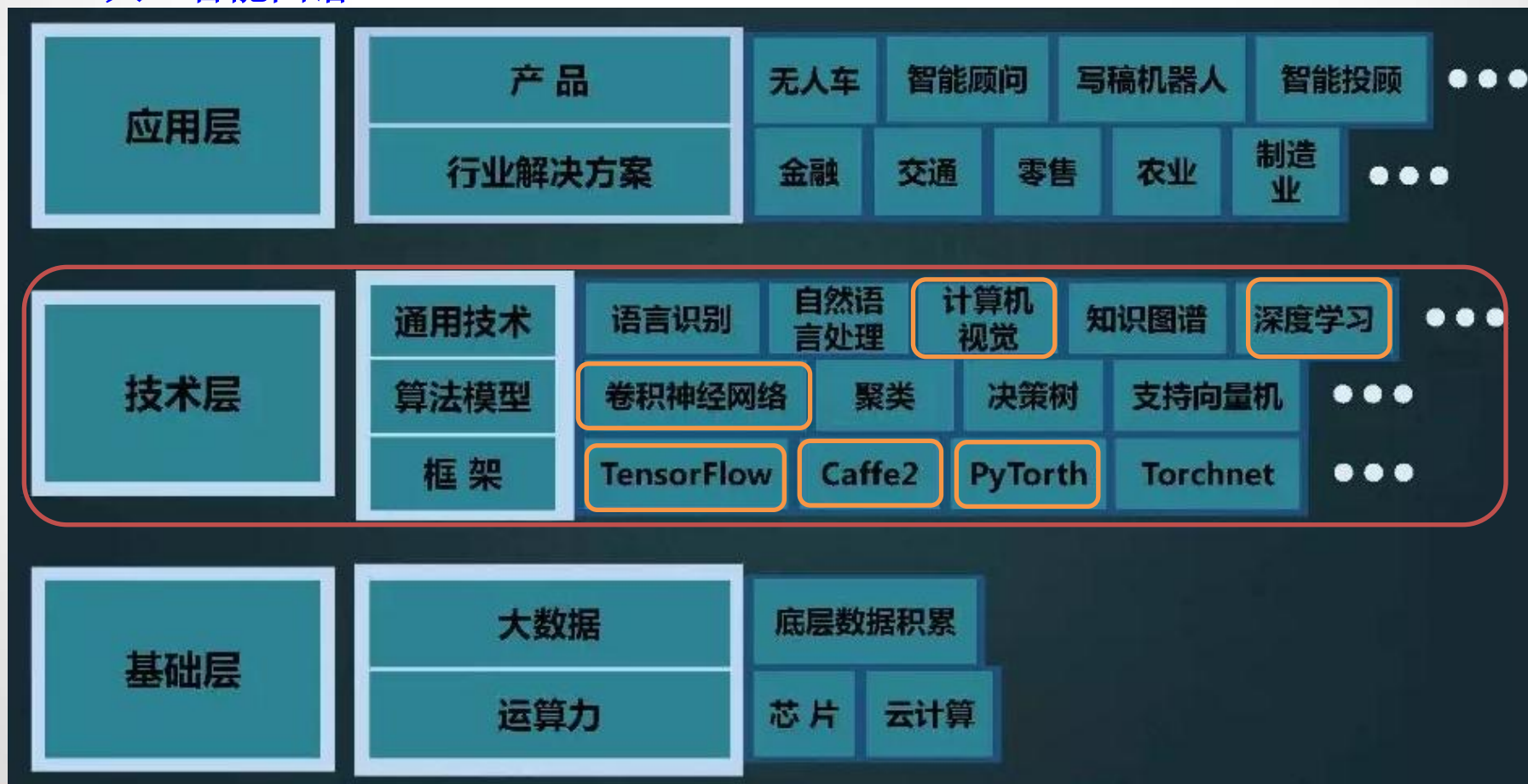


规划核心内容

新一代人工智能发展规划

2017





第一章：绪论

人工智能(Artificial Intelligence, AI) 1956(**达特茅斯会议**):

1950年“图灵测试”的提出, 由Alan Turing(人工智能之父)
——测试者与被测试者在隔离开的情况下, 向被测试者提出疑问



计算机科学之父
(1912-1954)

[1] **On computable numbers, with an application to the Entscheidungsproblem.** 1936

《论数字计算在决断难题中的应用》

[2] **Computing machinery and intelligence.** 1950. 《计算机与智能》

[3] **Can a machine think?** 1950, The world of mathematics. 《机器能思考吗? 》

人工智能是最新兴的科学与工程领域。机器学习为实现人工智能的必要手段, 其目标和任务是试图理解和创造智能实体。

人工智能的大量粉丝: 潜在的爱因斯坦们和爱迪生们, 被大多数领域的科学家们评为“最想参与的研究领域”



第一章：绪论

什么是人工智能(Artificial Intelligence, AI)：

- ◆ 电影和小说中描绘的人工智能（主宰的可怕未来）塑造了大众对人工智能的想象，但这些都是虚构的。在现实生活中，人工智能基本上是在改善人类健康、安全和提升生产力等好的方面。
- ◆ 多数研究型大学和科技公司（苹果、谷歌、facebook、IBM、微软、BAT）也投入巨资，并将人工智能视为未来发展的关键。
- ◆ 好莱坞也将人工智能技术搬上荧幕（反乌托邦人工智能幻想故事）

人工智能定义：

一直以来，人工智能缺乏一个精确的、被普遍接受的定义。目前，一个通用的定义：人工智能是致力于让机器变得智能的活动，而智能就是使实体在其环境中有远见地、适当地实现功能性的能力。

第一章：绪论

什么是人工智能(Artificial Intelligence, AI)?

◆ 像人一样思考

机器要有“脑”，而且会自己思考、决策、求解、学习等。初级的人工智能，需要人类去“教”会机器如何思考，也就是利用计算机模型来研究机器的智能（智力），使机器的自动感知、推理、行为，从计算上成为可能（智能计算）。

利用计算机完成人更加擅长的事情，称为计算智能。



第一章：绪论

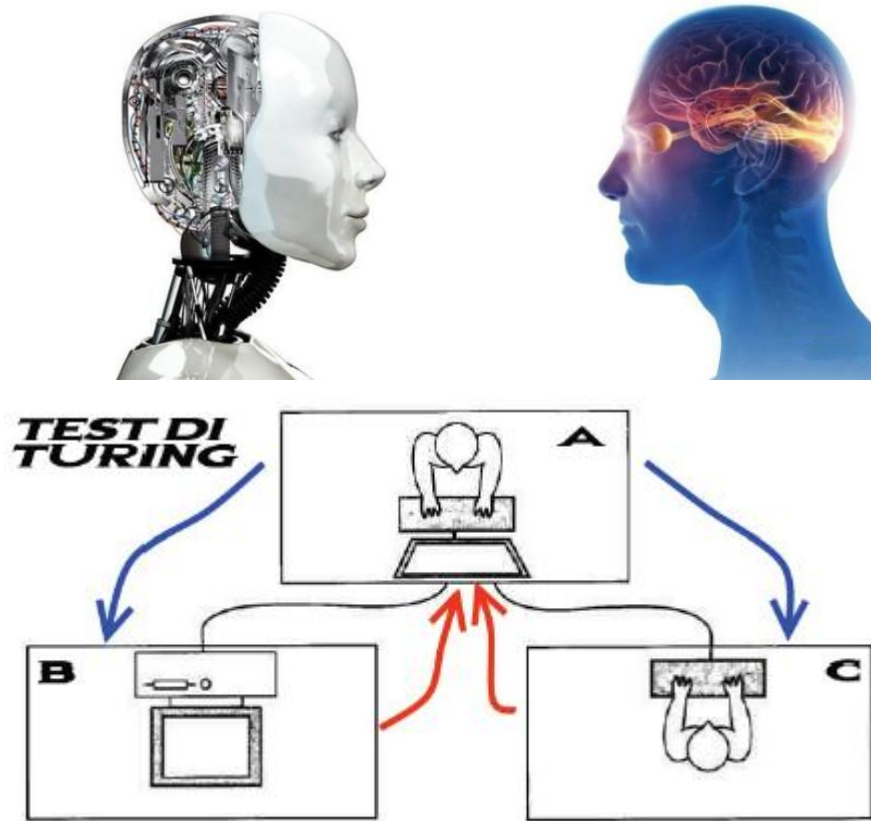


什么是人工智能(Artificial Intelligence, AI)?

◆ 像人一样行动（行为）

图灵测试：由Alan Turing1950提出，为人工智能提供了令人满意的可操作的定义。如果一位人类询问者提出一些问题后，**无法判断对方的回答是来自人还是计算机**，那么这台计算机通过测试（成功“骗”过人）。

60年以后，该测试仍然适合，值得称赞！



第一章：绪论

什么是人工智能(Artificial Intelligence, AI)?

◆ 像人一样行动（行为）

为了能“骗”过人类，还需要通过大量的计算数学模型和计算机编程工作。计算机需要具备以下能力：

知识表示与存储：用于计算机去“记忆”

机器学习：对新知识的认知和学习

自动推理：思考并回答问题和推出新结论

自然语言处理：“听、说”，用于外语交流

计算机视觉：“看”世界（感知）

机器嗅觉、触觉：“嗅”和“摸”（感知）

机器人学：操纵和移动对象



➡ 这些领域涉及人工智能(AI)的大部分内容



第一章：绪论

什么是人工智能(Artificial Intelligence, AI)?

◆ 像人一样行动（行为）

综上所述，要真正通过图灵测试，计算机必须具备理解语言、学习、记忆、推理、决策等能力。从而产生许多学科，如**机器感知**（计算机视觉、自然语言处理），**机器学习**（模式识别、深度学习、增强学习），**记忆**（知识表示），**智能决策**（规划、数据挖掘），这些都属于人工智能的研究范畴。

第一章：绪论

什么是人工智能(Artificial Intelligence, AI)?

飞机/飞行器属于人工智能吗??

航空领域的研究人员不会把研究目标定义为制造“能完全像鸽子一样飞行的机器，使得它们可以骗过其他真鸽子”。



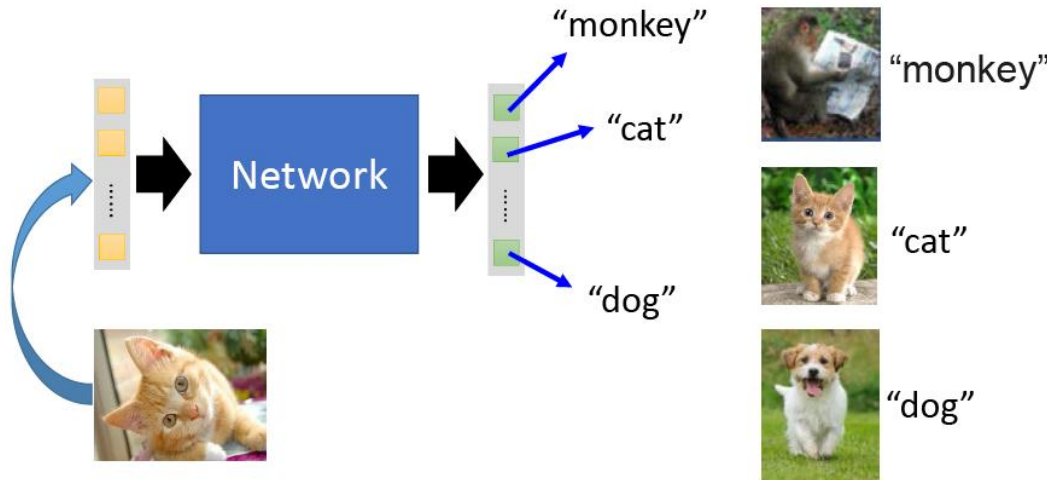
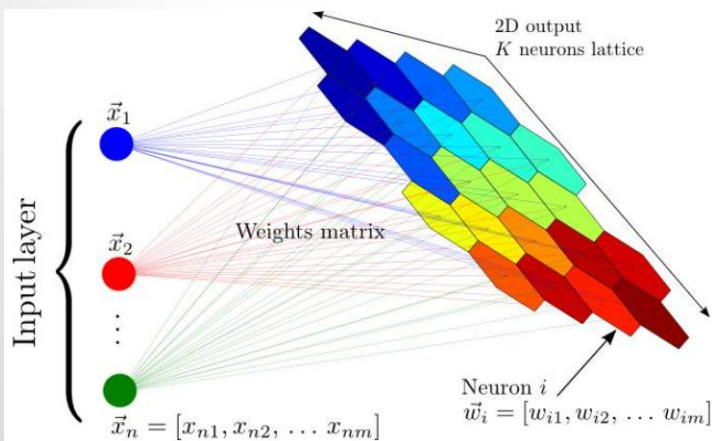


如何实现人工智能(AI)?

◆ 如何让机器像人一样“思考”？

首先，弄清楚人是如何思考，才能教会机器。这是关于逻辑学、心理学、神经科学、脑科学的复杂问题，**目前尚无精确的理论**。虽然人工智能通过计算机模型实现初步的思考、推理和行动，**但与人脑的工作原理之间的联系尚无解释**。

第一章：绪论



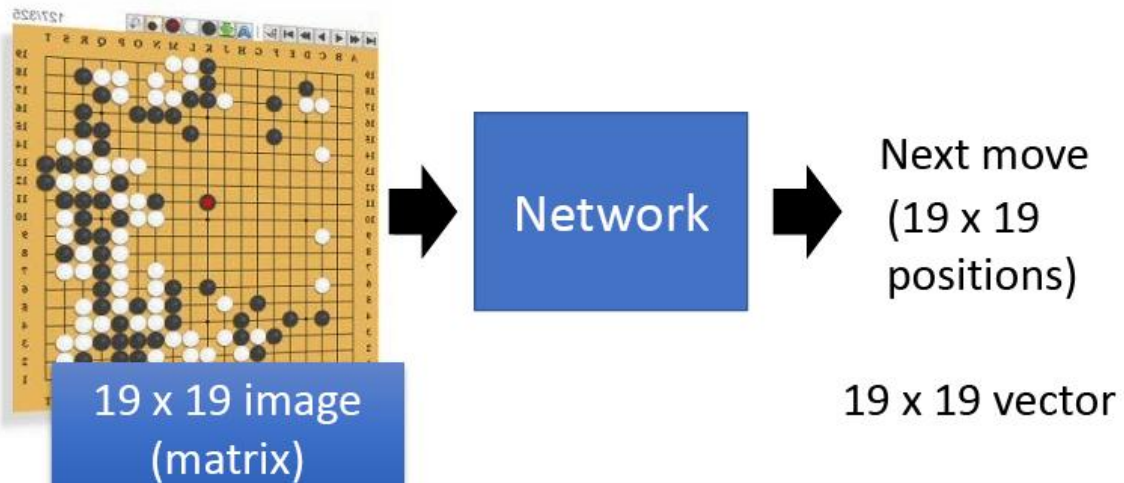
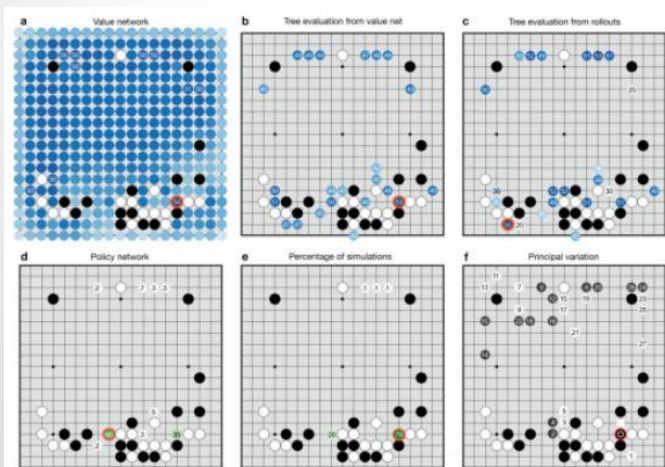
如何实现人工智能(AI)?

◆ 如何让机器像人一样“思考”？

目前，深度神经网络是较为热的研究方向，其能够实现高逼真的人类行为，甚至表现出超过人类的行为，也被誉为**最类似人脑的人工智能技术**，在自然语言处理、计算机视觉和围棋上的效果最为突出。

第一章：绪论

游戏领域（DeepMind）： AlphaGo惊奇问世（Nature 2016）



如何实现人工智能(AI)?

◆ 如何让机器像人一样“思考”？

类脑智能的研究逐渐展开，脑科学的研究人员开始和人工智能领域的计算机和数学研究相结合。以构造符合人脑思维的人工智能新理论和新方法。

第一章：绪论

结构生物学领域：AlphaFold大放异彩

DeepMind蛋白质结构预测：AlphaFold vs. AlphaFold2 （Nature 2021）

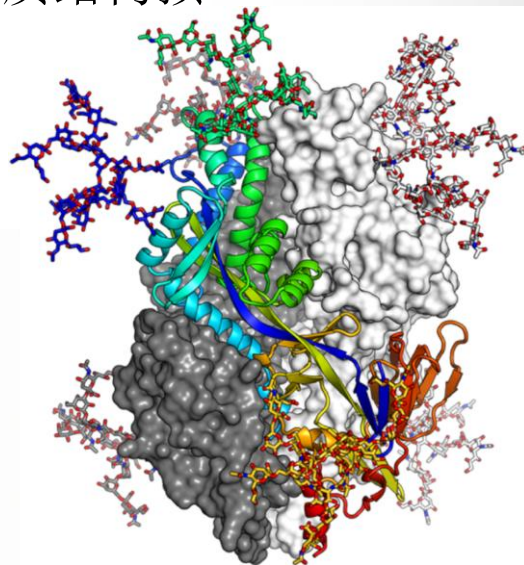
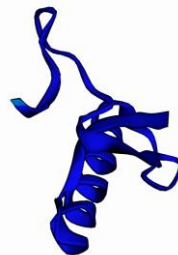
利用蛋白质氨基酸序列预测蛋白质三维结构。在国际蛋白质结构预测大赛（CASP）中成为接近实验方法的冠军。

传统蛋白质结构解析：X射线晶体学和冷冻电镜法。

PIAQIHILEGRSDEQKETLIREVSEAISRSLDAPLTSVRVITTEMAKGHFGIGGELASK

氨基酸序列

AI算法



蛋白质 3D 结构

第一章：绪论

求解数学猜想、奥数题：崭露头角（DeepMind, OpenAI定理证明器, 2021）

计算机编程领域：AlphaCode小试牛刀（2022）

可以编写与人类相媲美的计算机程序（在Codeforces挑战赛中击败46%的参赛者）

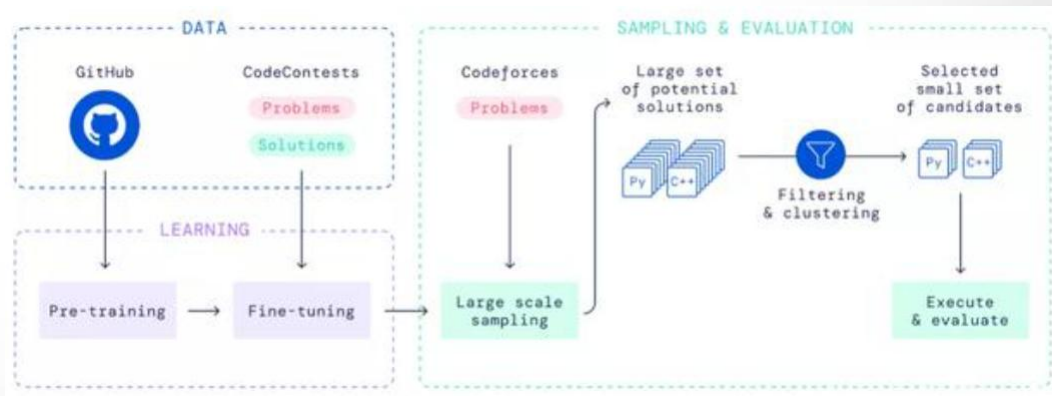
DeepMind

2022-2-2

Competition-Level Code Generation with AlphaCode

Yujia Li*, David Choi*, Junyoung Chung*, Nate Kushman*, Julian Schrittwieser*, Rémi Leblond*, Tom Eccles*, James Keeling*, Felix Gimeno*, Agustin Dal Lago*, Thomas Hubert*, Peter Choy*, Cyprien de Masson d'Audume*, Igor Babuschkin, Xinyun Chen, Po-Sen Huang, Johannes Welbl, Sven Gowal, Alexey Cherepanov, James Molloy, Daniel J. Mankowitz, Esme Sutherland Robson, Pushmeet Kohli, Nando de Freitas, Koray Kavukcuoglu and Oriol Vinyals

*Joint first authors



第一章：绪论

ChatGPT: 语言大模型-千亿参数（OpenAI, 2023）

服务所有人：被誉为互联网时代的颠覆性技术，掀起人工智能的新时代

可以扮演生活中各种各样的角色：

程序员、写作/创作、医生、翻译员、办公助手、历史学家、心理咨询、律师等

斯坦福大学学者评估其智力水平相当于9岁儿童

核心技术：RLHF—人类反馈的强化学习

三个步骤：预训练语言模型（GPT）—收集对话数据训练打分模型（RM）—强化学习微调（RL）

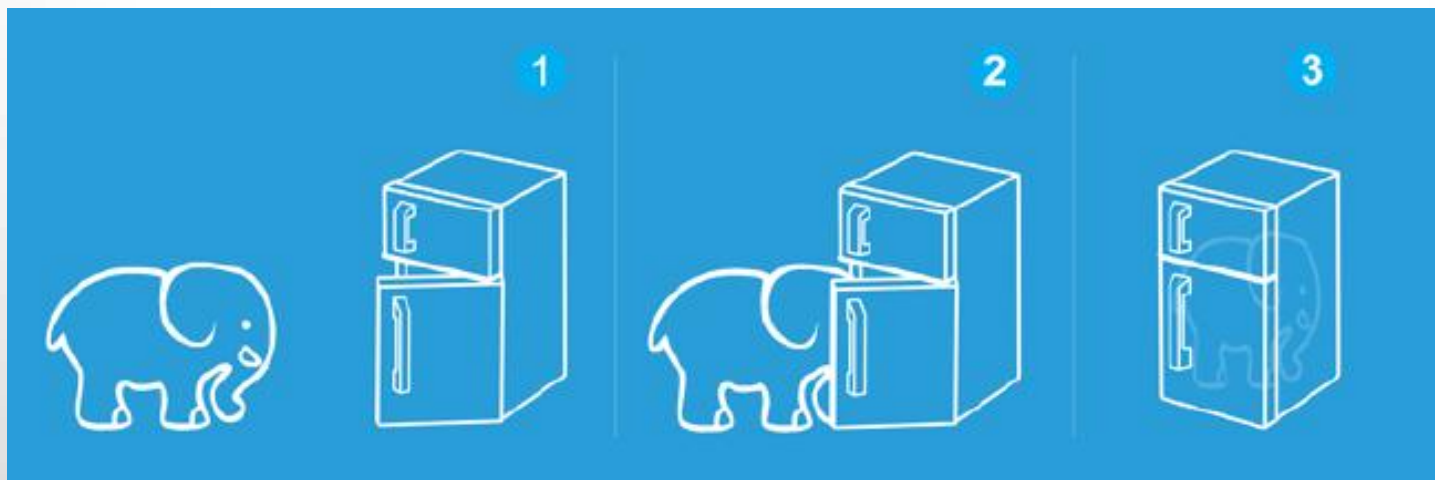
单次训练成本预计：1200万美元（算力：28.5万颗CPU+1万颗GPU A100；数据：45TB）

第一章：绪论

如何实现人工智能(AI)?

◆ 如何让机器像人一样“思考”？

深度学习的简单框架：大象和冰箱的故事。



第一章：绪论

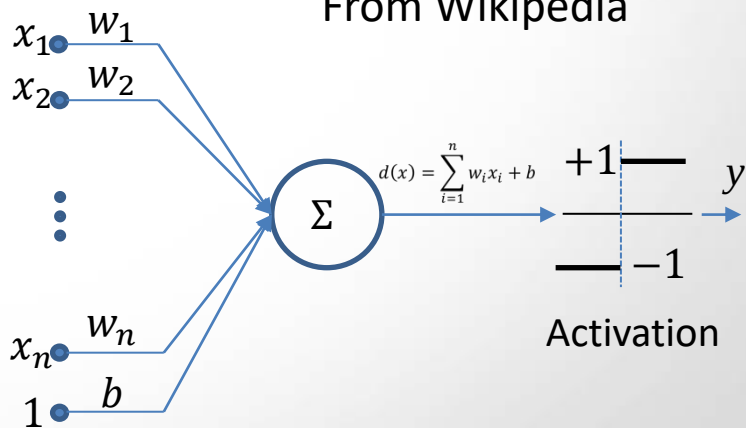
人工智能(AI)起源(60年前, 1950):

Rosenblatt 提出“**感知器**”概念，并在刚刚萌芽的AI界产生了不小的争论。

关于“认知”，由于“感知器”的提出，纽约时报称之为“可使电子计算机能够散步、说话、看、写、自我复制、产生意识的胚胎。”



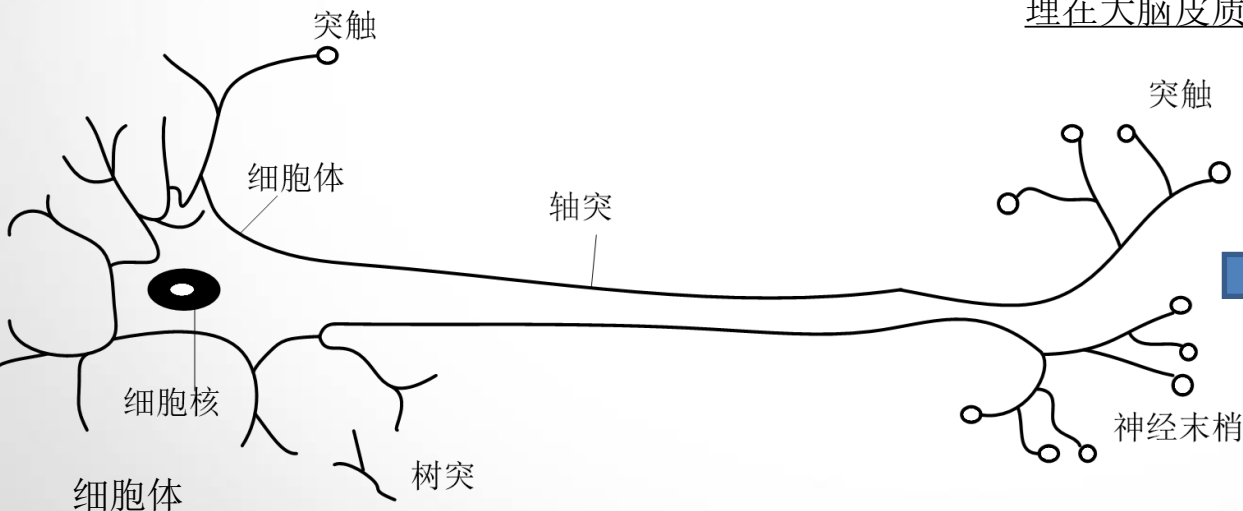
From Wikipedia



第一章：绪论

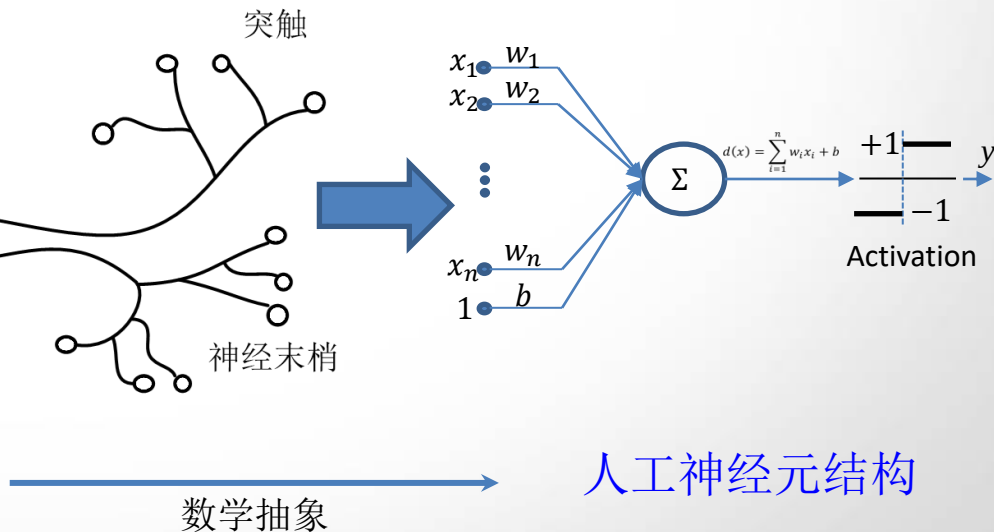
人工智能(AI)起源(60年前, 1950):

生物神经元（神经细胞）结构:



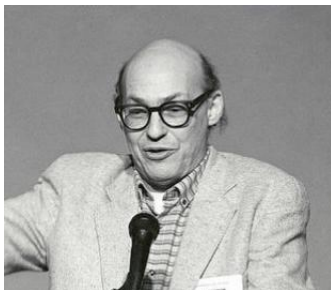
生物神经元结构

每个神经元由一个细胞体组成，其包含一个细胞核。从细胞体分支扩展出许多为树突的神经纤维和一根长的轴突。一个神经元与10到10万个其他神经元相连，连接处称为突触。信号通过复杂的化学反应从神经元传播到神经元。研究发现，大多数的信息处理在大脑皮质，即大脑外层进行。



人工神经元结构

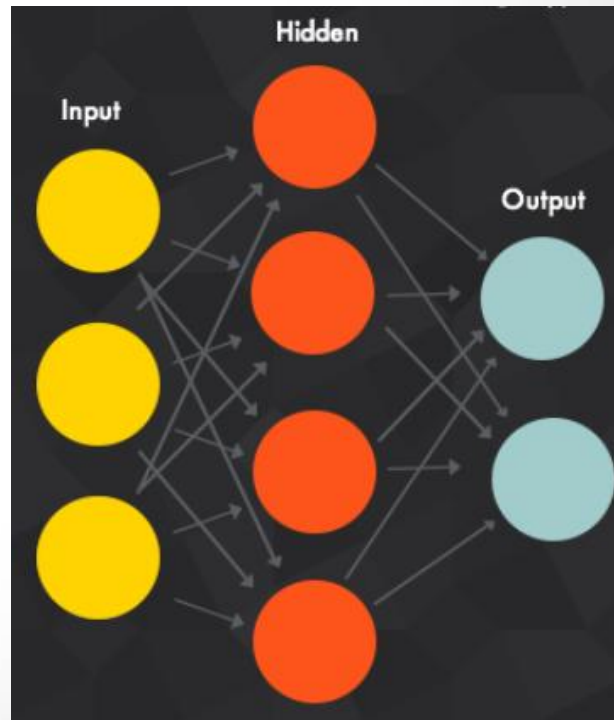
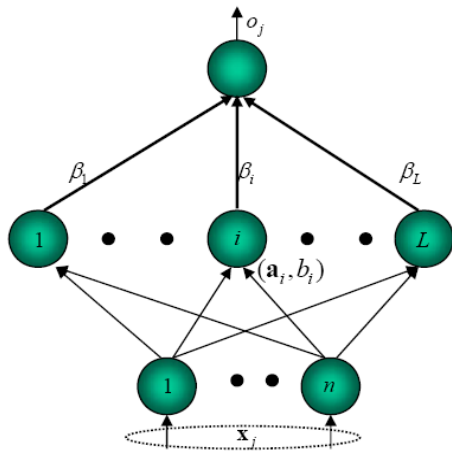
第一章：绪论



马文·明斯基(1927-2016)

人工智能(AI)冬天(1970s):

人工智能冬天也是神经网络的冬天，
Marvin Minsky说“两层的神经网络并不能
解决简单的XOR问题，导致AI winter的来临”



第一章：绪论

人工智能(AI)冬天(1970s):

人工智能冬天也是神经网络的冬天，
Minsky说“两层的神经网络并不能解决简单的XOR问题，导致AI winter的来临”

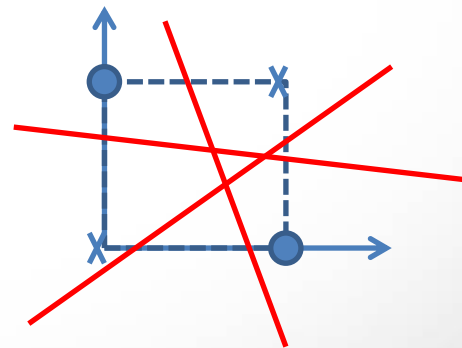
XOR(异或)问题:

0,0: 0

0,1: 1

1,0: 1

1,1: 0



无法解决线性不可分的问题

无法找到一条直线将+1和-1分开

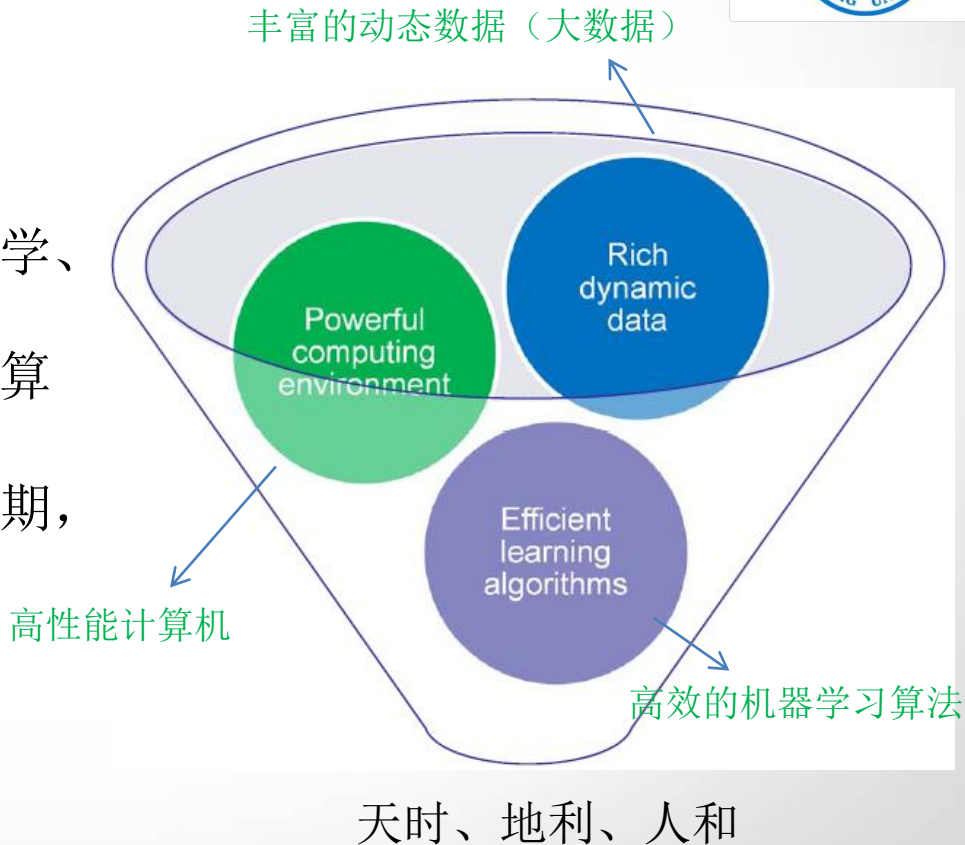
第一章：绪论

人工智能(AI)基础：

数学、计算科学、控制、神经科学、
心理学、语言学、哲学

过去60年，人工智能发展重点在算
法和模型上；

而今天，人工智能发展处于巅峰期，
取决于**三点**：



第一章：绪论

人工智能(AI)最新发展：

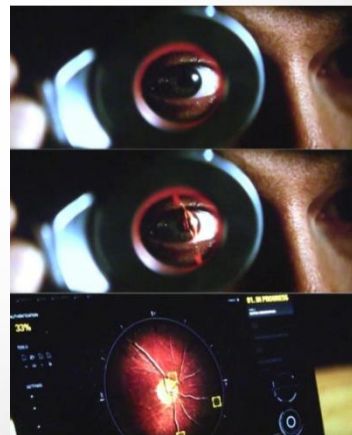
机器视、听、触、嗅、感觉及思维方式的模拟：指纹识别、人脸识别、虹膜识别、掌纹识别、图像/视频识别、语音识别、机器翻译、自然语言处理、搜索/检索、博弈（围棋、象棋）、无人驾驶等



人脸识别（谍影重重5）



步态分析与识别（碟中谍5）



视网膜识别（碟中谍5）

第一章：绪论



利用机器学习技术从大规模人脸图像数据中获取特征、知识表达、识别模型等



第一章：绪论

人工智能(AI)最新发展：

自然语言处理(NLP)：计算机科学和人工智能领域的重要方向之一。其研究人与计算机如何使用自然语言进行通信的理论和方法。主要包括两个方面：自然语言理解、自然语言生成。

难点：自然语言文本和对话存在不同的歧义性或多义性。

存在的技术问题：1. 局限于分析一个孤立的句子，上下文关系和谈话场景对该句子的影响缺乏系统研究。2. 人类理解一个句子不仅仅是凭语法，还运用大量有关知识，比如生活常识和专门技能，而这些知识无法存储在计算机中。



第一章：绪论

人工智能的局限性：语义理解（人机混合智能）



你在说什么
我好像没听懂

叠字问题：

- ❑ 人要是行，干一行行一行，一行行行行行；
- ❑ 今天下雨，我骑车差点摔倒，还好我一把把把把住了；
- ❑ 来到杨过曾经生活地方，小龙女动情地说：我也想过过过儿过过的生活；
- ❑ 多亏跑了两步，差点没上上上上海的车；
- ❑ 校长说：校服上除了校徽别别别的，让你们别别别的别别别的你非别别别的；

第一章：绪论

人工智能的局限性：语义理解（人机混合智能）

语言文化问题：

□ 那辆白车是黑车；

请问到底是白车还是黑车？

□ 冬天能穿多少穿多少；夏天能穿多少穿多少；

请问到底穿多还是穿少？

□ 剩女产生的原因：一是谁都看不上；二是谁都看不上；

请问到底谁看不上谁？

□ 女孩给男朋友打电话：如果你到了，我还没到，你就等着吧；如果我到了，你还没到，你就等着吧！！

请问男孩应该是等呢？还是等呢？



你在说什么
我好像没听懂

第一章：绪论

人工智能(AI)最新发展：

图像视频理解：人工智能和计算机视觉领域的重要方向。其研究如何利用计算机对图像和视频的内容、场景、语义的理解、标注、分类和识别。目前在视频监控、图像检索、图-文转换等领域应用较广。其实现过程分成4个层：

数据层：图像数据的获取（传感器）、压缩和传输（通信）；

描述层：特征提取，图像信号(像素)的形式化；

认知层：图像理解，包括机器学习和推理；

应用层：对特定任务（分类、识别、检测），设计模式识别和机器学习算法。



图像和文本之间的转换
是一项具有趣味性和挑战性的研究

第一章：绪论

人工智能(AI)最新发展：

图像视频理解：人工智能和计算机视觉领域的重要方向。其研究如何利用计算机对图像和视频的内容、场景、语义的理解、标注、分类和识别。目前在视频监控、图像检索、图-文转换等领域应用较广。其实现过程分成4个层：

数据层：图像数据的获取（传感器）、压缩和传输（通信）；

描述层：特征提取，图像信号(像素)的形式化；

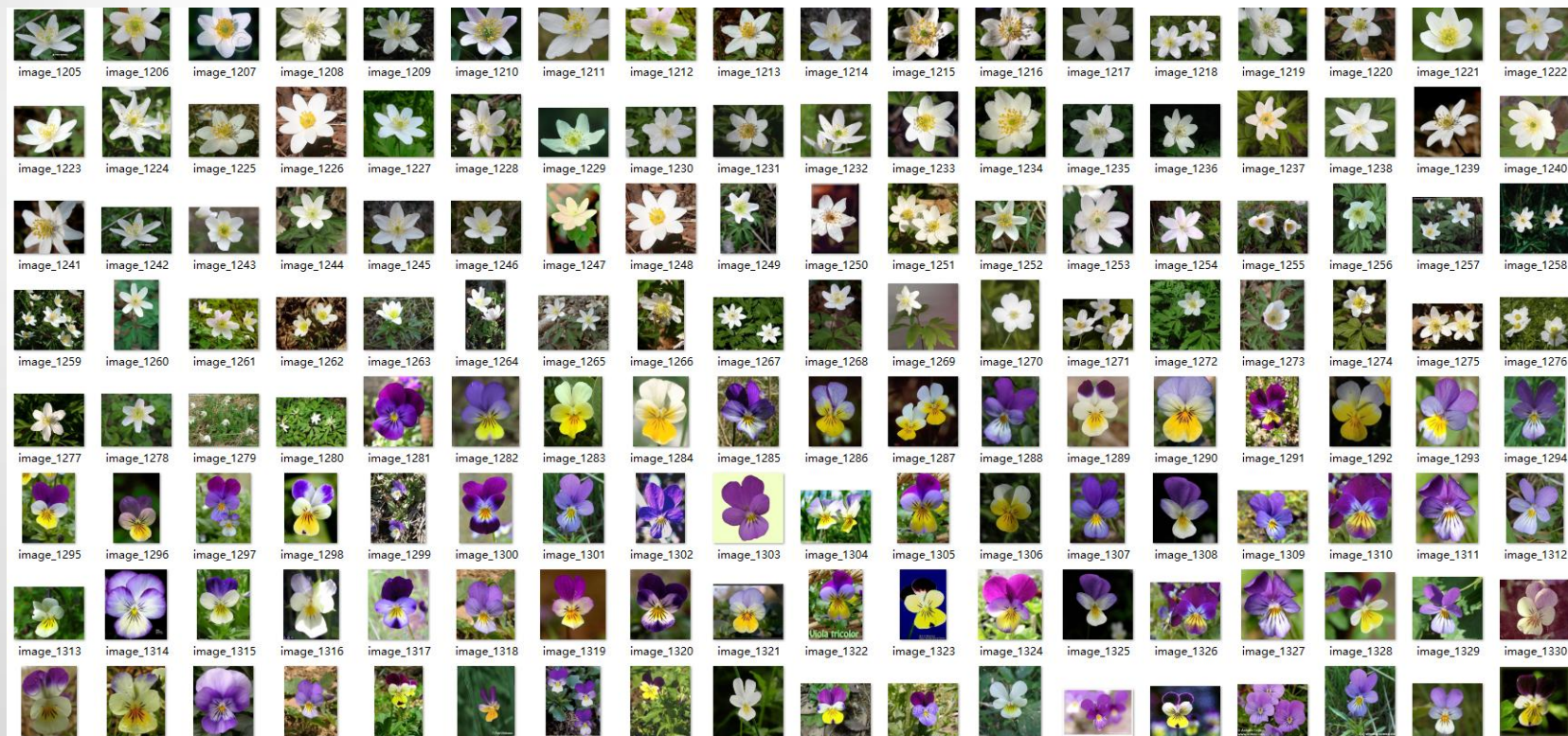
认知层：图像理解，包括机器学习和推理；

应用层：对特定任务（分类、识别、检测），设计模式识别和机器学习算法。



?

第一章：绪论



?

第一章：绪论



?



第一章：绪论

人工智能(AI)最新发展：

博弈：

IBM公司的深蓝(deep blue)第一个在象棋比赛中击败世界冠军(加里. 卡斯帕罗夫, 1997)。

深蓝是一台超级计算机，而非智能体（Agent）；

Google公司DeepMind团队开发的AlphaGo在围棋比赛中采用最新的深度学习技术战胜世界冠军(李世石, 2016)。

AlphaGo是一个人工智能程序，是当前人工智能的标志性事件。



第一章：绪论

人工智能(AI)争议：

Von Neumann(冯诺依曼)：计算机不会有智能；

Alan Turing(阿兰图灵)：计算机是能达到人的智力水平的；

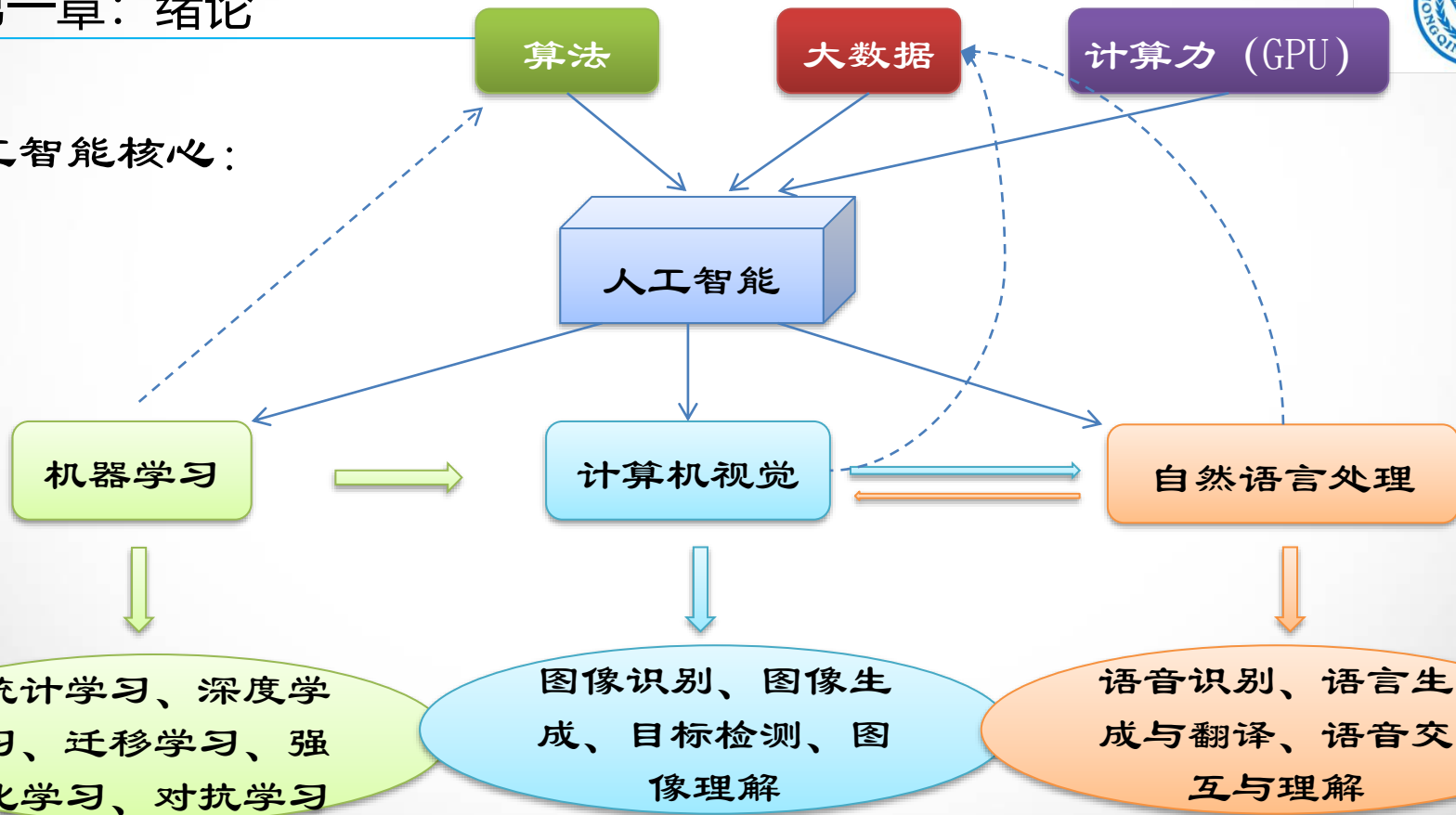
McCarthy(麦卡锡)：人工智能的主要问题是难解的；

Minsky(明斯基)：人工智能是最难的科学之一，是思维的社会无统一的知识表示和理论基础

反对派核心观点：计算机只能解决**形式化**的问题，而客观世界是非形式化的，变化无穷的。（国际象棋完全可以由一个非常简短的、完全形式化的规则列表来描述；大量的日常知识是主观的、直观的，因此很难通过形式化的方式表达清楚）

第一章：绪论

人工智能核心：





第一章：绪论

机器学习 课程：

人工智能涉及多个领域，本课程主要介绍机器学习的基础和方法，主要包括智能体Agent、线性建模、概率学习、演化进化算法、神经网络、深度学习、人脸识别、计算机视觉应用。

AI 到底能干什么？？！！

第一章：绪论

人工智能的常见应用



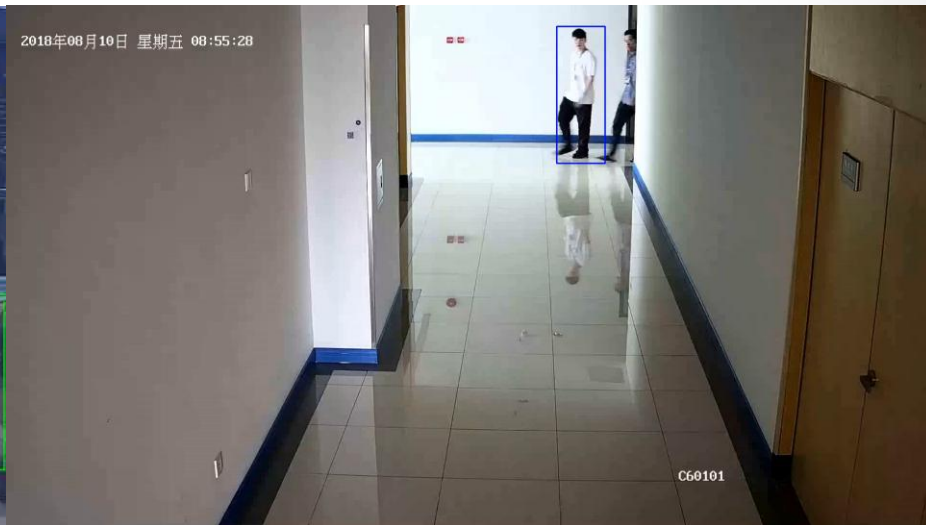
目标检测



道路环境感知
(目标语义分割)

第一章：绪论

人工智能的常见应用

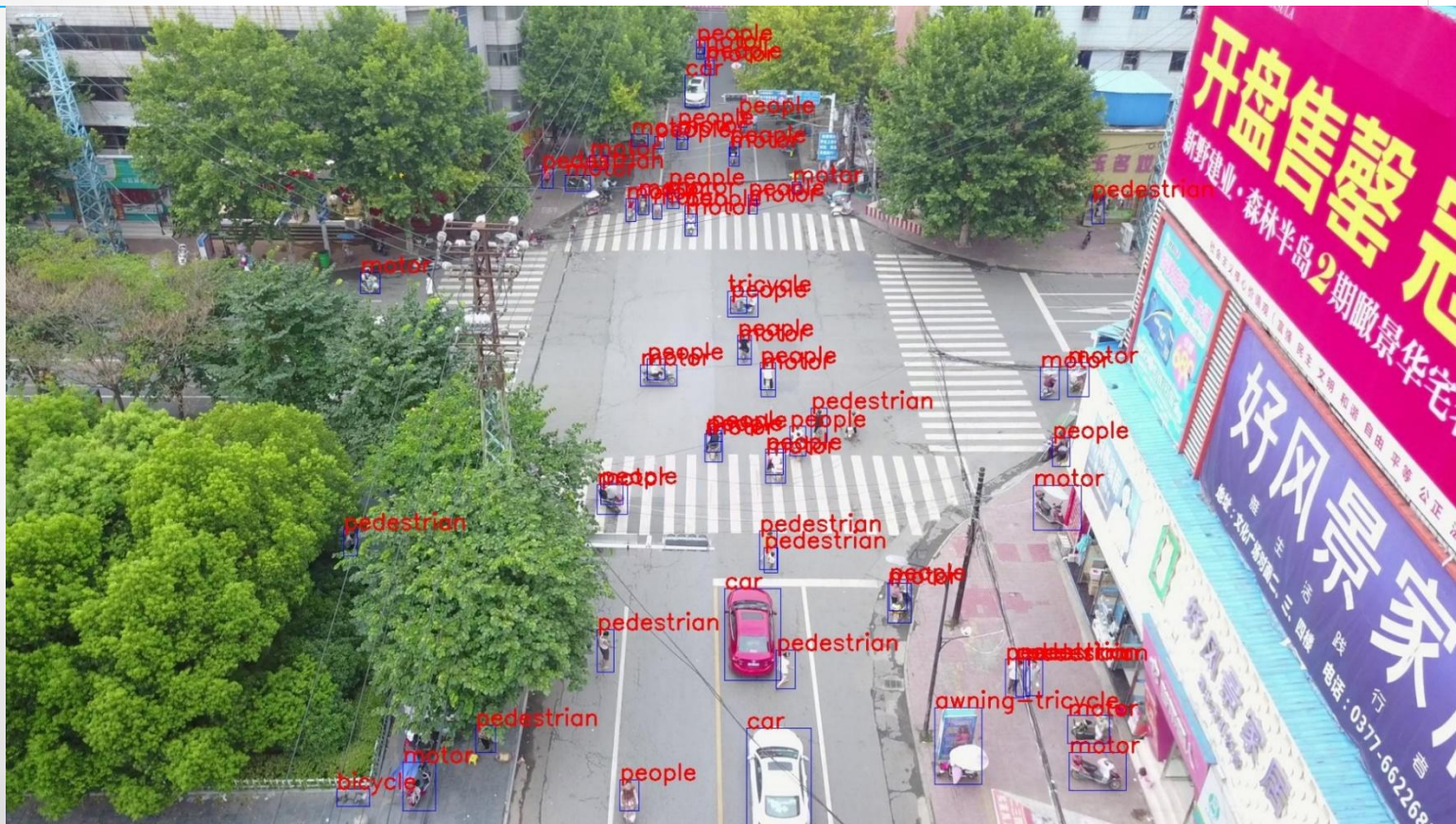


行人检测、跟踪与识别

第一章：绪论



第一章：绪论



第一章：绪论

基于Wi-Fi无线信号的AI应用（穿墙识别）



第一章：绪论

人工智能系统真的安全吗？

攻击行人检测算法（目标检测）



彩色图像块导致算法无法找到右边的人

第一章：绪论

人工智能系统真的安全吗？

攻击人脸识别算法



准确识别（相似度0.6）



贴上补丁

第一章：绪论

人工智能系统真的安全吗？

攻击人脸识别算法



错误识别（相似度0.1）



第一章：绪论

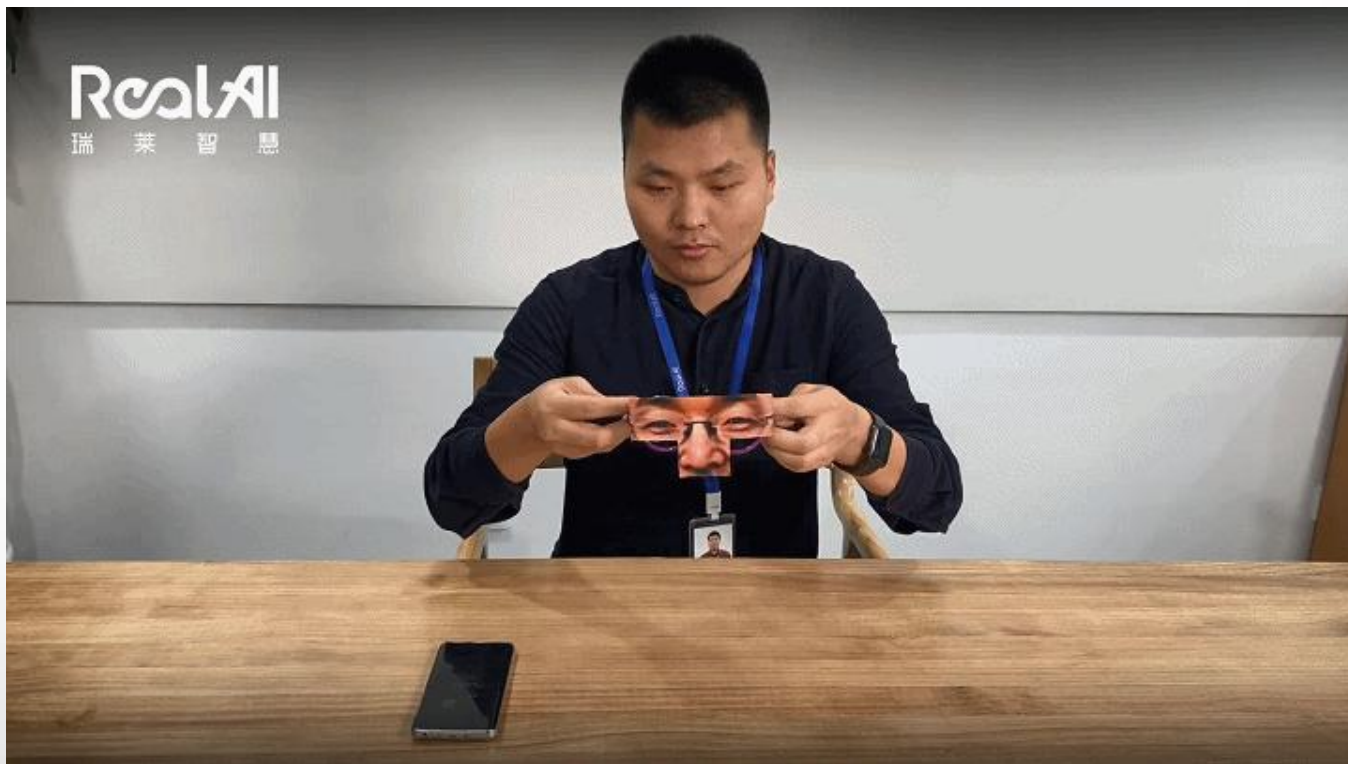
人工智能系统真的安全吗？

清华大学研究人员利用人脸识别技术的漏洞，在**15分钟**内解锁**19部**国产手机！

第一章：绪论

人工智能系统真的安全吗？

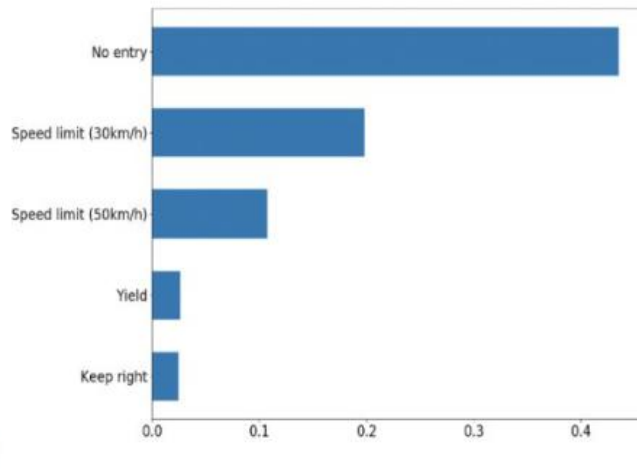
攻击基于人脸识别的手机解锁



第一章：绪论

人工智能系统真的安全吗？

攻击自动驾驶系统



禁行

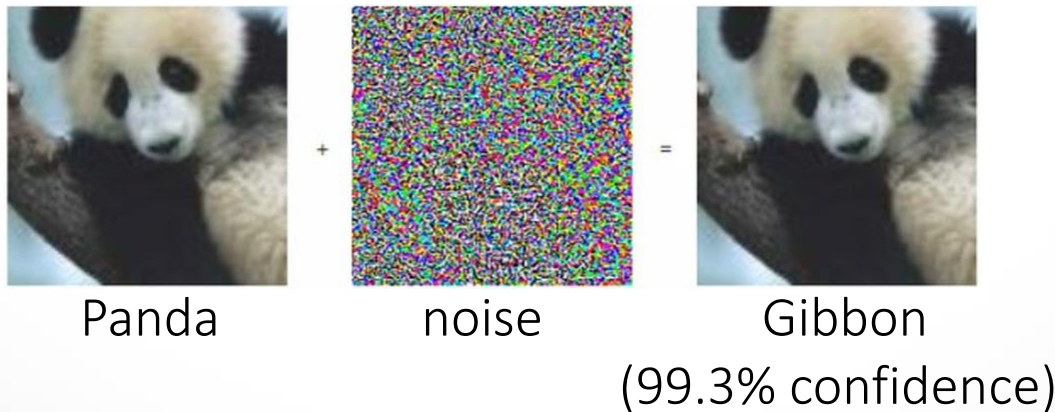
30km/h限速

50km/h限速

第一章：绪论

人工智能系统真的安全吗？

攻击背后的技术原理：对抗样本（对抗机器学习）





强人工智能可怕吗？

LSTM之父：Jürgen Schmidhuber

- ❑ 我不是很担心AI带来的变化。因为人类已经达到了自我毁灭的最大可能性；
- ❑ 从生物学角度，我们担心的应该是和你相近的物种，和你有共同目标的种群。当超人工出现的时候，它关心的不是我们，而是其他超人工智能；
- ❑ 科幻电影里，我们看到AI奴役人类的情景，这是非常愚蠢的，因为人类对于AI来说非常不好用，不如短时间内制造一大批机器人。



第一章：绪论

人工智能的几大瓶颈：（均与机器学习密切相关）

- ❑ 机器学习的鲁棒性差（不泛化）；
- ❑ 机器学习的迁移性差（不适应）；
- ❑ 机器学习的可解释性差（不透明）；
- ❑ 机器学习的对抗性差（不安全）；

导致AI的安全性、可靠性、可信性较脆弱！



第一章：绪论

什么是机器学习？

□ 概念（照本宣科）：

机器学习是一门多领域交叉的新兴技术，涉及概率论、统计学、凸分析、最优化、算法复杂度等，专门用于辅助**计算机**通过**数据**分析来**模拟人类**的学习行为，从数据中发现有用的知识，是人工智能的核心。

□ 机器学习的特点是需要数据，因此是一门数据驱动的技术。

□ 本质上讲，机器学习就是某种线性（非线性）函数 $f(\cdot)$ 逼近（近似）的技术，以实现给定输入 x 计算（预测）其输出 y ，如下式所示：

$$y = f(x)$$

□ 函数 $f(\cdot)$ 的获取过程，就是机器学习，需要利用统计建模、优化等，即**算法**。

算法

大数据

计算力 (GPU)

第一章：绪论

什么是机器学习？

□ 模拟人类：

人的大部分智能是通过后天的学习和训练获得，包括视觉智能、听觉智能、嗅觉等，通过外界获取/感知信息对大脑产生刺激，从而产生认知能力。

比如，简单的**抽象概念**的学习——“**看图识物**”



Cellular-----Mobile-----Smart



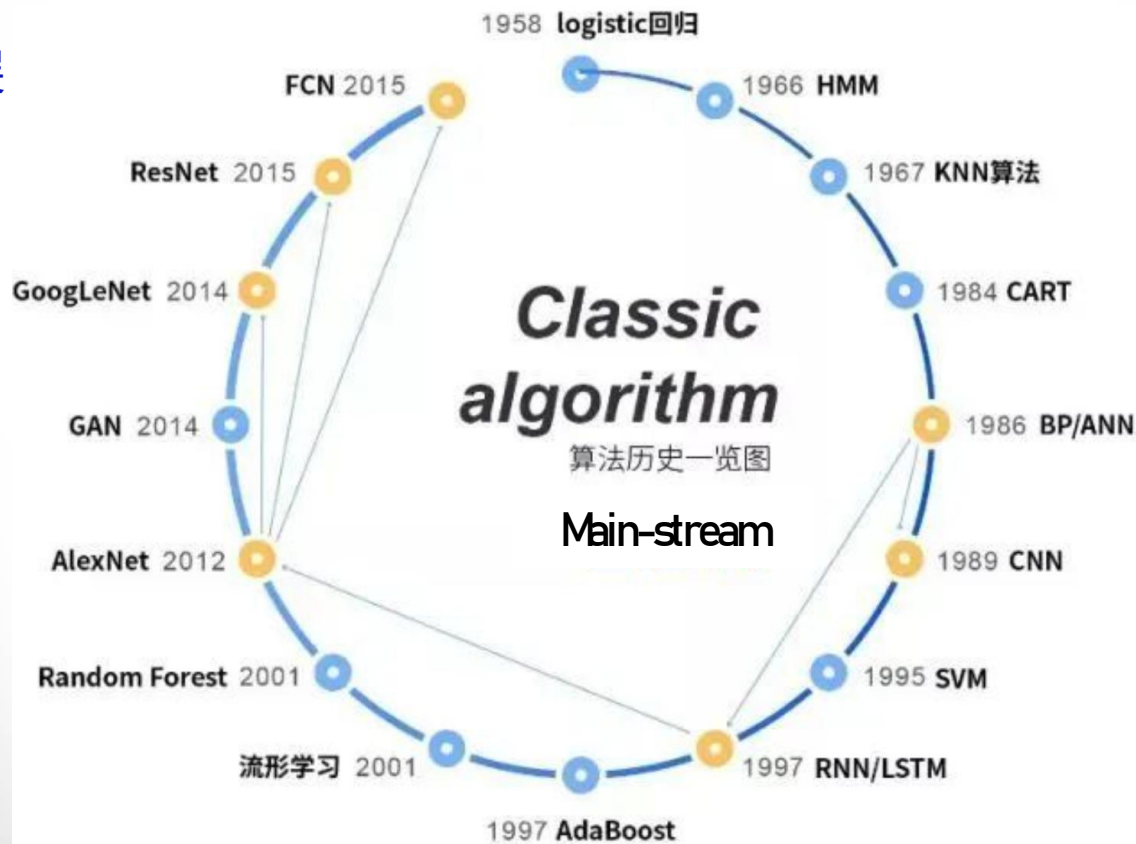
第一章：绪论

机器学习的发展

- 机器学习发展至今已有60余载，时间上主要分为五个阶段：
 - 1960s:** 逻辑回归（线性建模）、近邻搜索、隐马尔可夫模型
 - 1980s:** 分类回归树(CART)、后向传播算法(BP)、卷积神经网络(CNN)
 - 1990s:** 支持向量机、AdaBoost、循环神经网络RNN和LSTM、
 - 2000s:** 流形学习、随机森林、演化学习、稀疏表示
 - 2010s:** 深度学习和强化学习时代（CNN、GAN、RNN、Transformer）

第一章：绪论

机器学习的发展





第一章：绪论

机器学习的发展

□ 按照标注的特性，可分为四大类：

无监督学习：无标注 (主成分分析、流形学习、聚类、自编码器、自监督)

有监督学习：全标注

半监督学习：部分有标签和部分无标签

弱监督学习：标签质量不高、数据质量不高