THUAITR

人工智能之机器学习

Research Report of Machine Learning

2020年第1期

清华大学人工智能研究院
北京智源人工智能研究院
清华-中国工程院知识智能联合研究中心

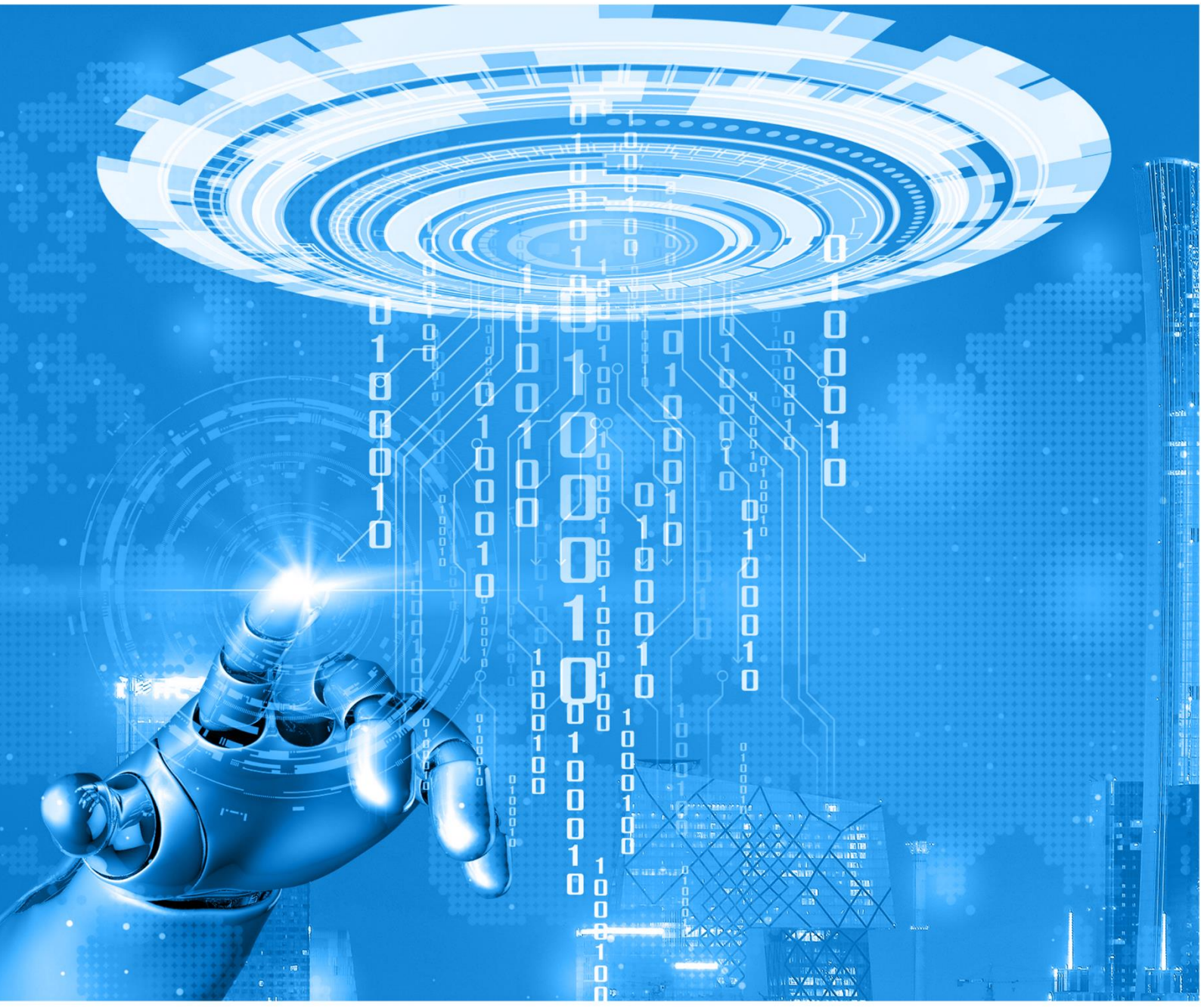
2020年1月

AMiner

人工智能之机器学习

Research Report of Machine Learning

2020年 第1期



清华大学人工智能研究院

清华-中国工程院知识智能联合研究中心

2020年1月

AMiner

CONTENTS

1 概述篇 …… 1

1.1 机器学习的概念 …… 1

1.2 机器学习的发展历史 …… 2

2 技术篇 …… 5

2.1 机器学习算法分类 …… 5

2.2 机器学习的经典代表算法 …… 10

2.3 生成对抗网络及对抗机器学习 …… 19

2.4 自动机器学习 …… 29

2.5 可解释性机器学习 …… 36

2.6 在线学习 …… 41

2.7 BERT …… 45

2.8 卷积与图卷积 …… 56

2.9 隐私保护 …… 61

3 深度学习篇 …… 67

3.1 卷积神经网络 …… 69

3.2 AutoEncoder …… 71

3.3 循环神经网络 RNN …… 73

3.4 网络表示学习与图神经网络 GNN …… 74

3.5 增强学习 …… 76

3.6 生成对抗网络 …… 78

3.7 老虎机 …… 79

3.8 图神经网络 …… 80

3.9 深度学习近期重要进展 …… 82

4 论文解读篇 …… 89

4.1 ICML 历年最佳论文解读 …… 91

4.2 NeurIPS 历年最佳论文解读 …… 99

4.3 专利解读 …… 112

CONTENTS

5 人才篇 …… 119

5.1 学者情况概览 …… 119

5.2 代表性学者简介 …… 121

5.3 NeurIPS 十年高引学者 …… 145

6 应用篇 …… 151

6.1 算法应用场景 …… 151

6.2 行业应用 …… 154

6.3 企业应用 …… 161

6.4 北京智谱华章科技有限公司介绍 …… 174

7 趋势篇 …… 177

8 资源篇 …… 181

8.1 开源代码 …… 181

8.2 预训练 …… 182

8.3 课程 …… 182

8.4 数据集 …… 183

8.5 机器学习知识树 …… 184

参考文献 …… 186

图目录

图 1-1 机器学习相关概念的辨识.....2
图 1-2 机器学习基本过程.....2
图 1-3 机器学习的发展历程（1956-1995）.....3
图 1-4 机器学习的发展历程（2010-2016）.....4
图 2-1 机器学习分类.....5
图 2-2 监督学习的基本流程.....6
图 2-3 非监督学习的基本流程.....7
图 2-4 一个典型的监督学习和非监督学习对比.....8
图 2-5 强化学习的基本框架.....8
图 2-6 强化学习的基本学习流程.....10
图 2-7 数据集的绘制 x 和 y 值.....11
图 2-8 一个简单的随机森林算法示意.....12
图 2-9 逻辑函数曲线图.....13
图 2-10 kNN 算法简单示例.....14
图 2-11 AdaBoost 执行.....15
图 2-12 K-均值算法图示.....16
图 2-13 SVM 的决策平面.....17
图 2-14 SVM 的核函数.....17
图 2-15 感知机.....18
图 2-16 典型的人工神经网络结构.....18
图 2-17 GAN 发展脉络.....19
图 2-18 GAN 网络的架构.....20
图 2-19 BigGAN 生成的图像.....21
图 2-20 StackGAN 生成的图像.....22
图 2-21 CycleGAN 生成的图像.....22
图 2-22 Pix2pix 生成的图像.....23
图 2-23 Age-cGAN 生成的图像.....23
图 2-24 GAN 创作的 Edmond de Belamy.....24
图 2-25 Deep Fakes 换脸.....24
图 2-26 标签操纵的分类准确率.....26
图 2-27 对输入进行操纵导致的结果.....26
图 2-28 建立影子模型.....29

图 2-29 AutoML 基本过程.....30
图 2-30 从 ML 角度看 AutoML.....30
图 2-31 从自动化角度看 AutoML.....30
图 2-32 网格搜索与随机搜索.....31
图 2-33 神经结构搜索方法示意图.....33
图 2-34 ATMSeer 自动机器学习定制化工具的用户友好型交互界面.....34
图 2-35 Online Learning 流程.....43
图 2-36 Transformer 的网络架构.....46
图 2-37 BERT 的模型结构.....46
图 2-38 GPT 与 ELMo 的对比.....47
图 2-39 BERT 模型输入.....47
图 2-40 BERT 在不同任务中的模型.....49
图 2-41 XLNet 模型框架图.....51
图 2-42 Two-Stream Self-Attention 机制.....52
图 2-43 Recurrence Mechanism 机制.....53
图 2-44 XLNet 与 BERT 的区别示例.....53
图 2-45 panBER 模型框架以及在 GLUE 中的实验结果.....54
图 2-46 MT-DNN 模型框架以及训练算法.....55
图 2-47 使用知识蒸馏对 MT-DNN 模型进行优化.....56
图 2-48 骰子点数示意图.....57
图 2-49 点数和为 4 的卷积示意图.....58
图 2-50 点数和为 n 的卷积示意图.....58
图 2-51 图卷积示意图.....59
图 2-52 一个图的度矩阵、邻接矩阵和拉普拉斯矩阵.....60
图 3-1 深度学习模型最近若干年的重要进展.....67
图 3-2 卷积神经网络的重要进展.....70
图 3-3 Auto-Encoder 的重要进展.....72
图 3-4 循环神经网络 RNN 的重要进展.....73
图 3-5 网络表示学习与图神经网络的重要进展.....75
图 3-6 增强学习的重要进展.....77
图 3-7 生成对抗网络的重要进展.....78
图 3-8 老虎机的重要进展.....79
图 3-9 Video to Video Synthesis 生成的城市风景图.....83
图 3-10 图网络模型.....84

图 3-11 MoCo 训练编码器.....85
图 3-12 三种对比损失机制的概念比较.....85
图 3-13 基于双通道处理理论的认知系统框架.....88
图 5-1 机器学习领域全球学者分布.....119
图 5-2 机器学习领域学者 h-index 分布.....120
图 5-3 机器学习领域中国学者分布.....120
图 6-1 自动驾驶目标识别、运动预测.....157
图 7-1 机器学习技术趋势.....178
图 7-2 机器学习国家趋势.....180

表目录

表 4-1 ICML 近 10 年 best paper.....89
表 4-2 NeurIPS 近 10 年 best paper.....90
表 5-1 机器学习领域中国与各国合作论文情况.....121
表 5-2 NeurIPS（2009-2019）高引学者 TOP100.....145
表 8-1 机器学习三级知识树.....**错误!未定义书签。**

AMiner

1 概述篇

1.1 机器学习的概念

机器学习已经成为了当今的热门话题，但是从机器学习这个概念诞生到机器学习技术的普遍应用经过了漫长的过程。在机器学习发展的历史长河中，众多优秀的学者为推动机器学习的发展做出了巨大的贡献。

从 1642 年 Pascal 发明的手摇式计算机，到 1949 年 Donald Hebb 提出的赫布理论——解释学习过程中大脑神经元所发生的变化，都蕴含着机器学习思想的萌芽。

事实上，1950 年图灵在关于图灵测试的文章中就已提及机器学习的概念。到了 1952 年，IBM 的亚瑟·塞缪尔（Arthur Samuel，被誉为“机器学习之父”）设计了一款可以学习的西洋跳棋程序。它能够通过观察棋子的走位来构建新的模型，用来提高自己的下棋技巧。塞缪尔和这个程序进行多场对弈后发现，随着时间的推移，程序的棋艺变得越来越好[1]。塞缪尔用这个程序推翻了以往“机器无法超越人类，不能像人一样写代码和学习”这一传统认识。并在 1956 年正式提出了“机器学习”这一概念。他认为“机器学习是在不直接针对问题进行编程的情况下，赋予计算机学习能力的一个研究领域”。

对机器学习的认识可以从多个方面进行，有着“全球机器学习教父”之称的 Tom Mitchell 则将机器学习定义为：对于某类任务 T 和性能度量 P，如果计算机程序在 T 上以 P 衡量的性能随着经验 E 而自我完善，就称这个计算机程序从经验 E 学习。这些定义都比较简单抽象，但是随着对机器学习了解的深入，我们会发现随着时间的变迁，机器学习的内涵和外延在不断的变化。因为涉及到的领域和应用很广，发展和变化也相当迅速，简单明了地给出“机器学习”这一概念的定义并不是那么容易。

普遍认为，机器学习（Machine Learning，常简称为 ML）的处理系统和算法是主要通过找出数据里隐藏的模式进而做出预测的识别模式，它是人工智能（Artificial Intelligence，常简称为 AI）的一个重要子领域，而人工智能又与更广泛的数据挖掘（Data Mining，常简称为 DM）和知识发现（Knowledge Discovery in Database，常简称为 KDD）领域相交叉。为了更好的理解和区分人工智能（Artificial Intelligence）、机器学习（Machine Leaning）、数据挖掘（Data Mining）、模式识别（Pattern Recognition）、统计（Statistics）、神经计算（Neuro Computing）、数据库（Databases）、知识发现（KDD）等概念，特绘制其交叉关系如下图所示：

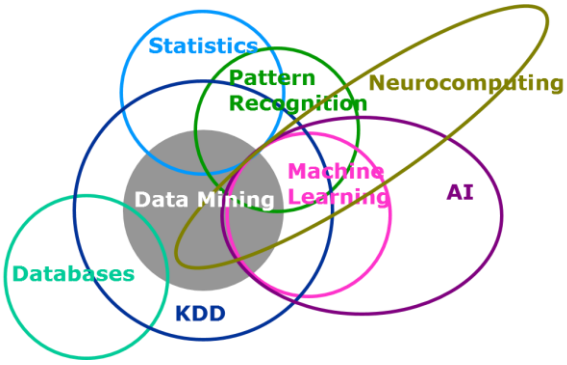


图 1-1 机器学习相关概念的辨识

机器学习是一门多领域交叉学科，涉及概率论、统计学、逼近论、凸分析、算法复杂度理论等多门学科。专门研究计算机怎样模拟或实现人类的学习行为，以获取新的知识或技能，重新组织已有的知识结构使之不断改善自身的性能。其过程可以用下图[2]简单表示：

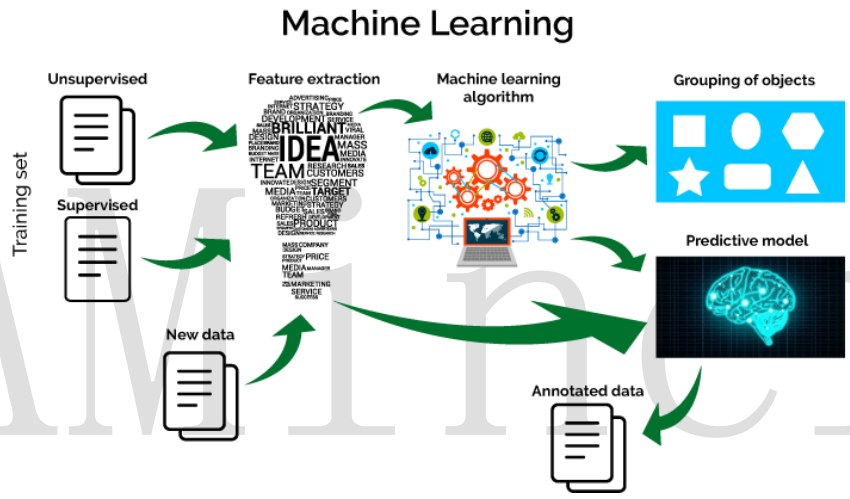
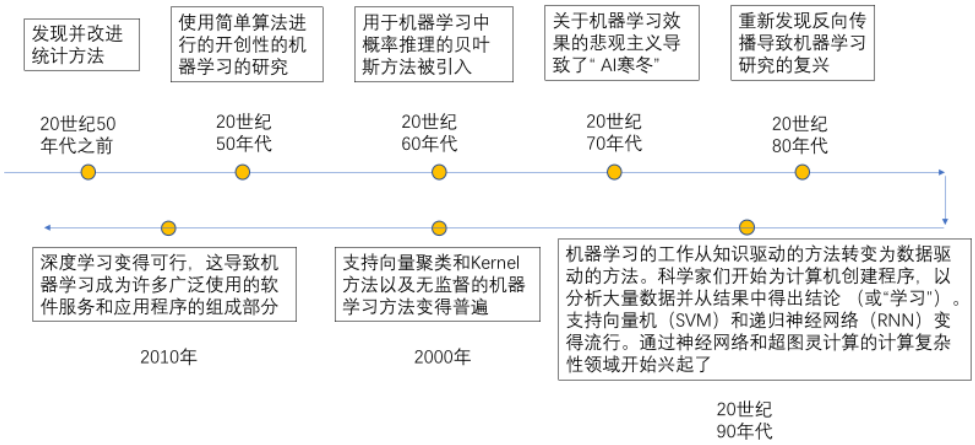


图 1-2 机器学习基本过程

1.2 机器学习的发展历史

从机器学习发展的过程上来说，其发展的时间轴如下所示：



此外，本节参考美国 Aggregated news around AI and co.对机器学习发展的分析[3]，将机器学习发展历程中重要的人物和事件作为机器学习领域发展的重要节点进行分析，将其发展历程展示如下：

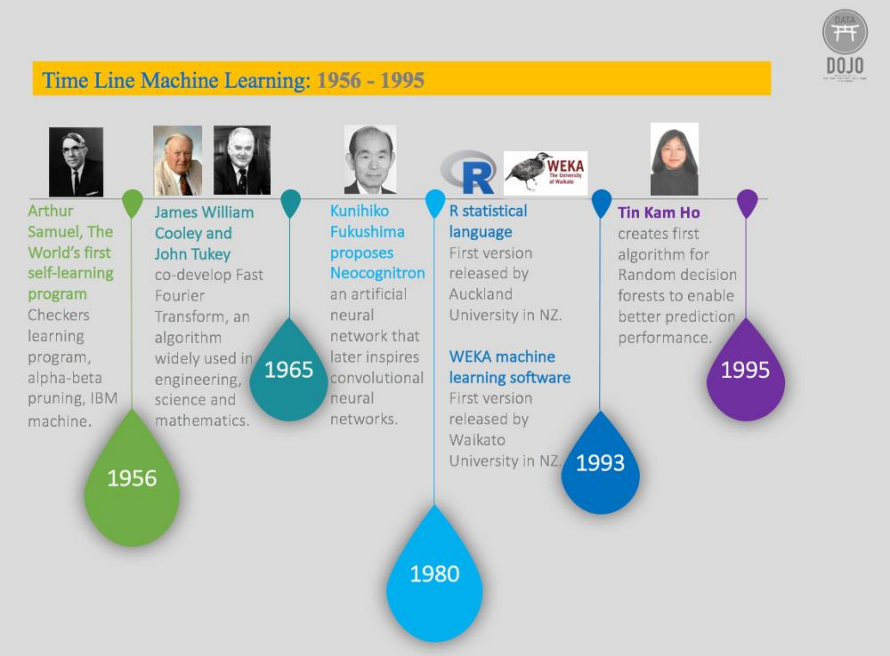


图 1-3 机器学习的发展历程（1956-1995）

1956 年机器学习的概念由 Arthur Samuel 正式提出。

1965 年，James William Cooley 和 John Tukey 设计了快速傅里叶变换（FFT）算法，用于计算由多个简单函数组合而成的原始信号的正弦曲线的幅度、相位和频率，该算法被广泛应用于各类工程、科学和数学问题中[4]。

1980 年，Kunihiko Fukushima 发明了 neocognitron，它是一个分层的多层人工神经网络，它的出现直接导致了后期卷积神经网络（Convolutional Neural Network，通常简称为 CNN）的发明[5]。

1993 年，免费的、非商业化机器学习以及数据挖掘软件 WEKA 面世，它是由新西兰怀卡托大学研发的[6]。WEKA 作为一个公开的数据挖掘工作平台，集合了大量能承担数据挖掘任务的机器学习算法，包括对数据进行预处理、分类、回归、聚类、关联规则以及在新的交互式界面上的可视化，它的出现极大地降低了学习机器学习的门槛。

1995 年，贝尔实验室的 Tin Kam Ho 利用随机子空间方法创建随机决策森林（Random Decision Forests）算法，该算法既可以用于回归也可以用于分类任务，并且很容易查看模型输入特征的相对重要性，是一个高度灵活并且应用广泛的算法[7]。

图 1-4 机器学习的发展历程（2010-2016）

2010 年，Kaggle 由其联合创始人、首席执行官 Anthony Goldbloom 在墨尔本创立，主要为开发商和数据科学家提供举办机器学习竞赛、托管数据库、编写和分享代码的平台。该平台已经吸引了 80 万名数据科学家的关注，极大地推动了机器学习在全球的推广。

2011 年，IBM 的认知计算系统 Watson 横空出世,在问答节目中首次击败了人类[8]。当年，Watson 身价大涨逐渐成为了 IBM，乃至全球 AI 项目的代表。Watson 当年的成功向人们预示着一个新时代似乎就要开始了。

2012 年，Andrew Ng 团队和 Jeff Dean 团队通过深度学习技术，让 16000 个中央处理器核心在学习了 1000 万张图片后，成功在 YouTube 视频中认出了猫的图像[9]，这在当时业界引起了极大的轰动。

2015 年，由 Google 旗下 DeepMind 公司戴密斯·哈萨比斯领衔的团队开发的阿尔法围棋 AlphaGo[10]，成为了第一个击败人类职业围棋选手、第一个战胜围棋世界冠军的人工智能机器人。其主要工作原理是“深度学习”，其成功使得“深度学习”概念深入人心，并在机器学习的更多广泛领域得到了应用。

2016 年，Evans data 的大数据和高级分析调查发现，超过三分之一的开发者表示他们在大数据和高级分析项目中使用了机器学习技术。微软团队开发了一套能像人类一样识别谈话内容的系统。该团队曾使用卷积（Convolutional）和长短期记忆（LSTM）神经网络开发出 Microsoft Cognitive Toolkit（CNTK）。Google Brain 团队公布了 Google Neural Machine Translation System，这个基于深度学习的系统目前每天被用于处理 1800 万次翻译请求。

2 技术篇

2.1 机器学习算法分类

机器学习算法可以按照不同的标准来进行分类。比如按函数 $f(x, \theta)$的不同，机器学习算法可以分为线性模型和非线性模型；按照学习准则的不同，机器学习算法也可以分为统计方法和非统计方法。但一般来说，我们会按照训练样本提供的信息以及反馈方式的不同，将机器学习算法分为监督学习、无监督学习和强化学习[11]。

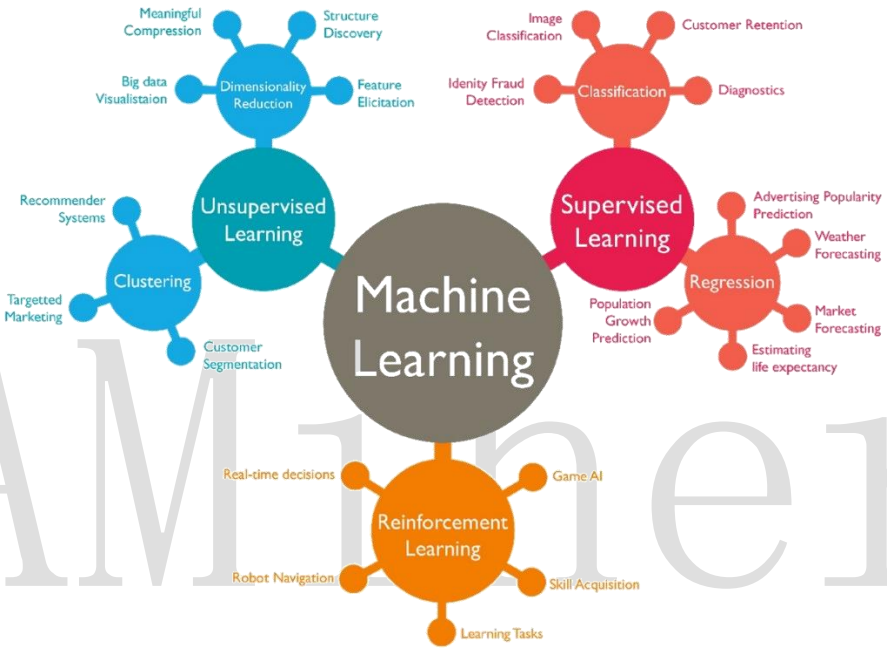


图 2-1 机器学习分类

2.1.1 监督学习

监督式学习（Supervised Learning），是机器学习的一种方法，可以由训练资料中学到或建立一个模式（函数/learning model），并依此模式推测新的实例[12]。训练资料是由输入物件（通常是向量）和预期输出所组成。函数的输出可以是一个连续的值，或是预测一个分类标签。一个监督式学习者的任务在观察完一些事先标记过的训练范例（输入和预期输出）后，去预测这个函数对任何可能出现的输入的输出。要达到此目的，学习者必须以“合理”（见归纳偏向）的方式从现有的资料中一般化到非观察到的情况[13]。

根据标签类型的不同，又可以将其分为分类问题和回归问题两类。分类问题的目标是通过输入变量预测出这一样本所属的类别，例如对于植物品种、客户年龄和偏好的预测问题都可以被归结为分类问题。这一领域中使用最多的模型便是支持向量机，用于生成线性分类的

决策边界。随着深度学习的发展，很多基于图像信号的分类问题越来越多的使用卷积神经网络来完成。回归主要用于预测某一变量的实数取值，其输出的不是分类结果而是一个实际的值。常见的例子是包括市场价格预测、降水量预测等。人们主要通过线性回归、多项式回归以及核方法等来构建回归模型[14]。

监督式学习有两种形态的模型一种是全域模型，会将输入物件对应到预期输出。另一种是将这种对应实作在一个区域模型（如案例推论及最近邻居法）。为了解决一个给定的监督式学习的问题（手写辨识），必须考虑以下步骤：

1) 决定训练资料的范例的形态。在做其它事前，工程师应决定要使用哪种资料为范例。譬如，可能是一个手写字符，或一整个手写的辞汇，或一行手写文字。

2) 搜集训练资料。这资料须要具有真实世界的特征。所以，可以由人类专家或（机器或感测器的）测量中得到输入物件和其相对应输出。

3) 决定学习函数的输入特征的表示法。学习函数的准确度与输入的物件如何表示是有很大的关联度。传统上，输入的物件会被转成一个特征向量，包含了许多关于描述物件的特征。因为维数灾难的关系，特征的个数不宜太多，但也要足够大，才能准确的预测输出。

4) 决定要学习的函数和其对应的学习算法所使用的数据结构。譬如，工程师可能选择人工神经网络和决策树。

5) 完成设计。工程师接着在搜集到的资料上跑学习算法。可以借由将资料跑在资料的子集（称为验证集）或交叉验证（cross-validation）上来调整学习算法的参数。参数调整后，算法可以运行在不同于训练集的测试集。

常见的监督学习算法有：k-近邻算法（k-Nearest Neighbors，kNN）、决策树（Decision Trees）、朴素贝叶斯（Naive Bayesian）等。监督学习的基本流程如下图所示：

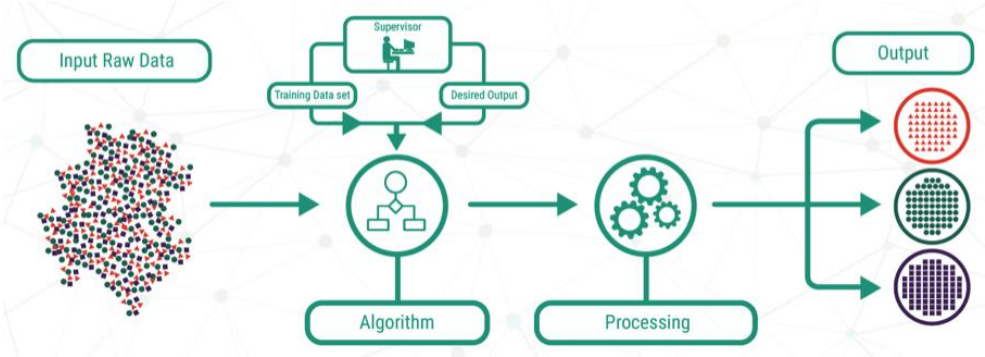


图 2-2 监督学习的基本流程

2.1.2 无监督学习

无监督学习（Unsupervised Learning）是机器学习的一种方法，没有给定事先标记过的训练示例，自动对输入的数据进行分类或分群[15]。与监督学习不同，非监督学习并不需要完整的输入输出数据集，并且系统的输出经常是不确定的。它主要被用于探索数据中隐含的模式和分布。非监督学习具有解读数据并从中寻求解决方案的能力，通过将数据和算法输入到机器中将能发现一些用其他方法无法见到的模式和信息。

常见的无监督学习算法包括：稀疏自编码（sparse auto-encoder）、主成分分析（Principal Component Analysis, PCA）、K-Means 算法（K 均值算法）、DBSCAN 算法（Density-Based Spatial Clustering of Applications with Noise）、最大期望算法（Expectation-Maximization algorithm, EM）等。利用无监督学习可以解决的问题可以分为关联分析、聚类问题和维度约减。

- 关联分析是指发现不同事物之间同时出现的概率。在购物篮分析中被广泛地应用。如果发现买面包的客户有百分之八十的概率买鸡蛋，那么商家就会把鸡蛋和面包放在相邻的货架上。
- 聚类问题是指将相似的样本划分为一个簇（cluster）。与分类问题不同，聚类问题预先并不知道类别，自然训练数据也没有类别的标签。
- 维度约减是指减少数据维度的同时保证不丢失有意义的信息。利用特征提取方法和特征选择方法，可以达到维度约减的效果。特征选择是指选择原始变量的子集。特征提取是将数据从高维度转换到低维度。广为熟知的主成分分析算法就是特征提取的方法。

非监督学习的基本处理流程如下图所示：

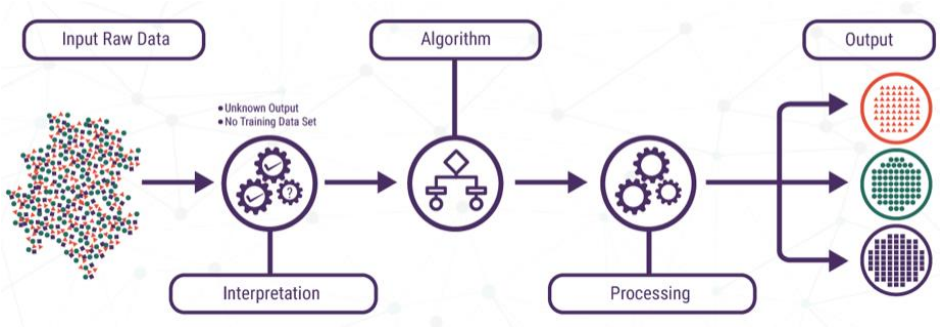


图 2-3 非监督学习的基本流程

可以很清楚的看到相对于监督学习，非监督学习的过程中没有监督者（Supervisor）的干预。下图是一个典型的监督学习和非监督学习的对比，左图是对一群有标签数据的分类，而右图是对一群无标签数据的聚类[16]。

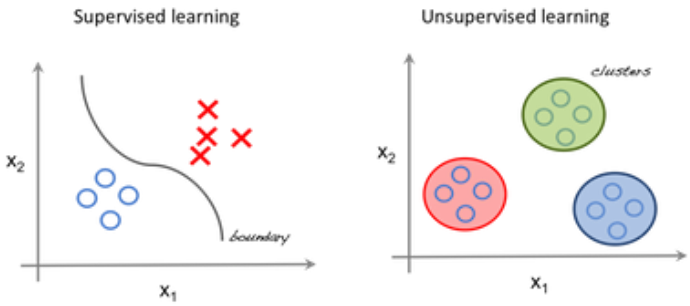


图 2-4 一个典型的监督学习和非监督学习对比

2.1.3 强化学习

强化学习（Reinforcement learning, RL）是机器学习中的一个领域，强调如何基于环境而行动，以取得最大化的预期利益。其灵感来源于心理学中的行为主义理论，即有机体如何在环境给予的奖励或惩罚的刺激下，逐步形成对刺激的预期，产生能获得最大利益的习惯性行为。这个方法具有普适性，因此在其他许多领域都有研究，例如博弈论、控制论、运筹学、信息论、仿真优化、多主体系统学习、群体智能、统计学以及遗传算法。在运筹学和控制理论研究的语境下，强化学习被称作“近似动态规划”。在最优控制理论中也有研究这个问题，虽然大部分的研究是关于最优解的存在和特性，并非是学习或者近似方面。在经济学和博弈论中，强化学习被用来解释在有限理性的条件下如何出现平衡[17]。

强化学习一般由 5 个构成要素，包括：系统环境（System Environment）、参与者（Agent）、观察（Observation）、行动（Action）、奖励（Reward）。强化学习是参与者为了最大化长期回报的期望，通过观察系统环境不断试错进行学习的过程[18]。从强化学习的定义可以看出，强化学习具有两个最主要的特征：通过不断试错来学习、追求长期回报的最大化。在监督学习或非监督学习中，数据是静态的，不需要与环境进行交互，比如图像识别，只要给出足够的差异样本，将数据输入深度网络中进行训练即可。然而，强化学习的学习过程是动态的，不断交互的，所以需要的数据也是通过与环境不断交互所产生的。

图 2-5 强化学习的基本框架

强化学习的基本框架如上图所示，参与者对系统环境进行观察后产生行动，从系统环境中获得相应的奖励，参与者观察系统对自己上一次行动的奖励信号后，重新调整自己的下一次的行动策略。由此可见，强化学习是参与者为了最大化长期回报的期望，通过观察系统环境不断试错进行学习的过程。如果参与者在学习的过程中，某个行为策略得到系统环境的奖励越大，那么参与者以后产生采用这个行动为策略的概率越大。

在强化学习的实际应用中，参与者才是学习的实际使用者，参与者一般具有 3 个构成要素，包括：

1）策略（Policy），是参与者在观察环境后产生的行动方案。具体地，策略 π 定义为状态 S 到行动 A 的映射函数，即 $\pi \doteq f(S \to A)$，这里的≒表示定义相等，例如 $x \doteq y$ 表示定义 x 等于 y。策略可分为确定性策略和随机性策略。给定一个状态 s，根据确定性策略 π，参与者就可以确定需要采取的行动 a，即：

$$a = \pi(\mathrm{s})$$

随机性策略给出参与者采取不同行动的概率，即给定一个状态 s，参与者采取行动 a 的概率为：

$$\pi(a|s) = \mathrm{P}\{A_t = a|S_t = s\}$$

2）值函数（Value Function），是针对状态或行动的评价函数；具体可分为两种：

- 状态值函数（State Value Function），是针对状态的评价指标；
- 行动值函数（Action Value Function），是针对行动的评价指标；

由于行动是在给定状态下产生的，一般也将行动值函数更明确地表达为状态-行动值函数（State-action Value Function）。状态值函数 v_π（s）是给定策略 π，评价状态 s 的指标。具体地，状态值函数 v_π（s）定义为：

$$v_\pi(s) \doteq E_\pi[G_t|S_t = s]$$

状态-行动值函数 $q_\pi(s, a)$ 是给定策略 π，在状态 s 下评价动作 a 的指标。具体地，状态-行动值函数 $q_\pi(s, a)$ 定义为，采用策略 π，在状态 s 下采用动作 a 获得的期望回报，即：

$$q_\pi(s, a) \doteq E_\pi[G_t|S_t = s, A_t = a]$$

3）模型（Model），是参与者对观察到的系统环境建立的模拟模型；马尔科夫决策过程可以利用五元组（S, A, P, R, γ）来描述，根据转移概率 P 是否已知，可以分为基于模型的动态规划法和基于无模型的强化学习法[19]。

强化学习是机器学习的重要部分，在为机器学习开拓新方向上做出了巨大的贡献。强化学习突破了非监督学习，为机器和软件如何获取最优化的结果给出了一种全新的思路。它将如何最优化主体的表现和如何优化这一能力之间建立起了强有力的链接。通过奖励函数的反馈来帮助机器改进自身的行为和算法。但强化学习在实践中并不简单，人们利用很多种算法来实现强化学习。简单来说，强化学习需要指导机器做出在当前状态下能获取最好结果的行为。强化学习中主体通过行为与环境相互作用，而环境通过奖励函数来帮助算法调整做出行为决策的策略函数。从而在不断的循环中得到表现优异的行为策略。它十分适合用于训练控制算法和游戏 AI 等场景[14]。

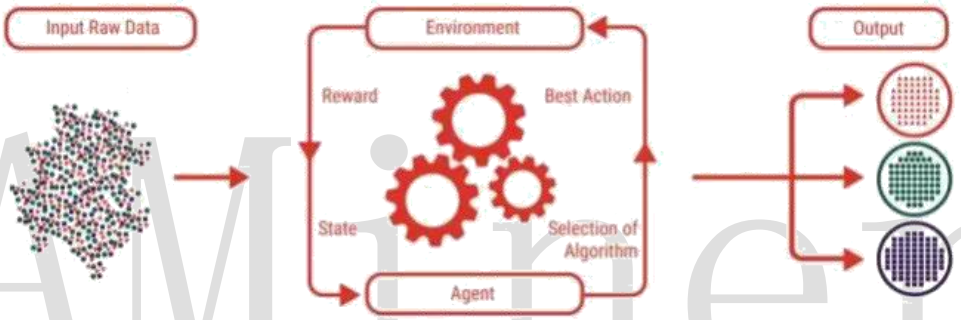


图 2-6 强化学习的基本学习流程

2.2 机器学习的经典代表算法

1980 年机器学习作为一支独立的力量登上了历史舞台。在这之后的 10 年里出现了一些重要的方法和理论，典型的代表是：分类与回归树（CART，1984）、反向传播算法（1986）、卷积神经网络（1989）。

从 1990 到 2012 年，机器学习逐渐走向成熟和应用，在这 20 多年里机器学习的理论和方法得到了完善和充实，可谓是百花齐放的年代。代表性的重要成果有：支持向量机（SVM，1995）、AdaBoost 算法（1997）、循环神经网络和 LSTM（1997）、流形学习（2000）、随机森林（2001）。

下面我们对部分机器学习代表算法进行介绍。

- 线性回归

在机器学习中，我们有一组输入变量（x）用于确定输出变量（y）。输入变量和输出变量之间存在某种关系，机器学习的目标是量化这种关系。

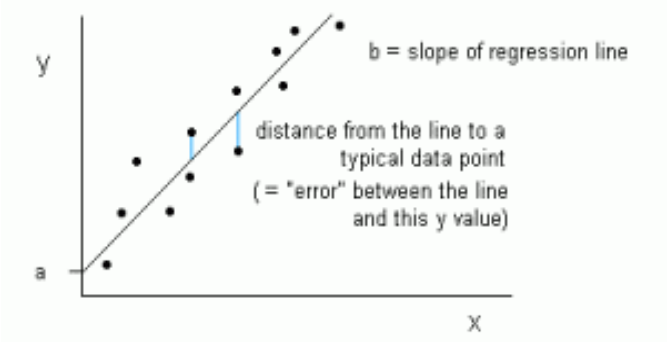


图 2-7 数据集的绘制 x 和 y 值

在线性回归中，输入变量（x）和输出变量（y）之间的关系表示为 $y = ax + b$ 的方程。因此，线性回归的目标是找出系数 a 和 b 的值。这里，a 是直线的斜率，b 是直线的截距。上图显示了数据集的 x 和 y 值，线性回归的目标是拟合最接近大部分点的线。

- 分类与回归树（CART）

CART 是决策树的一个实现方式，由 ID3，C4.5 演化而来，是许多基于树的 bagging、boosting 模型的基础。CART 可用于分类与回归。

CART 是在给定输入随机变量 x 条件下输出随机变量 y 的条件概率分布，与 ID3 和 C4.5 的决策树所不同的是，ID3 和 C4.5 生成的决策树可以是多叉的，每个节点下的叉数由该节点特征的取值种类而定，比如特征年龄分为（青年，中年，老年），那么该节点下可分为 3 叉。而 CART 为假设决策树为二叉树，内部结点特征取值为“是”和“否”。左分支取值为“是”，右分支取值为“否”。这样的决策树等价于递归地二分每一个特征，将输入空间划分为有限个单元，并在这些单元上预测概率分布，也就是在输入给定的条件下输出条件概率分布。

- 随机森林（Random Forest）

随机森林指的是利用多棵决策树对样本进行训练并预测的一种分类器。它包含多个决策树的分类器，并且其输出的类别是由个别树输出的类别的众数而定。随机森林是一种灵活且易于使用的机器学习算法，即便没有超参数调优，也可以在大多数情况下得到很好的结果。随机森林也是最常用的算法之一，因为它很简易，既可用于分类也能用于回归。

其基本的构建算法过程如下：

1） 用 N 来表示训练用例（样本）的个数，M 表示特征数目。

2） 输入特征数目 m，用于确定决策树上一个节点的决策结果；其中 m 应远小于 M。

3） 从 N 个训练用例（样本）中以有放回抽样的方式，取样 N 次，形成一个训练集（即 bootstrap 取样），并用未抽到的用例（样本）作预测，评估其误差。

4） 对于每一个节点，随机选择 m 个特征，决策树上每个节点的决定都是基于这些特征确定的。根据这 m 个特征，计算其最佳的分裂方式。

5） 每棵树都会完整成长而不会剪枝，这有可能在建完一棵正常树状分类器后被采用）。

一个简单的随机森林算法示意如下：

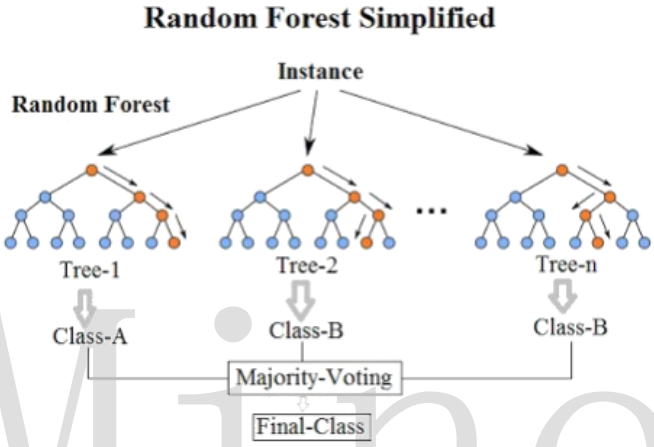


图 2-8 一个简单的随机森林算法示意

随机森林集成了所有的分类投票结果，将投票次数最多的类别指定为最终的输出，这就是一种最简单的 Bagging 思想。

- 逻辑回归

逻辑回归最适合二进制分类（y = 0 或 1 的数据集，其中 1 表示默认类）例如：在预测事件是否发生时，发生的事件被分类为 1。在预测人会生病或不生病，生病的实例记为 1）。它是以其中使用的变换函数命名的，称为逻辑函数 $h(x)=1/（1+e^{-x}）$，它是一个 S 形曲线。

在逻辑回归中，输出是以缺省类别的概率形式出现的。因为这是一个概率，所以输出在 0-1 的范围内。输出（y 值）通过对数转换 x 值，使用对数函数 $h(x)=1/（1+e^{-x}）$ 来生成。然后应用一个阈值来强制这个概率进入二元分类。

下图判断了肿瘤是恶性还是良性。默认变量是 $y=1$（肿瘤=恶性）；x 变量可以是肿瘤的信息，例如肿瘤的尺寸。如图所示，逻辑函数将数据集的各种实例的 x 值转换成 0 到 1 的范围。如果概率超过阈值 0.5（由水平线示出），则将肿瘤分类为恶性。

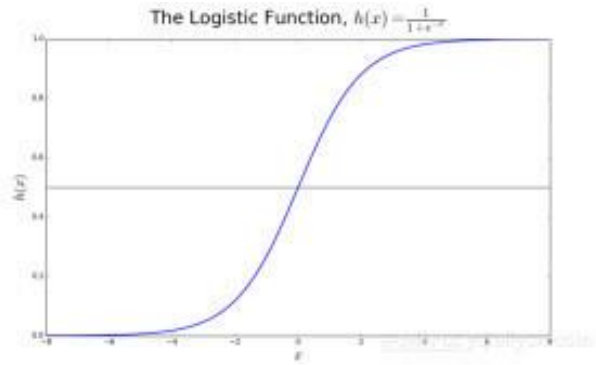


图 2-9 逻辑函数曲线图

逻辑回归的目标是使用训练数据来找到系数 b_0 和 b_1 的值，以使预测结果与实际结果之间的误差最小化。这些系数是使用最大似然估计来计算的。

$$p(x) = \frac{e^{b_0 + b_1 x}}{1 + e^{b_0 + b_1 x}}$$
$$\log\left(\frac{p(x)}{1-p(x)}\right) = b_0 + b_1 x$$

- 朴素贝叶斯（Naive Bayesian）

朴素贝叶斯法是基于贝叶斯定理与特征条件独立假设的分类方法。朴素贝叶斯分类器基于一个简单的假定：给定目标值时属性之间相互条件独立。

通过以上定理和“朴素”的假定，我们知道：

$$P(Category \mid Document) = P(Document \mid Category) * P(Category) / P(Document)$$

朴素贝叶斯的基本方法：在统计数据的基础上，依据条件概率公式，计算当前特征的样本属于某个分类的概率，选择最大的概率分类。

对于给出的待分类项，求解在此项出现的条件下各个类别出现的概率，哪个最大，就认为此待分类项属于哪个类别。其计算流程表述如下：

1）$x = \{a_1, a_2, ..., a_m\}$为待分类项，每个 a_i 为 x 的一个特征属性

2）有类别集合 $C = \{y_1, y_2, ..., y_n\}$

3）计算 $P(y_1|x), P(y_2|x), ..., P(y_n|x)$

4）如果 $P(y_k|x) = max\{P(y_1|x)$

- k 最近邻（kNN）

kNN（*k*-Nearest Neighbor）的核心思想是如果一个样本在特征空间中的 *k* 个最相邻的样本中的大多数属于某一个类别，则该样本也属于这个类别，并具有这个类别上样本的特性。该方法在确定分类决策上只依据最邻近的一个或者几个样本的类别来决定待分样本所属的类别。kNN 方法在做类别决策时，只与极少量的相邻样本有关。由于 kNN 方法主要靠周围有限的邻近的样本，而不是靠判别类域的方法来确定所属类别的，因此对于类域的交叉或重叠较多的待分样本集来说，kNN 方法较其他方法更为适合。

kNN 算法不仅可以用于分类，还可以用于回归。通过找出一个样本的 *k* 个最近邻居，将这些邻居的属性的平均值赋给该样本，就可以得到该样本的属性。如下图是 kNN 算法中，*k* 等于不同值时的算法分类结果：

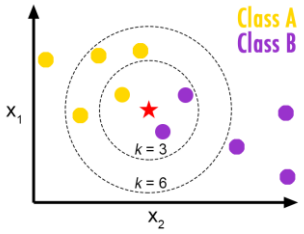


图 2-10 kNN 算法简单示例

简单来说，kNN 可以看成：有那么一堆你已经知道分类的数据，然后当一个新数据进入的时候，就开始跟训练数据里的每个点求距离，然后挑离这个训练数据最近的 *k* 个点，看看这几个点属于什么类型，然后用少数服从多数的原则，给新数据归类。

- AdaBoost

Adaptive Boosting 或称为 AdaBoost，是多种学习算法的融合。它是一种迭代算法，其核心思想是针对同一个训练集训练不同的分类器(弱分类器)，然后把这些弱分类器集合起来，构成一个更强的最终分类器(强分类器)。其算法本身是通过改变数据分布来实现的，它根据每次训练集之中每个样本的分类是否正确，以及上次的总体分类的准确率，来确定每个样本的权值。将修改过权值的新数据集送给下层分类器进行训练，然后将每次训练得到的分类器融合起来，作为最终的决策分类器。

AdaBoost 是最常用的算法。它可用于回归或者分类算法。相比其他机器学习算法，它克服了过拟合的问题，通常对异常值和噪声数据敏感。为了创建一个强大的复合学习器，AdaBoost 使用了多次迭代。因此，它又被称为“Adaptive Boosting”。通过迭代添加弱学习器，AdaBoost 创建了一个强学习器。一个新的弱学习器加到实体上，并且调整加权向量，作为对前一轮中错误分类的样例的回应。得到的结果，是一个比弱分类器有更高准确性的分类器。

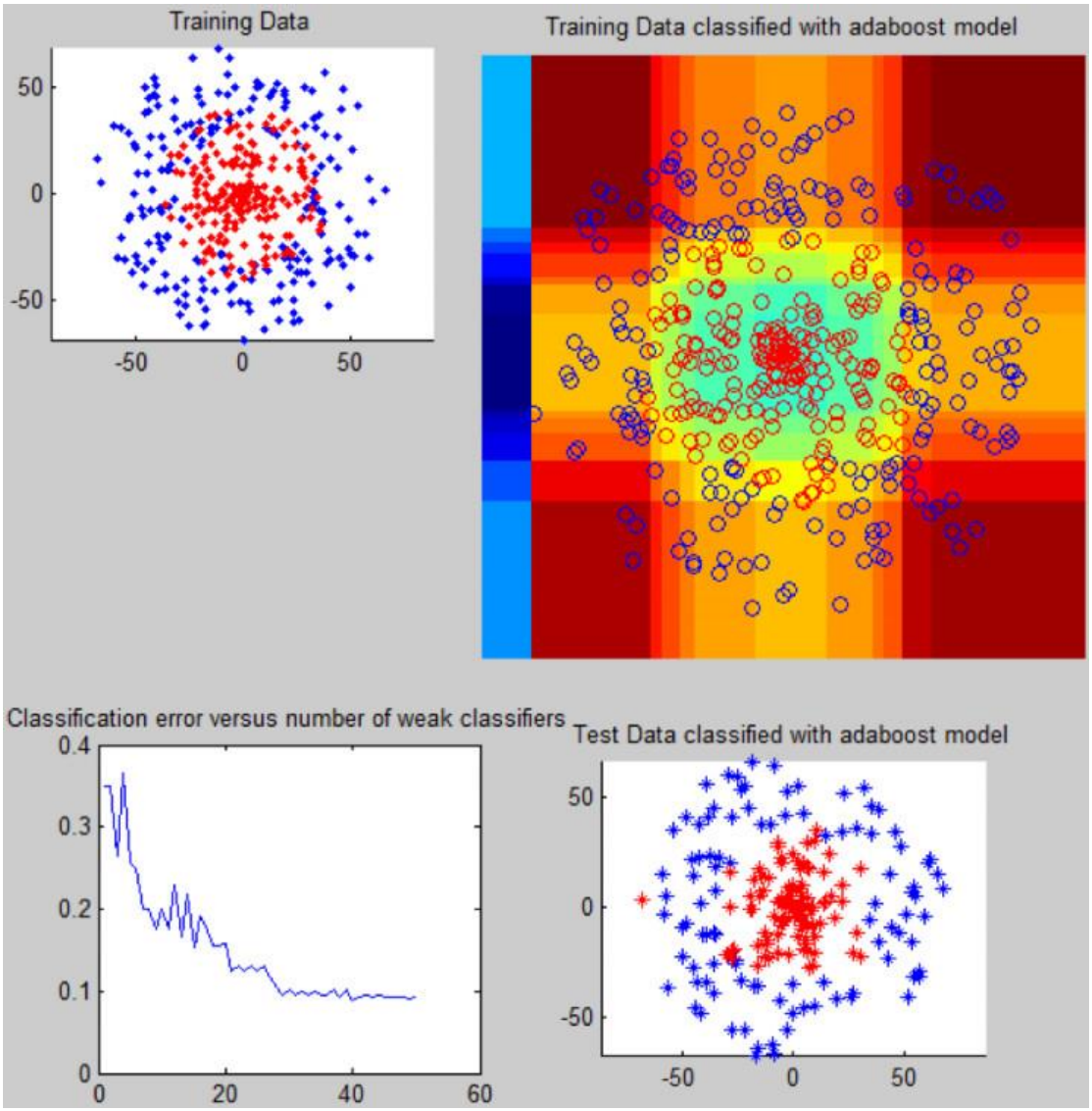


图 2-11 AdaBoost 执行

AdaBoost 有助于将弱阈值的分类器提升为强分类器。上面的图像描述了 AdaBoost 的执行，只用了简单易于理解的代码在一个文件中就实现了。这个函数包含一个弱分类器和 boosting 组件。弱分类器在一维的数据中尝试去寻找最理想的阈值来将数据分离为两类。boosting 组件迭代调用分类器，经过每一步分类，它改变了错误分类示例的权重。因此，创建了一个级联的弱分类器，它的行为就像一个强分类器。

目前，对 Adaboost 算法的研究以及应用大多集中于分类问题，同时近年也出现了一些在回归问题上的应用。Adaboost 系列主要解决了：两类问题、多类单标签问题、多类多标签问题、大类单标签问题和回归问题。它用全部的训练样本进行学习。

- K-均值算法（K-Means）

K-均值是著名聚类算法，它找出代表聚类结构的 k 个质心。如果有一个点到某一质心的距离比到其他质心都近，这个点则指派到这个最近的质心所代表的簇。依次，利用当前已聚类的数据点找出一个新质心，再利用质心给新的数据指派一个簇。

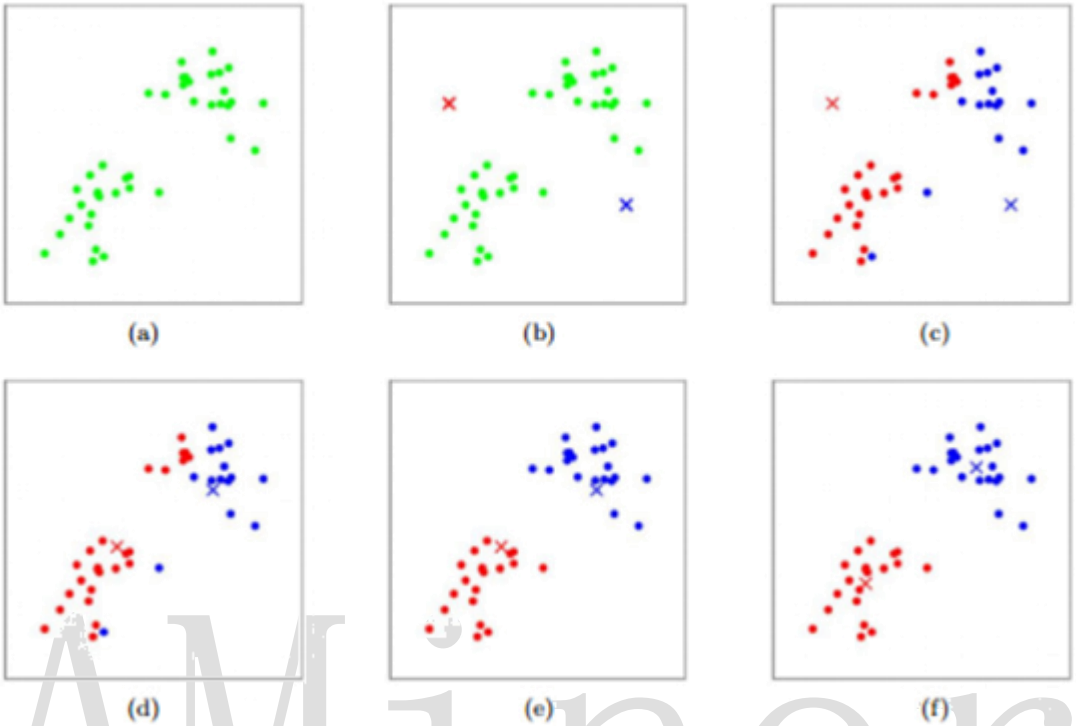


图 2-12 K-均值算法图示

K-均值算法：在上图中用“x”表示聚类质心，用点表示训练样本：

a) 原始数据集

b) 随机初始化聚类质心

c) (*c-f*)*k*-均值迭代 2 次的示意图

在每次迭代中每个训练样例都被指派到一个最近的聚类质心，每个聚类质心被移动到分配给它的点的平均值的位置。

- 支持向量机（SVM）

支持向量机（Support Vector Machine, SVM）是一类按监督学习（supervised learning）方式对数据进行二元分类（binary classification）的广义线性分类器（generalized linear classifier），其决策边界是对学习样本求解的最大边距超平面（maximum-margin hyperplane）。基本思想是：找到集合边缘上的若干数据（称为支持向量（Support Vector）），用这些点找出一个平面（称为决策面），使得支持向量到该平面的距离最大。由简至繁的 SVM 模型包括：

1）当训练样本线性可分时，通过硬间隔最大化，学习一个线性可分支持向量机；

2）当训练样本近似线性可分时，通过软间隔最大化，学习一个线性支持向量机；

3)当训练样本线性不可分时,通过核技巧和软间隔最大化学习一个非线性支持向量机；

在分类问题中，很多时候有多个解，如下图左边所示，在理想的线性可分的情况下其决策平面会有多个。而 SVM 的基本模型是在特征空间上找到最佳的分离超平面使得训练集上正负样本间隔最大，SVM 算法计算出来的分界会保留对类别最大的间距，即有足够的余量，如下图右边所示。

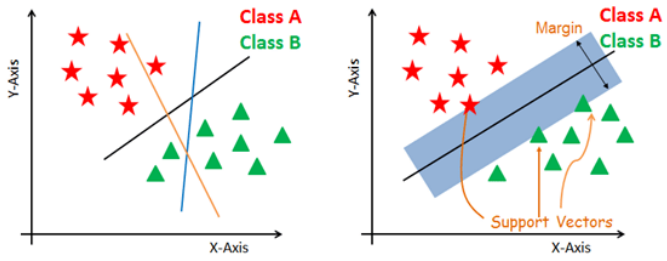


图 2-13 SVM 的决策平面

在解决线性不可分问题时，它可以通过引入核函数，巧妙地解决了在高维空间中的内积运算，从而很好地解决了非线性分类问题。如下图所示，通过核函数的引入，将线性不可分的数据映射到一个高纬的特征空间内，使得数据在特征空间内是可分的。如下图所示：

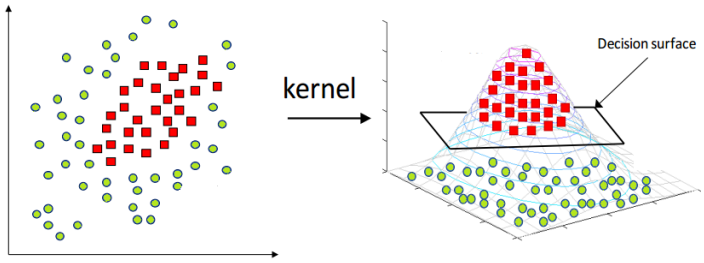


图 2-14 SVM 的核函数

- 人工神经网络 ANN（Artificial Neural Network）

人工神经网络 ANN（Artificial Neural Network）是由大量处理单元互联组成的非线性、自适应信息处理系统。它是一种模仿动物神经网络行为特征，进行分布式并行信息处理的算法数学模型。其基本过程可以概述如下：外部刺激通过神经末梢，转化为电信号，传导到神经细胞（又叫神经元）；无数神经元构成神经中枢；神经中枢综合各种信号，做出判断；人体根据神经中枢的指令，对外部刺激做出反应。

人工神经网络经历了漫长的发展阶段。最早是上个世纪六十年代提出的“人造神经元”模型，叫做“感知器”（perceptron）。感知机模型是机器学习二分类问题中的一个非常简单的模型。它的基本结构如下图所示：

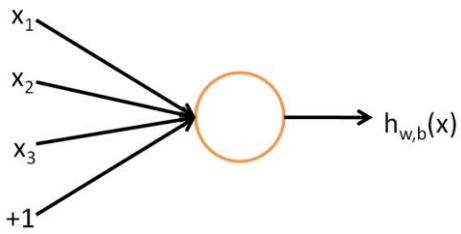


图 2-15 感知机

随着反向传播算法、最大池化（max-pooling）等技术的发明，神经网络进入了飞速发展的阶段。神经网络就是将许多个单一“神经元”联结在一起，这样，一个“神经元”的输出就可以是另一个“神经元”的输入。典型的人工神经网络具有以下三个部分：

结构（Architecture）指定了网络中的变量和它们的拓扑关系。

激励函数（Activity Rule）大部分神经网络模型具有一个短时间尺度的动力学规则，来定义神经元如何根据其他神经元的活动来改变自己的激励值。

学习规则（Learning Rule）指定了网络中的权重如何随着时间推进而调整。

一个典型的人工神经网络结构如下图所示：

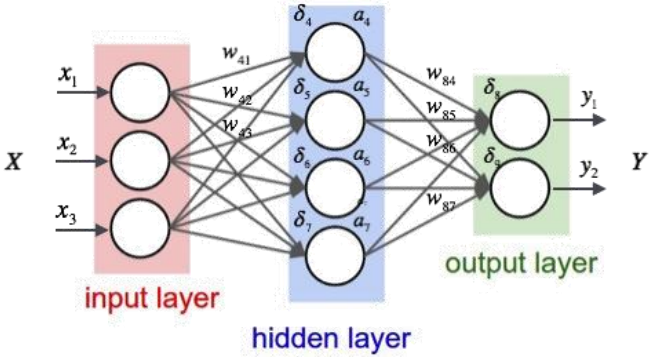


图 2-16 典型的人工神经网络结构

人工神经网络具有四个基本特征：非线性、非局限性、非常定性和非凸性。

人工神经网络的特点和优越性，主要表现在三个方面：具有自学习功能、具有联想存储功能和具有高速寻找最优解的能力[16]。

2.3 生成对抗网络及对抗机器学习

2.3.1 生成对抗网络

生成对抗网络（Generative Adversarial Networks, GAN）是用于无监督学习的机器学习模型，由 Ian Goodfellow 等人在 2014 年提出[20]，由神经网络构成判别器和生成器构成，通过一种互相竞争的机制组成的一种学习框架，GAN 在深度学习领域掀起了一场革命，这场革命产生了一些重大的技术突破，学术界和工业界都开始接受并欢迎 GAN 的到来。GAN 最厉害的地方是它的学习性质是无监督的，GAN 也不需要标记数据，这使 GAN 功能强大，因为数据标记的工作非常枯燥。GAN 的潜在用例使它成为交谈的中心，它可以生成高质量的图像，图片增强，从文本生成图像，将图像从一个域转换为另一个域，随年龄增长改变脸部外观等等。传统的生成模型最早要追溯到 80 年代的 RBM，以及后来逐渐使用深度神经网络进行包装的 AutoEncoder，然后就是现在称得上最火的生成模型 GAN[21]。

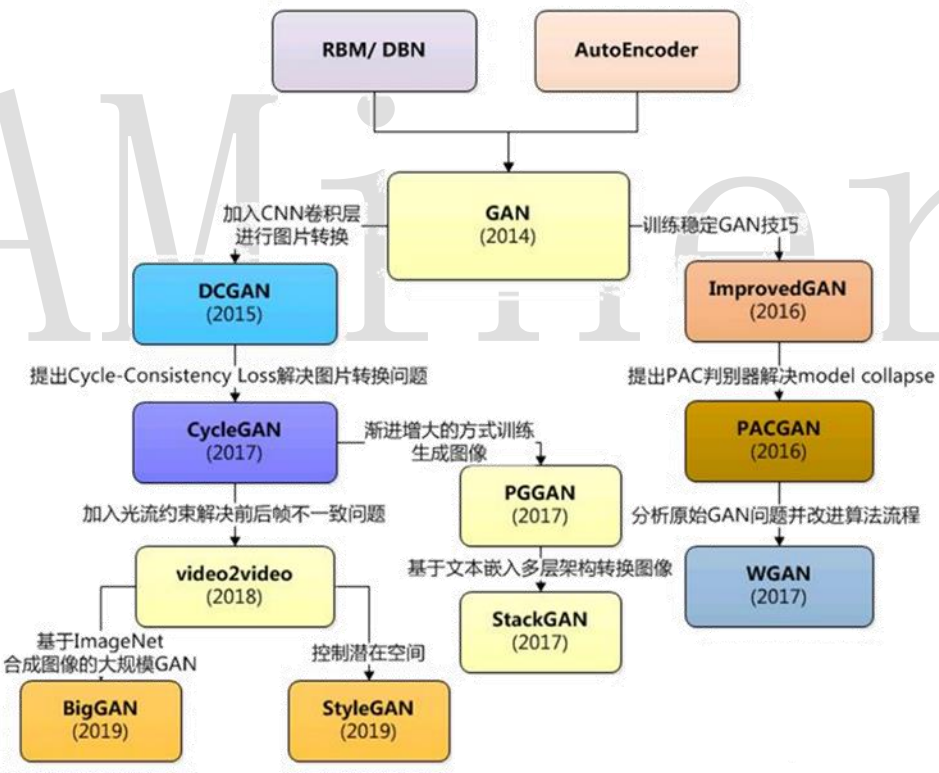


图 2-17 GAN 发展脉络

GAN 经历了如下的发展历程：

- 诞生

生成对抗网络（GAN）具有两个网络，生成器网络和鉴别器网络。这两个网络可以是神经网络，从卷积神经网络，递归神经网络到自动编码器。在这种配置中，两个网络参与竞争

游戏并试图相互超越，同时帮助他们完成自己的任务。经过数千次迭代后，如果一切顺利，生成器网络可以完美生成逼真的虚假图像，并且鉴别器网络可以很好地判断图像是真实的还是虚假的。换句话说，生成器网络将来自潜在空间的随机噪声矢量（不是来自潜在空间的所有 GAN 样本）变换为真实数据集的样本。GAN 的训练是一个非常直观的过程。GAN 具有大量的实际用例，如图像生成，艺术品生成，音乐生成和视频生成。此外，它还可以提高图像质量，图像风格化或着色，面部生成以及其他更多有趣的任务。

下图表示了一般的 GAN 网络的架构。首先，从潜在空间采样 D 维的噪声矢量并发送到生成器网络。生成器网络将该噪声矢量转换为图像。然后将生成的图像发送到鉴别器网络以进行分类。鉴别器网络不断地从真实数据集和由发生器网络生成的图像获得图像。它的工作是区分真实和虚假的图像。所有 GAN 架构都遵循这样的设计。

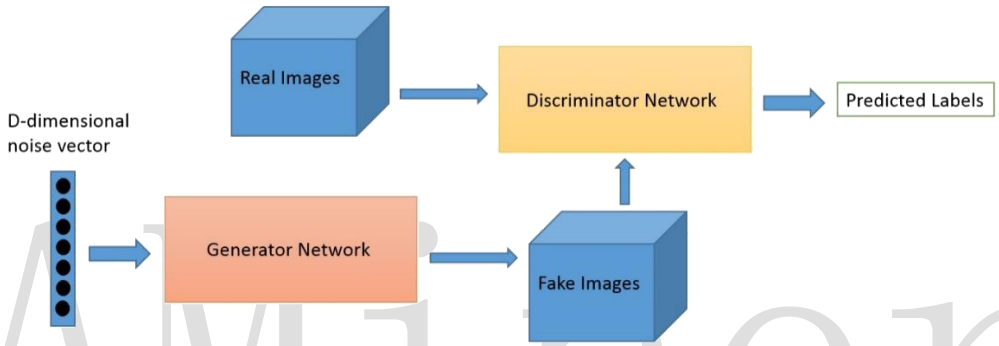


图 2-18 GAN 网络的架构

- 青春期

在青春期，GAN 产生了许多流行的架构，如 DCGAN，StyleGAN，BigGAN，StackGAN，Pix2pix，Age-cGAN，CycleGAN 等。这些结构的结果都非常令人满意。下面详细讨论这些 GAN 架构。

DCGAN：

这是第一次在 GAN 中使用卷积神经网络并取得了非常好的结果。之前，CNN 在计算机视觉方面取得了前所未有的成果。但在 GAN 中还没有开始应用 CNNs。Alec Radford，Luke Metz，Soumith Chintala 等人“Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks”提出了 DCGAN[22]。这是 GAN 研究的一个重要里程碑，因为它提出了一个重要的架构变化来解决训练不稳定，模式崩溃和内部协变量转换等问题。从那时起，基于 DCGAN 的架构就被应用到了许多 GAN 架构。

BigGAN：

这是 GAN 中用于图像生成的最新进展。一个谷歌的实习生和谷歌 DeepMind 部门的两名研究人员发表了一篇“Large Scale GAN Training for High Fidelity Natural Image Synthesis”的论文。本文是来自 Heriot-Watt 大学的 Andrew Brock 与来自 DeepMind 的 Jeff Donahue 和 Karen Simonyan 合作的实习项目。

图 2-19 BigGAN 生成的图像

这些图像都是由 BigGAN 生成，正如你看到的，图像的质量足以以假乱真。这是 GAN 首次生成具有高保真度和低品种差距的图像。之前的最高初始得分为 52.52，BigGAN 的初始得分为 166.3，比现有技术（SOTA）好 100％。此外，他们将 Frechet 初始距离（FID）得分从 18.65 提高到 9.6。这些都是非常令人印象深刻的结果。它最重要的改进是对生成器的正交正则化。

StyleGAN：

StyleGAN 是 GAN 研究领域的另一项重大突破。StyleGAN 由 Nvidia 在题为“A Style-Based Generator Architecture for Generative Adversarial Network”的论文中介绍[23]。StyleGAN 在面部生成任务中创造了新记录。算法的核心是风格转移技术或风格混合。除了生成面部外，它还可以生成高质量的汽车，卧室等图像。这是 GANs 领域的另一项重大改进，也是深度学习研究人员的灵感来源。

StackGAN：

StackGANs 由 Han Zhang，Tao Xu，Hongsheng Li 还有其他人在题为 StackGAN: Text to Photo-Realistic Image Synthesis with Stacked Generative Adversarial Networks 的论文中提出[24]。他们使用 StackGAN 来探索文本到图像的合成，得到了非常好的结果。一个 StackGAN 由一对网络组成，当提供文本描述时，可以生成逼真的图像。

如下图所示，提供文本描述时，StackGAN 生成了逼真的鸟类图像。最重要的是生成的图像正类似于所提供的文本。文本到图像合成有许多实际应用，例如从一段文本描述中生成图像，将文本形式的故事转换为漫画，创建文本描述的内部表现。

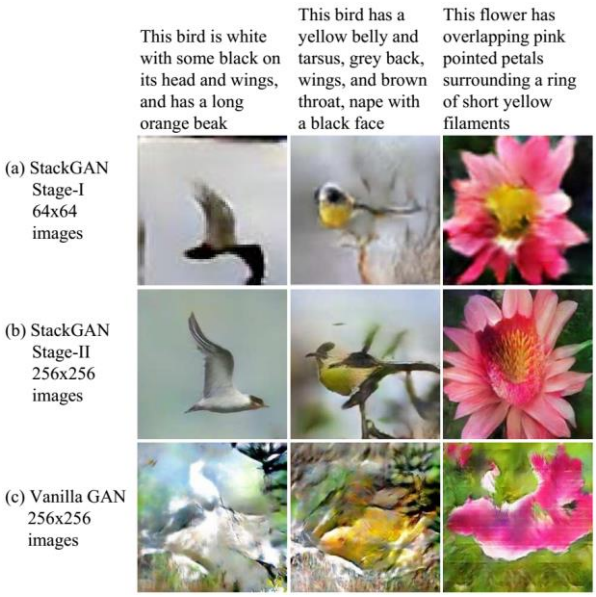


图 2-20 StackGAN 生成的图像

CycleGAN：

CycleGAN 有一些非常有趣的用例，例如将照片转换为绘画，将夏季拍摄的照片转换为冬季拍摄的照片，或将马的照片转换为斑马照片，或者相反。CycleGANs 由 Jun-Yan Zhu，Taesung Park，Phillip Isola 和 Alexei A. Efros 在题为“Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks”的论文中提出。CycleGAN 用于不同的图像到图像翻译[25]。

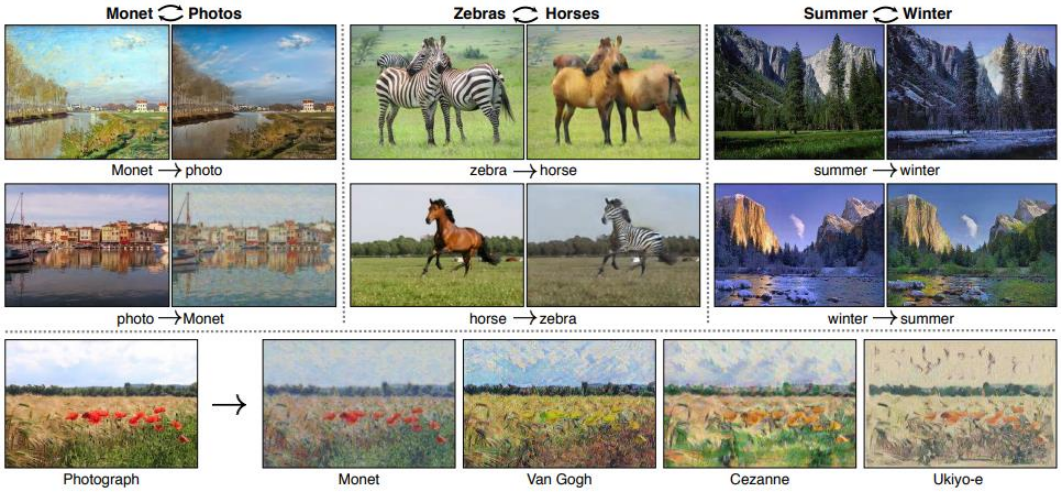


图 2-21 CycleGAN 生成的图像

Pix2pix：

Pix2pix 网络由 Phillip Isola，Jun-Yan Zhu，Tinghui Zhou 和 Alexei A. Efros 在他们的题为“Image-to-Image Translation with Conditional Adversarial Networks”的论文中提出[26]。对

于图像到图像的翻译任务，pix2pix 显示出了令人印象深刻的结果。无论是将夜间图像转换为白天的图像还是给黑白图像着色，或者将草图转换为逼真的照片等等，Pix2pix 在这些例子中都表现非常出色。这是一个交互式的演示，能够从草图生成真实图像。

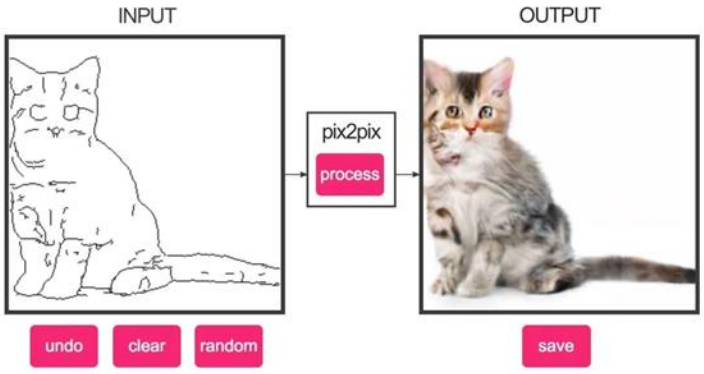


图 2-22 Pix2pix 生成的图像

Age-cGAN：

Age Conditional Generative Adversarial Networks（Age-cGAN），面部老化有许多行业用例，包括跨年龄人脸识别，寻找失踪儿童，或者用于娱乐。Grigory Antipov，Moez Baccouche 和 Jean-Luc Dugelay 在他们的题为“Face Aging with Conditional Generative Adversarial Networks”的论文中提出了用条件 GAN 进行面部老化[27]。

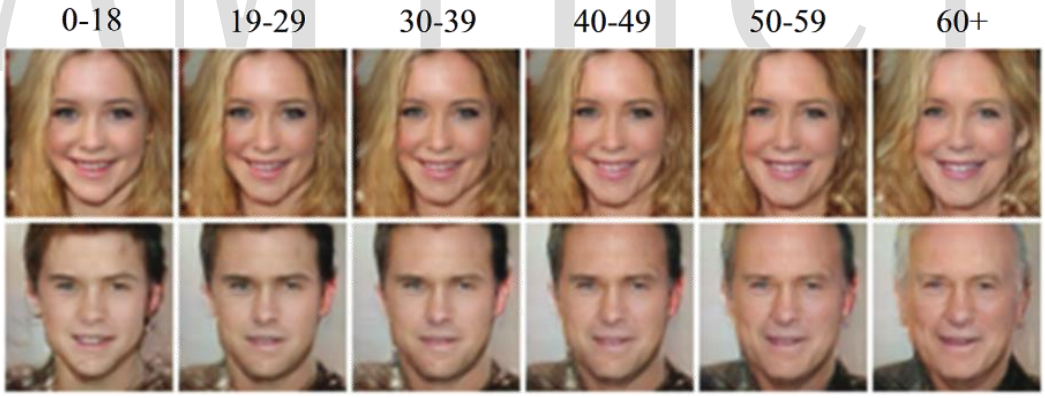


图 2-23 Age-cGAN 生成的图像

上图显示了 Age-cGAN 是怎样从原来的年龄转换为目标年龄的，这些都是非常流行的 GAN 架构，除了这些，还有数以千计的 GAN 架构，这取决什么样的需求。

- 崛起

正如着名理论物理学家理查德费曼所说：“What I can’t create, I don’t understand”，GAN 背后的思想是训练已知数据的网络。GAN 开始了解数据，通过这种了解，GAN 开始创建逼真的图像。

Edmond de Belamy：

由 GAN 创作的 Edmond de Belamy 在佳士得拍卖会上以 432,500 美元的价格成交。这是 GAN 发展的重要一步，全世界第一次目睹了 GAN 及其潜力。在此之前，GAN 主要局限于研究实验室，并由机器学习工程师使用。这一行为使 GAN 成为面向公众的一个入口。

图 2-24 GAN 创作的 Edmond de Belamy

https://thispersondoesnotexist.com 这个网站是由优步的软件工程师 Philip Wan 创建。他根据 NVIDIA 发布的名为 StyleGAN 的代码创建了这个网站。每当你刷新时，它都会生成一个新的不存在的人脸，看起来无法判断它是否是假的。这项技术有可能创造一个完全的虚拟世界。

Deep Fakes：

图 2-25 Deep Fakes 换脸

DeepFakes 是一种使用机器学习技术来创建逼真图像和视频的技术。基于 GAN，可以将人脸粘贴到视频中的目标人物上。事实上，人脸交换技术在电影制作领域已经不是个新鲜词

了，但是之前电影视频中的人脸交换非常复杂，专业的视频剪辑师和 CGI 专家需要花费大量时间和精力才能完成视频中的人脸交换。DeepFakes 的出现可以说是人脸交换技术的一个突破。利用 DeepFakes 技术，你只需要一个 GPU 和一些训练数据，就能够制作出以假乱真的换脸视频。这可以说是一个非常了不起的突破了，因为你只需要把上百张人物的样图输入至一个算法，就能完成人脸交换，制作出非常逼真的视频效果。就算你是个对视频剪辑一窍不通的外行，也能做到这样[28]。

- 未来发展

现在 GAN 已被用于增强游戏图形。我对 GAN 的这种用例感到非常兴奋。最近，NVIDIA 发布了一个视频，其中展示了如何使用 GAN 对视频中的环境进行游戏化。我们看到了 GAN 如何发展壮大并成为一种全球现象。我希望在未来几年 GAN 达到民主化。当我看到关于 GAN 的负面新闻时感到一些困惑。我相信，我们有责任让每个人都了解 GAN 带来的影响，以及我们如何在伦理道德上尽可能使用 GAN[29]。

GAN 是一个非常强大的框架，https://zhuanlan.zhihu.com/p/38533823 网站整理了自 2014 年，GAN 推出以来，一些优质的论文，分享给有需要的朋友[30]。

2.3.2 对抗机器学习

对抗机器学习是一个机器学习与计算机安全的交叉领域。对抗机器学习旨在给恶意环境下的机器学习技术提供安全保障。由于机器学习技术一般研究的是同一个或较为稳定的数据分布，当部署到现实中的时候，由于恶意用户的存在，这种假设并不一定成立。比如研究人员发现，一些精心设计的对抗样本（adversarial example）可以使机器学习模型失败输出正确的结果[31]。针对模型的攻击问题，我们主要分为两大类，就是从训练阶段和推理（inference）阶段来进行讨论[32]。

- 训练阶段的攻击

训练阶段的恶意攻击（Training in Adversarial Settings），主要的目的就是针对模型的参数进行微小的扰动，从让而模型的性能和预期产生偏差。这样的行为主要是通过数据投毒来完成的。

不过在此之前，有个前提，在 PAC 理论中，有一个已经论证的结论：对于任意的学习算法而言，其置信度 β，必须满足 $\beta \leq \Sigma/1+\Sigma$，其中 Σ 表示了学习准确率。那么也就是说，当需要达到 90%的学习准确率（$\Sigma = 0.1$），那么被扰动的数据量必须少于 10%（0.1/1+0.1）[33]。

1）标签操纵（label manipulation）

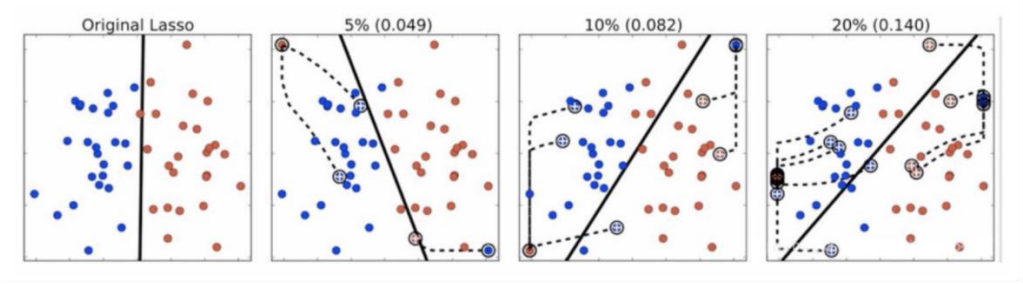


图 2-26 标签操纵的分类准确率

这个方法很直观，就是直接通过对于训练数据的标签进行替换，让数据样本和标签不对应，最后训练的结果一定是不如预期的。有前人在 SVM 的场景下，随机替换了约 40%的数据，对其算法进行了破坏，最后的效果也如预期的很好。其实这只是在二分类问题中起到了比较好的结果，但是在多分类的情况下并没有很好的解释，或者是实证性的研究。（这里可以有一个比较有趣的思考，如果二分类的分类替换了 40%的数据会导致模型的预测结果很不好，那么多分类的 SVM 需要替换多少数据样本的标签呢，是需要替换更少的标签，还是更多？是随机替换还是有目标性的都替换成一种？）后来的研究则是对这个标签操纵的过程更加优化，是否能通过更少的标签替换，来实现更强烈的模型扰动，从而产生更有说服力的攻击模型[34]。

2）输入操纵（input manipulation）

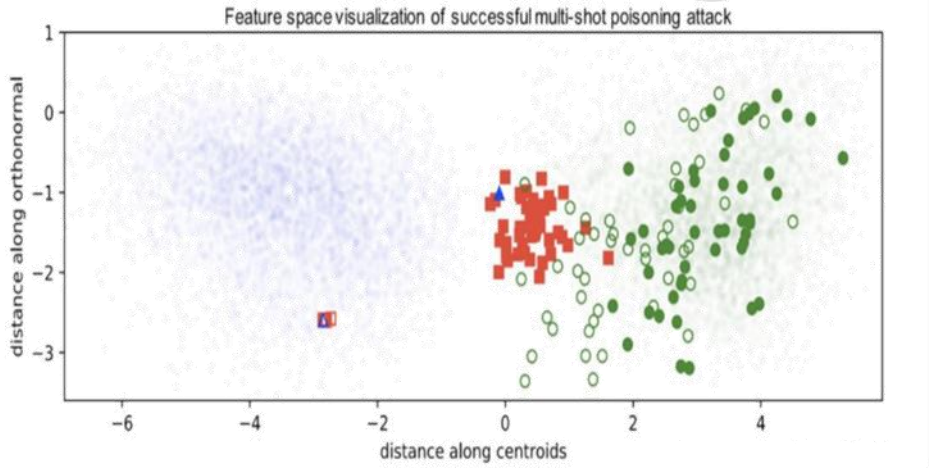


图 2-27 对输入进行操纵导致的结果

在此攻击场景下，攻击者需要获知模型的算法类型，并且能结束到训练集。比较直接的攻击方式，则是通过在线的方式获得训练数据的输入权，那么最终的结果就是直接通过恶意数据来扰动在线训练过程，自然最后的结果就是脱离预期，从而导致恶意者的操纵成功。而当我们无法接触到在线模型的时候，我们只能通过线下的方式操纵训练数据，那么则需要构

造尽量少且恶意程度尽量高的恶意样本，那么这就可以使用梯度上升的方法去达到局部分类错误最大的结果，从而完成样本构造，然后再输入到模型中进行训练。那么，当我们无法直接接触到在线训练模型，或离线时，我们也无法解除到训练数据，我们该怎么进行输入的操纵呢？从之前的流程介绍中我们也提到了，在物理世界获取数据的时候，这阶段并没有受到很好的保护。因此这阶段的数据，我们可以通过恶意的攻击物理世界中的数据，例如交通信号灯，或者是自动驾驶摄像头正在拍摄的图像等。通过其在数据转换之前，就进行数据的污染，或是数据表示的污染[35]。

- 推理阶段的攻击（Inference in Adversarial Settings）

当训练完成一个模型之后，这个模型就可以看做一个 BOX，那么这个盒子中，对于我们如果是透明的话，我们就把它当成是“白盒”模型，如果这个盒子中，我们什么都看不了，我们就把它当成“黑盒”模型。（我们在这个部分不讨论灰盒模型）那么针对白盒和黑盒的进攻手段自然是不同的，但是最终的目的都是希望能对模型的最终结果产生破坏，与预期脱离。其影响力以及攻击的构造粒度也是有所不同的。

1）白盒攻击（White-Box Adversarial）

当然这种所谓的“白盒攻击”，需要提供一个很“假”的前提——就是我们需要知道里面所有的模型参数，这个在现实生活中是非常不现实的。除非是，当模型被打包压缩到智能手机上之后，然后恶意者通过逆向工程来进行原有模型的复原，才有可能。当然这种情况出现的情况非常低了，因此我们需要有这种前提假设。

$$\underset{\gamma}{argmin}\ h(x+r)=l \qquad s.t. \qquad x+r\in D$$

看到如上公式，其中 x 是数据样本的特征，l 是数据样本通过函数 h（x）预测的结果，l 就是预测的结果。我们的数据样本通过模型的预测结果可能是 k，但是我们希望通过尽量小的扰动 r，最后通过模型预测的结果是 l（然而 x 的分类目标并不是 l），目标很明确[36]。这样的方法对于非凸的模型，例如深度神经网络也有类似的工作，同样也是能通过较小的扰动，来达成模型的误分类目的[37]。

当然可以看到，如上面公式所示，我们可以很明显的看到，其实如何快速求解这个扰动“r”是个问题，因此之后就有工作专门针对这个问题进行了探索，给出了如下方法，FGSM：

$$x^{*}=x+\varepsilon\cdot sign\left(\nabla_{\vec{x}}J_{h}\left(\theta,x,y\right)\right)$$

如上式所示，通过梯度可以快速求到，通过最小的扰动获得的最后的攻击目的。那么后续的工作无外乎就是从两个方向进行优化，一方面就是尽量少的对样本扰动，从而能达成攻

击，另一方面对尽量少的样本特征进行操纵，通过算法的优化，从而能达到更高的错误识别率[38]。

有一个很有趣的现象，是这样描述的，其实在数据进入预处理步骤之前，在物理世界中，如果没有一个很好的表示形态，即使经过了预处理，模型也很难识别。这就给了研究者一些启发，对图片进行打印之后，再拍照让模型进行识别；亦或是把人脸的图片打印在玻璃上，然后再进行识别。这样的结果，都会有很高的误识别率（虽然目前 CV 发展的势头很好，但是由此看来，还是有不少算法对于环境和背景的敏感程度很高）。

大家都认为，adversarial machine learning 应该关注在分类问题上，但是其实并不然，其实如果一个 AI 系统是以 agent 为核心，或是以 multi-agent 为核心的强化学习系统的话，那也是有可以攻击的点的，例如改变环境获取的结果？等（只是猜想），现在有课题组可以在一些固定模式下自动进行星际争霸的游戏，如果攻击了这样的系统，应该还是很有趣的。

不仅模型的预测结果是有脆弱的地方，同时，当我们拥有模型参数的时候，也是可以进行模型训练集数据分布的预测的。虽然这个并不是最重要的信息，但是也是一部分关于模型的隐私[39]。

2）黑盒攻击（Black-Box Adversarial）

当模型处于黑盒的时候，更加符合现实的场景，但是这比白盒的模型缺少了更多的模型信息。因此，大家就从几个角度考虑如何进行模型攻击：通过输入和输出猜测模型的内部结构；加入稍大的扰动来对模型进行攻击；构建影子模型来进行关系人攻击；抽取模型训练的敏感数据；模型逆向参数等。

其中我觉得比较有意思的是两个方法，一个是加入扰动来对模型进行攻击。这个方法最主要针对的是，找到原有模型的“blind spot”，或是说“blind area”。这些区域主要是原有模型模棱两可的区域，或是 boundry，这对二分类的问题来说可能这些区域比较小或是比较狭窄，但是如果针对的是多分类问题，就可能在高维空间中提现出更多的“blind area”。因此尽量高的命中这些盲区，是这种方法致力于的方向，同时这里也提出一个思考，这样的盲区是否是可以定向搜索的，或是说是否可以用一个模糊的算法 bound 住这些区域。

第二是建立影子模型，这个 process 很有意思，通过构建一个功能性类似的模型，来仿造一个攻击空间。这有点像军事演习的意思，我想要在战场上打出好的效果，就要模拟产战场上可能发生的情况，但是目前战场的情况我一无所知，所以我只能根据大致的情况去模拟。模型也是如此，只能对黑盒的情况进行对应的训练模拟，然后对其进行“白盒”的尝试，由于模型的迁移性还不错，或者说类似的算法都有不少的相同点，因此，影子模型的攻击成效还是不错的。

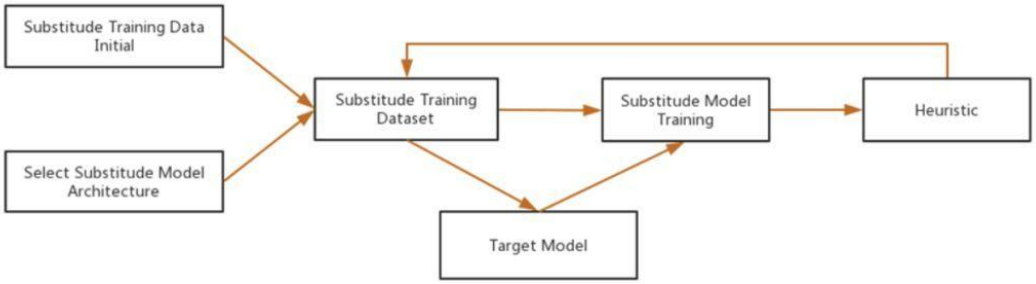


图 2-28 建立影子模型

2.4 自动机器学习

2.4.1 AutoML

自动机器学习（AutoML）旨在通过让一些通用步骤（如数据预处理、模型选择和调整超参数）自动化，来简化机器学习中生成模型的过程。AutoML 是指尽量不通过人来设定超参数，而是使用某种学习机制，来调节这些超参数。这些学习机制包括传统的贝叶斯优化，多臂老虎机（multi-armed bandit），进化算法，还有比较新的强化学习。当我们提起 AutoML 时，我们更多地是说自动化数据准备（即数据的预处理，数据的生成和选择）和模型训练（模型选择和超参数调优）。这个过程的每一步都有非常多的选项，根据我们遇到的问题，需要设定各种不同的选项。

对于机器学习的新用户而言，使用机器学习算法的一个主要的障碍就是算法的性能受许多的设计决策影响。随着深度学习的流行，工程师需要选择相应的神经网络架构，训练过程，正则化方法，超参数等等，所有的这些都对算法的性能有很大的影响。于是深度学习工程师也被戏称为调参工程师。自动机器学习的目标就是使用自动化的数据驱动方式来做出上述的决策。用户只要提供数据，自动机器学习系统自动的决定最佳的方案。领域专家不再需要苦恼于学习各种机器学习的算法。自动机器学习不光包括大家熟知的算法选择，超参数优化，和神经网络架构搜索，还覆盖机器学习工作流的每一步。自动机器学习的用处就在于此，它帮助研究人员和从业者，自动构建机器学习管道，将多个步骤及其对应的多个选项集成为工作流，以期快速找到针对给定问题的高性能机器学习模型[40]。

AutoML 的基本过程如下图所示：虚框是配置空间，包括特征、超参数和架构；左边训练数据进入，上面的优化器和它相连，定义的测度发现最佳配置，最后出来的是模型；测试数据在模型中运行，实现预测的目的。

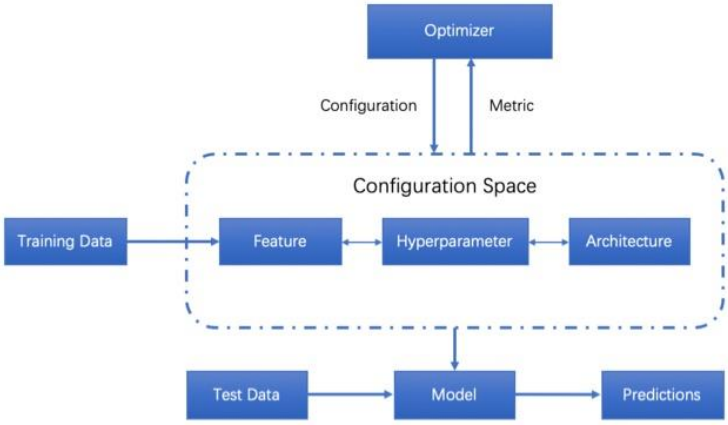


图 2-29 AutoML 基本过程

从 ML 角度看 AutoML：从这个角度来看，AutoML 本身也可以看作是一种学习工具，它对输入数据（即 E）和给定任务（即 T）具有良好的泛化性能（即 P）。然而，传统的 ML 研究更多地关注发明和分析学习工具，它并不关心这些工具的使用有多容易。一个这样的例子恰恰是从简单模型到深度模型的最新趋势，它可以提供更好的性能，但也很难配置。相比之下，AutoML 强调了学习工具的易用性。

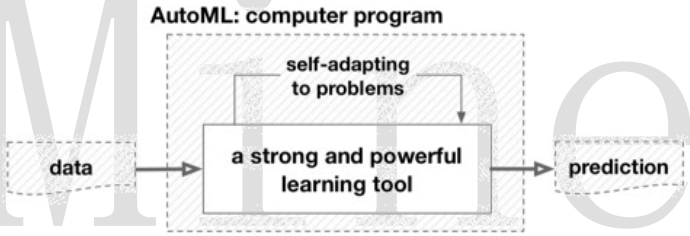


图 2-30 从 ML 角度看 AutoML

从自动化角度看 AutoML：另一方面，自动化是使用各种控制系统在构建模块下运行。为了更好地预测性能，ML 工具的配置应该通过输入数据适应任务，这通常是手动执行的。如图所示，从这个角度来看，AutoML 的目标是在学习工具下构建高级控制方法，以便在没有人工帮助的情况下找到正确的配置[41]。

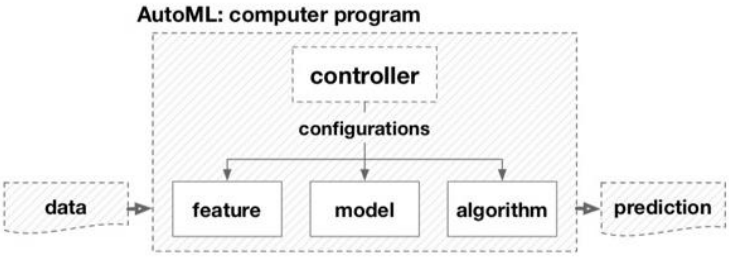


图 2-31 从自动化角度看 AutoML

下面介绍 AutoML 的几个重要方向：

- **超参数优化（HPO）**

学习器模型中一般有两类参数，一类是可以从数据中学习估计得到，还有一类参数时无法从数据中估计，只能靠人的经验进行设计指定，后者成为超参数。比如，支持向量机里面的 C, Kernal, game；朴素贝叶斯里面的 alpha 等。

超参数优化有很多方法，最常见的类型是黑盒优化（black-box function optimization）。所谓黑盒优化，就是将决策网络当作是一个黑盒来进行优化，仅关心输入和输出，而忽略其内部机制。决策网络通常是可以参数化的，这时候我们进行优化首先要考虑的是收敛性。以下的几类方法都是属于黑盒优化：

网格搜索（grid search）

Grid search 大家都应该比较熟悉，是一种通过遍历给定的参数组合来优化模型表现的方法。网格搜索的问题是很容易发生维度灾难，优点是很容易并行。

随机搜索（random search）

随机搜索是利用随机数求极小点而求得函数近似的最优解的方法。很多时候，随机搜索比网格搜索效果要更好，但是我们可以从上图看出，它们都不能保证找到最优解。

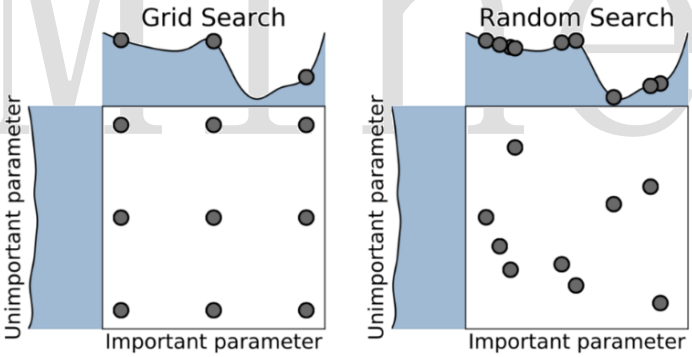


图 2-32 网格搜索与随机搜索

贝叶斯优化

贝叶斯优化是一种迭代的优化算法，包含两个主要的元素，输入数据假设的模型和一个采集函数用来来决定下一步要评估哪一个点。每一步迭代，都使用所有的观测数据 fit 模型，然后利用激活函数预测模型的概率分布，决定如何利用参数点，权衡是 Explaoration 还是 Exploitation。相对于其它的黑盒优化算法，激活函数的计算量要少很多，这也是为什么贝叶斯优化被认为是更好的超参数调优的算法。

黑盒优化的一些工具：

Hyperopt：是一个 Python 库，可以用来寻找实数,离散值,条件维度等搜索空间的最佳值。

Google Vizier：是 Google 的内部的机器学习系统，Google Vizier 能够利用迁移学习等技术自动优化其他机器学习系统的超参数。

Advisor：Google Vizier 的开源实现。

Katib：基于 Kubernetes 的超参数优化工具。

由于优化目标具有不连续、不可导等数学性质，所以一些搜索和非梯度优化算法被用来求解该问题，包括我们上面提到的这些黑盒算法。此类算法通过采样和对采样的评价进行搜索，往往需要大量对采样的评价才能获得比较好的结果。然而，在自动机器学习任务中评价往往通过 k 折交叉验证获得，在大数据集的机器学习任务上，获得一个评价的时间代价巨大。这也影响了优化算法在自动机器学习问题上的效果。所以一些减少评价代价的方法被提出来，其中多保真度优化（multi-fidelity methods）就是其中的一种。这里的技术包括：基于学习曲线来决定是否要提前终止训练，探索-利用困境（exploration exploitation）的多臂老虎机算法（Multi-armed bandit）等等。

- **元学习（Meta Learning）**

元学习也就是‘学习如何学习’，通过对现有的学习任务之间的性能差异进行系统的观测，学习已有的经验和元数据，用于更好的执行新的学习任务。这样做可以极大的改进机器学习流水线或者神经网络架构的设计，也可以用数据驱动的方式取代手工作坊似的算法工程工作。

从某种意义上来说，元学习覆盖了超参数优化，因为元数据的学习包含了：超参数、流水线的构成、神经网络架构、模型构成、元特征等等。机器学习的算法又称为‘学习器’，学习器是假定一个模型，该模型拥有很多未知参数，利用训练数据和优化算法来找到最适合这些训练数据的参数，生成一个新的算法，或者参数已知的模型，并利用该模型/算法来预测新的未知数据。如果说世界上只有一个模型，那么问题就简单了，但实际上是模型有很多，不同的模型拥有不同的超参数，我们往往还会把模型和算法组装在一起构成复合模型和机器学习的流水线，这个时候，就需要知道解决不同的问题要构建那些不同的模型。元学习可以把超参数、流水线、神经网络架构这些都看成是一个新模型的未知参数，把不同学习任务的性能指标看成是输入数据，这样我们就可以利用优化算法来找到性能最好的那组参数。这个模式可以一直嵌套，也就是说，你可以有‘元元元学习’，当然我希望你不要走得太远，找不到回来的路。

元学习的方法包括：1）通过模型评估来学习；2）通过任务的属性，元特征来学习。元学习的一个很大的挑战就是如果通过很少的训练数据来学习一个复杂的模型，这就是 one-shot 或者 few-shot 的问题。像人类的学习一样，每次学习无论成功失败，我们都收获一定的经验，人类很少从头学习。在构建自动学习的时候，我们也应该充分利用已有的每一次的学习经验，逐步的改进，使得新的学习更加有效。

- 神经网络架构搜索（Neural Architecture Search, NAS）

提起 AutoML，其实大多数人都是因为 Google 的 AutoML 系统才知道这个故事的。随着深度学习的流行，神经网络的架构变得越来越复杂，越来越多的手工工程也随之而来。神经网络架构搜索就是为了解决这个问题。

NAS 主要包含三个部分：

搜索空间（search space）：搜索空间原则上定义了可以代表哪些体系结构。结合适用于任务属性的先验知识可以减小搜索空间大小并简化搜索。然而，这也引入了人为偏见，可能会阻止找到超越当前人类知识的新颖架构构建块（building blocks）。

搜索策略（search strategy）：搜索策略说明了如何做空间搜索。它包含了经典的探索-开发（exploration-exploitation）之间的权衡。一方面，需要快速找到性能良好的架构，另一方面，避免过早收敛到次优架构（suboptimal architecture）区域。

性能估计策略（performance estimation strategy）：NAS 的目标通常是找到在未知数据实现高预测性能的架构。性能评估是指评估此性能的过程：最简单的选择是对数据架构执行标准训练和验证，但遗憾的是，这种方法计算成本很高，限制了可以探索的体系结构量。因此，最近的研究大多集中在开发出方法去降低这些性能估计成本。

如下是神经结构搜索方法的示意图：“搜索策略”从预定义的“搜索空间”A 中选择体系结构 A；该架构被传递到“性能估计策略”，该策略将 A 估计的性能返回到搜索策略[42]。

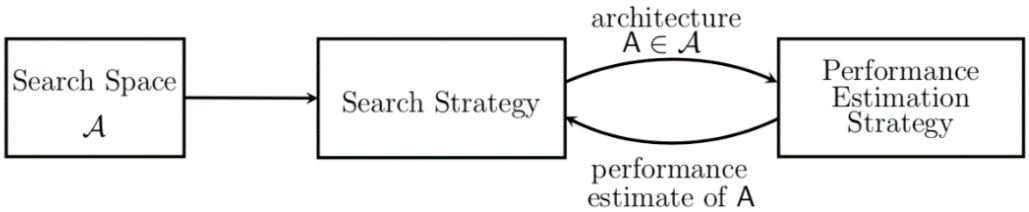


图 2-33 神经结构搜索方法示意图

2.4.2 ATMSeer

为特定任务设计机器学习模型（如图像分类，疾病诊断和股市预测等）是一个艰巨而耗时的过程。研究人员首先要从多种不同的算法中进行选择来构建模型。然后在模型开始训练之前，手动调整“超参数”，确定模型的整体结构。近期出现的 AutoML 系统可以对算法和超参数进行迭代式的测试和修改，并在此过程中选择最适合的模型。但系统的运行机制是不透明的，相当于一个“黑盒子”，也就是说系统选择了什么技术、什么模型，用户是看不见的。因此，用户就可能不信任模型给出的结果，而且很难根据自己的搜索需求来对系统进行定制。

近日，在 ACM CHI 计算系统中人的因素会议上，麻省理工学院，香港科技大学和浙江大学的研究人员共同研发出一种工具，将 AutoML 方法的分析和控制权给到用户手中。该工具名为 ATMSeer，它将 AutoML 系统、数据集和有关用户任务的一些信息作为输入，然后在用户友好型的界面内实现可视化搜索过程，界面中还能提供更多关于模型性能的深入信息。

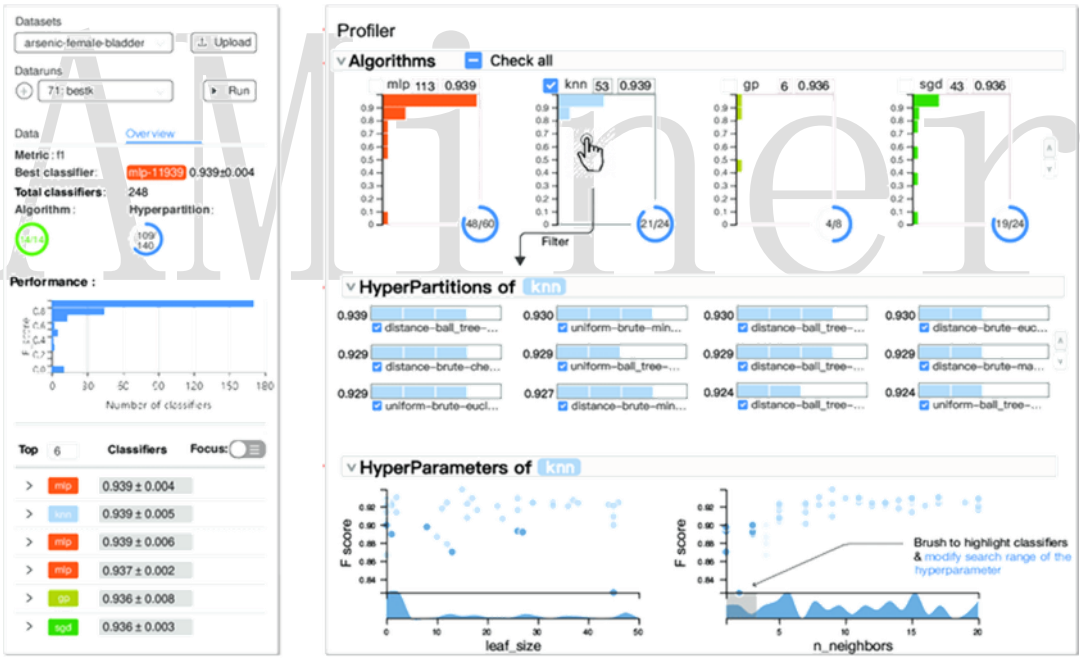


图 2-34 ATMSeer 自动机器学习定制化工具的用户友好型交互界面

“使用 ATMSeer，用户可以自己选择和观察 AutoML 系统是如何工作的，”该研究论文的共同作者之一 Kalyan Veeramachaneni 说道，他是麻省理工学院信息与决策系统实验室（LIDS）的首席研究科学家，负责将数据引入 AI 团队。“用户可以只选择一些性能最好的模型，或者结合其他因素或某些领域的专业知识，来指导 AutoML 系统去搜索某些特定模型。”在对 AutoML 新手的案例研究中，研究人员发现大约 85％使用 ATMSeer 的人对系统选择的模型充满信心。几乎所有参与者都表示，该工具让使用 AutoML 系统变得更舒服了。

上图是 ATMSeer 生成的一个用户友好界面，显示有关所选模型性能的深入信息，以及可调整的算法和参数的选项[43]。

“数据可视化是实现人与机器之间更好协作的有效方法。ATMSeer 体现了这一理念，”论文合作者之一、香港科技大学的 Wang Qianwen 说。“ATMSeer 主要会让机器学习从业者受益，无论他们从事什么领域，专业水平如何，都能获益。ATMSeer 可以缓解手动选择机器学习算法和调整超参数的不便。”ATMSeer 的特点如下：

便捷可视化工具实现“可视即可调”

ATMSeer 工具的核心是一款定制的 AutoML 系统，名为“自动调整模型”（ATM），由 Veeramachaneni 等研究人员在 2017 年开发。与传统的 AutoML 系统不同的是，ATM 在尝试拟合模型时会对所有搜索结果进行完整的编目。

ATM 将任何数据集和编码预测任务作为输入。系统随机选择算法类别，比如神经网络，决策树、随机森林和逻辑回归，并选择模型的超参数，如决策树的大小或神经网络层数等。

然后，系统针对数据集运行模型，迭代式调整超参数，并衡量模型性能。ATM 利用掌握到了模型性能来选择另一个模型。最后，由系统针对任务输出几个表现最理想的模型。

诀窍在于，每个模型基本上可以被视为带有一系列变量的数据点：这里说的变量包含算法，超参数和性能。在此基础上，研究人员设计了一套系统，在指定的图形和图表上绘制数据点和变量。以此为起点，开发了一系列新技术，能够实时重新配置数据。“亮点在于，使用这些工具，你能够可视化的任何东西，都可以修改。”史密斯说。

类似的可视化工具专门用于分析一种特定的机器学习模型，并能够在有限的搜索空间内实现定制化。“因此，这些工具可以为分析和观察 AutoML 的运行流程提供了有限的支持，还需要对许多搜索模型的配置进行分析。相比之下，ATMSeer 支持分析使用各种算法生成的机器学习模型。”

将 AutoML 控制权交给用户，使用体验和信心明显提升

ATMSeer 的可视化界面由三部分组成。用户可以通过控制面板上传数据集和 AutoML 系统，并启动或暂停搜索过程。下图是一个概览面板，显示了基本统计数据，如搜索的算法和超参数的数量，还有按降序排列的最佳模型的“排行榜”。Veeramachaneni 表示：“如果你不是特别在意技术细节的专家，这可能是你最感兴趣的点。”

ATMSeer 包含一个“AutoML Profiler”，其中的面板包含有关算法和超参数的深入信息，这些信息都可以进行调整。面板可以将所有算法类别表示为直方图形式，用条形图显示算法

性能分数的分布，范围为 0 到 10，具体取决于其超参数。用一个单独的面板呈现散点图，显示不同超参数和算法类型的性能折衷。

对没有 AutoML 经验的机器学习专家的案例研究表明，让用户掌握控制权确实有助于提高 AutoML 应用的性能和效率。对生物学、金融等不同科学领域的 13 位研究生的研究也表明，确定用户对 AutoML 的搜索的自定义关键有三点：搜索的算法数量、系统运行时间以及查找表现最好的模型。研究人员表示，这些信息可用来为用户量身定制系统[44]。

研究人员表示，目前对 AutoML 的应用缺乏足够的灵活性。“现在所有这些信息都集中在一个地方，如果人们能够清楚看到幕后发生的事情，有能力控制这些流程，未来对 AutoML 的应用将跨入一个崭新的阶段。”

2.5 可解释性机器学习

可解释性是指人类能够理解决策原因的程度。机器学习模型的可解释性越高，人们就越容易理解为什么做出某些决定或预测。模型可解释性指对模型内部机制的理解以及对模型结果的理解。其重要性体现在：建模阶段，辅助开发人员理解模型，进行模型的对比选择，必要时优化调整模型；在投入运行阶段，向业务方解释模型的内部机制，对模型结果进行解释。比如基金推荐模型，需要解释：为何为这个用户推荐某支基金。

机器学习流程步骤：收集数据、清洗数据、训练模型、基于验证或测试错误或其他评价指标选择最好的模型。第一步，选择比较小的错误率和比较高的准确率的高精度的模型。第二步，面临准确率和模型复杂度之间的权衡，但一个模型越复杂就越难以解释。一个简单的线性回归非常好解释，因为它只考虑了自变量与因变量之间的线性相关关系，但是也正因为如此，它无法处理更复杂的关系，模型在测试集上的预测精度也更有可能比较低。而深度神经网络处于另一个极端，因为它们能够在多个层次进行抽象推断，所以他们可以处理因变量与自变量之间非常复杂的关系，并且达到非常高的精度。但是这种复杂性也使模型成为黑箱，我们无法获知所有产生模型预测结果的这些特征之间的关系，所以我们只能用准确率、错误率这样的评价标准来代替，来评估模型的可信性。事实上，每个分类问题的机器学习流程中都应该包括模型理解和模型解释，原因如下：

- **模型改进：**理解指标特征、分类、预测，进而理解为什么一个机器学习模型会做出这样的决定、什么特征在决定中起最重要作用，能让我们判断模型是否符合常理。一个深度的神经网络来学习区分狼和哈士奇的图像。模型使用大量图像训练，并使用另外的一些图像进行测试。90%的图像被准确预测，这值得我们高兴。但是在没有计算解释函数（explainer function）时，我们不知道该模型主要基于背景：狼图像通常有一个下雪的背景，而哈士奇的图像很少有。所以我们不知不觉地做了一个雪地探测器，如果只看准

确率这样的指标，我们就不会看到这一点。知道了模型是如何使用特征进行预测的，我们就能直觉地判断我们的模型是否抓住了有意义的特征，模型是或否能泛化到其他样本的预测上。

- **模型可信性与透明度：**理解机器学习模型在提高模型可信度和提供审视预测结果透明度上是非常必要的，让黑箱模型来决定人们的生活是不现实的，比如贷款和监狱刑法。另一个对机器学习结果可信度提出质疑的领域是药品，模型结果会直接决定病人的生与死。机器学习模型在区分恶性肿瘤和不同类型的良性肿瘤方面是非常准确的，但是我们依然需要专家对诊断结果进行解释，解释为什么一个机器学习模型将某个患者的肿瘤归类为良性或恶性将大大帮助医生信任和使用机器学习模型来支持他们工作。长久来看，更好地理解机器学习模型可以节省大量时间、防止收入损失。如果一个模型没有做出合理的决定，在应用这个模型并造成不良影响之前，我们就可以发现这一点。

- **识别和防止偏差：**方差和偏差是机器学习中广泛讨论的话题。有偏差的模型经常由有偏见的事实导致，如果数据包含微妙的偏差，模型就会学习下来并认为拟合很好。一个有名的例子是，用机器学习模型来为囚犯建议定罪量刑，这显然反映了司法体系在种族不平等上的内在偏差。其他例子比如用于招聘的机器学习模型，揭示了在特定职位上的性别偏差，比如男性软件工程师和女性护士。机器学习模型在我们生活的各个层面上都是强有力的工具，而且它也会变得越来越流行。所以作为数据科学家和决策制定者来说，理解我们训练和发布的模型如何做出决策，让我们可以事先预防偏差的增大以及消除他们，是我们的责任。

可解释性动机

在工业界中，数据科学或机器学习的主要焦点是更偏“应用”的解决复杂的现实世界至关重要的问题，而不是理论上有效地应用这些模型于正确的数据。机器学习模型本身由算法组成，该算法试图从数据中学习潜在模式和关系，而无需硬编码固定规则。因此，解释模型如何对业务起作用总是会带来一系列挑战。有一些领域的行业，特别是在保险或银行等金融领域，数据科学家通常最终不得不使用更传统的机器学习模型（线性或基于树的）。原因是模型可解释性对于企业解释模型所采取的每个决策非常重要。

残酷的现实是，如果没有对机器学习模型或数据科学 pipeline 如何运作的合理理解，现实中的项目很少成功。现实中的数据科学项目，通常会有业务和技术两方面。数据科学家通常致力于构建模型并为业务提供解决方案。但是，企业可能不知道模型如何工作的复杂细节。

数据科学从业者将知道存在典型的模型可解释性与模型性能权衡。这里需要记住的一点是，模型性能不是运行时或执行性能，而是模型在决策中的准确程度。有几种模型，包括简单的线性模型甚至是基于树的模型，它们可以很容易地解释模型为获得特定的洞察力或预测

而做出的决策，但是你可能需要牺牲模型性能，因为它们总是不能产生最好的结果是由于高偏差（线性模型）或高方差的固有问题，导致过度拟合（完全成长的树模型）。更复杂的模型，如集合模型和最近的深度学习模型系列通常会产生更好的性能，但被认为是黑盒模型，因为很难解释模型如何真正做出决定。

理解模型可解释性

模型解释作为一个概念仍然主要是理论和主观的。任何机器学习模型的核心都有一个响应函数，它试图映射和解释独立（输入）自变量和（目标或响应）因变量之间的关系和模式。当模型预测或寻找见解时，需要做出某些决定和选择。模型解释试图理解和解释响应函数所做出的这些决定，即 what，why 以及 how。模型解释的关键是透明度，质疑能力以及人类理解模型决策的难易程度。模型解释的三个最重要的方面解释如下。

- 是什么驱动了模型的预测？我们应该能够查询我们的模型并找出潜在的特征交互，以了解哪些特征在模型的决策策略中可能是重要的。这确保了模型的公平性。
- 为什么模型会做出某个决定？我们还应该能够验证并证明为什么某些关键特征在预测期间驱动模型所做出的某些决策时负有责任。这确保了模型的可靠性。
- 我们如何信任模型预测？我们应该能够评估和验证任何数据点以及模型如何对其进行决策。对于模型按预期工作的关键利益相关者而言，这应该是可证明且易于理解的。这确保了模型的透明度。

在比较模型时，除了模型性能之外，如果模型的决策比其他模型的决策更容易理解，那么模型被认为比其他模型具有更好的可解释性。

可解释性的重要性

在解决机器学习问题时，数据科学家往往倾向于关注模型性能指标，如准确性，精确度和召回等等（毫无疑问，这很重要！）。这在大多数围绕数据科学和机器学习的在线竞赛中也很普遍。但是，指标只能说明模型预测决策的部分故事。随着时间的推移，由于环境中的各种因素导致的模型概念漂移，性能可能会发生变化。因此，了解推动模型采取某些决策的因素至关重要。

如果一个模型工作得很好，为什么还要深入挖掘呢？在解决现实世界中的数据科学问题时，为了让企业信任您的模型预测和决策，他们会不断提出“我为什么要相信您的模型？”这一问题，这一点非常有意义。如果一个人患有癌症或糖尿病，一个人可能对社会构成风险，或者即使客户会流失，您是否会对预测和做出决策（如果有的话）感到满意？也许不是，如果我们能够更多地了解模型的决策过程（原因和方式），我们可能会更喜欢它。这使我们更

加透明地了解模型为何做出某些决策，在某些情况下可能出现的问题，并且随着时间的推移它有助于我们在这些机器学习模型上建立一定程度的信任。

了解预测背后的原因在评估信任方面非常重要，如果计划基于预测采取行动，或者选择是否部署新模型，那么这是至关重要的。无论人类是直接使用机器学习分类器作为工具，还是在其他产品中部署模型，仍然存在一个至关重要的问题：如果用户不信任模型或预测，他们就不会使用它。

可解释性的标准

有一些特定的标准可用于分类模型解释方法。Christoph Molnar，2018 年“可解释的机器学习，制作黑箱模型可解释指南”中提到了一个很好的指南。

- **内在还是事后？**内在可解释性就是利用机器学习模型，该模型本质上是可解释的（如线性模型，参数模型或基于树的模型）。事后可解释性意味着选择和训练黑匣子模型（集合方法或神经网络）并在训练后应用可解释性方法（特征重要性，部分依赖性图）。我们将更多地关注我们系列文章中的事后模型可解释方法。
- **模型特定或模型不可知？**特定于模型的解释工具非常特定于内在模型解释方法，这些方法完全依赖于每个模型的功能和特征。这可以是系数，p 值，与回归模型有关的 AIC 分数，来自决策树的规则等等。与模型无关的工具与事后方法更相关，可用于任何机器学习模型。这些不可知方法通常通过分析（和输入的扰动）特征输入和输出对来操作。根据定义，这些方法无法访问任何模型内部，如权重，约束或假设。
- **本地还是全局？**这种解释分类讨论了解释方法是解释单个预测还是整个模型行为？或者如果范围介于两者之间？我们将很快谈论全球和地方的解释。

可解释性的范围

如何定义可解释性的范围和界限？一些有用的方面可以是模型的透明度，公平性和责任性。全局和局部模型解释是定义模型解释范围的明确方法。

- **全局可解释：**就是试图理解“模型如何进行预测？”和“模型的子集如何影响模型决策？”。要立即理解和解释整个模型，我们需要全局可解释性。全局可解释性是指能够基于完整数据集上的依赖（响应）变量和独立（预测变量）特征之间的条件交互来解释和理解模型决策。尝试理解特征交互和重要性始终是理解全球解释的一个很好的一步。当然，在尝试分析交互时，在超过两维或三维之后可视化特征变得非常困难。因此，经常查看可能影响全局知识模型预测的模块化部分和特征子集会有所帮助。全局解释需要完整的模型结构，假设和约束知识。

- **局部解释**：试图理解“为什么模型为单个实例做出具体决策？”和“为什么模型为一组实例做出具体决策？”。对于本地可解释性，我们不关心模型的固有结构或假设，我们将其视为黑盒子。为了理解单个数据点的预测决策，我们专注于该数据点并查看该点周围的特征空间中的局部子区域，并尝试基于该局部区域理解该点的模型决策。本地数据分布和特征空间可能表现完全不同，并提供更准确的解释而不是全局解释。局部可解释模型-不可知解释（LIME）框架是一种很好的方法，可用于模型不可知的局部解释。我们可以结合使用全局和局部解释来解释一组实例的模型决策。

- **模型透明度**：为试图理解“如何根据算法和特征创建模型？”。我们知道，通常机器学习模型都是在数据特征之上利用算法来构建将输入映射到潜在输出（响应）的表示。模型的透明度可能试图了解模型的构建方式以及可能影响其决策的更多技术细节。这可以是神经网络的权重，CNN 滤波器的权重，线性模型系数，决策树的节点和分裂。但是，由于业务可能不太精通这些技术细节，因此尝试使用不可知的局部和全局解释方法来解释模型决策有助于展示模型透明度。

可解释性的作用

对于想要了解模型如何工作的数据科学家来说，评估模型的准确性通常是不够的。数据科学家通常想知道模型输入变量如何工作以及模型的预测如何根据输入变量的值而变化。

机器学习算法和模型的工程应用中用到最多的主要是树类模型（lgb, xgb）和神经网络（cnn, rnn），使用者往往习惯于很少去思考其中的含义和解释性。需要思考一个模型的哪些东西是可解释的，所以有几个问题值得讨论：

- 哪些特征在模型看到是最重要的？
- 关于某一条记录的预测，每一个特征是如何影响到最终的预测结果的？
- 从大量的记录整体来考虑，每一个特征如何影响模型的预测的？

这些解释信息的作用如下：

- **调试模型**：一般的真实业务场景会有很多不可信赖的，没有组织好的脏数据。你在预处理数据时就有可能加进来了潜在的错误，或者不小心泄露了预测目标的信息等，考虑各种潜在的灾难性后果，debug 的思路就尤其重要了。当你遇到了用现有业务知识无法解释的数据的时候，了解模型预测的模式，可以帮助你快速定位问题。

- **指导工程师做特征工程**：特征工程通常是提升模型准确率最有效的方法。特征工程通常涉及到到反复的操作原始数据(或者之前的简单特征)，用不同的方法来得到新的特征。有时候你完成 FE 的过程只用到了自己的直觉。这其实还不够，当你有上百个原始特征

的时候，或者当你缺乏业务背景知识的时候，你将会需要更多的指导方向。如何创造出这样优秀的特征呢？如何找到最重要的特征的方法，并且可以发现两个特别相关的特征，当面对越来越多的特征的时候，这些方法就会很重要了。

- **指导数据采集的方向**：对于网上下载的数据集你完全控制不了。不过很多公司和机构用数据科学来指导他们从更多方面收集数据。一般来说，收集新数据很可能花费比较高或者不是很容易，所以大家很想要知道哪些数据是值得收集的。基于模型的洞察力分析可以教你很好的理解已有的特征，这将会帮助你推断什么样子的新特征是有用的。

- **指导人们做决策**：一些决策是模型自动做出来的，虽然亚马逊不会用人工来决定展示给你网页上的商品，但是很多重要的决策是由人来做出的，而对于这些决定，模型的洞察力会比模型的预测结果更有价值。

- **建立模型和人之间的信任**：很多人在做重要决策的时候不会轻易的相信模型，除非他们验证过模型的一些基本特性，这当然是合理的。实际上，把模型的可解释性展示出来，如果可以匹配上人们对问题的理解，那么这将会建立起大家对模型的信任，即使是在那些没有数据科学知识的人群中[45]。

2.6 在线学习

- **概述**

传统的机器学习算法是批量模式的，假设所有的训练数据预先给定，通过最小化定义在所有训练数据上的经验误差得到分类器。这种学习方法在小规模规模上取得了巨大成功，但当数据规模大时，其计算复杂度高、响应慢，无法用于实时性要求高的应用。与批量学习不同，在线学习假设训练数据持续到来，通常利用一个训练样本更新当前的模型，大大降低了学习算法的空间复杂度和时间复杂度，实时性强。在大数据时代，大数据高速增长的特点为机器学习带来了严峻的挑战，在线学习可以有效地解决该问题，引起了学术界和工业界的广泛关注。早期在线学习应用于线性分类器产生了著名的感知器算法，当数据线性可分时，感知器算法收敛并能够找到最优的分类面。经过几十年的发展，在线学习已经形成了一套完备的理论，既可以学习线性函数，也可以学习非线性函数，既能够用于数据可分的情况，也能够处理数据不可分的情况。下面我们给出一个在线学习形式化的定义及其学习目标。

在线学习可以定义为学习器和对手之间的博弈：在每一个时刻，学习器从决策空间选择一个决策，同时对手选择一个损失函数，这样学习器在当前时刻遭受损失；根据遭受的损失，学习器对当前的决策进行更新，从而决定下一时刻的决策。学习器的目的是最小化个时刻的累计损失，即，以线性分类为例，学习器所选择的决策就是分类平面，对手选择的损失函数

则是一个训练样本上的分类误差，学习器的目的是最小化在个训练样本上的累计误差。在分析在线学习算法的效果时，我们通常将在线学习的累计误差与批量学习的累计误差相比较，将其差值称为遗憾（regret）。因此，在线学习最小化累计误差也等价于最小化遗憾，遗憾的上界也就成为衡量在线学习算法性能的标准。

根据学习器在学习过程中观测信息的不同，在线学习还可以再进一步分为：**完全信息下的在线学习和赌博机在线学习。**前者假设学习器可以观测到完整的损失函数，而后者假设学习器只能观测到损失函数在当前决策上的数值，即，依旧以在线分类为例，如果学习器可以观测到训练样本，该问题就属于完全信息下的在线学习，因为基于训练样本就可以定义完整的分类误差函数；如果学习器只能观测到分类误差而看不到训练样本，该问题就属于赌博机在线学习。由于观测信息的不同，针对这两种设定的学习算法也存在较大差异，其应用场景也不同。

与赌博机在线学习相比，完全信息下的在线学习观测到的信息更多，因此相对容易。由于损失函数是已知的，因此可以计算其梯度、海森矩阵等信息，辅助学习器更新决策。在线梯度下降是针对该设定最常用的算法，该算法利用损失函数的梯度更新当前的决策。理论可以证明，当损失函数是连续凸函数时，在线梯度下降可以达到最优的遗憾上界；当损失函数是强凸函数时，可以达到的遗憾上界。其他常用的学习算法还包括在线牛顿法、正则化最优决策法、在线核学习等。

虽然完全信息下的在线学习已有大量成熟算法，但在许多现实应用中，学习器能够观测到损失函数的这种假设并不成立，使得这些算法不能被直接应用。以在线广告推荐为例，当学习器向用户推荐广告后，可以得到用户是否点击该广告的反馈，但是用户产生该反馈的机制学习器并不知晓。这种情况就是赌博机在线学习的研究范畴。之所以被称为赌博机在线学习，是因为这类研究最早被用来建模赌场中的多臂赌博机问题。

由于观测的不充分，赌博机在线学习存在探索和利用两者之间的困境。一方面，为了准确地估计损失函数的结构，学习器需要尝试更多的新决策；而另一方面，为了最小化遗憾，学习器又倾向于选择能最小化损失函数的决策。与完全信息相比，赌博机在线学习更加复杂，学习算法达到的遗憾上界也更大；并且难以设计通用的学习算法，需要针对不同的函数类型、不同的随机假设设计不同的算法。置信上界和指数加权是用来解决探索和利用之间困境的常用策略，前者适用于损失函数是随机产生的情况，后者针对非随机情况。

一方面，在线学习存在丰富的理论研究，侧重于从理论上刻画算法的遗憾上界；另一方面，在线学习也有广阔的应用场景，并被成功应用于许多实际问题中。完全信息下的在线学习主要被应用到在线分类、在线物体识别等反馈充分的问题中，主要目的是降低训练复杂度，

提高算法实时性。完全信息下的在线学习研究前沿包括非凸函数在线学习、非线性函数在线学习等问题[46]。

Online Learning 能够根据线上反馈数据，实时快速地进行模型调整，使得模型及时反映线上的变化，提高线上预测的准确率。Online Learning 的流程包括：将模型的预测结果展现给用户，然后收集用户的反馈数据，再用来训练模型，形成闭环的系统。如下图所示：

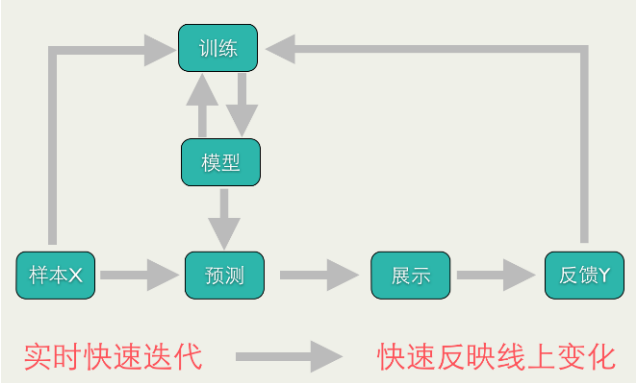


图 2-35 Online Learning 流程

- **FTRL**

FTRL（Follow the Regularized Leader）是由 H. Brendan McMahan 提出，是一种适用于处理超大规模数据的，含大量稀疏特征的在线学习的常见优化算法，方便实用，而且效果很好，常用于更新在线的 CTR 预估模型；FTRL 算法兼顾了 FOBOS 和 RDA 两种算法的优势，既能同 FOBOS 保证比较高的精度，又能在损失一定精度的情况下产生更好的稀疏性。FTRL 在处理带非光滑正则项（如 L1 正则）的凸优化问题上表现非常出色，不仅可以通过 L1 正则控制模型的稀疏度，而且收敛速度快。

- **算法要点与推导**

Algorithm 1 Per-Coordinate FTRL-Proximal with L_1 and L_2 Regularization for Logistic Regression

#With per-coordinate learning rates of Eq. (2).
Input: parameters α, β, λ_1, λ_2
$(\forall i \in \{1, \ldots, d\})$, initialize $z_i = 0$ and $n_i = 0$
for $t = 1$ **to** T **do**
  Receive feature vector $\mathbf{x}_t$ and let $I = \{i \mid x_i \neq 0\}$
  For $i \in I$ compute

$$w_{t,i} = \begin{cases} 0 & \text{if } |z_i| \leq \lambda_1 \\ -\left(\frac{\beta+\sqrt{n_i}}{\alpha} + \lambda_2\right)^{-1}(z_i - \text{sgn}(z_i)\lambda_1) & \text{otherwise.} \end{cases}$$

  Predict $p_t = \sigma(\mathbf{x}_t \cdot \mathbf{w})$ using the $w_{t,i}$ computed above
  Observe label $y_t \in \{0, 1\}$
  for all $i \in I$ **do**
    $g_i = (p_t - y_t)x_i$ *#gradient of loss w.r.t. w_i*
    $\sigma_i = \frac{1}{\alpha}\left(\sqrt{n_i + g_i^2} - \sqrt{n_i}\right)$ *#equals $\frac{1}{\eta_{t,i}} - \frac{1}{\eta_{t-1,i}}$*
    $z_i \leftarrow z_i + g_i - \sigma_i w_{t,i}$
    $n_i \leftarrow n_i + g_i^2$
  end for
end for

- **FTRL-Proximal 工程实现上的 tricks：**

1）saving memory

- Poisson Inclusion：对某一维度特征所来的训练样本，以 p 的概率接受并更新模型。
- Bloom Filter Inclusion：用 bloom filter 从概率上做某一特征出现 k 次才更新。

2）浮点数重新编码

- 特征权重不需要用 32bit 或 64bit 的浮点数存储，存储浪费空间
- 16bit encoding，但是要注意处理 rounding 技术对 regret 带来的影响(注：python 可以尝试用 numpy.float16 格式)

3）训练若干相似 model

- 对同一份训练数据序列，同时训练多个相似的 model
- 这些 model 有各自独享的一些 feature，也有一些共享的 feature
- 出发点：有的特征维度可以是各个模型独享的，而有的各个模型共享的特征，可以用同样的数据训练。

4）Single Value Structure

- 多个 model 公用一个 feature 存储（例如放到 cbase 或 redis 中），各个 model 都更新这个共有的 feature 结构
- 对于某一个 model，对于他所训练的特征向量的某一维，直接计算一个迭代结果并与旧值做一个平均

5）使用正负样本的数目来计算梯度的和（所有的 model 具有同样的 N 和 P）

$$\omega_t = \begin{cases} 1 & \text{event } t \text{ is in a clicked query} \\ \frac{1}{r} & \text{event } t \text{ is in a query with no clicks} \end{cases}$$

6）subsampling Training Data

- 在实际中，CTR 远小于 50%，所以正样本更加有价值。通过对训练数据集进行 subsampling，可以大大减小训练数据集的大小
- 正样本全部采（至少有一个广告被点击的 query 数据），负样本使用一个比例 r 采样（完全没有广告被点击的 query 数据）。但是直接在这种采样上进行训练，会导致比较大的 biased prediction

- 解决办法：训练的时候，对样本再乘一个权重。权重直接乘到 loss 上面，从而梯度也会乘以这个权重[47]。

2.7 BERT

BERT 的全称是 Bidirectional Encoder Representation from Transformers，即双向 Transformer 的 Encoder。可以说是近年来自残差网络最优突破性的一项技术了。BERT 主要特点以下几点：

1）使用了 Transformer 作为算法的主要框架，Trabsformer 能更彻底的捕捉语句中的双向关系[48]；

2）使用了 Mask Language Model（MLM）[49]和 Next Sentence Prediction（NSP）的多任务训练目标；

3）使用更强大的机器训练更大规模的数据，使 BERT 的结果达到了全新的高度，并且 Google 开源了 BERT 模型，用户可以直接使用 BERT 作为 Word2Vec 的转换矩阵并高效的将其应用到自己的任务中。

BERT 的本质上是通过在海量的语料的基础上运行自监督学习方法为单词学习一个好的特征表示，所谓自监督学习是指在没有人工标注的数据上运行的监督学习。在以后特定的 NLP 任务中，我们可以直接使用 BERT 的特征表示作为该任务的词嵌入特征。所以 BERT 提供的是一个供其它任务迁移学习的模型，该模型可以根据任务微调或者固定之后作为特征提取器。BERT 的源码和模型已经在 Github 上开源，简体中文和多语言模型也已开源。

- **网络架构**

BERT 的网络架构使用的是《Attention is all you need》中提出的多层 Transformer 结构，其最大的特点是抛弃了传统的 RNN 和 CNN，通过 Attention 机制将任意位置的两个单词的距离转换成 1，有效的解决了 NLP 中棘手的长期依赖问题。Transformer 的网络架构如下图所示，Transformer 是一个 encoder-decoder 的结构，由若干个编码器和解码器堆叠形成。下图的左侧部分为编码器，由 Multi-Head Attention 和一个全连接组成，用于将输入语料转化成特征向量。右侧部分是解码器，其输入为编码器的输出以及已经预测的结果，由 Masked Multi-Head Attention, Multi-Head Attention 以及一个全连接组成，用于输出最后结果的条件概率。

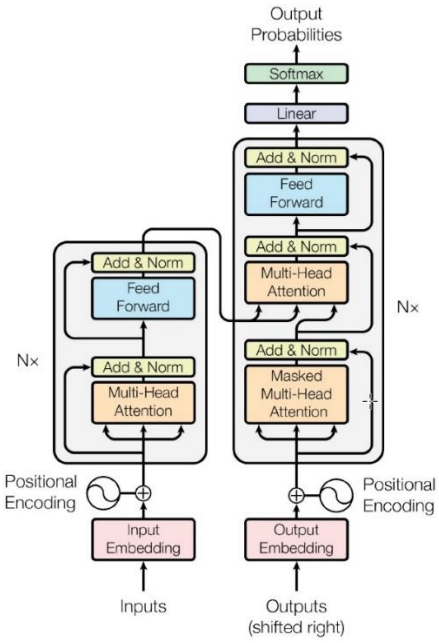


图 2-36 Transformer 的网络架构

上图左侧部分是一个 Transformer Block，对应到下图一个“Trm”：

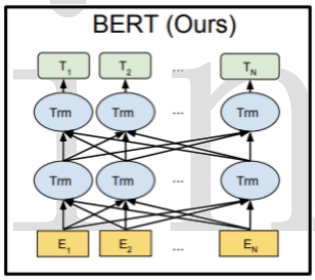


图 2-37 BERT 的模型结构

BERT 提供了简单和复杂两个模型，对应的超参数分别如下：

$BERT_{BASE}$: L=12，H = 768，A = 12，参数总量 110M；

$BERT_{BASE}$: L=24，H = 1024，A = 16，参数总量 340M；

在上面的超参数中，L 表示网络的层数（即 Transformer blocks 的数量），A 表示 Multi-Head Attention 中 self-Attention 的数量，filter 的尺寸是 4H。

论文中还对比了 BERT 和 GPT[50]和 ELMo[51]，它们两个的结构图如下图所示。

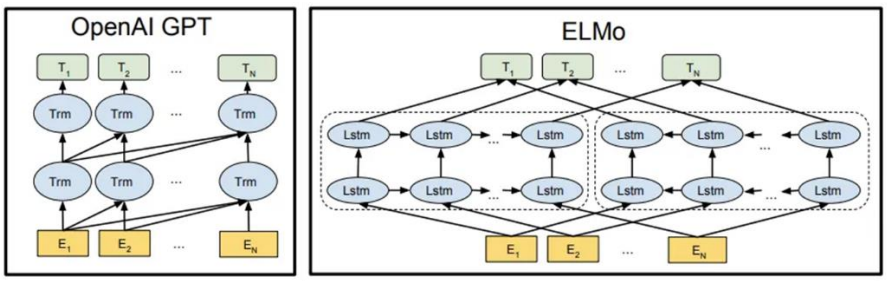


图 2-38 GPT 与 ELMo 的对比

BERT 对比这两个算法的优点是只有 BERT 表征会基于所有层中的左右两侧语境，这一点得益于 Transformer 中 Attention 机制将任意位置的两个单词的距离转换成了 1。

- **输入表示**

BERT 的输入的编码向量（长度是 512）是 3 个嵌入特征的单位和，如下图，这三个词嵌入特征是：

- WordPiece 嵌入[52]：WordPiece 是指将单词划分成一组有限的公共子词单元，能在单词的有效性和字符的灵活性之间取得一个折中的平衡。例如下图的示例中‘playing’被拆分成了‘play’和‘ing’；
- 位置嵌入（Position Embedding）：位置嵌入是指将单词的位置信息编码成特征向量，位置嵌入是向模型中引入单词位置关系的至关重要的一环。位置嵌入的具体内容参考我之前的分析；
- 分割嵌入（Segment Embedding）：用于区分两个句子，例如 B 是否是 A 的下文。对于句子对，第一个句子的特征值是 0，第二个句子的特征值是 1。

最后，说明一下下图中的两个特殊符号[CLS]和[SEP]，其中[CLS]表示该特征用于分类模型，对非分类模型，该符合可以省去。[SEP]表示分句符号，用于断开输入语料中的两个句子。

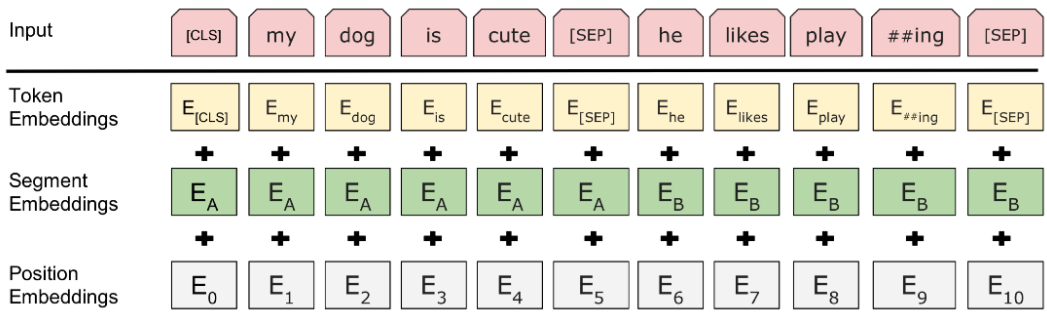


图 2-39 BERT 模型输入

- **预训练任务**

BERT 是一个多任务模型，它的任务是由两个自监督任务组成，即 MLM 和 NSP。

1）Task #1： Masked Language Model

Masked Language Model（MLM）和核心思想取自 Wilson Taylor 在 1953 年发表的一篇论文。所谓 MLM 是指在训练的时候随即从输入预料上 mask 掉一些单词，然后通过的上下文预测该单词，该任务非常像我们在中学时期经常做的完形填空。正如传统的语言模型算法和 RNN 匹配那样，MLM 的这个性质和 Transformer 的结构是非常匹配的。

在 BERT 的实验中，15%的 WordPiece Token 会被随机 Mask 掉。在训练模型时，一个句子会被多次喂到模型中用于参数学习，但是 Google 并没有在每次都 mask 掉这些单词，而是在确定要 Mask 掉的单词之后，80%的时候会直接替换为[Mask]，10%的时候将其替换为其它任意单词，10%的时候会保留原始 Token。

80%：my dog is hairy -> my dog is [mask]

10%：my dog is hairy -> my dog is apple

10%：my dog is hairy -> my dog is hairy

这么做的原因是如果句子中的某个 Token100%都会被 mask 掉，那么在 fine-tuning 的时候模型就会有一些没有见过的单词。加入随机 Token 的原因是因为 Transformer 要保持对每个输入 token 的分布式表征，否则模型就会记住这个[mask]是 token ‘hairy’。至于单词带来的负面影响，因为一个单词被随机替换掉的概率只有 15%*10% =1.5%，这个负面影响其实是可以忽略不计的。另外文章指出每次只预测 15%的单词，因此模型收敛的比较慢。

2）Task #2: Next Sentence Prediction

Next Sentence Prediction（NSP）的任务是判断句子 B 是否是句子 A 的下文。如果是的话输出‘IsNext’，否则输出‘NotNext’。训练数据的生成方式是从平行语料中随机抽取的连续两句话，其中 50%保留抽取的两句话，它们符合 IsNext 关系，另外 50%的第二句话是随机从预料中提取的，它们的关系是 NotNext 的。这个关系保存在 [CLS]符号中。

- **微调**

在海量单预料上训练完 BERT 之后，便可以将其应用到 NLP 的各个任务中了。对于 NSP 任务来说，其条件概率表示为 $P = softmax(CW^T)$，其中 C 是 BERT 输出中的[CLS]符号，W 是可学习的权值矩阵。

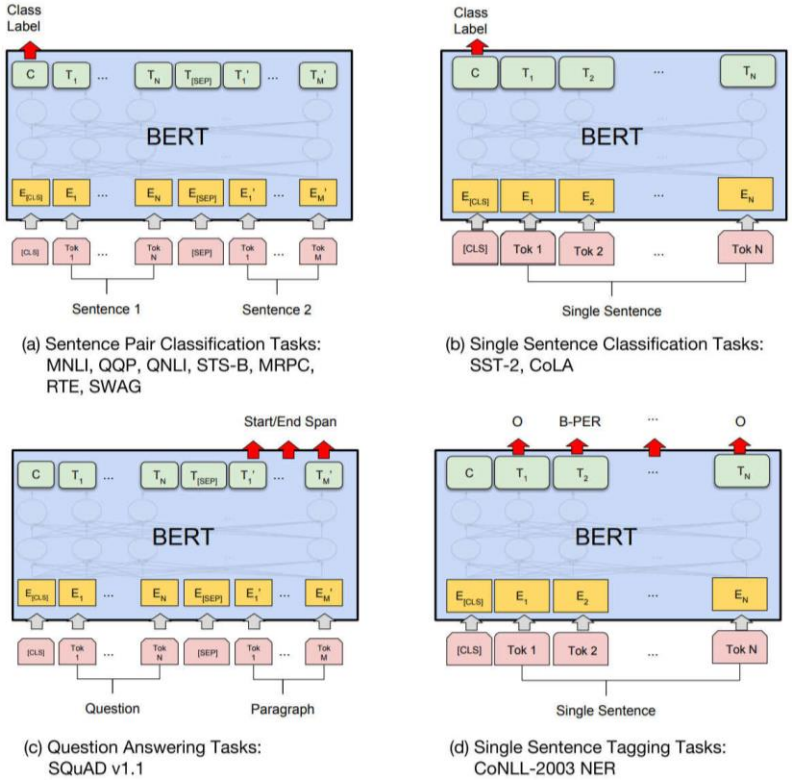


图 2-40 BERT 在不同任务中的模型

对于其它任务来说，我们也可以根据 BERT 的输出信息作出对应的预测。上图展示了 BERT 在 11 个不同任务中的模型，它们只需要在 BERT 的基础上再添加一个输出层便可以完成对特定任务的微调。这些任务类似于我们做过的文科试卷，其中有选择题，简答题等等。下图中其中 Tok 表示不同的 Token，E 表示嵌入向量，T_i 表示第 i 个 Token 在经过 BERT 处理之后得到的特征向量。

微调的任务包括：

（a）基于句子对的分类任务：

MNLI：给定一个前提，根据这个前提去推断假设与前提的关系。该任务的关系分为三种，蕴含关系、矛盾关系以及中立关系。所以这个问题本质上是一个分类问题，我们需要做的是去发掘前提和假设这两个句子对之间的交互信息。

QQP：基于 Quora，判断 Quora 上的两个问题句是否表示的是一样的意思。

QNLI：用于判断文本是否包含问题的答案，类似于我们做阅读理解定位问题所在的段落。

STS-B：预测两个句子的相似性，包括 5 个级别。

MRPC：也是判断两个句子是否是等价的。

RTE：类似于 MNLI，但是只是对蕴含关系的二分类判断，而且数据集更小。

SWAG：从四个句子中选择为可能为前句下文的那个。

（b）基于单个句子的分类任务

SST-2：电影评价的情感分析。

CoLA：句子语义判断，是否是可接受的。

对于 GLUE 数据集的分类任务（MNLI，QQP，QNLI，SST-B，MRPC，RTE，SST-2，CoLA），BERT 的微调方法是根据[CLS]标志生成一组特征向量 C，并通过一层全连接进行微调。损失函数根据任务类型自行设计，例如多分类的 softmax 或者二分类的 sigmoid。

SWAG 的微调方法与 GLUE 数据集类似，只不过其输出是四个可能选项的 softmax：

$$P_i = \frac{e^{V \cdot C_i}}{\sum_{j=1}^{4} e^{V \cdot C_i}}$$

（c）问答任务

SQuAD v1.1：给定一个句子（通常是一个问题）和一段描述文本，输出这个问题的答案，类似于做阅读理解的简答题。SQuAD 的输入是问题和描述文本的句子对。输出是特征向量，通过在描述文本上接一层激活函数为 softmax 的全连接来获得输出文本的条件概率，全连接的输出节点个数是语料中 Token 的个数。

$$P_i = \frac{e^{S \cdot T_i}}{\sum_j e^{S \cdot T_i}}$$

（d）命名实体识别

CoNLL-2003 NER：判断一个句子中的单词是不是 Person，Organization，Location，Miscellaneous 或者 other（无命名实体）。微调 CoNLL-2003 NER 时将整个句子作为输入，在每个时间片输出一个概率，并通过 softmax 得到这个 Token 的实体类别[53]。

- BERT 相关模型进展

BERT 自从在 arXiv 上发表以来获得了很大的成功和关注，打开了 NLP 中 2-Stage 的潘多拉魔盒。随后涌现了一大批类似于“BERT”的预训练（pre-trained）模型，有引入 BERT 中双向上下文信息的广义自回归模型 XLNet，也有改进 BERT 训练方式和目标的 RoBERTa 和 SpanBERT，还有结合多任务以及知识蒸馏（Knowledge Distillation）强化 BERT 的 MT-DNN 等。除此之外，还有人试图探究 BERT 的原理以及其在某些任务中表现出众的真正原因。以上种种，被戏称为 BERTology。本文尝试汇总上述内容

1）XLNet 及其与 BERT 的对比

BERT 是典型的自编码模型(Autoencoder)，旨在从引入噪声的数据重建原数据。而 BERT 的预训练过程采用了降噪自编码（Variational Autoencoder）思想，即 MLM（Mask Language Model）机制，区别于自回归模型（Autoregressive Model），最大的贡献在于使得模型获得了双向的上下文信息，但是会存在一些问题：

- Pretrain-finetune Discrepancy：预训练时的[MASK]在微调（fine-tuning）时并不会出现，使得两个过程不一致，这不利于 Learning。
- Independence Assumption：每个 token 的预测是相互独立的。而类似于 New York 这样的 Entity，New 和 York 是存在关联的，这个假设则忽略了这样的情况。

自回归模型不存在第二个问题，但传统的自回归模型是单向的。XLNet 团队想做的，就是让自回归模型也获得双向上下文信息，并避免第一个问题的出现。

他们主要使用了以下三个机制：

Permutation Language Model

Two-Stream Self-Attention

Recurrence Mechanism

接下来我们将分别介绍这三种机制

- **Permutation Language Model：**

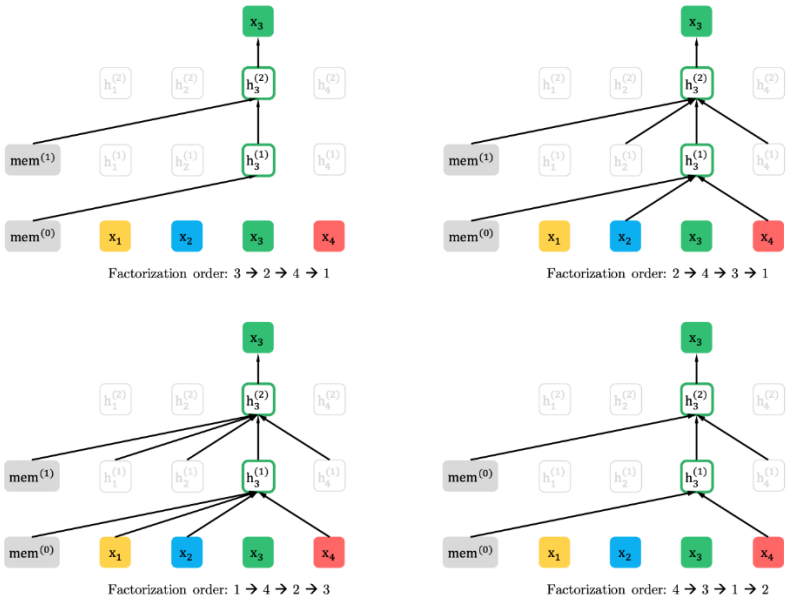


图 2-41 XLNet 模型框架图

在预测某个 token 时，XLNet 使用输入的 permutation 获取双向的上下文信息，同时维持自回归模型原有的单向形式。这样的好处是可以不用改变输入顺序，只需在内部处理。

它的实现采用了一种比较巧妙的方式：使用 token 在 permutation 的位置计算上下文信息。如对于，当前有一个 2 -> 4 ->3 ->1 的排列，那么我们就取出 token_2 和 token_4 作为 AR 的输入预测 token_3。不难理解，当所有 permutation 取完时，我们就能获得所有的上下文信息[54]。这样就得到了我们的目标公式：

$$\text{New Target:} \quad \max_{\theta} \quad \mathbb{E}_{\mathbf{z}\sim\mathcal{Z}_T}\left[\sum_{t=1}^{T}\log p_\theta(x_{z_t}\mid \mathbf{x}_{\mathbf{z}<t})\right]$$

但是在原来的公式中，我们只使用了 h_θ (x_(Z < t))来表示当前 token “上文” 的 hidden representation，使得不管模型要预测哪个位置的 token，如果“上文”一致，那么输出就是一致的。因此，新的公式做出了改变，引入了要预测的 token 的位置信息。

$$\text{Position Info:} \quad p_\theta(X_{z_t}=x\mid \mathbf{x}_{z<t})=\frac{\exp\left(e(x)^\top g_\theta(\mathbf{x}_{\mathbf{z}<t},z_t)\right)}{\sum_{x'}\exp\left(e(x')^\top g_\theta(\mathbf{x}_{\mathbf{z}<t},z_t)\right)}$$

此外，为了降低模型的优化难度，XLNet 使用了 Partial Prediction，即只预测当前 permutation 位置 c 之后的 token，最终优化目标如下所示：

$$\text{Partial Prediction:}$$

$$\max_{\theta} \quad \mathbb{E}_{\mathbf{z}\sim\mathcal{Z}_T}\left[\log p_\theta(\mathbf{x}_{\mathbf{z}>c}\mid \mathbf{x}_{\mathbf{z}\le c})\right]=\mathbb{E}_{\mathbf{z}\sim\mathcal{Z}_T}\left[\sum_{t=c+1}^{|\mathbf{z}|}\log p_\theta(x_{z_t}\mid \mathbf{x}_{\mathbf{z}<t})\right]$$

- **Two-Stream Self-Attention：**

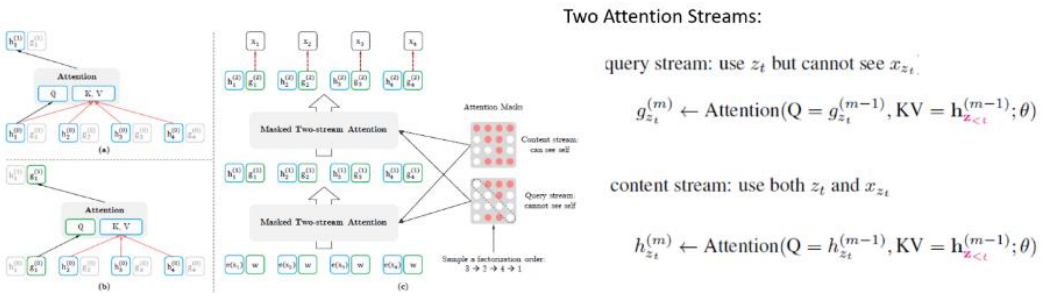


图 2-42 Two-Stream Self-Attention 机制

该机制所要解决的问题是，当我们获得了 g_θ (x_{Z<t},z_t)后，我们只有该位置信息以及“上文”的信息，不足以去预测该位置后的 token；而原来的 h_θ (x_{Z<t})则因为获取不到位置信息，依然不足以去预测。因此，XLNet 引入了 Two-Stream Self-Attention 机制，将两者结合起来。

- **Recurrence Mechanism：**

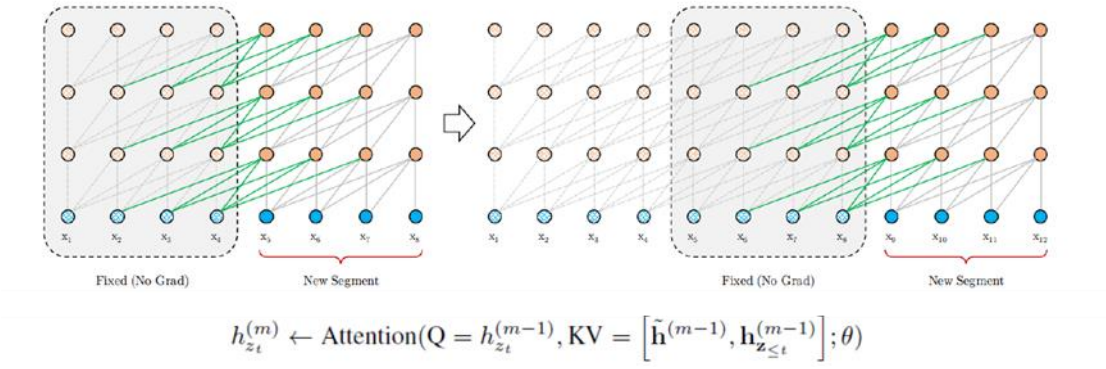


图 2-43 Recurrence Mechanism 机制

该机制来自 Transformer-XL[55]，即在处理下一个 segment 时结合上个 segment 的 hidden representation，使得模型能够获得更长距离的上下文信息。而在 XLNet 中，虽然在前端采用相对位置编码，但在表示 h_θ (x_{Z<t})的时候，涉及到的处理与 permutation 独立，因此还可以沿用这个机制。该机制使得 XLNet 在处理长文档时具有较好的优势。

- **XLNet 与 BERT 的区别示例：**

为了说明 XLNet 与 BERT 的区别，作者举了一个处理“NewYorkisacity”的例子。这个可以直接通过两个模型的公式得到。假设我们要处理 NewYork 这个单词，BERT 将直接 mask 这两个 tokens，使用“isacity”作为上下文进行预测，这样的处理忽略了 New 和 York 之间的关联；而 XLNet 则通过 permutation 的形式，可以使得模型获得更多如 York|New,isacity 这样的信息。

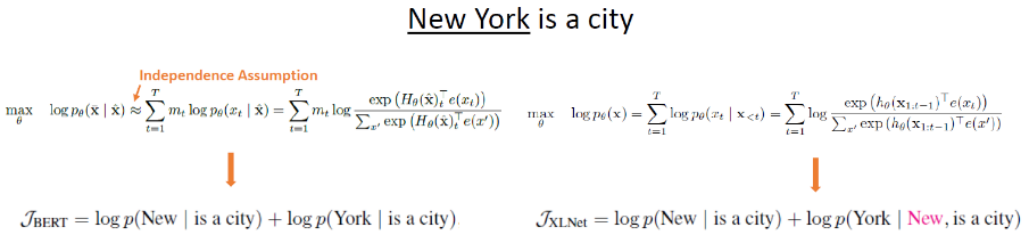


图 2-44 XLNet 与 BERT 的区别示例

2）RoBERTa: A Robustly Optimized BERT Pretraining Approach

RoBERTa 是最近 Facebook AI 联合 UW 发布的 BERT 预训练模型[56]，除了调参外，还引入了 Dynamically Change Mask Pattern 并移除 Next Sentence Prediction，使得模型在 GLUE Benchmark 排名第一，作者的观点是：BERT is significantly undertrained。

不同于原有的 BERT 的 MLM 机制，作者在总共 40 个 epoch 中使用 10 种不同的 MaskPattern，即每种 MaskPattern 训练 4 代，作为 static 策略；作者还引入了 dynamic masking 策略，即每输入一个 sequence 就为其生成一个 maskpattern。最终发现，新策略都比原 BERT 好，而 dynamic 总体上比 static 策略要好一些，并且可以用于训练更大的数据集以及更长的训练步数，因此最终选用 dynamicmaskingpattern。作者还通过替换 NSP 任务进行预训练。虽然 BERT 中已经做了尝试去掉 NSP 后的对比，结果在很多任务中表现会下降，但是包括前文 XLNet 团队所做的实验都在质疑这一结论。

选用的新策略包括：

Sentence-Pair+NSP Loss：与原 BERT 相同；

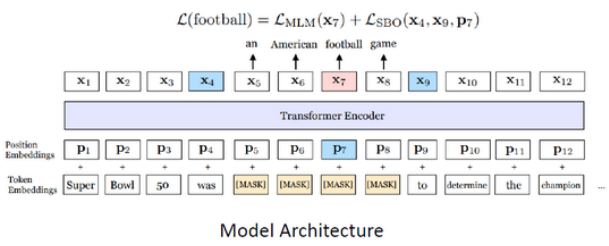
Segment-Pair+NSP Loss：输入完整的一对包含多个句子的片段，这些片段可以来自同一个文档，也可以来自不同的文档；

Full-Sentences：输入是一系列完整的句子，可以是来自同一个文档也可以是不同的文档；

Doc-Sentences：输入是一系列完整的句子，来自同一个文档；

结果发现完整句子会更好，来自同一个文档的会比来自不同文档的好一些，最终选用 Doc-Sentences 策略。

3）SpanBERT: Improving Pre-training by Representing and Predicting Spans



Model Architecture

	CoLA	SST-2	MRPC	STS-B
Google BERT	59.3	**95.2**	88.5/84.3	86.4/88.0
Our BERT	58.6	93.9	90.1/86.6	88.4/89.1
Our BERT-1seq	63.5	94.8	**91.2**/87.8	89.0/88.4
SpanBERT	**64.3**	94.8	90.9/**87.9**	**89.9/89.1**

QQP	MNLI	QNLI	RTE	(Avg)
71.2/89.0	86.1/85.7	93.0	71.1	80.4
71.8/89.3	87.2/86.6	93.0	74.7	81.1
72.1/89.5	88.0/87.4	93.0	72.1	81.7
71.9/**89.5**	**88.1/87.7**	**94.3**	**79.0**	**82.8**

SpanBERT in GLUE Test

- Span Masking
- Span Boundary Objective
- Single-Sequence Training

图 2-45 panBER 模型框架以及在 GLUE 中的实验结果

不同于 RoBERTa，SpanBERT 通过修改模型的预训练任务和目标使模型达到更好的效果[57]。其修改主要是三个方面：

SpanMasking：这个方法与之前 BERT 团队放出 WWM（WholeWordMasking）类似，即在 mask 时 mask 一整个单词的 token 而非原来单个 token。每次 mask 前，从一个几何分布

中采样得到需要 mask 的 span 的长度，并等概率地对输入中为该长度的 span 进行 mask，直到 mask 完 15%的输入。

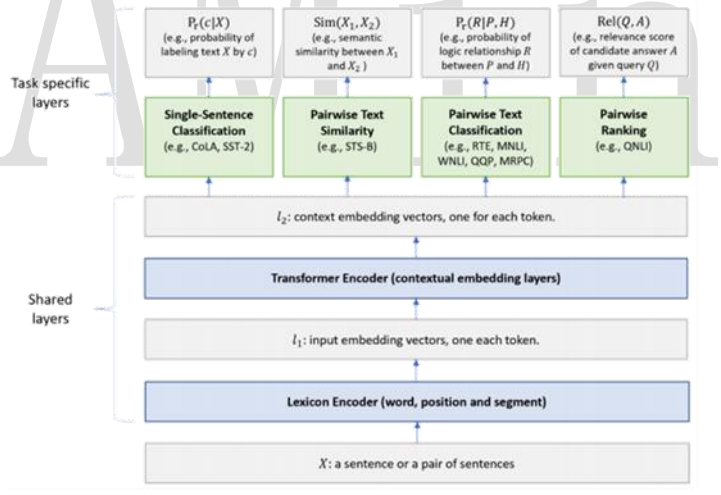
SpanBoundaryObject：使用 span 前一个 token 和末尾后一个 token 以及 token 位置的 fixed-representation 表示 span 内部的一个 token，并以此来预测该 token，使用交叉熵作为新 loss 加入到最终的 loss 函数中。该机制使得模型在 Span-Level 的任务种能获得更好的表现。

Single-SequenceTraining：直接输入一整段连续的 sequence，这样可以使得模型获得更长的上下文信息。

在这三个机制下，SpanBERT 使用与 BERT 相同的语料进行训练，最终在 GLUE 中获得 82.8 的表现，高于原版 GoogleBERT2.4%，高于他们调参后的 BERT1%，同时在 CoreferenceResolution 上将最好结果提高了 6.6%。

4）MT-DNN 与知识蒸馏

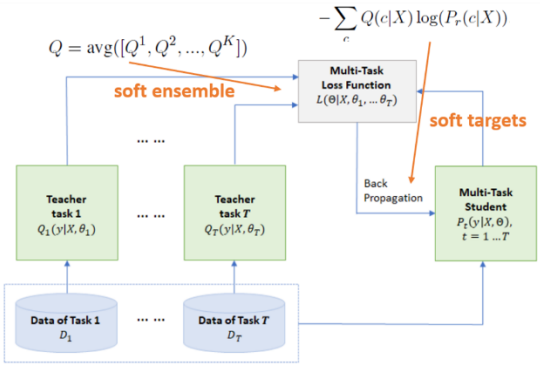
Multi-Task Deep Neural Networks for Natural Language Understanding 这篇论文旨在将 Multi-Task 与 BERT 结合起来，使得模型能在更多的数据上进行训练的同时还能获得更好的迁移能力（Transfer Ability）[58]。



Algorithm 1: Training a MT-DNN model.
Initialize model parameters Θ randomly.
Pre-train the shared layers (i.e., the lexicon encoder and the transformer encoder).
Set the max number of epoch: $epoch_{max}$.
//Prepare the data for T tasks.
for t *in* $1, 2, ..., T$ **do**
  Pack the dataset t into mini-batch: D_t.
end
for $epoch$ *in* $1, 2, ..., epoch_{max}$ **do**
  1. Merge all the datasets: $D = D_1 \cup D_2 ... \cup D_T$
  2. Shuffle D
  for b_t *in* D **do**
    //b_t is a mini-batch of task t.
    3. Compute loss : $L(\Theta)$
      $L(\Theta)$ = Eq. 6 for classification
      $L(\Theta)$ = Eq. 7 for regression
      $L(\Theta)$ = Eq. 8 for ranking
    4. Compute gradient: $\nabla(\Theta)$
    5. Update model: $\Theta = \Theta - \epsilon\nabla(\Theta)$
  end
end

图 2-46 MT-DNN 模型框架以及训练算法

模型架构如上图所示，在输入以及 Transformer 层，采用与 BERT 相同的机制，但是在后续处理不同任务数据时使用不同的任务参数与输出的表示做点积（Dot Production），用不同的激活函数（Activation Function）和损失函数（Loss Function）进行训练。



Process of Knowledge Distillation

Model	CoLA 8.5k	SST-2 67k	MRPC 3.7k	STS-B 7k	QQP 364k
BiLSTM+ELMo+Attn [1]	36.0	90.4	84.9/77.9	75.1/73.3	64.8/84.7
Singletask Pretrain Transformer [2]	45.4	91.3	82.3/75.7	82.0/80.0	70.3/88.5
GPT on STILTs [3]	47.2	93.1	87.7/83.7	85.3/84.8	70.1/88.1
$\text{BERT}_{\text{LARGE}}$ [4]	60.5	94.9	89.3/85.4	87.6/86.5	72.1/89.3
MT-DNN [5]	61.5	95.6	90.0/86.7	88.3/87.7	72.4/89.6
Snorkel MeTaL [6]	63.8	**96.2**	91.5/88.5	**90.1/89.7**	73.1/89.9
ALICE *	63.5	95.2	**91.8/89.0**	89.8/88.8	**74.0/90.4**
$\textbf{MT-DNN}_{\text{KD}}$	**65.4**	95.6	91.1/88.2	89.6/89.0	72.7/89.6
Human Performance	66.4	97.8	86.3/80.8	92.7/92.6	59.5/80.4

MNLI-m/mm 393k	QNLI 108k	RTE 2.5k	WNLI 634	AX	Score
76.4/76.1	79.8	56.8	65.1	26.5	70.0
82.1/81.4	87.4	56.0	53.4	29.8	72.8
80.8/80.6	-	69.1	65.1	29.4	76.9
86.7/85.9	92.7	70.1	65.1	39.6	80.5
86.7/86.0	-	75.5	65.1	40.3	82.2
87.6/87.2	93.9	80.9	65.1	39.9	83.2
87.9/87.4	95.7	80.9	65.1	40.7	83.3
87.5/86.7	**96.0**	**85.1**	65.1	**42.8**	**83.7**
92.0/92.8	91.2	93.6	95.9	-	87.1

MT-DNN_{KD} in GLUE Test

图 2-47 使用知识蒸馏对 MT-DNN 模型进行优化

由于 MT-DNN 可以看作一个 ensemble 过程，所以就可以用知识蒸馏（KnowledgeDistillation）进行优化[58]，该方法能提升很多 ensemble 模型的表现本文的知识蒸馏过程即对于不同的任务，使用相同的结构在对应的数据集上进行微调，这就可以看作每个任务的 Teacher，他们分别擅长解决对应的问题。Student 则去拟合 targetQ，并且使用 soft 交叉熵损失（CrossEntropyLoss）。为什么使用 soft 交叉熵损失呢？因为有些句子的意思可能并不是绝对的，比如“Ireallyenjoyedtheconversationwith Tom"有一定概率说的是反语，而不是 100%的积极意思。这样能让 Student 学到更多的信息。采用知识蒸馏后，模型在 GLUE 中的表现增长了 1%，目前排名前三。我们还可以期待 MT-DNN 机制在 XLNet 上等其他预训练模型中的表现[60]。

2.8 卷积与图卷积

2.8.1 卷积

两个函数的卷积，本质上就是先将一个函数翻转，然后进行滑动叠加。在连续情况下，叠加指的是对两个函数的乘积求积分，在离散情况下就是加权求和，为简单起见就统一称为叠加。教科书上一般定义函数 f, g 的卷积 $f * g(n)$如下：

连续形式：

$$(f * g)(n) = \int_{-\infty}^{\infty} f(\tau)g(n-\tau)d\tau$$

离散形式：

$$(f * g)(n) = \sum_{\tau=-\infty}^{\infty} f(\tau)g(n-\tau)$$

从计算的方式上对公式进行的解释为：先对 g 函数进行翻转，相当于在数轴上把 g 函数从右边褶到左边去，也就是卷积的“卷”的由来。然后再把 g 函数平移到 n，在这个位置对两个函数的对应点相乘，然后相加，这个过程是卷积的“积”的过程。整体看来是这么个过程：

翻转→滑动→叠加→滑动→叠加→滑动→叠加

多次滑动得到的一系列叠加值，构成了卷积函数。卷积的“卷”，指的的函数的翻转，从 $g(t)$变成 $g(-t)$的这个过程；同时，“卷”还有滑动的意味在里面。如果把卷积翻译为“褶积”，那么这个“褶”字就只有翻转的含义了。卷积的“积”，指的是积分/加权求和。对卷积的意义的理解如下：

1）从“积”的过程可以看到，我们得到的叠加值，是个全局的概念。以信号分析为例，卷积的结果是不仅跟当前时刻输入信号的响应值有关，也跟过去所有时刻输入信号的响应都有关系，考虑了对过去的所有输入的效果的累积。在图像处理的中，卷积处理的结果，其实就是把每个像素周边的，甚至是整个图像的像素都考虑进来，对当前像素进行某种加权处理。所以说，“积”是全局概念，或者说是一种“混合”，把两个函数在时间或者空间上进行混合。

2）进行“卷”（翻转）的目的其实是施加一种约束，它指定了在“积”的时候以什么为参照。在信号分析的场景，它指定了在哪个特定时间点的前后进行“积”，在空间分析的场景，它指定了在哪个位置的周边进行累积处理。

下面通过丢骰子的实例进一步解释卷积：

有两枚骰子，把它们都抛出去，两枚骰子点数加起来为 4 的概率是多少?

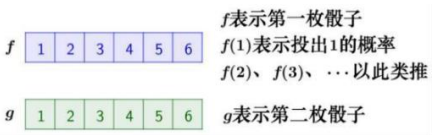


图 2-48 骰子点数示意图

分析一下，两枚骰子点数加起来为 4 的情况有三种情况：1+3=4, 2+2=4, 3+1=4；因此，两枚骰子点数加起来为 4 的概率为：$f(1)g(3)+f(2)g(2)+f(3)g(1)$，写成卷积的方式就是：

$$(f*g)(4)=\sum_{m=1}^{3}f(4-m)g(m)$$

首先，因为两个骰子的点数和是 4，为了满足这个约束条件我们还是把函数 g 翻转一下，然后阴影区域上下对应的数相乘再累加，相当于求自变量为 4 的卷积值，如下图所示：

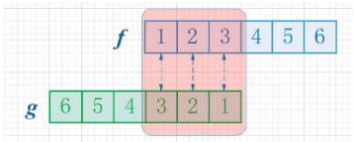


图 2-49 点数和为 4 的卷积示意图

进一步，如此翻转以后，可以方便地进行推广去求两个骰子点数和为 n 时的概率，为 f 和 g 的卷积 $f*g(n)$，如下图所示：

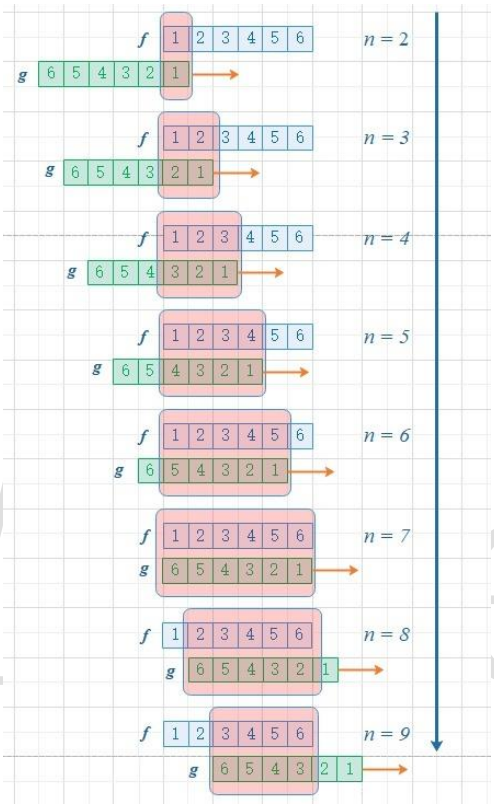


图 2-50 点数和为 n 的卷积示意图

由上图可以看到，函数 g 的滑动，带来的是点数和的增大。这个例子中对 f 和 g 的约束条件就是点数和，它也是卷积函数的自变量。有兴趣还可以算算，如果骰子的每个点数出现的概率是均等的，那么两个骰子的点数和 $n = 7$ 的时候，概率最大[61]。

2.8.2 图卷积

要理解图卷积网络的核心操作图卷积，可以类比卷积在 CNN 的地位。如下图所示，数字图像是一个二维的离散信号，对数字图像做卷积操作其实就是利用卷积核（卷积模板）在图像上滑动，将图像点上的像素灰度值与对应的卷积核上的数值相乘，然后将所有相乘后的值相加作为卷积核中间像素对应的图像上像素的灰度值，并最终滑动完所有图像的过程。

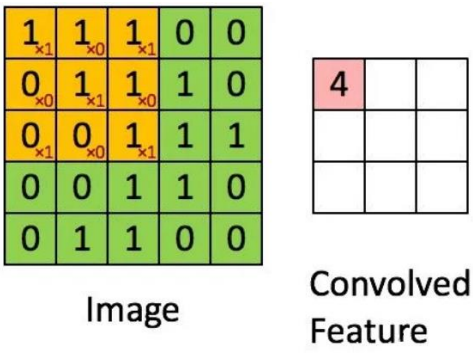


图 2-51 图卷积示意图

现实中更多重要的数据集都是用图的形式存储的，例如社交网络信息、知识图谱、蛋白质网络、万维网等等。这些图网络的形式并不像图像，是排列整齐的矩阵形式，而是非结构化的信息，那有没有类似图像领域的卷积一样，有一个通用的范式来进行图特征的抽取呢？这就是图卷积在图卷积网络中的意义。对于大多数图模型，有一种类似通式的存在，这些模型统称图卷积网络。因此可以说，图卷积是处理非结构化数据的大利器，随着这方面研究的逐步深入，人类对知识领域的处理必将不再局限于结构化数据，会有更多的目光转向这一存在范围更加广泛，涵盖意义更为丰富的知识领域。

- 图的定义：

对于图，我们有以下特征定义：

对于图 G =（V，E），V 为节点的集合，E 为边的集合，对于每个节点 i，均有其特征 xi，可以用矩阵 XN*D 表示。其中 N 表示节点数，*D* 表示每个节点的特征数，也可以说是特征向量的维度。图中的每个结点无时无刻不因为邻居和更远的点的影响而在改变着自己的状态直到最终的平衡，关系越亲近的邻居影响越大。

- 图相关矩阵的定义：

邻接矩阵和拉普拉斯矩阵可以用来度量节点的邻居节点这个关系。举个简单的例子，对于下图中的左图（为了简单起见，举了无向图且边没有权重的例子）而言，它的度矩阵 *D*，邻接矩阵 *A* 和拉普拉斯矩阵 *L* 分别如下图所示，度矩阵 *D* 只有对角线上有值，为对应节点的度，其余为 0；邻接矩阵 *A* 只有在有边连接的两个节点之间为 1，其余地方为 0；拉普拉斯矩阵 *L* 为 *D-A*。但需要注意的是，这是最简单的一种拉普拉斯矩阵，除了这种定义，还有接下来介绍的几种拉普拉斯矩阵。

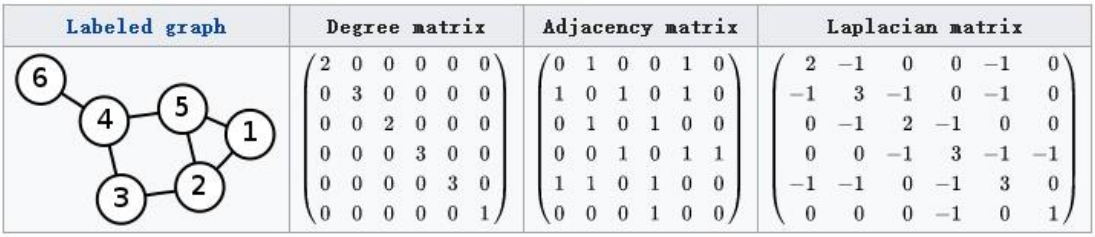


图 2-52 一个图的度矩阵、邻接矩阵和拉普拉斯矩阵

- 图卷积的通式：

任何一个图卷积层都可以写成这样一个非线性函数：

$$H^{l+1} = f(H^l, A)$$

$H^0 = X$ 为第一层的输入，$X \in R^{N*D}$，N 为图的节点个数，D 为每个节点特征向量的维度，A 为邻接矩阵，不同模型的差异点在于函数 f 的实现不同。

下面介绍几种具体的实现，但是每一种实现的参数大家都统称拉普拉斯矩阵。

实现一：

$$H^{l+1} = \sigma(AH^lW^l)$$

其中 W^l 为第 l 层的权重参数矩阵，$\sigma(\cdot)$为非线性激活函数，例如 ReLU。这种思路是基于节点特征与其所有邻居节点有关的思想。邻接矩阵 A 与特征 H 相乘等价于某节点的邻居节点的特征相加。这样多层隐含层叠加，能利用多层邻居的信息。但这样存在两个问题：1）没有考虑节点自身对自己的影响；2）邻接矩阵 A 没有被规范化，这在提取图特征时可能存在问题，比如邻居节点多的节点倾向于有更大的影响力。因此实现二和实现三针对这两点进行了优化。

实现二：

$$H^{l+1} = \sigma(LH^lW^l)$$

拉普拉斯矩阵 $L = D\text{-}A$，学名 Combinatorial Laplacian，是针对实现一的问题 1 的改进：引入了度矩阵，从而解决了没有考虑自身节点信息自传递的问题。

实现三：

$$H^{l+1} = \sigma(D^{-\frac{1}{2}}\hat{A}D^{-\frac{1}{2}}H^lW^l)$$

对于这里的拉普拉斯矩阵 $L^{sym} = D^{-\frac{1}{2}}\hat{A}D^{-\frac{1}{2}} = D^{-\frac{1}{2}}(D-A)D^{-\frac{1}{2}} = I_n - D^{-\frac{1}{2}}AD^{-\frac{1}{2}}$，学名 Symmetric normalized Laplacian，也有论文或者博客写为 $L = I_n + D^{-\frac{1}{2}}AD^{-\frac{1}{2}}$，就是一个符号的

差别，但本质上还是对实现一的两个问题进行的改进：1）引入自身度矩阵，解决自传递问题；2）对邻接矩阵的归一化操作，通过对邻接矩阵两边乘以节点的度开方然后取逆得到。具体到每一个节点对 *i*、*j*，矩阵中的元素由下面的式子给出（对于无向无权图）：

$$L_{i,j}^{\text{sym}} := \begin{cases} 1 & \text{if } i = j \text{ and } \deg(v_i) \neq 0 \\ -\frac{1}{\sqrt{\deg(v_i)\deg(v_j)}} & \text{if } i \neq j \text{ and } v_i \text{ is adjacent to } v_j \\ 0 & \text{otherwise.} \end{cases}$$

其中 deg(vi), deg(vj)分别为节点 i, j 的度，也就是度矩阵在节点 i, j 处的值。

我们回顾下矩阵的逆的定义，对于式子 A * X = B，假如我们希望求矩阵 X，那么当然是令等式两边都乘以 A-1，然后式子就变成了 X = A-1 * A * X = A-1B。举个例子对于，单个节点运算来说，做归一化就是除以它节点的度，这样每一条邻接边信息传递的值就被规范化了，不会因为某一个节点有 10 条边而另一个只有 1 条边导致前者的影响力比后者大，因为做完归一化后者的权重只有 0.1 了，从单个节点上升到二维矩阵的运算，就是对矩阵求逆了，乘以矩阵的逆的本质，就是做矩阵除法完成归一化。但左右分别乘以节点 i, j 度的开方，就是考虑一条边的两边的点的度。

上面是以矩阵的形式计算，可能会看起来非常让人疑惑，下面从单个节点的角度来重新看下这些个公式（本质是一样的，上文解释过，对于单个节点就是除法，对于矩阵就是乘以度矩阵的逆），对于第 l+1 层的节点的特征h_i^{l+1}，对于它的邻接节点 j ∈ N，N 是节点 i 的所有邻居节点的集合，可以通过以下公式计算得到：

$$h_i^{l+1} = \sigma(\sum_j \frac{1}{c_{ij}} h_{v_j}^l W^l)$$

其中，$c_{i,j} = \sqrt{d_i d_j}$，$j \in N_i$，N_i 为 *i* 的邻居节点，*di*, *dj* 为 *i*, *j* 的度，这跟上面的公式其实是等价的，所以有些地方的公式是这个，有些的上面那个[62]。

2.9 隐私保护

2019 年，清华大学人工智能研究院长张钹院士、唐杰教授、李涓子教授等人联合发起“AI TIME”science debate，希望用辩论的形式，探讨人工智能和人类未来之间的矛盾，探索人工智能领域的未来。AI TIME 是一群关注人工智能发展，并有思想情怀的青年人创办的圈子。AI TIME 旨在发扬科学思辨精神，邀请各界人士对人工智能理论、算法、场景、应用的本质问题进行探索，加强思想碰撞，打造成为北京乃至全国知识分享的聚集地。

在“AI TIME 4”及“AI TIME in U 之走进北邮”活动中，受邀的专家对隐私保护以及机器学习与隐私保护的联系展开了深入的探讨。

2.9.1 AI TIME 4

如何处理数据共享与隐私保护之间的矛盾早已成为了当前数据圈的热议话题，AI TIME 4 邀请到了明略科技集团首席科学家吴信东教授、清华大学计算机系朱小燕教授、清华大学交叉信息研究院徐葳副教授，以及微众银行人工智能部副总经理吴海山博士，共同论道了“数据共享开放与隐私保护”这个似乎高深，又与每个人息息相关的话题。

- 数据开放的三大必要条件

我们共享位置信息以便预约车的司机找到自己，也暴露了自己的行踪；用浏览纪录调教 APP 获得更合心意的推荐，也让个人喜好一览无余。开放个人数据的同时，我们冒着暴露隐私的危险，也享受着它带来的便利。有统计数据显示，每天全世界会上传 5 亿张图片，每分钟就有 20 小时的视频被分享，我们整个人类文明所产生的全部数据中有 90%是过去两年所产生的。有人说，发挥数据的价值，主要在流通。的确，数据共享可以使更多的人充分地使用已有数据资源，减少资料收集、数据采集等重复劳动和相应费用，而把精力重点放在开发新的应用程序及系统集成上。但是，要真的让数据流通起来，需要以下这些必要条件：

数据资源的标准化

数据开放共享，首先要做到的就是数据资源的标准化。我们需要解决大规模的、来自多个来源的、异构的数据集成问题，实现海量多元异构数据源的统一管理。

数据质量

数据质量是数据开放共享中需要解决的关键问题。比如，对于数据的发布者来说，怎么样来保证开放的数据没有敏感内容，怎么样保证这个数据是可信的？自动的评估和控制数据质量，是一个关键指标。明略科技集团首席科学家、IEEE Fellow 吴信东教授介绍了他最近发表在《软件学报》上的“数据治理技术”论文，强调数据治理包括数据规范、数据清洗、数据交换和数据集成。

开放和共享不等于免费

清华大学计算机系朱小燕教授提到“开放和共享不等于免费”，分配权益，其实也是数据流通的基本动力，必须要保证数据的拥有者，持有者和开发者，都能有满意的权益分配。

- 数据共享和开放在产业界的趋势和挑战

清华大学交叉信息研究院徐葳副教授提到，“来自业内的数据可能不如分布在地方政府手里的数据多，但是很多人会明显觉得 BAT 似乎把数据用的更好。那是因为业内特定领域已经打通了数据并且形成了闭环，他们更清楚数据应该怎么使用，理解根据这些使用需要采

集怎样的数据、怎样去对数据进行清洗。”的确，数据必须要流动起来它才能产生价值，否则的话它就是一个孤岛，没有什么太大的价值。数据共享，也需要一个前后背景，以学术研究还是产业应用为前提进行共享，这两者的管理治理完全不一样。

以金融行业为例，微众银行人工智能部副总经理吴海山认为，金融行业对数据的应用和管控会更加严格。比如，如果用来投资，被标为非公开信息的数据会被禁止使用。而关于个人用户隐私层面的管控可能更严，在金融领域里面，有一种“另类数据”。它不是类似传统银行财报这样公开的信息，而是一种新型的数据，比如卫星遥感图像、手机上的 GPS 数据、网站 APP 下载的数据。这些也可以用来分析一个公司或者一个国家经济层面的运转程度。

- “离开数据服务谈数据隐私都是耍流氓”

机器学习需要大量数据，数据的共享无疑是学界和业界共同期待的，但是数据的共享也离不开对于数据和隐私的保护。

对于用户隐私的保护，几位专家有不同的看法。徐葳教授认为隐私是一种个人感受；吴信东教授认为企业的隐私就是其核心竞争力。

而吴海山博士则认为隐私的背后意味着数据是一种资产，“我们去看病的时候，恨不得把所有的信息都告诉医生，我们买房子贷款的时候，恨不得把以往所有的信息都给银行看，才能让它给你贷款。这个时候数据已经作为一种资产，有一个隐含的定价前提。你得到更好的金融服务，得到更好的企业服务，个性化服务。所以谈任何个人隐私、企业隐私，其背后都有服务和隐私之间的一个平衡，这是在讨论隐私之前需要关注的问题”。

- 数据加密技术大盘点

大数据生命周期分为数据发布、数据储存、分析和挖掘、数据使用，在这些环节中都存在数据隐私保护的问题。加密是保护数据的一个手段，但是加密之后的数据无法使用。现在的技术需要保证数据在流通使用过程中也不造成泄露，也就是限制数据的使用。在沙龙现场，几位嘉宾也探讨了目前几种常见的数据加密技术。

差分隐私

差分隐私其实是一种度量方式。通过一群人里算出来的模型，和去除 A 算出来的是一样的，这样就无从判断 A 是否还在这群人中，就起到保护 A 隐私的作用。这个方法对于保护“泯然众人”的数据是有用的，但是却很难保护那些“很个性”的数据，因为这些“个性”的数据对于整体数据的计算印象很大。

安全多方计算

安全多方计算（SMC,Secure Multi-Party Computation）是解决一组互不信任的参与方之间保护隐私的协同计算问题，SMC 要确保输入的独立性，计算的正确性，同时不泄露各输入值给参与计算的其他成员。主要是针对无可信第三方的情况下，如何安全地计算一个约定函数的问题，在电子选举、电子投票、电子拍卖、秘密共享、门限签名等场景中有着重要的作用。

k 匿名

k-匿名技术是 1998 年由 Samarati 和 Sweeney 提出的,要求发布的数据中存在一定数量（至少为 k）的在准标识符上不可区分的记录,使攻击者不能判别出隐私信息所属的具体个体,从而保护了个人隐私。吴信东教授举例解释，“比如在西方国家，为了避免报警者受到报复，警察记录的是方圆多少距离的人打来的报警电话，通过对位置信息的泛化，保护了报警者的位置信息，但同时也会降低数据的可用性。可能警察记录是五公里以内的人打了电话，但是警察自己也找不到那个人是谁”。吴教授也介绍了他 2003 年在 TKDE 上同中南大学张师超教授一起发表的 Local Analysis 方法，这种方法利用本地学习的思想做信息保护和模型共享，但模型共享可能还是有信息保护的顾虑。

- 隐私保护的政策问题

2018 年 5 月 25 日，欧洲联盟出台《通用数据保护条例》（GDPRGeneral Data Protection Regulation）。这是全球目前最严格的数据保护条例。其最高的一笔罚单给了英国航空公司，罚金数额为 1.8339 亿英镑（约合 15.8 亿元人民币）。

国际方面对于数据保护的政策愈发严格，中国在保护个人信息方面也发布了推荐性国家标准《信息安全技术个人信息安全规范》，可以说在数据隐私保护规定方面,中国走在了亚洲前列。这项规范也参考了欧盟的《通用数据保护条例》，ISO29000 系列等国际范围内的个人信息保护法律法规及标准，同时也从国内主要存在的个人信息保护现状和问题出发制定标准，更侧重标准的实用性。

欧盟《通用数据保护条例》（即 GDPR）的制定确实在一定程度上保护了数据，但是也阻碍了欧洲人工智能产业的发展。而且，因为 GDPR 罚款高达公司全球营业额的 4%，这对传统产业的企业很不友好、也不利于小公司的生存和发展。

从政策制定角度来讲，隐私保护政策需要可操作性以及合理合法的指导，让受众接受这条政策并积极施行。从经济学角度来讲，隐私保护政策会提高数据的价值，毕竟数据本身就是一种资产。

更严的隐私无疑会增加数据的成本，让整个行业尤其是小公司生存更加困难；更开放的数据共享，只会让大众和媒体放大数据隐私的侵犯，反而忘记数据共享带来的价值。我们需要的是灵活的隐私保护和数据共享方案。

2.9.2 AI TIME in U

2019 年 11 月 29 日，初雪的北京，AI TIME in U 之走进北京邮电大学。本次活动由北京邮电大学张忠宝副教授和 AI TIME 的何芸老师主持，特别邀请到了清华大学计算机系唐杰教授，中科院计算所研究员沈华伟，北京邮电大学程祥副教授和中国计算机学会中文信息技术专委委员李磊博士。来自学术界与工业界的四位大咖就大家广泛关注的“智能与隐私”的相关问题，围坐、论道“机器学习与隐私保护”。

智能时代，你的隐私如何得到保护？

- 唐杰教授提到在技术发展的初期阶段，可能可以放松对隐私保护的要求，而需要加大力度推进 AI。近年来，随着技术的快速发展，隐私保护日益受到关注。对个人隐私保护至关重要。但是目前大家的关注度还不够。在隐私保护、数据共享方面，企业方面需要做到以下两点。第一，坚决不要做恶；第二，数据不能随意交换。有些场景下，如果需要做某种数据分享，联邦学习或许是一个解决之道，这也是未来机器学习和人工智能发展的一个可能趋势。
- 针对这个话题，沈华伟总结了三点：一是隐私保护需要一个过程；二是隐私保护的尺度需要技术和规则的磨合，不是一成不变；三是隐私保护一定程度上依赖于 AI 技术，AI 技术发展到一定程度，会以更好的方式为大家提供服务，不觉得你的隐私被使用了。AI 和隐私保护技术之间需要一个平衡，法律和技术都可以使这个平衡过程逐渐向一个好的去向发展。
- 从工业界角度讲，李磊博士则认为，对于负责任的公司来讲，用户隐私永远是第一重要的，可以通过法律法规，还有技术来保护。至于在数据层面使用什么样的技术进行保护，随着机器学习技术的不断更新，隐私保护技术也应该不断更新。
- 程祥教授则认为从数据源头上保护隐私之后，深度学习、机器学习还需不需要隐私保护？从源头来讲，从数据信息的角度，对数据信息加了隐私保护，看上去就不再需要机器学习和隐私保护了。还有一些场景，例如银行或者公安机关、医院，如果把所学模型的参数发布出去，可以反推出样本当中的敏感信息。如果是可信的数据收集者，收集的是真实信息，对于发布出来的学习模型或者是统计信息，也需要做一些保护，否则可以通过所学习到的模型或者统计信息，推断出样本当中的敏感信息。

机器学习与隐私保护究竟路在何方？经过 2 个多小时的思辨与互动，得到以下结论：

- 机器学习应用在工业界中的瓶颈在于性能和能耗，而学术界应该比工业界看得更远。例如对于多源机器学习的形式化/数学定义、概率表示与概率编程、逻辑和深度学习的结合等。

- 目前处在人工智能的第三阶段，下一波的研究浪潮可能会是推理；Pre-train 在文本和图像领域发展迅猛，他可能是一个实现推理的方法；也可能仍然需要超大规模的知识图谱。知识图谱最终也许走向知识自动化，一旦走到这个地步，它可能以另外一种形式存在。

- 只发展 AI，不谈隐私，或者只顾隐私，不发展 AI，是两个极端。两者需要磨合才能做到相辅相成，共同发展。隐私保护技术需要全新的发展，传统的方法如：差分隐私、k-anonymity 法、基于 Dimensionality-reduction 方法、联邦学习以及数据加密的方法。这些方法可能都还不足以解决目前的隐私安全隐患问题。因此，需要技术和隐私保护公共政策的共同发展。

在未来阶段，我们期待让机器能够真正具有认知能力，能够自主地解决问题，或者说具备如同科幻电影中那样自主思考的能力。虽然显得十分遥远，但随着科技的爆发，谁能确定现在的科幻是不是未来平淡无奇的技术？在未来，数据融合用于提供更智能化的服务是不可阻挡的趋势，但是不管是在法律层面还有技术层面，我们都应该给予更高的关注度来加强公众的隐私保护意识。

机器学习与隐私保护并不是一场零和博弈。近年来提出的差分隐私和联邦学习技术为在保护数据贡献者部分隐私的条件下实现有效的机器学习提供了可能的思路。人们在未来需要去探索的，正是机器学习与隐私保护中的那个平衡的度，那个能让人们既能享受到机器学习带来的便利，又能确保自己所认为的个人隐私不会被泄露出去的平衡点。如何发现这个度？如何去界定这个度？我们期待未来二者的发展能带给我们答案。

如今，AI Time 已经发展成为系列活动，包括：AI Time Debate、AI Time PhD、AI Time in U 等，欢迎大家关注“AI Time 论道”公众号，与我们共同关注 AI 焦点。

3 深度学习篇

深度学习是近 10 年机器学习领域发展最快的一个分支，由于其重要性，三位教授（Geoffrey Hinton、Yann Lecun、Yoshua Bengio）因此同获图灵奖。深度学习模型的发展可以追溯到 1958 年的感知机（Perceptron）。1943 年神经网络就已经出现雏形（源自 NeuroScience），1958 年研究认知的心理学家 Frank 发明了感知机，当时掀起一股热潮。后来 Marvin Minsky（人工智能大师）和 Seymour Papert 发现感知机的缺陷：不能处理异或回路等非线性问题，以及当时存在计算能力不足以处理大型神经网络的问题。于是整个神经网络的研究进入停滞期。

最近 30 年来取得快速发展。总体来说，主要有 4 条发展脉络。

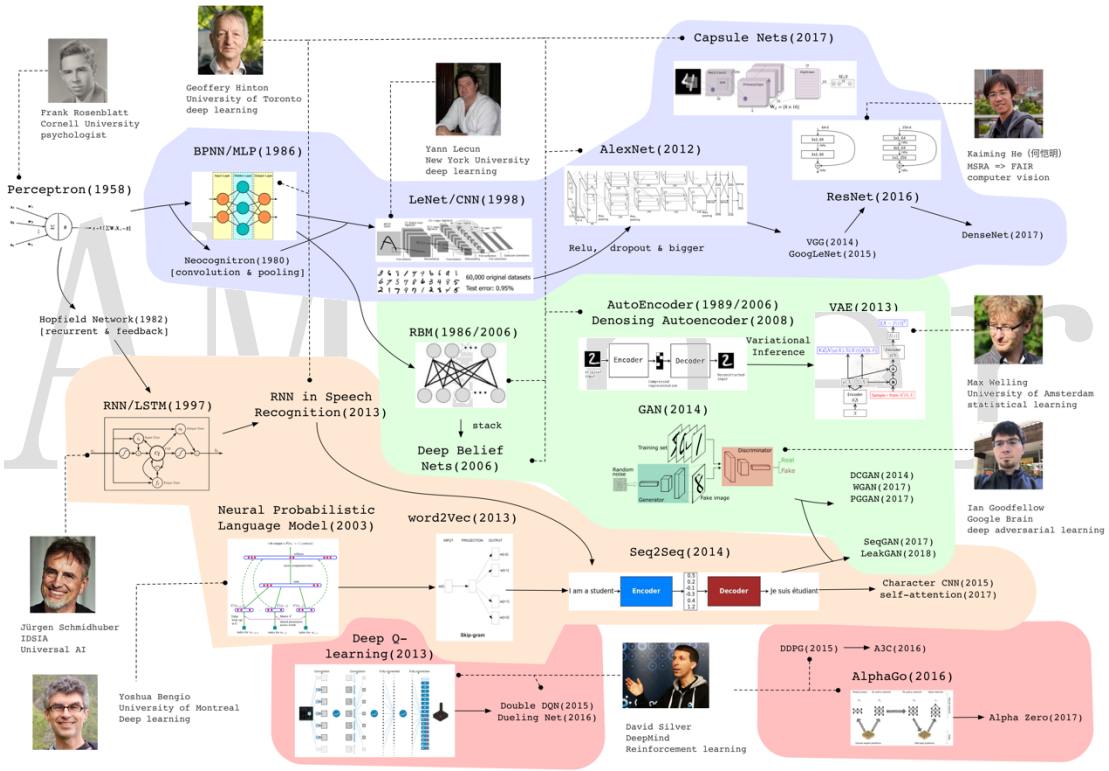


图 3-1 深度学习模型最近若干年的重要进展

第一个发展脉络（上图浅紫色区域）以计算机视觉和卷积网络为主。这个脉络的进展可以追溯到 1979 年，Fukushima 提出的 Neocognitron。该研究给出了卷积和池化的思想。1986 年 Hinton 提出了反向传播训练 MLP（之前也有几个类似的研究），该研究解决了感知机不能处理非线性学习的问题。1998 年，以 Yann LeCun 为首的研究人员实现了一个七层的卷积神经网络 LeNet-5 以识别手写数字。现在普遍把 Yann LeCun 的这个研究作为卷积网络的源头，但其实在当时由于 SVM 的迅速崛起，这些神经网络的方法还没有引起广泛关注。真正使得卷积神经网络荣耀登上大雅之堂的事件是，2012 年 Hinton 组的 AlexNet（一个设计精

巧的 CNN）在 ImageNet 上以巨大优势夺冠，这引发了深度学习的热潮。AlexNet 在传统 CNN 的基础上加上了 ReLU、Dropout 等技巧，并且网络规模更大。这些技巧后来被证明非常有用，成为卷积神经网络的标配，被广泛发展，于是后来出现了 VGG、GoogLenet 等新模型。2016 年，青年计算机视觉科学家何恺明在层次之间加入跳跃连接，提出残差网络 ResNet。ResNet 极大增加了网络深度，效果有很大提升。一个将这个思路继续发展下去的是近年的 CVPR Best Paper 中黄高提出的 DenseNet。在计算机视觉领域的特定任务出现了各种各样的模型（Mask-RCNN 等），这里不一一介绍。2017 年，Hinton 认为反向传播和传统神经网络还存在一定缺陷，因此提出 Capsule Net，该模型增强了可解释性，但目前在 CIFAR 等数据集上效果一般，这个思路还需要继续验证和发展。

第二个发展脉络（上图浅绿色区域）以生成模型为主。传统的生成模型是要预测联合概率分布 $P(x, y)$。机器学习方法中生成模型一直占据着一个非常重要的地位，但基于神经网络的生成模型一直没有引起广泛关注。Hinton 在 2006 年的时候基于受限玻尔兹曼机（RBM，一个 19 世纪 80 年代左右提出的基于无向图模型的能量物理模型）设计了一个机器学习的生成模型，并且将其堆叠成为 Deep Belief Network，使用逐层贪婪或者 wake-sleep 的方法训练，当时模型的效果其实并没有那么好。但值得关注的是，正是基于 RBM 模型，Hinton 等人开始设计深度框架，因此这也可以看做深度学习的一个开端。Auto-Encoder 也是上个世纪 80 年代 Hinton 就提出的模型，后来随着计算能力的进步也重新登上舞台。Bengio 等人又提出了 Denoise Auto-Encoder，主要针对数据中可能存在的噪音问题。Max Welling（也是变分和概率图模型的高手）等人后来使用神经网络训练一个有一层隐变量的图模型，由于使用了变分推断，并且最后长得跟 Auto-Encoder 有点像，被称为 Variational Auto-Encoder。此模型中可以通过隐变量的分布采样，经过后面的 Decoder 网络直接生成样本。生成对抗模型 GAN（Generative Adversarial Network）是 2014 年提出的非常火的模型，它是一个通过判别器和生成器进行对抗训练的生成模型，这个思路很有特色，模型直接使用神经网络 G 隐式建模样本整体的概率分布，每次运行相当于从分布中采样。后来引起大量跟随的研究，包括：DCGAN 是一个相当好的卷积神经网络实现，WGAN 是通过维尔斯特拉斯距离替换原来的 JS 散度来度量分布之间的相似性的工作，使得训练稳定。PGGAN 逐层增大网络，生成逼真的人脸。

第三个发展脉络（上图橙黄色区域）是序列模型。序列模型不是因为深度学习才有的，而是很早以前就有相关研究，例如有向图模型中的隐马尔科夫 HMM 以及无向图模型中的条件随机场模型 CRF 都是非常成功的序列模型。即使在神经网络模型中，1982 年就提出了 Hopfield Network，即在神经网络中加入了递归网络的思想。1997 年 Jürgen Schmidhuber 发明了长短期记忆模型 LSTM（Long-Short Term Memory），这是一个里程碑式的工作。当然，真正让序列神经网络模型得到广泛关注的还是 2013 年 Hinton 组使用 RNN 做语音识别的工

作，比传统方法高出一大截。在文本分析方面，另一个图灵奖获得者 Yoshua Bengio 在 SVM 很火的时期提出了一种基于神经网络的语言模型（当然当时机器学习还是 SVM 和 CRF 的天下），后来 Google 提出的 word2vec（2013）也有一些反向传播的思想，最重要的是给出了一个非常高效的实现，从而引发这方面研究的热潮。后来，在机器翻译等任务上逐渐出现了以 RNN 为基础的 seq2seq 模型，通过一个 Encoder 把一句话的语义信息压缩成向量再通过 Decoder 转换输出得到这句话的翻译结果，后来该方法被扩展到和注意力机制（Attention）相结合，也大大扩展了模型的表示能力和实际效果。再后来，大家发现使用以字符为单位的 CNN 模型在很多语言任务也有不俗的表现，而且时空消耗更少。Self-attention 实际上就是采取一种结构去同时考虑同一序列局部和全局的信息，Google 有一篇很有名的文章“attention is all you need”把基于 Attention 的序列神经模型推向高潮。当然 2019 年 ACL 上同样有另一篇文章给这一研究也稍微降了降温。

第四个发展脉络（上图粉色区域）是增强学习。这个领域最出名的当属 Deep Mind，图中标出的 David Silver 博士是一直研究 RL 的高管。Q-learning 是很有名的传统 RL 算法，Deep Q-learning 将原来的 Q 值表用神经网络代替，做了一个打砖块的任务。后来又应用在许多游戏场景中，并将其成果发表在 Nature 上。Double Dueling 对这个思路进行了一些扩展，主要是 Q-Learning 的权重更新时序上。DeepMind 的其他工作如 DDPG、A3C 也非常有名，它们是基于 Policy Gradient 和神经网络结合的变种。大家都熟知的 AlphaGo，里面其实既用了 RL 的方法也有传统的蒙特卡洛搜索技巧。Deep Mind 后来提出了的一个用 AlphaGo 框架，但通过主学习来玩不同（棋类）游戏的新算法 Alpha Zero。

下面对深度学习的不同方面进行分别解读。有些地方解读可能稍微会简单一些，不完整的地方还请见谅。

3.1 卷积神经网络

卷积神经网络的发展，最早可以追溯到 1962 年，Hubel 和 Wiesel 对猫大脑中的视觉系统的研究。1980 年，一个日本科学家福岛邦彦（Kunihiko Fukushima）提出了一个包含卷积层、池化层的神经网络结构。在这个基础上，Yann Lecun 将 BP 算法应用到这个神经网络结构的训练上，就形成了当代卷积神经网络的雏形。

其实最初的 CNN 效果并不算好，而且训练也非常困难。虽然也在阅读支票、识别数字之类的任务上有一定的效果，但由于在一般的实际任务中表现不如 SVM、Boosting 等算法好，因此一直处于学术界的边缘地位。直到 2012 年，ImageNet 图像识别大赛中，Hinton 组的 AlexNet 引入了全新的深层结构和 Dropout 方法，一下子把 error rate 从 25%降低到了 15%，这颠覆了图像识别领域。AlexNet 有很多创新，尽管都不是很难的方法。其最主要的结果是

让人们意识到原来那个福岛邦彦提出的、Yann LeCun 优化的 LeNet 结构原来是有很大改进空间的：只要通过一些方法能够加深这个网络到 8 层左右，让网络表达能力提升，就能得到出人意料的好结果。

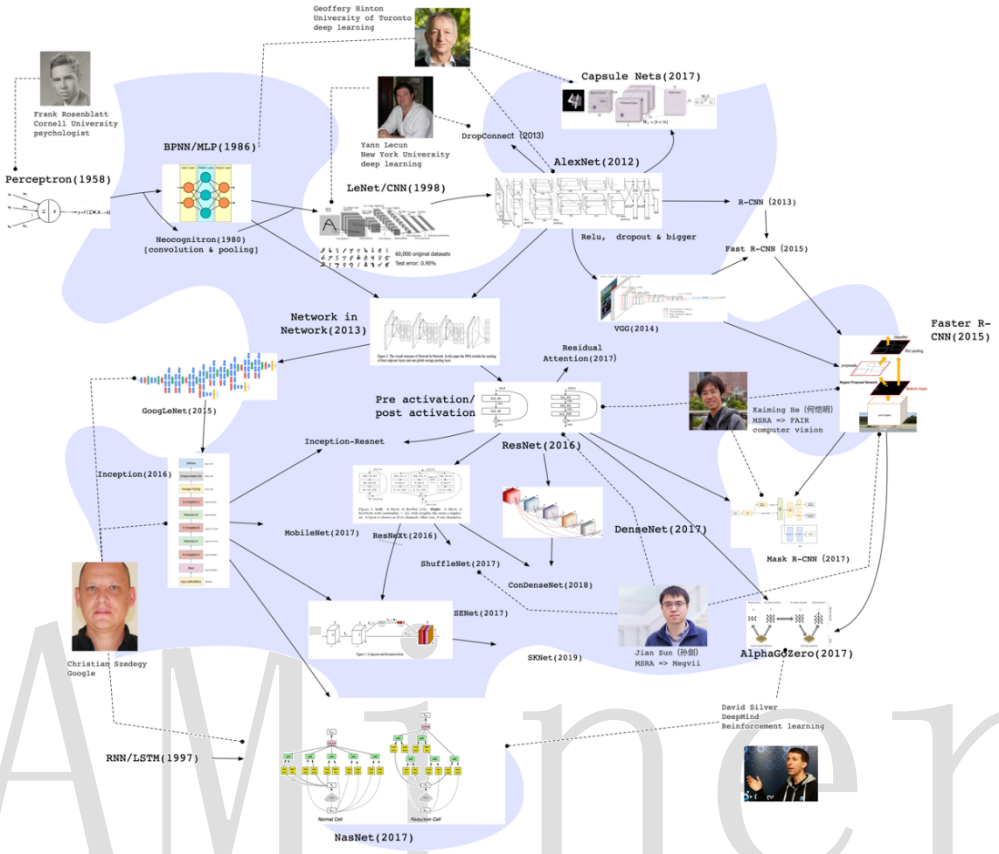


图 3-2 卷积神经网络的重要进展

顺着 AlexNet 的思想，LeCun 组 2013 年提出了一个 DropConnect，把 error rate 降低到了 11%。而 NUS 的颜水成组则提出了一个重要的 Network in Network（NIN）方法，NIN 的思想是在原来的 CNN 结构中加入了一个 1*1 conv 层，NIN 的应用也得到了 2014 年 Imagine 另一个挑战——图像检测的冠军。Network in Network 更加引发了大家对 CNN 结构改变的大胆创新。因此，两个新的架构 Inception 和 VGG 在 2014 年把网络加深到了 20 层左右，图像识别的 error rate（越小越好）也大幅降低到 6.7%，接近人类错误率的 5.1%。2015 年，MSRA 的任少卿、何恺明、孙剑等人，尝试把 Identity 加入到卷积神经网络中提出 ResNet。最简单的 Identity 却出人意料的有效，直接使 CNN 能够深化到 152 层、1202 层等，error rate 也降到了 3.6%。后来，ResNeXt, Residual-Attention，DenseNet，SENet 等也各有贡献，各自引入了 Group convolution，Attention，Dense connection，channelwise-attention 等，最终 ImageNet 将 error rate 降到了 2.2%，远远低于人类的错误率。现在，即使手机上的神经网络，也能达到超过人类的水平。而另一个挑战——图像检测中，也是任少卿、何恺明、孙剑等优化了原先的 R-CNN, fast R-CNN 等通过其他方法提出 region proposal，然后用 CNN 去判断是否是

object 的方法，提出了 faster R-CNN。Faster R-CNN 的主要贡献是使用和图像识别相同的 CNN feature，发现 feature 不仅可以识别图片内容，还可以用来识别图片的位置。也就是说，CNN 的 feature 非常有用，包含了大量的信息，可以同时用来做不同的任务。这个创新一下子把图像检测的 MAP 也翻倍了。在短短的 4 年中，ImageNet 图像检测的 MAP（越大越好）从最初的 0.22 达到了最终的 0.73。何恺明后来还提出了 Mask R-CNN，即给 faster R-CNN 又加了一个 Mask Head，发现即使只在训练中使用 Mask Head，其信息可以传递回原先的 CNN feature 中，获得了更精细的信息。由此，Mask R-CNN 得到了更好的结果。何恺明在 2009 年时候就以一个简单有效的去雾算法得到了 CVPR Best Paper，在计算机视觉领域声名鹊起。后来更是提出了 ResNet 和 Faster R-CNN 两大创新，直接颠覆了整个计算机视觉/机器学习领域。

当然，CNN 结构变得越来越复杂，很多结构都很难直觉的来解释和设计。于是谷歌提出了自动架构学习方法 NasNet（Neural Architecture Search Network）来自动用 Reinforcement Learning 去搜索一个最优的神经网络结构。Nas 是目前 CV 界一个主流的方向，可以自动寻找出最好的结构，以及给定参数数量/运算量下最好的结构（这样就可以应用于手机），是目前图像识别的一个重要发展方向。今年何恺明（2019 年 4 月）又发表了一篇论文，表示即使 Random 生成的网络连接结构（只要按某些比较好的 Random 方法），都会取得非常好的效果，甚至比标准的好很多。Random 和 Nas 哪个是真的正确的道路，这有待进一步的研究了。

卷积神经网络 CNN 的发展引发了其他领域的很多变革。比如：利用 CNN，AlphaGo 战胜了李世石，攻破了围棋（基础版本的 AlphaGo 其实和人类高手比起来是有胜有负的）。后来利用了 ResNet 和 Faster-RCNN 的思想，一年后的 Master 则完全战胜了所有人类围棋高手。后来又有很多复现的开源围棋 AI，每一个都能用不大的计算量超过所有的人类高手。以至于现在人们讲棋的时候，都是按着 AI 的胜率来讲了。

3.2 AutoEncoder

AutoEncoder 的基本思想是利用神经网络来做无监督学习，就是把样本的输入同时作为神经网络的输入和输出。本质上是希望学习到输入样本的表示（encoding）。早期 AutoEncoder 的研究主要是数据过于稀疏、数据高维导致计算复杂度高。比较早用神经网络做 AutoEncoder 的可以追溯到 80 年代的 BPNN 和 MLP 以及当时 Hinton 推崇的 RBM。后来到了 2000 年以后还坚持在做的只剩下 Hinton 的 RBM 了。从 2000 年以后，随着神经网络的快速兴起，AutoEncoder 也得到快速发展，基本上有几条线：稀疏 AutoEncoder、噪音容忍 AutoEncoder、卷积 AutoEncoder、变分 AutoEncoder。最新的进展是结合对抗思想的对抗 AutoEncoder。

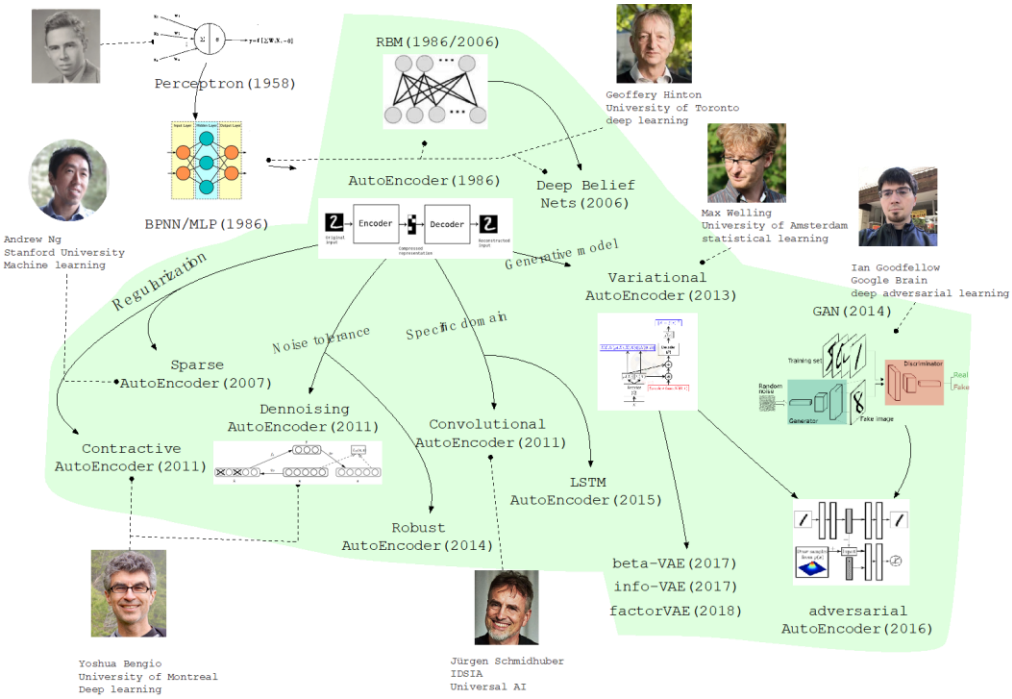


图 3-3 Auto-Encoder 的重要进展

稀疏 AutoEncoder 在学习输入样本表示的时候可以学习到相对比较稀疏的表示结果，这在 Overcomplete AutoEncoder（就是学习得到高维表示）方法中尤为重要。代表性人物包括斯坦福大学的 Andrew Ng 和蒙特利尔的 Yoshua Bengio 教授。具体方法就是在原来的损失函数中加一个控制稀疏化的正则化项，通过控制优化过程来实现。

Denoising AutoEncoder 的核心思想就是提高 Encoder 的鲁棒性，本质上就是避免可能的 overfitting。一个办法是在输入中加入随机噪音（比如随机置 0 一些输入，或者随机把部分输入变为 marked），这些思想后来在 BERT 等模型中也有广泛使用；另一个办法就是结合正则化的思想，比如在目标函数中加上 eEncoder 的 Jacobian 范数。Jacobian 范数可以让学习到的特征表示更具有差异性。

著名研究者 Jurgen Schmidhuber 提出了基于卷积网络的 AutoEncoder 以及后来的 LSTM AutoEncoder。Max Welling 基于变分思想提出变分 AutoEncoder 方法 VAE，这也是一个里程碑式的研究成果。后面很多研究者在这个工作上进行了扩展，包括 info-VAE、beta-VAE 和 factorVAE 等。最近还有人借鉴 Ian Goodfellow 等人提出的对抗建模思想提出 Adversarial AutoEncoder，也取得了很好的效果。这和之前的噪音容忍的 AE 学习也有一定呼应。除了上面的思想，就是可以把上面的各种方法 stacking 起来。

3.3 循环神经网络 RNN

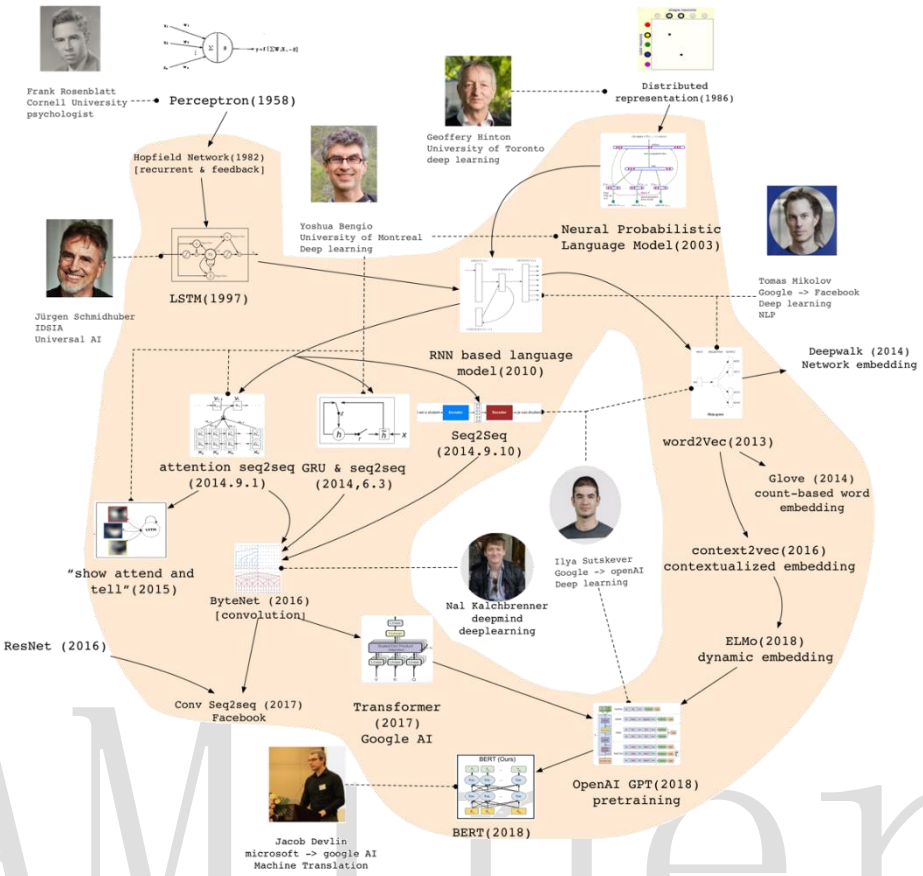


图 3-4 循环神经网络 RNN 的重要进展

1982 年，美国加州理工学院物理学家 John Hopfield 发明了一种单层反馈神经网络 Hopfield Network，用来解决组合优化问题。这是最早的 RNN 的雏形。86 年，另一位机器学习的泰斗 Michael I. Jordan 定义了 Recurrent 的概念，提出 Jordan Network。1990 年，美国认知科学家 Jeffrey L. Elman 对 Jordan Network 进行了简化,并采用 BP 算法进行训练，便有了如今最简单的包含单个自连接节点的 RNN 模型。但此时 RNN 由于梯度消失（Gradient Vanishing）及梯度爆炸（Gradient Exploding）的问题，训练非常困难，应用非常受限。直到 1997 年，瑞士人工智能研究所的主任 Jurgen Schmidhuber 提出长短期记忆（LSTM），LSTM 使用门控单元及记忆机制大大缓解了早期 RNN 训练的问题。同样在 1997 年，Mike Schuster 提出双向 RNN 模型（Bidirectional RNN）。这两种模型大大改进了早期 RNN 结构，拓宽了 RNN 的应用范围，为后续序列建模的发展奠定了基础。此时 RNN 虽然在一些序列建模任务上取得了不错的效果，但由于计算资源消耗大，后续几年一直没有太大的进展。

2010 年，Tomas Mikolov 对 Bengio 等人提出的 feedforward Neural network language model (NNLM)进行了改进，提出了基于 RNN 的语言模型（RNN LM），并将其用在语音识别任务中，大幅提升了识别精度。在此基础上 Tomas Mikolov 于 2013 年提出了大名鼎鼎的 word2vec，

与 NNLM 及 RNNLM 不同，word2vec 的目标不再专注于建模语言模型，而是如何利用语言模型学习每个单词的语义化向量（distributed representation），当然 distributed representation 概念最早要来源于 Hinton 1986 年的工作。word2vec 引发了深度学习在自然语言处理领域的浪潮，除此之外还启发了 knowledge representation，network representation 等新的领域。

另一方面，2014 年 Bengio 团队与 Google 几乎同时提出了 seq2seq 架构，将 RNN 用于机器翻译。没过多久，Bengio 团队又提出注意力 Attention 机制，对 seq2seq 架构进行改进。自此机器翻译全面进入到神经机器翻译（NMT）的时代，NMT 不仅过程简单，而且效果要远超统计机器翻译的效果。目前主流的机器翻译系统几乎都采用了神经机器翻译的技术。除此之外，Attention 机制也被广泛用于基于深度学习的各种任务中。

近两年，相关领域仍有一些突破性进展，2017 年，Facebook 人工智能实验室提出基于卷积神经网络的 seq2seq 架构，将 RNN 替换为带有门控单元的 CNN，提升效果的同时大幅加快了模型训练速度。此后不久，Google 提出 Transformer 架构，使用 Self-Attention 代替原有的 RNN 及 CNN，更进一步降低了模型复杂度。在词表示学习方面，Allen 人工智能研究所 2018 年提出上下文相关的表示学习方法 ELMo，利用双向 LSTM 语言模型对不同语境下的单词，学习不同的向量表示，在 6 个 NLP 任务上取得了提升。OpenAI 团队在此基础上提出预训练模型 GPT，把 LSTM 替换为 Transformer 来训练语言模型，在应用到具体任务时，与之前学习词向量当作特征的方式不同，GPT 直接在预训练得到的语言模型最后一层接上 Softmax 作为任务输出层，然后再对模型进行微调，在多项任务上 GPT 取得了更好的效果。

不久之后，Google 提出 BERT 模型，将 GPT 中的单向语言模型拓展为双向语言模型（Masked Language Model），并在预训练中引入了 sentence prediction 任务。BERT 模型在 11 个任务中取得了最好的效果，是深度学习在 NLP 领域又一个里程碑式的工作。BERT 自从在 arXiv 上发表以来获得了研究界和工业界的极大关注，感觉像是打开了深度学习在 NLP 应用的潘多拉魔盒。随后涌现了一大批类似于“BERT”的预训练（pre-trained）模型，有引入 BERT 中双向上下文信息的广义自回归模型 XLNet，也有改进 BERT 训练方式和目标的 RoBERTa 和 SpanBERT，还有结合多任务以及知识蒸馏（Knowledge Distillation）强化 BERT 的 MT-DNN 等。这些种种，还被大家称为 BERTology。

3.4 网络表示学习与图神经网络 GNN

这个方面的研究可以追溯到 Hinton 当年 1986 的 Distributed Representation，后来 Stanford 的 Andrew Ng 实验室做了个 Neural Tensor Network，本质就是把知识之间的关系和表示学习一起放到 tensor 里面来做，算是一个 smart 的扩展。后来 Facebook 的 Antonie Bordes 提出了 TransE 是一个 milestone 的工作，把知识网络的三元组融合到了表示学习中，这是 NLP 和知

识图谱中的一个非常重要的研究，后面延续了一系列的工作，包括 TransH、TransR、TransA、TransG。

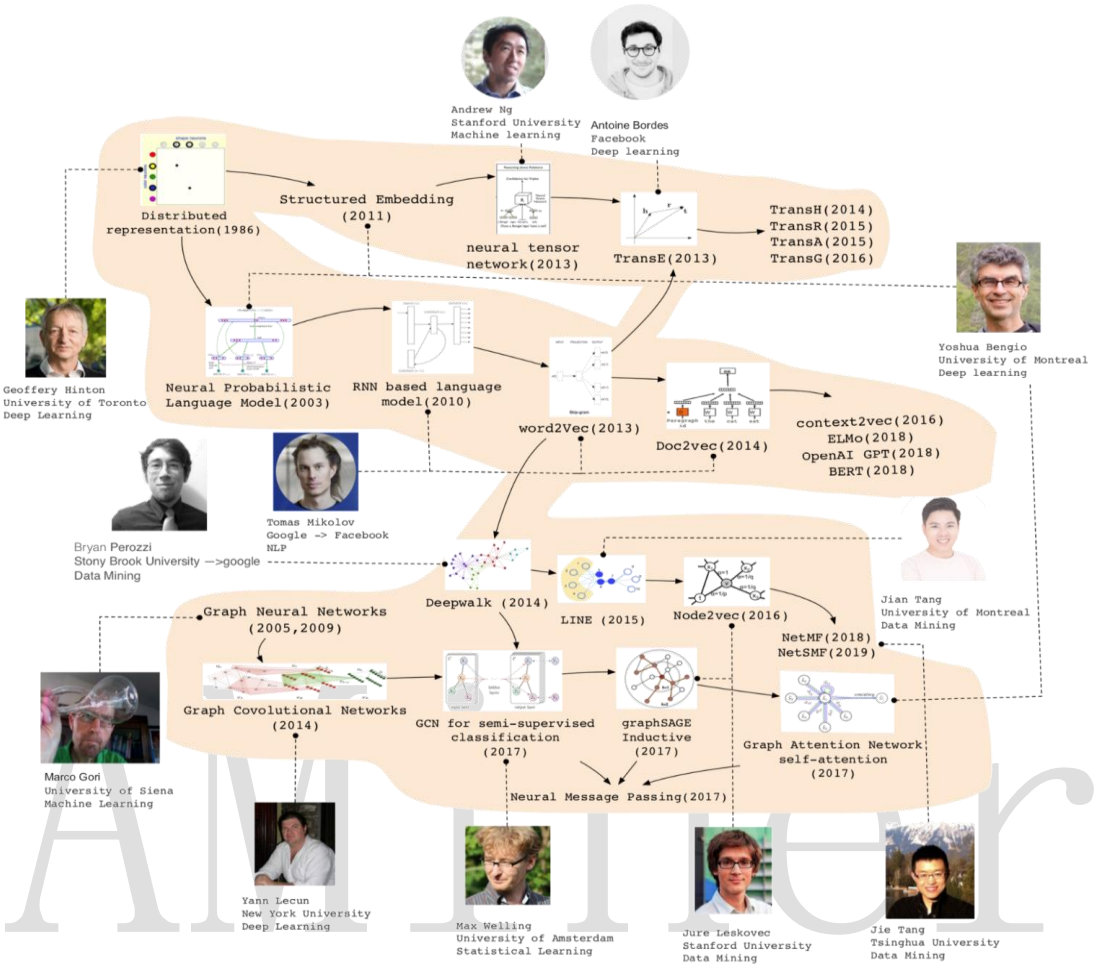


图 3-5 网络表示学习与图神经网络的重要进展

从表示学习本身来看，Neural Language Model 是对于单词和文本的表示，是对原来向量模型的一个自然扩展，其实本质上类似一个隐含语义分析，只是这里用的是神经网络来做学习。RNN based language model 是利用 RNN 进行表示学习，更好的保持了语言模型的连续性。但这个阶段的研究当时大部分都没有火起来，一是当时深度学习还没火起来，二是这些算法都还比较慢。2013 年 Tomas Mikolov 和 Jeff Dean 等人做 word2vec，可以说占据了“天时、地利、人和”：深度学习开始发热、算法简单有效、大神作品。现在 word2vec 已经轻松超过 1 万多引用了。后面的扩展也很多，如 pharagraph2vec、doc2vec，context2vec。以至于后面有一段时间，“2vec”成了流行取名字的方法。最近的进展是 ELMo、OpenAI 的 GPT 和谷歌的 BERT。

表示学习的另一个脉络就是扩展到网络数据上，在 NLP 领域的 Structured Embedding、TransE 等模型更多的是语言中的局部结构信息，而网络中还有更加复杂的拓扑结果。Bryan

（原 Stony Brook 大学的，现在去了谷歌）提出 DeepWalk，这个算最早把 word2vec 稍微扩展了一下，应用于网络数据，这篇文章获得了当年 KDD 的最佳论文和后来 KDD 的最佳博士论文。很快这个工作吸引了大量关注，Jian Tang（原北大、微软，现在去了 Bengio 那边）等人做了两阶扩展，斯坦福的 Jure Leskovec 做了面向社交网络的“三阶”扩展 node2vec，后来清华也给出了一个理论证明，证明这些不同方法本质上都在做一个矩阵分解，并基于此提出了一个 NetMF 的算法以及其适用于大规模网络的实现 NetSMF。ProNE 是另一个清华作品，其主要特点是高效和高精度。该方法非常简单，本质上是在原来的表示学习上引入了一个类似卷积但又不是卷积的操作，大大提高了精度。

最近的网络表示学习更多的是用卷积网络直接对图做，大方向是 Graph Neural Network，最早是 Siena 大学的 Marco 等人在 2005 和 2009 年提出的，但当时没引起太大关注。后来 Yann Lecun 提出的 Graph Convolutional Networks，还有 Kipf & Welling 等人提出的 semi-supervised 的 GCN。这一系列的研究本质上就是 Neural Message Passing，在最近引起大量关注。斯坦福的 Jure 也提出了 GraphSage，利用 NMP 简化了卷积，提高了速度，并且支持 inductive learning，再后来 Yoshua 他们团队又提出了 Graph Attention Network，进一步提高了图卷积精度。最近网络表示学习非常热，前前后后都能看到三大巨头 Hinton、Yoshua 和 Yann 的影子。在未来若干年还会继续是个研究热点。

3.5 增强学习

Deep Mind 是一家英国人工智能公司，是对增强学习影响最大的一个公司。创立于 2010 年，2014 年被 Google 收购。创始人哈萨比斯出身于伦敦，母亲为新加坡华裔，13 岁便已经获得国际象棋大师的头衔，19 岁开始学习围棋，当前是围棋业余初段。DeepMind 于 2014 年开始开发 AlphaGO。来看看 AlphaGO 的战绩吧。2015 年 10 月，AlphaGO 5:1 樊麾；2016 年 3 月，AlphaGo 4 : 1 李世石；2017 年 5 月，AlphaGO 3 : 0 柯洁；2017 年 10 月 19 日，AlphaGo Zero 发表在 Nature，其思路是从零开始，自我对弈，40 天超过所有版本。2018 年 12 月 7 日，AlphaZero 再次发表于 Science, AlphaZero 使用与 AlphaGo Zero 类似但更一般性的算法，在不做太多改变的前提下，并将算法从围棋延伸到将棋与国际象棋上。2018 年 12 月，Deep Mind 公司推出 AlphaFold, 可以根据基因序列预测蛋白质结构。2019 年 1 月 25 日，Deep Mind 公司推出的 AlphaStar，在《星海争霸 II》以 10：1 战胜人类职业玩家。另一条在美国的战线，可能最著名的是 Open AI 公司，这是 Hinton 的高徒 Ilya Sutskever（AlexNet 发明人）创立的公司。2019 年 4 月，Open AI 推出 five dota2，2-0 战胜 Dota2 的 TI8 冠军战队 OG。

在研究方法上 Deep Q-Network（DQN）利用神经网络对 Q 值进行函数近似，并利用了 experience replay 和 fixed target network 的策略让 DQN 可以收敛，在 Atari 的不少游戏上都

超过了人类水平。Double DQN 是深度学习版本的 double Q-learning，它通过微小的修改就成功减小了 DQN 中 max 操作带来的 bias。再后来，Dueling DQN 将 Q-network 分成了 action-dependent 和 action-independent 两个部分，从而提高了 DQN。DQN 是为 Value 的期望建模，greedy 的时候也是最大化期望的形式，Categorical DQN 的想法是直接为 Value 的分布进行建模。Noise DQN 在网络中添加了噪声，从而达到 exploration 的效果。DQN 还有非常多的提升版本，rainbow 整合了多种 DQN 版本。Ape-X 从 Rainbow 的工作中发现 Replay 的优先级对于性能影响是最大的，故扩大 Prioritised Replay Buffer，并使用 360 个 actor 做分布式的训练，比 rainbow 更快，也更好。

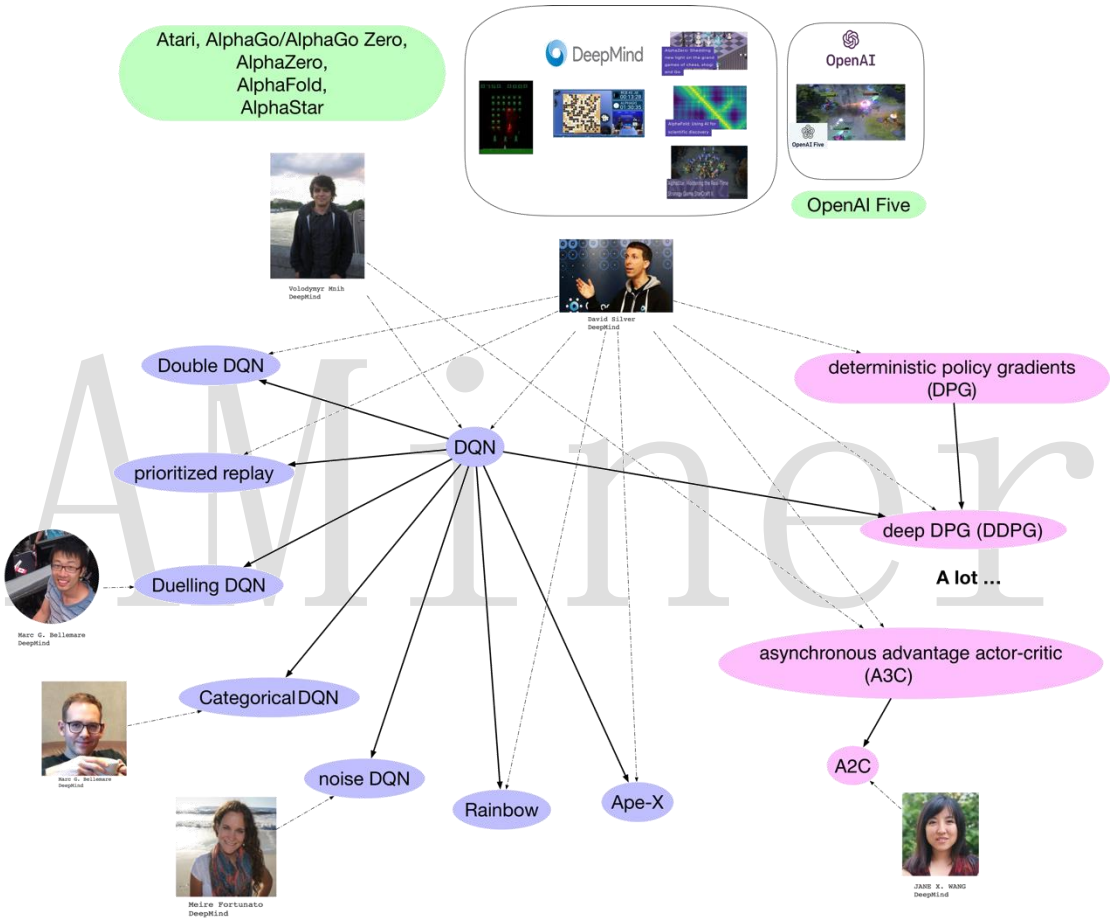


图 3-6 增强学习的重要进展

Deterministic policy gradients（DPG）将 policy gradients 方法中随机的 policy 推广为确定性 policy。Deep DPG 使用了神经网络表示高维 state，是结合了 DQN 和 DPG 的 actor critic 算法。A3C 是经典的 policy gradient 方法，可以并行 multiple agent 的训练，并异步更新参数。A2C 是 A3C 的同步、确定性 policy 版本，同步的梯度更新，可以让并行训练更快收敛。

3.6 生成对抗网络

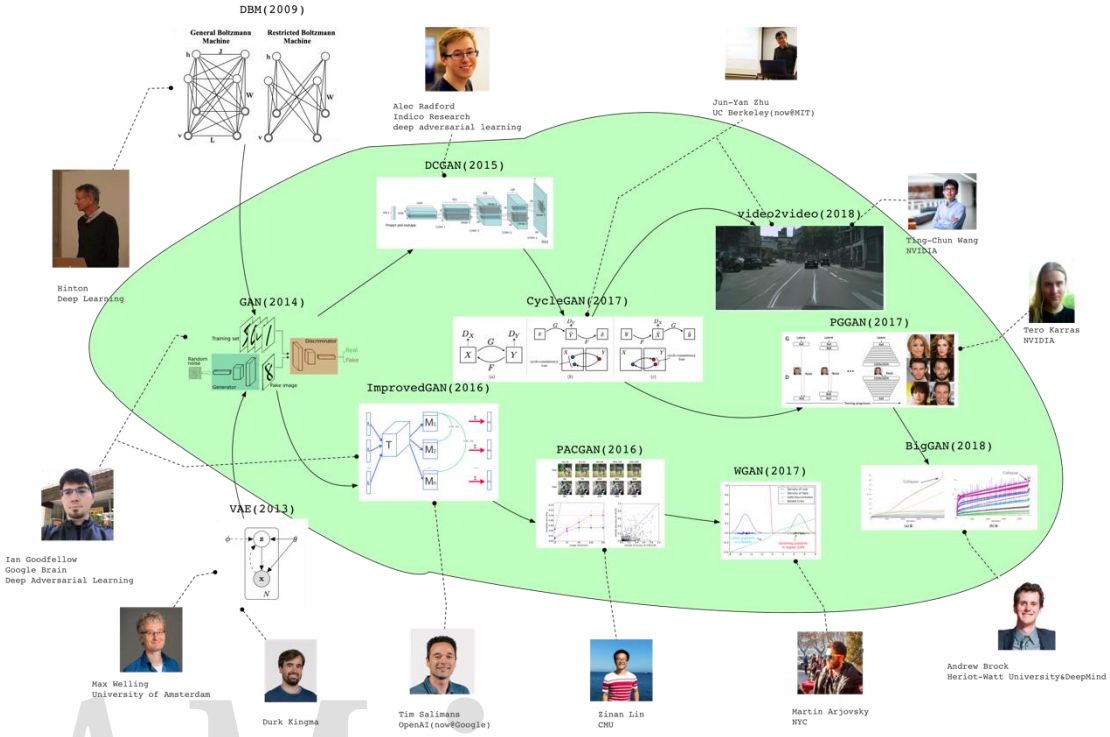


图 3-7 生成对抗网络的重要进展

GAN 最近几年发展非常快，这也是 Yoshua Bengio 获得图灵奖的贡献之一。传统的生成模型是要预测联合概率分布 $P(x, y)$。首先玻尔兹曼机（RBM）这个模型其实是一个基于能量的模型，1986 年的时候就有，Hinton 在 2006 年的时候重新拿出来作为一个生成模型，并且将其堆叠成为 Deep Belief Network，使用逐层贪婪或者 wake-sleep 的方法训练。

AutoEncoder 也是上个世纪 80 年代 Hinton 就提出的模型，此时由于计算能力的进步也重新登上舞台。Bengio 等人又搞了 Denoise AutoEncoder。Max welling 等人使用神经网络训练一个有一层隐变量的图模型，由于使用了变分推断，并且最后长得跟 AutoEncoder 有点像，被称为 Variational AutoEncoder。此模型中可以通过隐变量的分布采样，经过后面的 decoder 网络直接生成样本。

在生成模型方面，最近一个最重要的进展就是对抗生成网络（GAN），可以说是现在最火的生成模型。2014 年 Ian Goodfellow 在 NIPS 上发表了最初的 GAN 文章，到现在已经有近九千引用。为什么这个模型引起如此大的关注呢？一个原因是这个模型理论上非常优雅，大家理解起来简单方便；二就是效果确实好。看图中上面这一排，是基于 GAN 的一些应用文章，下面这些是改进 GAN 的训练的一些文章。这些文章都引起了广泛关注。可以看出，GAN 的发明人 Ian Goodfellow 是少年得志的典范。他本科在斯坦福，硕士在 Andrew Ng 手下，博士就跑到蒙特利尔 Yoshua Bengio 手下了。他另外还有一个导师 Aaron Courville。大

家现在经常用的教科书《Deep Learning》，作者就是 Ian Goodfellow 和他两个博士导师。他是 85 年人，发表 GAN 在 2014 年，29，还差一年才 30。GAN 这个工作也给 Goodfellow 带来了很多荣誉，比如 17 年就被 MIT under 35 选中了。Goodfellow 博士毕业后去了 Google Brain，后来又跳到 Open AI，又跳回 Google，现在在苹果做特别项目机器学习项目负责人，实际上现在他也才 34 岁。另外，GAN 是 Ian Goodfellow 在蒙特利尔的时候的工作。大家知道今年图灵奖给了深度学习三巨头，其中的 Bengio，在图灵奖官网上给获奖理由，选的三个贡献之一就是 GAN。另外两个贡献分别是 90 年代的序列概率模型和 00 年代的语言模型。GAN 可以说是 Bengio 的代表作之一了，甚至可以说帮助他拿图灵奖。

另外还有几个有名的 GAN 的扩展，包括：cycleGAN 和 vid2vid。去年 NIPS 企业展示会场，英伟达把 vid2vid 配合方向盘，做了个实物 demo，非常引人关注。

3.7 老虎机

老虎机也是机器学习的一个重要分支，和深度学习有着或多或少的联系。老虎机实际上是个赌博机器。走进拉斯维加斯赌场，你就能看到一排排闪亮的机器。老虎机模型这个数学模型，现在追本溯源基本认为是一个病理学家 Thompson 在 1933 年提出的。他当时觉得验证新药的医学的随机双盲实验有些残酷的地方，对于被分到药效较差的新药的那一组病人并不公平。他想知道能否在实验中途就验证药物药效，从而避免给病人带来痛苦，因此他提出了一个序列决策模型。但是，实际使用还是有很多问题，比如中途效果不好评价。所以直到现在，美国 FDA 对在医学随机双盲实验中使用这种自适应调整的多臂老虎机方法，仍然只是建议使用。就现在而言，老虎机模型实际是在搜索和推荐方面的应用很多。

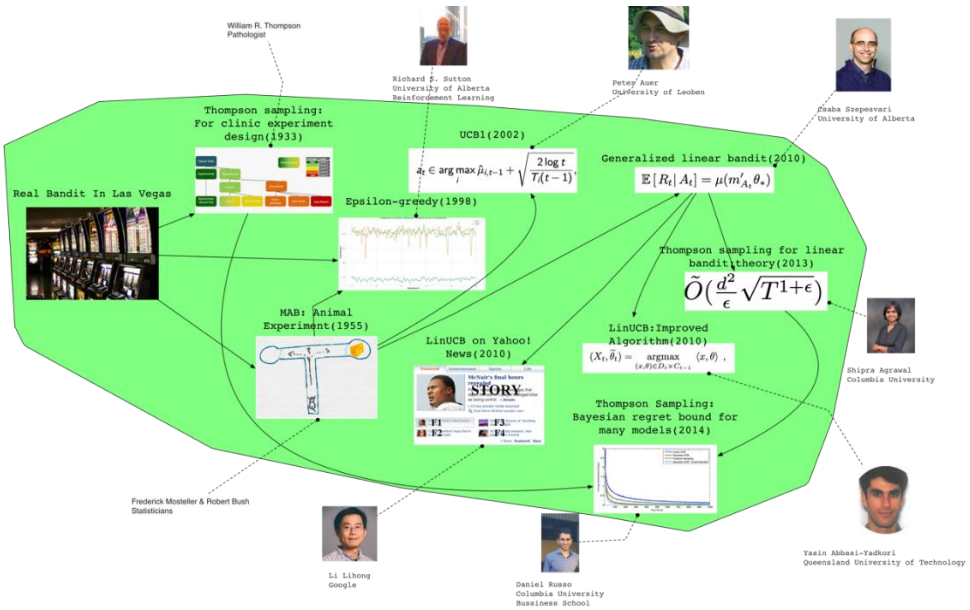


图 3-8 老虎机的重要进展

Epsilon-greedy 是种预留一点点机会去尝试的思想。这种想法很自然，学术界也不清楚最初的 credit 该给谁。现在就放在 sutton 名下。他是强化学习方面的大佬，写的那本教材 *Reinforcement Learning* 引用五位数，里边讲解了这个算法。Peter Auer 这个工作不仅分析了 UCB 算法的理论性质，还顺道分析了 Epsilon-greedy 的理论性质。这篇文章用到的技术，是此后很多更复杂技术的基础，很值得一看。这篇纯理论文章的引用量也达到了两千多。Frederick Mosteller 是哈佛统计系奠基人，20 世纪统计学界的超级牛人。他们当时做老虎机模型，主要是想给真实的动物或者人的序列决策建模，想抽象一个框架出来。所以他们作了一个老鼠找蛋糕的实验。当然，也做了关于人玩赌博用的老虎机的实验。Li Lihong 是清华 02 级校友。他在 Yahoo! news 上的 LinUCB 的工作发表在 WWW 上，这篇应用文章获得了大量关注，引用上千。他后来又翻出来 Thompson sampling 这个很古旧的方法，做了一些系统性的实验，从实验结果的角度说明 Thompson sampling 效果很好。这篇文章发在 NIPS2011 上，也获得了大量关注。后来大批做理论的人就跟进，就把 Thompson sampling 在线性模型上的理论基础建立起来了。比如 Russo 这篇文章可以看到，从 Thompson 1933 年用 Thompson sampling，到 2010 年后这个方法的理论基础才建立起来，这个时间跨度是很大的。当然，因为线性情况下都还比较简单，所以 2011 年后受到广泛关注没几年，理论就建立。这个现象和神经网络的理论建立基本是一个样子，都是线性的容易又基础，就先做着。研究老虎机模型确实比较偏理论，但老虎机应用也很广。上图里边除了有做医学的、做统计的、做计算机科学的，还有在商学院任教的，就是这个 Russo。

3.8 图神经网络

图是一种数据结构，它对一组对象（节点）及其关系（边）进行建模。近年来，由于图结构的强大表现力，用机器学习方法分析图的研究越来越受到重视。图神经网络（GNN）是一类基于深度学习的处理图域信息的方法。由于其较好的性能和可解释性，GNN 最近已成为一种广泛应用的图分析方法。

GNN 的第一个动机源于卷积神经网络（CNN）。CNN 的广泛应用带来了机器学习领域的突破并开启了深度学习的新时代。然而 CNN 只能在规则的 Euclidean 数据上运行，如图像（2 维网格）和文本（1 维序列）。如何将 CNN 应用于图结构这一非欧几里德空间，成为 GNN 模型重点解决的问题。

GNN 的另一个动机来自图嵌入（GraphEmbedding），它学习图中节点、边或子图的低维向量空间表示。DeepWalk、LINE、SDNE 等方法在网络表示学习领域取得了很大的成功。然而，这些方法在计算上较为复杂并且在大规模上的图上并不是最优的，GNN 旨在解决这些问题。

- 发展历史

图神经网络的概念首先由 Gori 等人于 2005 年提出，并由 Scarselli 等人进一步阐明。这些早期的研究以迭代的方式通过循环神经架构传播邻近信息来学习目标节点的表示，直到达到稳定的固定点。该过程所需计算量庞大，而近来也有许多研究致力于解决这个难题。一般情况下，图神经网络代表的是所有用于图数据的深度学习方法。

受到卷积网络在计算机视觉领域所获巨大成功的激励，近来出现了很多为图数据重新定义卷积概念的方法。这些方法属于图卷积网络（GCN）的范畴。Bruna 等人于 2013 年提出了关于图卷积网络的第一项重要研究，他们基于谱图论（spectralgraphtheory）开发了一种图卷积的变体。自此，基于谱的图卷积网络不断改进、拓展、进阶。由于谱方法通常同时处理整个图，并且难以并行或扩展到大图上，基于空间的图卷积网络开始快速发展。这些方法通过聚集近邻节点的信息，直接在图结构上执行卷积。结合采样策略，计算可以在一个批量的节点而不是整个图中执行，这种做法有望提高效率。除了图卷积网络，近几年还开发出了很多替代的图神经网络。这些方法包括图注意力网络（GAT）、图自编码器、图生成网络以及图时空网络。

Battaglia 等人将图网络定位为从关系数据中学习的构建块，并在统一的框架下回顾了部分图神经网络。然而，他们整体的框架是高度抽象的，失去了每种方法在原论文中的见解。Lee 等人对图注意力模型（一种图神经网络）进行了部分调查。最近，Zhang 等人提出了一项关于图深度学习的最新调查，却忽略了对图生成网络和图时空网络的研究。总之，现有的研究没有一个对图神经网络进行全面的回顾，只覆盖了部分图卷积神经网络且检查的研究有限，因此遗漏了图神经网络替代方法的最新进展，如图生成网络和图时空网络。

- 未来发展方向

加深网络。深度学习的成功在于深度神经架构。例如在图像分类中，模型 ResNet 具有 152 层。但在图网络中，实证研究表明，随着网络层数增加，模型性能急剧下降。这是由于图卷积的影响，因为它本质上推动相邻节点的表示更加接近彼此，所以理论上，通过无限次卷积，所有节点的表示将收敛到一个点。

感受野。节点的感受野是指一组节点，包括中心节点和其近邻节点。节点的近邻（节点）数量遵循幂律分布。有些节点可能只有一个近邻，而有些节点却有数千个近邻。尽管采用了采样策略，但如何选择节点的代表性感受野仍然有待探索。

可扩展性。大部分图神经网络并不能很好地扩展到大型图上。主要原因是当堆叠一个图卷积的多层时，节点的最终状态涉及其大量近邻节点的隐藏状态，导致反向传播变得非常复

杂。虽然有些方法试图通过快速采样和子图训练来提升模型效率，但它们仍无法扩展到大型图的深度架构上。

动态性和异质性。大多数当前的图神经网络都处理静态同质图。一方面，假设图架构是固定的。另一方面，假设图的节点和边来自同一个来源。然而，这两个假设在很多情况下是不现实的。在社交网络中，一个新人可能会随时加入，而之前就存在的人也可能退出该社交网络。在推荐系统中，产品可能具有不同的类型，而其输出形式也可能不同，也许是文本，也许是图像。因此，应当开发新方法来处理动态和异质图结构[63]。

3.9 深度学习近期重要进展

在过去几年中，深度学习改变了整个人工智能的发展。深度学习技术已经开始在医疗保健，金融，人力资源，零售，地震检测和自动驾驶汽车等领域的应用程序中出现。至于现有的成果表现也一直在稳步提高。本小节将介绍深度学习近期的一些重要进展。

3.9.1 2018 年三大进展

- BERT 模型

BERT 的全称是 Bidirectional Encoder Representation from Transformers，是基于深度双向 Transformer 的预训练模型，能用所有层的上下文语境训练深度双向表征。自 Google 在 2018 年公布 BERT 在 11 项 nlp 任务中的卓越表现后，BERT 就成为 NLP 领域大火的模型。关于 BERT 的详细介绍请参见 2.9 节的内容。

- 视频到视频合成（Video-to-Video Synthesis）

我们通常习惯由图形引擎创建的模拟器和视频游戏进行环境交互。虽然令人印象深刻，但经典方法的成本很高，因为必须精心指定场景几何、材料、照明和其他参数。一个很好的问题是：是否可以使用例如深度学习技术自动构建这些环境。NVIDIA 的研究人员解决了这个问题。他们的目标是在源视频和输出视频之间提供映射功能，精确描绘输入内容。作者将其建模为分布匹配问题，其目标是使自动创建视频的条件分布尽可能接近实际视频的条件分布。为实现这一目标，他们建立了一个基于生成对抗网络（GAN）的模型。在 GAN 框架内的关键思想是，生成器试图产生真实的合成数据，使得鉴别器无法区分真实数据和合成数据。他们定义了一个时空学习目标，旨在实现暂时连贯的视频，下图是 Video to Video Synthesis 生成的城市风景图：

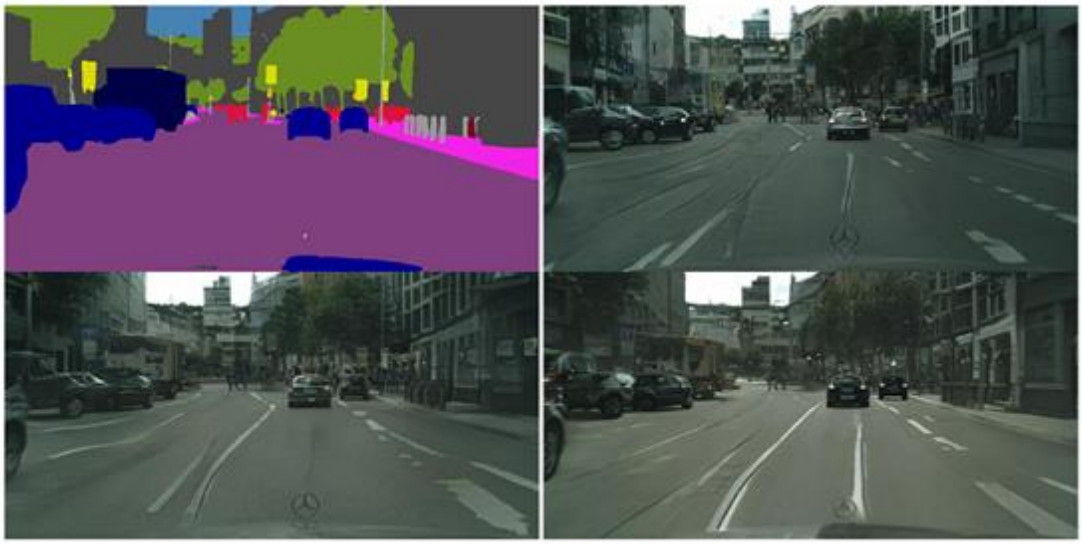


图 3-9 Video to Video Synthesis 生成的城市风景图

输入视频位于左上象限，它是来自 Cityscapes 数据集的街道场景视频的分段图。作者将他们的结果（右下）与两个基线进行比较：pix2pixHD（右上）和 COVST（左下）。这种方法甚至可以用于执行未来的视频预测。你可以尝试用 NVIDIA 开源 vid2vid 代码（基于 PyTorch）执行它[64]。

- 图网络（Graph Network）

DeepMind 联合谷歌大脑、MIT 等机构 27 位作者发表重磅论文“*Relational inductive biases, deep learning, and graph networks*”，提出“图网络”（Graph network），将端到端学习与归纳推理相结合，有望解决深度学习无法进行关系推理的问题。作者认为组合泛化是人工智能实现与人类相似能力的首要任务，而结构化表示和计算是实现这一目标的关键，实现这个目标的关键是结构化的表示数据和计算。该论文讨论了图网络如何支持关系推理和组合泛化，为更复杂的、可解释的和灵活的推理模式奠定基础。

作者在自己的模型中没有使用神经元这个词，意在强调这个模型不一定需要通过 neural network 实现，也可以使用别的函数。graph network 的主要计算单元是 GN block，GN block 是一个输入输出都是 graph 的 graph-to-graph module。在 graph 中，前面说过的 entity 就被表示成节点（node），而 relation 被表示成边（edge），系统层面的特征用 global attribute 表示。

由于 GN 的行为和人类对世界的理解类似，都是将世界解释成物体和相互关系组成的，因此 GN 的行为可能会更加容易解释，变得更加易于分析，更容易可视化。探索 GN 的可解释性也是未来一个有趣的方向[65]。

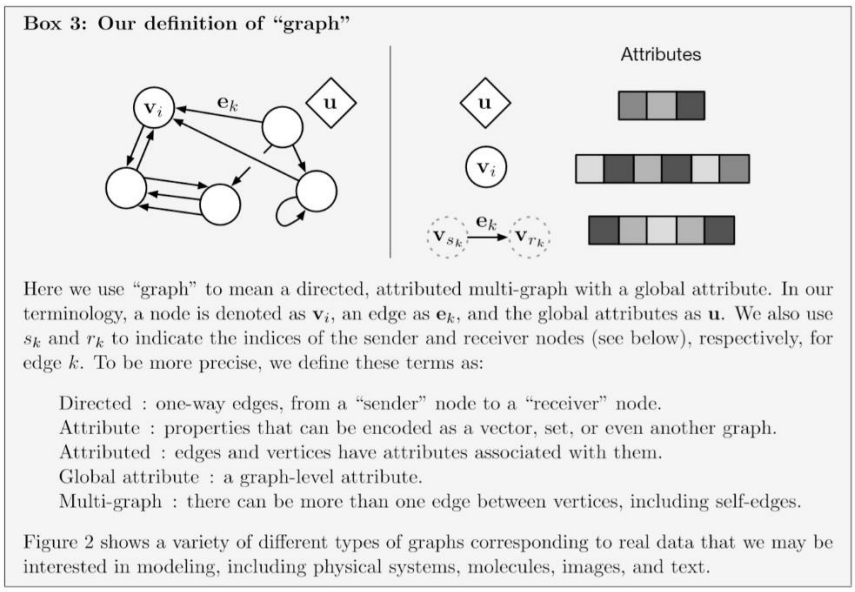


图 3-10 图网络模型

3.9.2 2019 年三大进展

- XLNet 模型

XLNet 是 CMU 与谷歌大脑提出的全新 NLP 模型，在 20 个任务上超过了 BERT 的表现，并在 18 个任务上取得了当前最佳效果，包括机器问答、自然语言推断、情感分析和文档排序。关于 XLNet 及其与 BERT 关系的详细介绍请参见 2.9 节的内容。

- MoCo

何恺明在其工作“*Momentum Contrast for Unsupervised Visual Representation Learning*”中提出了动量对比度（MoCo）用于无监督的视觉表示学习。从作为字典查找的对比学习的角度来看，作者构建了一个带有队列和移动平均编码器的动态字典。这样就可以实时构建大型且一致的词典，从而促进对比性的无监督学习。MoCo 在 ImageNet 分类的通用线性协议下提供了竞争性的结果。更重要的是，MoCo 学习到的表示将转移到下游任务。MoCo 可以胜过在 PASCAL VOC，COCO 和其他数据集上进行监督的预训练对等任务中的检测/细分任务，有时会大大超过它。这表明在许多视觉任务中，无监督和有监督的表征学习之间的鸿沟已被大大消除。

动量对比度（MoCo）通过使用对比损失将编码查询与编码键字典匹配来训练视觉表示编码器。字典键{k0，k1，k2，…}是由一组数据样本即时定义的。字典被构建为一个队列，其中排队了当前的迷你批处理，而最早的迷你批处理则排队。批量出队，将其与迷你批量脱钩。关键码由缓慢进行的编码器编码，由查询编码器进行动量更新驱动，此方法可为学习视

觉表示提供大而一致的字典。这是一种无监督目标函数，用来训练表征查询和键的编码器网络。

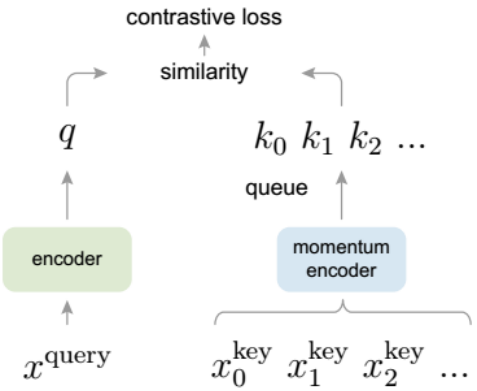


图 3-11 MoCo 训练编码器

对比学习是一种在诸如图像的高维连续输入上构建离散词典的方法。字典是动态的，在这种意义上，密钥是随机采样的，并且密钥编码器在训练过程中会不断演变。作者的假设是，大型词典可以学习良好的功能，涵盖大量否定样本，而词典密钥的编码器尽管不断进化，却始终保持一致。从下图中，可以看到三种不同对比损失机制的不同。端到端方法，是通过反向传播对计算查询和键的表征进行端到端更新。Memory bank 方法中，键的表征是从存储库中提取的。而 MoCo 方法则通过基于动量更新的编码器对键进行动态编码，并维持键的队列。

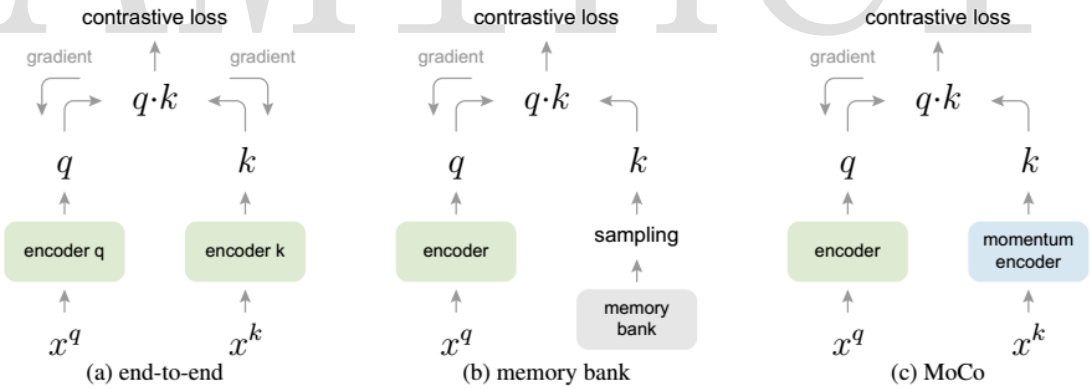


图 3-12 三种对比损失机制的概念比较

对于最后的效果而言，在三种不同机制的对比中，字典规模越大，三种方法的表现就越好。在针对不同的任务进行微调之后，MoCo 可以很好地迁移到下游任务中，表现甚至优于有监督预训练模型[66]。

- DL System 2

Yoshua Bengio 在 NeuIPS 2019 上的报告“*FROM SYSTEM 1 DEEP LEARNING TO SYSTEM 2 DEEP LEARNING*”讨论了深度学习发展的方向，引起了广泛关注，清华大学的唐杰教授对其进行了深度解读。

Bengio 首先肯定了人工智能已经在“听、说、看”等感知智能领域达到甚至超越人类水准，但在需要外部知识、逻辑推理以及领域迁移的认知领域还处于初级阶段。认知智能将从认知心理学、脑科学中汲取灵感，并结合知识图谱、因果推理等技术，建立知识表示、推理的有效机制，实现从感知智能到认知智能的关键突破。Bengio 介绍了人的认知系统包含两个子系统（这是认知理论中大家共识的观点）：System 1（子系统 1）是直觉系统，主要负责快速、无意识、非语言的认知，比如当人被问到一个问题的时候，可能下意识的或者说习惯性的回答，这就属于 System 1 的范畴。Bengio 认为目前深度学习主要就在做 System 1 的事情；System 2（子系统 2）是逻辑分析系统，是有意识的、带逻辑、规划、推理以及可以语言表达的系统。人在通过 System 2 处理问题的时候，往往要收集相关数据、进行逻辑分析和推理，最终做出决策。目前的绝大多数人工智能系统都还没有能实现 System 2，Bengio 提出这正是未来深度学习需要着重考虑的。当然 Bengio 也提到多智能体角度来实现 AI、以及从计算机角度需要考虑的问题，比如更好的模型和知识搜索。

对于如何用深度学习来实现 System 2 呢，Bengio 提到对于计算机来说，最关键就是处理数据分布中的变化。对于 System 2 来说，基本的要素包括：注意力和意识。注意力（Attention）其实现在在深度学习模型中已经有大量的实现和探讨，比如 GAT（图注意力机制）等，意识这部分是比较难的。笔者认为意识最关键是定义到怎样的边界。Bengio 提到意识先验可以使用稀疏因子图模型来实现，这是一个思路，实现了因果关系。从整体的理论框架方面可以考虑元学习（Meta-learning），局部修正假设（Localized change hypothesis），因果发现（Causal discovery）。最后是架构方面可以考虑如何学习不同对象的操作。

对于处理数据分布，传统机器学习都是基于 IID，也就是独立同分布的假设，但实际现状是很多真实场景下我们感兴趣的数据往往是出现次数非常少的数据，也就是我们在处理的时候需要关注更多的是 OOD（Out of distribution），也就是在训练数据中没怎么出现的分布，当然这需要我们在机器学习算法中有新的数据假设。尤其是从多智能体的角度来考虑，需要考虑哪些是影响数据分布变化的因素，以及不同分布的可组合性等方法如何对现在的 IID 和 OOD 进行泛化。相对传统的符号 AI 系统，当前的 AI 更多地需要具有泛化能力的机器学习能力。

注意力机制是最近几年深度学习发展的一个重要技术，最近几年在很多系统里面都有大量应用，注意力机制可以看做实现意识的第一步，在人类大脑中有自上而下的注意力和自下

而上的注意力。从认知角度来说，意识是一个很复杂的机制，Global Workspace Theory 是对 1988 年 Baars 等人提出的一个认知神经理论，其核心思想就是意识内容在各种不同认知过程中全局存在，包括 Attention（注意力）, Evaluation（评价）, Memory（记忆）, and Verbal report（逐字报告）。概念听起来有点抽象，后来 Dehaene 等人提出来一个 Global workspace architecture 的实现模型。Global workspace theory 和前面介绍的 System 2 很相似，除此之外，其他和意识相关的认知理论还包括 Multiple drafts theory，这是 Daniel Dennett 在 1991 年提出的一个理论。机器学习和意识模型相结合的关键是如何在机器学习中实现意识或者说意识相关的理论/模型怎么能帮到机器学习。比如可以基于意识理论构造一些假设，然后用机器学习的方法来验证这些假设。当然从人的角度来看意识，高层次的表示可以说是语言，这需要把人的两个认知系统 System 1 和 System 2 有机的结合起来，也就是说把低层次的表示和高层次的决策结合起来。

Bengio 还提到了前意识/意识先验。具体实现可以使用稀疏因子图，稀疏因子图不是一个新的模型，可以看做图模型的统一框架，因子图的好处是可以把有向图和无向图都统一起来。稀疏因子图可以用来学习变量之间的因果关系，从而构造变量之间的因果关系（找到真正的因果关系，而不是给不同变量给一个权重，这是为什么考虑稀疏的原因）。

元学习（学习学习的模型）是可能实现机器学习到 OOD 和模型快速迁移的一个办法。说到 OOD，究其原因是有行为的变化，或者说是用户行为对于数据的干预。元学习的知识表示可以有效帮助克服 OOD，一个例子是通过元迁移学习到变量之间的因果关系，这里挑战是如何学习到未知干预变量的因果特性。最后是如何学习样本的可能操作，类似自动机器学习，但这里是在对象的不同操作层面。

笔者所在的课题组也在这一领域上做了一定研究。从 2018 年开始，笔者在 CNCC 大会上开始组织认知图谱研讨会，探索认知理论和知识图谱的结合。今年笔者和阿里巴巴达摩研究院一起提出 Cognitive Graph，并有幸在今年 8 月去 Mila 和 Bengio 本人进行了这一问题的探讨。Cognitive Graph 的本质思想就是用深度学习同时实现人类认知的 System 1 和 System 2。

下图展示了我们提出的基于双通道处理理论的认知系统框架。System 1 我们采用了 BERT 来实现，通过预训练可以得到每个实体的表示，在表示的基础上可以实现知识扩展；System 2 我们则采用图神经网络，这是因为 System 1 扩展的信息都传递给 System 2，使得 System 2 可以基于多方面的信息做决策。这个方法在推理方面还有所欠缺，但在多跳问题回答任务上取得了不错的结果，后续在推理方面可能还可以做很多有意思的扩展。相关论文发表在 ACL 2019 上[67]。

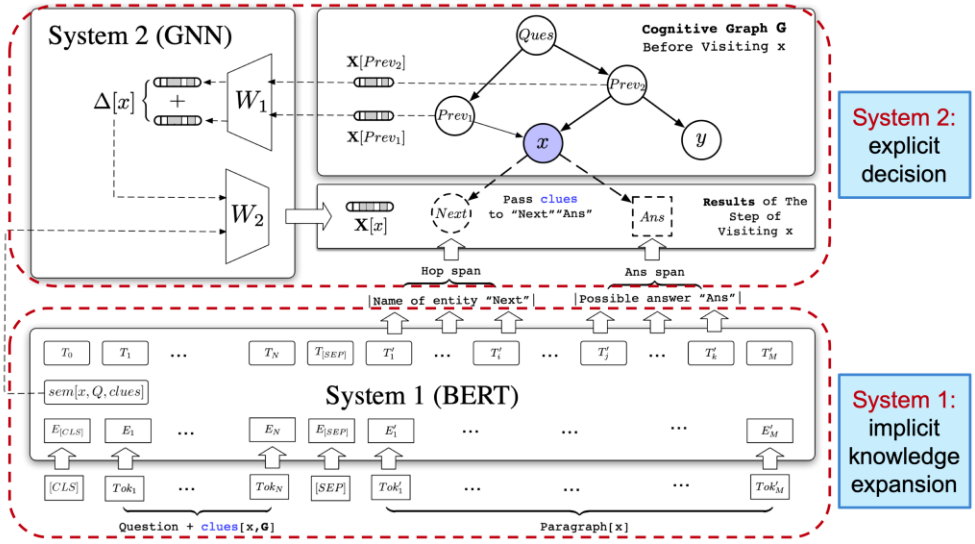


图 3-13 基于双通道处理理论的认知系统框架

4 论文解读篇

ICML 和 NeurIPS 是机器学习领域的两个顶级学术会议。

- ICML

ICML，全称 International Conference on Machine Learning，是由国际机器学习学会（IMLS）主办的年度机器学习国际顶级会议，由国际机器学习学会（IMLS）主办，每年一届，举办地各有不同。每年 ICML 都会接收到来自全世界学术机构、科技公司的论文，但审查非常严格，这很大程度上保证了 ICML 刊发出的论文质量。许多科研人员以在 ICML 发表论文为荣，几乎领域中每一个世界级的“技术大牛”都会在 ICML 发表过论文。

- NeurIPS

NeurIPS，全称 Conference and Workshop on Neural Information Processing Systems，是机器学习和计算神经科学的国际顶级会议，由 NIPS 基金会主办。早期 NeurIPS 会议上提出的研究包括从解决纯粹工程问题的努力到使用计算机模型作为理解生物神经系统的工具的广泛主题。最近的 NeurIPS 程序主要是关于机器学习，人工智能和统计学的论文。在 2018 年 11 月 17 日，神经信息处理系统基金会董事会决定将会议的官方首字母缩略词从 NIPS 更改为 NeurIPS。

我们选取了 ICML 与 NeurIPS 近 10 年来的最佳论文奖，如表 4-1、表 4-2 所列举：

表 4-1 ICML 近 10 年 best paper

ICML (International Conference on Machine Learning)		
年份	论文标题	作者
2019	Challenging Common Assumptions in the Unsupervised Learning of Disentangled Representations	Francesco Locatello, Stefan Bauer, Mario Lucic, Gunnar Rätsch, Sylvain Gelly, Bernhard Schölkopf, Olivier Bachem
	Rates of Convergence for Sparse Variational Gaussian Process Regression	David R. Burt, Carl E. Rasmussen, Mark van der Wilk
2018	Delayed Impact of Fair Machine Learning	Lydia T. Liu, University of California Berkeley; et al.
	Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples	Anish Athalye, Massachusetts Institute of Technology; et al.
2017	Understanding Black-box Predictions via Influence Functions	Pang Wei Koh & Percy Liang, Stanford University
2016	Ensuring Rapid Mixing and Low Bias for Asynchronous Gibbs Sampling	Christopher De Sa, Stanford University; et al.
	Pixel Recurrent Neural Networks	Aaron Van den Oord, Google; et al.
	Dueling Network Architectures for Deep Reinforcement Learning	Ziyu Wang, Google; et al.
2015	A Nearly-Linear Time Framework for Graph-Structured Sparsity	Chinmay Hegde, Massachusetts Institute of Technology; et al.

ICML (International Conference on Machine Learning)		
	Optimal and Adaptive Algorithms for Online Boosting	Alina Beygelzimer, Yahoo! Research; et al.
2014	Understanding the Limiting Factors of Topic Modeling via Posterior Contraction Analysis	Jian Tang, Peking University; et al.
2013	Vanishing Component Analysis	Roi Livni, The Hebrew University of Jerusalum; et al.
	Fast Semidifferential-based Submodular Function Optimization	Rishabh Iyer, University of Washington; et al.
2012	Bayesian Posterior Sampling via Stochastic Gradient Fisher Scoring	Sungjin Ahn, University of California Irvine; et al.
2011	Computational Rationalization: The Inverse Equilibrium Problem	Kevin Waugh, Carnegie Mellon University; et al.
2010	Hilbert Space Embeddings of Hidden Markov Models	Le Song, Carnegie Mellon University; et al.
2009	Structure preserving embedding	Blake Shaw, Tony Jebara, Columbia University

表 4-2 NeurIPS 近 10 年 best paper

NeurIPS（Neural Information Processing Systems）		
年份	论文标题	作者
2018	Non-delusional Q-learning and Value-iteration	Tyler Lu, Dale Schuurmans, Craig Boutilier
	Optimal Algorithms for Non-Smooth Distributed Optimization in Networks	Kevin Scaman, Francis Bach, Sebastien Bubeck, Laurent Massoulié, Yin Tat Lee
	Nearly Tight Sample Complexity Bounds for Learning Mixtures of Gaussians via Sample Compression Schemes	Hassan Ashtiani, Shai Ben-David, ick Harvey，Christopher Liaw, Abbas Mehrabian, Yaniv Plan
	Neural Ordinary Differential Equations	Tian Qi Chen, Yulia Rubanova, Jesse Bettencourt，David Duvenaud
2017	Safe and Nested Subgame Solving for Imperfect-Information Games	Noam Brown, Tuomas Sandholm
	Variance-based Regularization with Convex Objectives	Hongseok Namkoong, John Duchi
	A Linear-Time Kernel Goodness-of-Fit Test	Wittawat Jitkrittum, Wenkai Xu, Zoltan Szabo，Kenji Fukumizu, Arthur Gretton
2016	Value Iteration Networks	Aviv Tamar, Yi Wu, Garrett Thomas, Sergey Levine, Pieter Abbeel
	Matrix Completion has No Spurious Local Minimum	Rong Ge, Jason Lee, Tengyu Ma
	Interactive musical improvisation with Magenta	Adam Roberts, Jesse Engel, Curtis Hawthorne, Ian Simon, Elliot Waite, Sageev Oore, Natasha Jaques, Cinjon Resnick, Douglas Eck
2015	Competitive Distribution Estimation: Why is Good-Turing Good	Alon Orlitsky, Ananda Theertha Suresh
	Fast Convergence of Regularized Learning in Games	Vasilis Syrgkanis, Alekh Agarwal, Haipeng Luo，Robert Schapire
2014	Asymmetric LSH (ALSH) for sublinear time Maximum Inner Product Search (MIPS)	Anshumali Shrivastava, Ping Li
	A* Sampling	Chris J. Maddison, Daniel Tarlow, Tom Minka
	A Memory Frontier for Complex Synapses	Subhaneil Lahiri, Surya Ganguli

NeurIPS（Neural Information Processing Systems）		
2013	Submodular Optimization with Submodular Cover and Submodular Knapsack Constraints	Rishabh Iyer, Jeff Bilmes
	Scalable Influence Estimation in Continuous-Time Diffusion Networks	Nan Du, Le Song, Manuel Gomez-Rodriguez，Hongyuan Zha
2012	No voodoo here! Learning discrete graphical models via inverse covariance estimation	Po-Ling Loh, Martin Wainwright
	Discriminative Learning of Sum-Product Networks	Robert Gens, Pedro Domingos
2011	Efficient Inference in Fully Connected CRFs with Gaussian Edge Potentials	Philipp Krähenbühl, Vladlen Koltun
	Priors Over Recurrent Continuous Time Processes	Ardavan Saeedi, Alexandre Bouchard-Côte
	Fast and Accurate K-means for Large Datasets	Michael Shindler, Alex Wong, Adam Meyerson
2010	Construction of dependent dirichlet Processes based on Poisson Processes	Dahua Lin, Eric Grimson, John Fisher
	A Theory of Multiclass Boosting	Indraneel Mukherje，Robert E Schapire
2009	An LP View of the M-Best MAP Problem	Menachem Fromer，Amir Globerson
	Fast Subtree Kernels on Graphs	Nino Shervashidze，Karsten Borgwardt

4.1 ICML 历年最佳论文解读

- 2019 年最佳论文

论文题目：*Challenging Common Assumptions in the Unsupervised Learning of Disentangled Representations*

中文题目：挑战无监督分离式表征的常见假设

论文作者：Francesco Locatello, Stefan Bauer, Mario Lucic, Gunnar Rätsch, Sylvain Gelly, Bernhard Schölkopf, Olivier Bachem

参与单位：ETH Zurich, Department for Computer Science; MaxPlanck Institute for Intelligent Systems; Google Research Brain Team

论文地址：https://aminer.cn/pub/5c04967517c44a2c74709162/challenging-common-assumptions-in-the-unsupervised-learning-of-disentangled-representations

论文解读：文章主要从理论和实践两方面对这一领域中的一些基本假设提出了挑战。文章从理论上证明，如果没有对所考虑的学习方法和数据集产生归纳偏置，那么解耦表示的无监督学习基本上是不可能的。文章还采用了完善的无监督解耦学习实验方案，进行了一个超级大规模的实验研究。最后还发布了 disentanglement_lib，这是一个用于训练和评估解耦表示的新库。由于复制这个结果需要大量的计算工作，论文还发布了超过 10000 个预训练的模型，可以作为未来研究的基线方法。

论文题目：*Rates of Convergence for Sparse Variational Gaussian Process Regression*

中文题目：稀疏变分高斯过程回归的收敛速度

论文作者：David R. Burt, Carl E. Rasmussen,Mark van der Wilk

参与单位：University of Cambridge; PROWLER.io,Cambridge

论文地址：https://www.aminer.cn/pub/5cede106da562983788e64b9/rates-of-convergence-for-sparse-variational-gaussian-process-regression

论文解读：这篇文章来自英国剑桥大学。自从许多研究人提出了对高斯过程后验的变分近似法后，避免了数据集大小为 N 时 $O(N^3)$ 的缩放。它们将计算成本降低到 $O(NM^2)$，其中 $M \leqslant N$ 是诱导变量的数量。虽然 N 的计算成本似乎是线性的，但算法的真正复杂性取决于 M 如何增加以确保一定的近似质量。论文证明了稀疏 GP 回归变分近似到后验变分近似的 KL 散度的界限，该界限仅依赖于先验核的协方差算子的特征值的衰减。这些边界证明了直观的结果，平滑的核、训练数据集中在一个小区域，允许高质量、非常稀疏的近似。这些边界证明了用 $M \leqslant N$ 进行真正稀疏的非参数推理仍然可以提供可靠的边际似然估计和点后验估计。对非共轭概率模型的扩展，是未来研究的一个有前景的方向。

- 2018 年最佳论文

论文题目：*Delayed Impact of Fair Machine Learning*

中文题目：公正机器学习的滞后影响

论文作者：Lydia T.Liu, Sarah Dean, Esther Rolf, Max Simchowitz, Moritz Hardt

参与单位：Department of Electrical Engineering and Computer Sciences, University of California, Berkeley

论文地址：https://www.aminer.cn/pub/5aed14d617c44a44381595bd/delayed-impact-of-fair-machine-learning

论文解读：机器学习的公平性主要在静态分类设置中得到研究，但却没有关注这些决策如何随时间改变潜在的群体。传统的观点认为公平性标准能提升他们想保护的群体的长期利益。本文研究了静态公平性标准如何与暂时的利益指标相互作用，例如利益变量的长期提升、

停滞和下降。本文证实了即使在一步反馈模型中，常见的公平性准则没有随时间带来改善，实际上可能给特定案例带来了伤害。

论文题目：*Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples*

中文题目：混淆梯度的虚假安全感：对抗样本防御

论文作者：Anish Athalye, Nicholas Carlini, David Wagner

参与单位：Equal contribution; Massachusetts Institute of Technology; University of California, Berkeley

论文地址：https://www.aminer.cn/pub/5a9cb66717c44a376ffb89eb/obfuscated-gradients-give-a-false-sense-of-security-circumventing-defenses-to-adversarial

论文解读：如果在一张图片添加干扰，可能就可以骗过分类器。为了抵御对抗样本的攻击，使得神经网络在受到迭代攻击时不受对抗样本干扰，研究人员在寻找强大的对抗样本防御器，使其在面对基于优化的攻击之下，可以实现对对抗样本的鲁棒性防御。

- 2017 年最佳论文

论文题目：*Understanding Black-box Predictions via Influence Functions*

中文题目：利用影响函数理解黑箱预测

论文作者：Pang Wei Koh, Percy Liang

参与单位：Stanford University

论文地址：https://www.aminer.cn/pub/599c7983601a182cd2646c6a/understanding-black-box-predictions-via-influence-functions

论文解读：这篇论文利用影响函数（稳健统计学中的经典技术），通过学习算法跟踪模型的预测并追溯到训练数据，从而确定对给定预测影响最大训练点来解释黑箱模型的预测。为了将影响函数扩展到现代机器学习中，论文中设计了一个简单高效的实验，仅需梯度 oracle 访问和 Hessian 矢量积。而且即使在非凸和非微分模型上，影响函数的近似值算法仍然可以提供有价值的信息。在线性模型和卷积神经网络中，论文中也证明，影响函数可用于理解模型行为，调试模型，检测数据集错误，甚至是生成视觉上无法区分的训练集攻击。

- 2016 年最佳论文

论文题目：*Ensuring Rapid Mixing and Low Bias for Asynchronous Gibbs Sampling*

中文题目：确保异步吉布斯采样的快速混合和低偏差

论文作者：Christopher De Sa, Kunle Olukotun, Christopher Ré

参与单位：Stanford University

论文地址：https://www.aminer.cn/pub/5c8bcd474895d9cbc6ad8be0/ensuring-rapid-mixing-and-low-bias-for-asynchronous-gibbs-sampling

论文解读：吉布斯采样（Gibbs Sampling）是一种常被用于估计边缘分布（marginal distribution）的马尔可夫链蒙特卡罗技术（Markov chain Monte Carlo technique）。为了加速吉布斯采样，人们最近产生了通过异步执行并行处理它的兴趣。尽管一些经验结果表明许多模型都可以有效地进行异步采样，但传统的马尔克夫链分析却无法应用于异步的情况，因此对异步吉布斯采样只有很少的了解。在这篇论文中，我们设法更好地了解了异步吉布斯的两个主要挑战：偏差（bias）和混合时间（mixing time）。我们通过实验证明了我们的理论结果是符合实际结果的。

论文题目：*Pixel Recurrent Neural Networks*

中文题目：像素循环神经网络

论文作者：Aaron van den Oord, Nal Kalchbrenner, Koray Kavukcuoglu

参与单位：Google DeepMind

论文地址：https://arxiv.org/abs/1601.06759

论文解读：在无监督学习中，给自然图像分布建模是一个里程碑式的问题。这项任务要求得到可以同时表现图像、易于处理并且具备可扩展性的图像模型。我们展示了一个可以沿二维空间维度依次预测图像中像素的深度神经网络。我们的方法建立了原始像素值的离散概率模型，并且编码了图像中完整的依赖关系集合。该架构的不同之处在于它包括快速二维循环层（recurrent layers）和对深度循环网络中残差连接（residual connections）的有效利用。我们完成了自然图像上的对数似然分数，其比之前最先进的还要好很多。我们主要的成果还包括提供多样化的 ImageNet 数据集基准。从模型中生成了新鲜多样且全局同一的样本。此论文提出了一系列生成模型，可直接对像素的统计依赖关系进行建模。这些模型包括两个 PixelRNN：Row LSTM 和 Diagonal BiLSTM（区别主要在于它们进行预测使用到的条件信息所在的领域）；一个 PixelCNN，以及一个多尺度 PixelRNN。

论文题目：*Dueling Network Architectures for Deep Reinforcement Learning*

中文题目：深度强化学习中的竞争网络架构

论文作者：Ziyu Wang, Tom Schaul, Matteo Hessel, Hado van Hasselt, Marc Lanctot, Nando de Freitas

参与单位：Google DeepMind

论文地址：https://arxiv.org/abs/1511.06581

论文解读：近几年，已经有很多在强化学习中使用深度表征获得成功的例子。然而，这些应用中的很多例子仍然使用传统的架构，比如卷积网络、LSTMs，或者是自动编码器。在此论文中，我们提出了一个新的用于无模型（model free）强化学习的神经网络架构。我们的竞争网络（dueling network)表示了两种独立的评估量：一个用于状态价值函数（state value function)，一个用于状态依存动作优势函数（state-dependent action advantage function）。这一分解的主要好处是在没有将任何变化强加于低层的强化学习算法的情况下，在动作（action）间归纳学习。我们的结果显示，这一架构在多种价值相似的动作面前能引发更好的政策评估。此外，这一竞争架构使得我们的强化学习代理胜过 Atari 2600 领域最前沿的研究。在这篇论文中，作者基于分开建模状态值和动作优势的想法，提出了一款可供选择的用于深度 Q 网络（DQN）的架构和相关的学习方案。当被应用于 Atari 学习环境（Atari Learning Environment）基准时，这项技术显著推进了当前最先进的研究成果。

- 2015 年最佳论文

论文题目：*A Nearly-Linear Time Framework for Graph-Structured Sparsity*

中文题目：图结构稀疏性的近似线性时间框架

论文作者：Hegde, Chinmay, Indyk, Piotr, Schmidt, Ludwig

参与单位：Massachusetts Institute of Technology

论文地址：http://proceedings.mlr.press/v37/hegde15.pdf

论文解读：本文引入了一个通过图定义的稀疏结构框架。其方法较灵活，并且推广到了以前研究过的几个稀疏模型。此外，本文还为该稀疏度模型提供了有效的投影算法，该模型几乎在线性时间内运行。在稀疏恢复的背景下，本文证明了该框架在理论上实现了广泛参数下的信息最优样本复杂性。本文用实验来补充该理论分析，证明该算法在实践中也改进了先前的工作。

论文题目：*Optimal and Adaptive Algorithms for Online Boosting*

中文题目：Online Boosting 的优化和自适应算法

论文作者：Alina Beygelzimer, Satyen Kale, Haipeng Luo

参与单位：Yahoo Labs; Princeton University

论文地址：https://arxiv.org/abs/1502.02651

论文解读：我们学习在线促进，这是一项将任何一个弱的在线学习者转变为强的在线学习者的任务。基于对网络学习能力弱的一个新的自然定义，我们开发了两种在线增强算法。第一种算法是在线版本的 Boost by Majority。通过证明一个匹配下界，我们证明了该算法对于弱学习者的数量和达到指定精度所需的样本复杂度是本质上最优的。然而，这种优化算法并不具有自适应性。利用在线损失最小化的工具，推导了一种无参数但非最优的自适应在线增强算法。这两种算法都与基础学习者一起工作，基础学习者可以直接处理示例重要性权重，也可以使用升迁者定义的概率拒绝抽样示例。结果与广泛的实验研究相辅相成。

- 2014 年最佳论文

论文题目：*Understanding the Limiting Factors of Topic Modeling via Posterior Contraction Analysis*

中文题目：经由过程后验收缩分析理解主题建模的限制因素

论文作者：Ming Zhang, Jian Tang, Zhaoshi Meng

参与单位：School of EECS, Peking University; Department of EECS, University of Michigan; Department of Statistics, University of Michigan; School of Information, University of Michigan

论文地址：http://proceedings.mlr.press/v32/tang14.pdf

论文解读：潜在狄利克雷分布（LDA）已经成为了机器学习建模工具箱中的一个标准工具。它们已被应用于各种不同程度的数据集、背景和任务，但是迄今为止，几乎没有正式的理论来解释 LDA 的行为，并且尽管对其很熟悉，但是对影响模型推理性能的数据的性质几乎没有系统性的分析和指导。本文试图通过对影响 LDA 的性能的因素进行系统分析来解决此问题。本文提出的定理阐明了随着数据量的增加后验概率，并使用综合和真实的数据集进行了全面的支持性实证研究。基于这些结果，本文对如何为主题模型识别合适的数据集以及如何制定特定的模型参数提供了实际指导。

- 2013 年最佳论文

论文题目：*Vanishing Component Analysis*

中文题目：经由过程后验收缩分析理解主题建模的限制因素

论文作者：Roi Livni, Shai Shalevshwartz, Amir Globerson

参与单位：Hebrew University; Hewlett-Packard Laboratories Israel Ltd

论文地址：http://proceedings.mlr.press/v28/livni13.pdf

论文解读：传统的特征选择方法通常是在采样中选择显著的特征，作者研究的是，在特征选择时，是否能够选择一些不变的特征。文章描述并分析了构造一组消失理想生成器的有效过程。该过程是数值稳定的，并且可以用于近似消失多项式。由此得到的多项式捕捉数据中的非线性结构，例如可用于监督学习。与核方法的实证比较表明，文章提出的方法构造了更紧凑的分类器，具有相当的精度。

论文题目：*Fast Semidifferential-based Submodular Function Optimization*

中文题目：基于半微分的快速子模块函数优化

论文作者：Iyer, Rishabh, Jegelka, Stefanie, Bilmes, Jeff

参与单位：Department of EE, University of Washington

论文地址：http://export.arxiv.org/pdf/1308.1006

论文解读：本文提出了一种实用而强大的基于离散半微分（子微分和超微分）的无约束和约束子模函数优化新框架。所得到的算法反复计算并有效地优化了子模半梯度，为子模优化提供了新的、通用的方法。此外，本文的方法还采取步骤，提供适用于次模最小化和最大化的统一范式，这些问题在历史上得到了相当明显的处理。本文的算法的实用性很重要，因为子模性由于其自然和广泛的适用性，最近在机器学习中占据了优势。分析了本文的极小化和最大化算法的理论性质，表明许多最先进的最大化算法都是特殊情况。最后，本文将理论分析与实证实验相补充。

- 2012 年最佳论文

论文题目：*Bayesian Posterior Sampling via Stochastic Gradient Fisher Scoring*

中文题目：通过随机梯度 Fisher 得分进行贝叶斯后验采样

论文作者：S.Ahn, A.Korattikara, M.Welling

参与单位：Dept. of Computer Science, UC Irvine, Irvine

论文地址：https://arxiv.org/ftp/arxiv/papers/1206/1206.6380.pdf

论文解读：在本文中，讨论了以下问题：如果我们只允许对生成的每个样本接触一小批数据项，那么我们是否可以近似地从贝叶斯后验分布中提取样本？本文提出了一种基于随机梯度朗格文方程（SGLD）的混合算法，但是其混合速率慢。通过利用贝叶斯中心极限定理，我们扩展了 SGLD 算法，使其在高混合速率下从后验函数的正态近似中采样，而在慢混合速率下，它将使用预调节矩阵模拟 SGLD 的行为。作为一个额外的好处，该算法使人想起费希尔评分（随机梯度），因此在老化过程中是一个有效的优化器。

- 2011 年最佳论文

论文题目：*Computational Rationalization: The Inverse Equilibrium Problem*

中文题目：计算合理化：逆向平衡问题

论文作者：Kevin Waugh, Brian D.Ziebart, J. Andrew (Drew) Bagnell

参与单位：Carnegie Mellon University

论文地址：https://www.ri.cmu.edu/pub_files/2011/6/paper.pdf

论文解读：从少量的观察结果中模拟不完美因素的有目的的行为是一项具有挑战性的任务。当限制在单智能体决策理论设置下时，逆最优控制技术假定观测行为是未知决策问题的近似最优解。这些技术学习解释示例行为的实用函数，然后可用于准确预测或模拟类似观察到或未观察到的情况下的未来行为。在这项工作中，我们考虑了竞争和合作多代理领域中的类似任务。在这里，不同于单一代理设置，玩家不能近似地最大化其回报-它必须推测其他代理如何行动，以影响游戏的结果。利用遗憾博弈论的概念和最大熵原理，提出了一种预测和概括行为的方法，并在此领域中恢复了奖励函数。

- 2010 年最佳论文

论文题目：*Hilbert Space Embeddings of Hidden Markov Models*

中文题目：隐马尔科夫模型的希尔伯特空间嵌入

论文作者：Le Song, Byron Boots, Sajid M. Siddiqi, Geoffrey J. Gordon

参与单位：School of Computer Science, Carnegie Mellon University; Google; Yahoo! Research

论文地址：https://storage.googleapis.com/pub-tools-public-publication-data/pdf/36408.pdf

论文解读：隐马尔可夫模型是序列数据建模的重要工具。然而，它们仅限于离散的潜在状态，并且主要限于高斯和离散观测。而且，HMM 的学习算法主要依赖于局部搜索启发式

算法，除了下面描述的谱方法。本文提出了一个非参数 HMM，它将传统的 HMM 扩展到结构化和非高斯连续分布。此外，本文还导出了一个学习这些 HMM 的局部最小自由核谱算法。本文将该方法应用于机器人视觉数据、槽车惯性传感器数据和音频事件分类数据，结果表明，在这些应用中，嵌入式 HMM 的性能超过了以往的先进水平。

- 2009 年最佳论文

论文题目：*Structure preserving embedding*

中文题目：结构保留嵌入

论文作者：Blake Shaw, Tony Jebara

参与单位：Department of Computer Science, Columbia University

论文地址：https://www.aminer.cn/pub/53e9981db7602d970203e4a8/structure-preserving-embedding

论文解读：结构保留嵌入（SPE）是一种用于在欧几里得空间中嵌入图形的算法，该嵌入是低维的，并保留了输入图的全局拓扑属性。如果诸如 k 最近邻之类的连通性算法可以在嵌入后仅从节点的坐标轻松恢复输入图的边缘，则可以保留拓扑。SPE 公式化为半定程序，该程序学习受一组线性不等式约束的低阶内核矩阵，该不等式捕获输入图的连通性结构。SPE 在图形的可视化和无损压缩方面提供了显著的改进，胜过了诸如光谱嵌入和 Laplacian 特征图之类的流行方法。我们发现，仅需使用几个维度就可以正确嵌入许多经典图和网络。

4.2 NeurIPS 历年最佳论文解读

- 2018 年最佳论文

论文题目：*Non-delusional Q-learning and Value-iteration*

中文题目：非妄想 Q 学习和价值迭代

论文作者：Tyler Lu, Dale Schuurmans, Craig Boutilier

参与单位：Google AI

论文地址：https://www.aminer.cn/pub/5c2348ceda562935fc1d5724/non-delusional-q-learning-and-value-iteration

论文解读：本文用函数逼近法确定了 Q-学习和其他形式的动态规划中误差的根本来源。当近似结构限制了可表达的贪婪策略的类别时，就会产生偏差。由于标准 Q-updates 对可表达的策略类做出了全局不协调的动作选择，因此可能导致不一致甚至冲突的 Q 值估计，从而导致病态行为，例如过度/低估、不稳定甚至发散。为了解决这个问题，本文引入了策略一致性的新概念，并定义了一个本地备份流程，通过使用信息集，也就是记录与备份 Q 值一致的策略约束集，来确保全局一致性。本文证明了使用这种备份的基于模型和无模型的算法都能消除妄想偏差，从而产生第一种已知算法，保证在一般条件下的最优结果。此外，这些算法只需要多项式的多个信息集（从潜在的指数支持）。最后，本文建议使用其他实用的启发式价值迭代和 Q 学习方法去尝试减少妄想偏差。

论文题目：*Optimal Algorithms for Non-Smooth Distributed Optimization in Networks*

中文题目：非光滑凸函数的分布式优化算法

论文作者：Kevin Scaman, Francis Bach, Sebastien Bubeck, Laurent Massoulié, Yin Tat Lee

参与单位：Noah’s Ark Lab, Huawei Technologies

论文地址：https://arxiv.org/pdf/1806.00291.pdf

论文解读：在本文中，我们考虑使用计算单元网络的非光滑凸函数的分布式优化。我们在两个正则性假设下研究这个问题：（1）全局目标函数的 Lipschitz 连续性；（2）局部个体函数的 Lipschitz 连续性。在局部正则性假设下，本文给出了称为多步原对偶（MSPD）的一阶最优分散算法及其相应的最优收敛速度。这个结果的一个显著特点是，对于非光滑函数，当误差的主要项在 O(1/t)中时，通信网络的结构仅影响 O(1/t)中的二阶项，其中 t 是时间。换言之，即使在非强凸目标函数的情况下，由于通信资源的限制而导致的误差也以快速率减小。在全局正则性假设下，基于目标函数的局部平滑，给出了一种简单而有效的分布式随机平滑（DRS）算法，并证明了 DRS 在最优收敛速度的 d/4 乘因子内，其中 d 为底层。

论文题目：*Nearly Tight Sample Complexity Bounds for Learning Mixtures of Gaussians via Sample Compression Schemes*

中文题目：通过样本压缩方案学习混合高斯模型的近乎紧密的样本复杂性边界

论文作者：Hassan Ashtiani, Shai Ben-David, NicholasJ.A.Harvey, Chritopher Liaw, AbbasMehrabian, YanivPlan

参与单位：Department of Computing and Software McMaster University; School of Computer Science, University of Waterloo; Department of Computer Science, University of British

Columbia; School of Computer Science McGill University Montréal; Department of Mathematics, University of British Columbia

论文地址：https://papers.NeurIPS.cc/paper/7601-nearly-tight-sample-complexity-bounds-for-learning-mixtures-of-gaussians-via-sample-compression-schemes.pdf

论文解读：本文证明了 $O(k\ d^2/\varepsilon^2)$样本对于学习 R^d 中 k 个高斯的混合，直至总变差距离中的误差 ε 来说，是充分必要条件。这改善了已知的上界和下界这一问题。对于轴对准高斯混合，本文证明了 $O(k\ d/\varepsilon^2)$样本匹配一个已知的下界是足够的。上限是基于样本压缩概念的分布学习新技术。任何允许这种样本压缩方案的分布类都可以用很少的样本来学习。此外，如果一类分布具有这样的压缩方案，那么这些产品和混合物的类也是如此。本文主要结果的核心是证明了 R^d 中的高斯类能有效的进行样本压缩。

论文题目：*Neural Ordinary Differential Equations*

中文题目：神经常微分方程

论文作者：Tian Qi Chen, Yulia Rubanova, Jesse Bettencourt, David Duvenaud

参与单位：University of Toronto

论文地址：https://arxiv.org/pdf/1806.07366.pdf

论文解读：本文介绍了一系列新的深度神经网络模型。本文使用神经网络参数化隐藏状态的导数，而不是指定隐藏层的离散序列。使用黑盒微分方程求解器计算网络的输出。这些连续深度模型具有恒定的内存成本，使其评估策略适应每个输入，并且可以明确地交换数值精度以获得速度。本文在连续深度残差网络和连续时间潜变量模型中证明了这些性质。本文还构建了连续归一化流，这是一种可以通过最大似然进行训练的生成模型，无需对数据维度进行分区或排序。为了训练，本文展示了如何通过任何 ODE 求解器进行可扩展反向传播，而无需访问其内部操作。这允许在较大模型中对 ODE 进行端到端训练。

- 2017 年最佳论文

论文题目：*Safe and Nested Subgame Solving for Imperfect-Information Games*

中文题目：不完全信息博弈的安全嵌套子博弈求解

论文作者：Noam Brown, Tuomas Sandholm

参与单位：Computer Science Department, Carnegie Mellon University

论文地址：https://arxiv.org/pdf/1705.02955.pdf

论文解读：和完美信息博弈不同，不完美信息博弈不能通过将博弈分解为可独立求解的子博弈而求得占优策略。因此本文越来越多地使用计算密集的均衡判定技术，并且所有的决策必须将博弈的策略当作一个整体。本文提出了一种无论在理论上还是在实践上都超越了之前方法的子博弈求解技术。本文还展示了如何对它们和以前的子博弈求解技术进行调整，以对超出初始行动提取（original action abstraction）的对手的行动做出应答；这远远超越了之前的顶尖方法，即行动转化（action translation）。最后，本文展示了当博弈沿着博弈树向下进行时，子博弈求解可能会重复进行，从而大大降低可利用性。

论文题目：*Variance-based Regularization with Convex Objectives*

中文题目：带有凸对象的基于方差的正则化方法

论文作者：Hongseok Namkoong, John Duchi

参与单位：Stanford University

论文地址：https://arxiv.org/pdf/1610.02581.pdf

论文解读：本文研究了一种风险最小化和随机优化的方法，该方法可以为方差提供一个凸属性的替代项，并允许在逼近和估计误差间实现近似最优与高效计算间的权衡。本文的方法建立在分布鲁棒性优化和 Owen 经验性似然度的基础上，并提供了一些有限样本（finite-sample）和渐进结果以展示估计器的理论性能。具体来说，本文证明了该过程具有最优性保证（certificates of optimality），并通过逼近和最优估计误差间良好的权衡在更一般的设定下比经验风险最小化方法有更快的收敛率。本文还给出了确凿的经验性证据，表明估计器在实践中会在训练样本的方差和绝对性能之间进行权衡。此外，估计器也会提升标准经验风险最小化方法在许多分类问题上的测试性能。

论文题目：*A Linear-Time Kernel Goodness-of-Fit Test*

中文题目：一种线性时间核的拟合优度测试方法

论文作者：Wittawat Jitkrittum, Wenkai Xu, Zoltan Szabo, Kenji Fukumizu, Arthur Gretton.

参与单位：Gatsby Unit, UCL; CMAP, École Polytechnique

论文地址：https://arxiv.org/pdf/1705.07673.pdf

论文解读：本文提出了一个全新的拟合优度（goodness-of-fit）的适应性测试法，其中计算资源的消耗与样本数呈线性关系。本文通过最小化假负类率来学习最能展示观察样本和参考模型之间差异的测试特征。这些特征是通过 Stein 法构造的——这意味着没有必要计算模型的归一化常数。本文分析了新测试的 Bahadur 渐进效率，并证明了在均值偏移（mean-shift）

的情况下，无论选择哪个测试参数，本文的测试总是比先前的线性时间核测试具有更高的相对效率。在高维和模型结构可用的情况下，本文的拟合优度测试在模型中抽取样本，表现远远超越基于最大平均差异（Maximum Mean Discrepancy）的二次时序双样本测试。

- 2016 年最佳论文

论文题目：*Value Iteration Networks*

中文题目：价值迭代网络

论文作者：Aviv Tamar, Yi Wu, Garrett Thomas, Sergey Levine, Pieter Abbeel

参与单位：Dept. of Electrical Engineering and Computer Sciences, UC Berkeley

论文地址：https://arxiv.org/pdf/1602.02867.pdf

论文解读：本文介绍了一个价值迭代网络（VIN）：一种完全可微分的神经网络，内置“规划模块”。VIN 可以学习计划，并且适用于预测涉及基于计划的推理的结果，例如加强学习的政策。我们的方法的关键是一种新的可微近似值迭代算法，它可以表示为卷积神经网络，并使用标准的反向传播训练端到端。本文基于离散和连续路径规划域以及基于自然语言的搜索任务评估基于 VIN 的策略。本文表明，通过学习一个明确的规划计算，VIN 策略可以更好地推广到新的、未发现的领域。

论文题目：*Matrix Completion has No Spurious Local Minimum*

中文题目：矩阵填充没有假的局部最小值

论文作者：Rong Ge, Jason Lee, Tengyu Ma

参与单位：Duke University; University of Southern California; Princeton University

论文地址：https://arxiv.org/pdf/1605.07272.pdf

论文题目：矩阵填充是一个基本的机器学习问题，具有广泛的应用，尤其是在协作过滤和推荐系统中。简单的非凸优化算法在实践中很流行且有效。我们证明了用于矩阵填充的常用非凸目标函数没有假的局部最小值——所有局部最小值也必须是全局的。因此，许多流行的优化算法（例如随机梯度下降）可以通过多项式时间内的任意初始化可证明地解决矩阵填充问题。当观察到的条目包含噪声时，结果可以推广到该设置。我们认为，我们的主要证明策略对于理解其他涉及部分或嘈杂观测值的统计问题的几何性质很有用。

论文题目：*Interactive musical improvisation with Magenta*

文题目：基于 Magenta 的即兴音乐交互体验

论文作者：Adam Roberts, Jesse Engel, Curtis Hawthorne, Ian Simon, Elliot Waite, Sageev Oore, Natasha Jaques, Cinjon Resnick, Douglas Eck

参与单位：Google Brain; Dalhousie University; MIT

论文地址：https://nips.cc/Conferences/2016/ScheduleMultitrack?event=6307

论文解读：作者结合了基于 LSTM 的循环神经网络和 Deep Q-learning 建立了实时生成音乐序列。LSTM 的任务是学习音乐评分（编码为 MIDI，而不是音频文件）的一般结构。Deep Q-learning 用来改进基于奖励的序列，如期望的类型，组成正确性和预测人类协作者演奏的内容。基于 RNN 模型的生成与强化学习的结合是一种生成音乐的全新方式。这种方式比单独使用 LSTM 更为稳定，生成的音乐更加好听。该方法有两个任务：生成对短旋律输入的响应，以及实时生成对旋律输入的伴奏，持续对未来输出进行预测。本方法在 TensorFlow 中加入了一个全新的 MIDI 接口产生即兴的音乐体验，让使用者可以与神经网络实时交互。

- 2015 年最佳论文

论文题目：*Competitive Distribution Estimation: Why is Good-Turing Good*

中文题目：竞争分布估计：为什么 Good-Turing 好

论文作者：Alon Orlitsky, Ananda Theertha Suresh

参与单位：UC San Diego

论文地址：http://120.52.51.17/papers.NeurIPS.cc/paper/5762-competitive-distribution-estimation-why-is-good-turing-good.pdf

论文解读：该论文属于统计学习的理论研究范畴，它对估计离散变量的分布律这一普遍问题，提出了基于 Good-Turing 估计量的两种改进方法，借助对先验的最优估计量，给出了针对任意分布律的近似最优的高效估计。论文不仅指出这两种方法可以快速收敛，同时还给出相应的理论分析。

论文题目：*Fast Convergence of Regularized Learning in Games*

中文题目：博弈中正则化学习的快速收敛

论文作者：Vasilis Syrgkanis, Alekh Agarwal, Haipeng Luo, Robert Schapire

参与单位：Microsoft Research New York; Princeton University

论文地址：http://120.52.51.17/papers.NeurIPS.cc/paper/5763-fast-convergence-of-regularized-learning-in-games.pdf

论文解读：我们证明了具有新近偏置形式的自然类正则化学习算法，可以在多人正常形式博弈中达到更快的收敛速度，从而有效地近似并达到粗略的相关均衡。当博弈中的每个玩家使用我们类中的算法时，它们会在 $O(T^{-3/4})$处衰减，而效用的总和会在 $O(T^{-1})$处收敛至最佳值——在最差的情况 $O(T^{-1/2})$比率下有所改善情况。我们展示了该类中任何算法的黑盒衰减，以针对对手达到 $\tilde{O}(T^{-1/2})$的速率，同时保持该类中算法的较快速率。我们的结果扩展了 Rakhlin、Shridharan 和 Daskalakis 等人的结果，它们只针对特定算法分析了两人零和博弈。

- 2014 年最佳论文

论文题目：*Asymmetric LSH (ALSH) for sublinear time Maximum Inner Product Search (MIPS)*

中文题目：次线性时间的不对称 LSH（ALSH）最大内积检索（MIPS）

论文作者：Anshumali Shrivastava, Ping Li

参与单位：Department of Computer Science, Cornell University; Department of Statistics and Biostatistics Department of Computer Science, Rutgers University

论文地址：https://arxiv.org/pdf/1405.5869.pdf

论文解读：我们提出了第一个可证明的次线性时间哈希算法，用于近似最大内积检索（MIPS）。使用（未归一化的）内积作为基础相似性度量进行检索是一个已知的难题，并且为 MIPS 查找哈希方案是很困难的事情。虽然现有的本地敏感哈希（LSH）框架不足以解决 MIPS，但在本文中，我们将 LSH 框架扩展为允许非对称哈希方案。我们的方法基于一个关键的观察，即在独立的不对称变换之后，找到最大内积的问题可以转化为经典设置中的近似近邻搜索问题。这个关键的发现使针对 MIPS 的高效亚线性哈希方案成为可能。我们提出的算法简单易实现。所提出的散列方案与协作过滤中的两种流行的常规 LSH 方案相比，显著节省了计算量：（i）符号随机投影（SRP）和（ii）基于 L-2 范数的 p 稳定分布（L2LSH），在 Netflix 和 Movielens（10M）数据集上的项目推荐任务。

论文题目：*A* Sampling*

中文题目：A*采样

论文作者：Chris J. Maddison, Daniel Tarlow, Tom Minka

参与单位：Dept. of Computer Science, University of Toronto; Microsoft Research

论文地址：https://arxiv.org/pdf/1411.0030.pdf

论文解读：从离散分布中提取样本的问题可以转化为离散优化问题。在这项工作中，本文展示了如何将连续分布的采样转化为连续空间上的优化问题。该方法的核心是最近在数学统计学中描述的一个随机过程，本文称之为 Gumbel 过程。本文提出了一种新的 Gumbel 过程和 A*采样结构，这是一种实用的通用采样算法，它使用 A*搜索来搜索 Gumbel 过程的最大值。本文分析了 A*抽样的正确性和收敛时间，并从经验上证明了它比最相关的自适应拒绝抽样算法更有效地利用了边界和似然估计。

- 2013 年最佳论文

论文题目：*A Memory Frontier for Complex Synapses*

中文题目：复杂突触的记忆边界

论文作者：Subhaneil Lahiri, Surya Ganguli

参与单位：Department of Applied Physics, Stanford University

论文地址：http://120.52.51.14/papers.NeurIPS.cc/paper/4872-a-memory-frontier-for-complex-synapses.pdf

论文解读：一个令人难以置信的鸿沟将突触的理论模型分开，通常仅由表示突触后电位大小的单个标量值描述，来自真实突触下的分子信号传导途径的巨大复杂性。为了理解这种分子复杂性对学习和记忆的功能贡献，必须将突触的理论概念从单个标量扩展到具有许多内部分子功能状态的整个动力系统。这里产生了一个基本问题，突触复杂性如何产生记忆？为了解决这个问题，本文开发了新的数学定理，阐明了复杂突触的结构组织和记忆特性之间的关系，这些突触本身就是分子网络。此外，在证明这些定理时，本文发现了一个基于第一次通过时间理论的框架，对复杂突触模型的内部状态施加顺序，从而简化了突触结构和功能之间的关系。

论文题目：*Submodular Optimization with Submodular Cover and Submodular Knapsack Constraints*

中文题目：具有子模块覆盖和子模块背包约束的子模块优化

论文作者：Rishabh Iyer, Jeff Bilmes

参与单位：Department of Electrical Engineering, University of Washington

论文地址：https://www.aminer.cn/pub/53e9ae5cb7602d97038795fb/submodular-optimization-with-submodular-cover-and-submodular-knapsack-constraints

论文解读：我们研究了两个新的优化问题——最小化受子模块化下界约束（子模块化覆盖）的子模函数和最大化子模块函数受下模块化上限约束（子模块化背包）的约束。我们受到机器学习中许多实际应用的启发，这些应用包括传感器放置和数据子集选择，这些应用要求最大化某个子模块功能（例如覆盖范围或分集），同时最小化另一个子模块功能（例如合作成本）。我们发现通过将这些问题表述为约束优化（对于许多应用程序而言更自然），可以实现许多有界逼近的保证。我们还表明，这两个问题都是密切相关的，可以使用求解一个问题的近似算法来获得对另一个问题的近似保证。我们提供了两个问题的结果，从而表明我们的逼近因子严格到对数因子。最后，我们通过实验证明了算法的性能和良好的可伸缩性。

论文题目：*Scalable Influence Estimation in Continuous-Time Diffusion Networks*

中文题目：连续时间扩散网络中的可扩展影响估计

论文作者：Nan Du, Le Song, Manuel Gomez-Rodriguez, Hongyuan Zha

参与单位：Georgia Institute of Technology; MPI for Intelligent Systems

论文地址：https://www.aminer.cn/pub/53e9ad87b7602d970377ee23/scalable-influence-estimation-in-continuous-time-diffusion-networks

论文解读：如果从媒体站点发布一条信息，我们能否预测它是否可以在一个月内传播到一百万个网页？由于需要同时处理任务的时间敏感性和可伸缩性要求，因此影响估计问题非常具有挑战性。在本文中，我们提出了一种用于连续时间扩散网络中影响估计的随机算法。我们的算法可以用|V|估计网络中每个节点的影响。节点和|ε|使用 $n = O(1/\varepsilon^2)$随机化并以对数因子 $O(n|\varepsilon|+n|V|)$计算边缘到 ε 的精度。当在贪婪影响最大化方法中用作子例程时，我们提出的算法可确保找到一个至少受（1-1/ε|）OPT-2$C\varepsilon$|影响的 C 节点集，其中 OPT 是最佳值。对合成数据和实际数据进行的实验均表明，该算法可以轻松扩展至数百万个节点的网络，同时在估计影响力的准确性和质量方面都大大优于以前的最新技术，选择节点以最大程度地发挥影响力。

- 2012 年最佳论文

论文题目：*No voodoo here! Learning discrete graphical models via inverse covariance estimation*

中文题目：通过逆协方差估计学习离散图模型

论文作者：Po-Ling Loh, Martin Wainwright

参与单位：UC Berkeley, Department of Statistics

论文地址：https://www.aminer.cn/pub/5c75518df56def97985c42b1/no-voodoo-here-learning-discrete-graphical-models-via-inverse-covariance-estimation

论文解读：本文研究了广义协方差矩阵的逆的支持与离散图形模型的结构之间的关系。本文证明了对于某些图结构，指标变量的逆协方差矩阵对图的顶点的支持反映了图的条件独立结构。本文的工作扩展了以前仅针对多元高斯分布建立的结果，并且部分地回答了关于非高斯分布的逆协方差矩阵含义的开放问题。本文提出了基于可能损坏的观测值的具有有界度的一般离散图形模型的图选择方法，并通过模拟验证本文的理论结果。在此过程中，本文还在基于损坏和缺失观测的稀疏高维线性回归设置中建立支持恢复的新结果。

论文题目：*Discriminative Learning of Sum-Product Networks*

中文题目：和积网络的判别学习

论文作者：Robert Gens, Pedro Domingos

参与单位：Department of Computer Science and Engineering, University of Washington

论文地址：http://papers.nips.cc/paper/4516-discriminative-learning-of-sum-product-networks.pdf

论文解读：Sum-product 网络是一种新的深度架构，可以对高树宽模型进行快速、准确的推断。迄今为止，仅提出了用于生成 SPN 的生成方法。在本文中，我们提出了第一种针对 SPN 的判别式训练算法，将前者的高精度与后者的表示能力和易处理性相结合。我们表明，可分辨的判别式 SPN 的类别比可处理的可区分性 SPN 的类别更广泛，并提出了一种有效的反向传播算法来计算条件对数似然度的梯度。我们在标准图像分类任务上测试判别式 SPN。我们使用迄今在 CIFAR-10 数据集上获得最佳结果的方法，其性能比具有 SPN 架构的方法（具有判别性学习本地图像结构）的性能要少。即使仅使用数据集的标记部分，我们也报告了 STL-10 上公布的最高测试准确性。

- 2011 年最佳论文

论文题目：*Efficient Inference in Fully Connected CRFs with Gaussian Edge Potentials*

中文题目：具有高斯边缘电位的完全连接 CRF 中的有效推理

论文作者：Philipp Krähenbühl, Vladlen Koltun

参与单位：Computer Science Department, Stanford University

论文地址：https://static.aminer.org/pdf/20160902/web- conf/NEURIPS/NEURIPS-2011-1998.pdf

论文解读：用于多类图像分割和标记的大多数最新技术使用在像素或图像区域上定义的条件随机字段。尽管区域级模型通常具有密集的成对连通性，但像素级模型却要大得多，并且只允许稀疏图结构。在本文中，我们考虑在图像的完整像素集上定义的完全连接的 CRF 模型。生成的图具有数十亿条边，这使得传统的推理算法不切实际。我们的主要贡献是针对全连接 CRF 模型的高效近似推理算法，其中成对边缘势能由高斯核的线性组合定义。我们的实验表明，像素级的密集连接性可显著改善分割和标记的准确性。

论文题目：*Priors Over Recurrent Continuous Time Processes*

中文题目：连续时间过程的优先级

论文作者：Ardavan Saeedi, Alexandre Bouchard-Côte

参与单位：Department of Statistics, University of British Columbia

论文地址：https://static.aminer.org/pdf/20160902/web- conf/NEURIPS/NEURIPS-2011-2195.pdf

论文解读：本文引入 Gamma 指数过程（GEP），这是一个大型连续时间过程系列的先验。该先验的分层版本（HGEP; Hierarchical GEP）产生用于分析复杂时间序列的有用模型。基于 HGEP 的模型显示出许多有吸引力的特性：等待时间的共轭性，可交换性和封闭形式预测分布，以及时间尺度参数的精确 Gibbs 更新。在建立这些属性之后，本文展示了如何使用粒子 MCMC 方法有效地进行后验推理。本文将本文的模型应用于估计多发性硬化症的疾病进展和 RNA 进化建模的问题。在这两个领域，本文发现本文的模型优于标准的速率矩阵估计方法。

论文题目：*Fast and Accurate K-means for Large Datasets*

中文题目：大型数据集的快速准确 K-means

论文作者：Michael Shindler, Alex Wong, Adam Meyerson

参与单位：School of EECS, Oregon State University; Department of Computer Science, UCLA; Google, Inc. Mountain View, CA

论文地址：http://120.52.51.15/papers.NeurIPS.cc/paper/4362-fast-and-accurate-k-means-for-large-datasets.pdf

论文解读：群集是许多应用程序中的一个普遍问题。在数据太大而无法存储在主内存中、并且必须顺序访问（例如从磁盘）、必须使用尽可能少的内存的情况下，我们考虑 k 均值问题。我们的算法基于最新的理论结果，并进行了重大改进以使其实用。然后，我们合并近似最近邻搜索以计算 *o*(nk)中的 k 均值（其中 n 是数据点的数量；请注意，在给定解的情况下，计算成本需要 Θ (nk)时间）。我们证明了我们的算法在理论上和实验上都优于现有算法，从而在理论和实践上均提供了最先进的性能。

- 2010 年最佳论文

论文题目：*Construction of dependent dirichlet Processes based on Poisson Processes*

中文题目：基于泊松过程的 DDP 构建

论文作者：Dahua Lin, Eric Grimson, John Fisher

参与单位：CSAIL, MIT

论文地址：https://static.aminer.org/pdf/20160902/web- conf/NEURIPS/NEURIPS-2010-3901.pdf

论文解读：本文提出了一种构造依赖 Dirichlet 过程的方法。新的方法揭示了 Dirichlet 和泊松过程之间的内在关系，以便创建一个适合用作先前演化混合模型的 Dirichlet 过程的马尔可夫链。该方法允许组件模型随时间的创建、移除和位置变化，同时保持随机测量略微 DP 分布的属性。此外，本文推导出用于模型推理的 Gibbs 采样算法，并在合成和实际数据上进行测试。实证结果表明该方法可有效地估算动态变化的混合模型。

论文题目：*A Theory of Multiclass Boosting*

中文题目：多类别 Boosting 算法的理论

论文作者：Indraneel Mukherje, Robert E Schapire

参与单位：Google; Princeton University

论文地址：https://static.aminer.org/pdf/20160902/web- conf/NEURIPS/NEURIPS-2010-3934.pdf

论文解读：Boosting 将弱分类器组合在一起，以形成高度准确的预测器。尽管二进制分类的情况已广为人知，但在多类设置中，缺少对弱分类器的“正确”要求或最有效的增强算法的概念。在本文中，我们创建了一个广泛而通用的框架，在此框架内，我们可以对弱分类器进行精确确定并确定最佳要求，在某种意义上设计最有效的 Boosting 算法来满足此类要求。

- 2009 年最佳论文

论文题目：*An LP View of the M-Best MAP Problem*

论文作者：Menachem Fromer, Amir Globerson

参与单位：School of Computer Science and Engineering, Hebrew University of Jerusalem

论文地址：https://static.aminer.org/pdf/20160902/web- conf/NEURIPS/NEURIPS-2009-4089.pdf

论文解读：本文考虑在概率图形模型中以最大概率找到 M 指派的问题。本文展示了如何将这个问题表述为特定多面体上的线性程序（LP）。本文证明，对于树形图（和一般的交叉树），这个多面体具有特别简单的形式，并且与单个不等式约束中的边际多面体不同。本文使用这种表征来为非树图提供近似方案，通过使用这些图上的生成树集。本文提出的方法在 LP 松弛的背景下提出了 M-最佳推理问题，LP 松弛最近得到了相当多的关注，并且已经证明在解决困难的推理问题方面是有用的。本文凭经验证明，本文的方法经常为高树宽度的问题找到可证明的精确 M 最佳配置。

论文题目：*Fast Subtree Kernels on Graphs*

中文题目：图的快速子树核

论文作者：Nino Shervashidze, Karsten Borgwardt

参与单位：Interdepartmental Bioinformatics Group, Max Planck Institutes Tubingen

论文地址：https://www.aminer.cn/pub/53e9a7dcb7602d9703118c82/fast-subtree-kernels-on-graphs

论文解读：在本文中，我们提出了图的快速子树核。在具有 n 个节点和 m 个边，且最大度为 d 的图上，这些高度为 h 的比较子树核可以用 $O(mh)$计算，而 Ramon＆Gartner 经典子树核的缩放比例为 $O(n^2 4^d h)$。效率性的关键是观察到，根据图论进行的 Weisfeiler-Lehman 同构检验很好地计算了作为副产品的子树核。我们的快速子树核可以处理带标签的图形，可以轻松扩展到大型图形，并且可以在准确性和运行时间方面在多个分类基准数据集上胜过最新的图形核。

4.3 专利解读

学术论文代表着研究热点与技术前沿，而专利更能代表本领域的应用转化情况，是研发机构实用化技术储备水平的写照，本小节将介绍对机器学习领域的近期专利。

专利名称：用于照明控制的图像分析方法和装置

专利号：US10477641B2

发明人：Zhao, Nan; Paradiso, Joseph

单位：MIT

年份：2019

概述：

鉴于传统照明系统中复杂的灯光控制和预设定照明场景控制系统可选场景的有限性，以及最新照明系统的部署又极度依赖于用户的评分，无法实现大范围部署应用。因此，MIT 提出一种基于图像分析的照明控制系统。该方法通过摄像机捕捉房间不同照明场景下的高动态范围（HDR）图像集，在此基础上对图像数据进行降维处理，以获得低维度的基于图像的映射集，在该映射集中，每个数据点对应其中的一张图像，即对应每一种照明场景，并且基于图像的映射集可以根据用户对新房间不同照明场景的感知进行调整，来作为房间照明系统的控制空间，从而实现房间照明系统的精准、个性化的控制。该发明的优势在于：在某些情况下，它可以在不收集用户对新房间照明场景的评分情况下，即可控制新房间的照明；或者，只需收集新房间中三个照明场景的用户评分，便可在新房间中部署照明系统。

专利名称：Systems and methods for determining whether a mobile device is inside an environment experiencing adverse pressure variation conditions（用于确定移动设备是否处于不利的压力变化环境的系统和方法）

专利号：US10477358B1

发明人：Michael Dormody, Guiyuan Han, Badrinath Nagarajan

单位：NextNav, LLC

年份：2019

概述：

确定移动设备（如：用户的智能手机）在环境中的确切位置极具挑战性，特别是当移动设备位于城市环境或位于建筑物内时。在特殊情形下，对移动设备高度的不精确估计可能会对移动设备的用户造成危及生命的后果，因为不精确的高度估计可能会延长搜救时间，延误最佳的救治时间。在其他情况下，不精确的海拔估计可能会导致用户前往错误的位置。

基于气压的定位系统，高度可以通过测量来自校准过的移动设备压力传感器的压力和来自校准过的网络气象传感器的环境压力和环境温度的测量值来计算。然而有些环境可能产生供热通风与空气调节（HVAC）效应，例如：密封良好和温度可控的建筑物或汽车。环境的 HVAC 效应表现为环境内压力传感器测量的压力突然跳跃（上升或下降），而网络气象传感器测量的室外压力并没有反映出这种突然跳跃。因而移动设备计算高度的准确性会受到 HVAC 效应的影响。为了准确地计算出移动设备所处的准确高度，NextNav 提出了用于确定移动设备是否处于不利压力变化条件下的方法。

该专利的方法为：根据不同时间段内多次检测到的环境压力分布图以及室外环境的基准压力分布图判断移动设备是否处在有 HVAC 效应的环境中。从而估算出移动设备所处的经度和维度，并给出该位置的置信度。然后，基于移动设备相对于建筑物的估计位置确定移动设备在建筑物内的可能性，并且基于移动设备在建筑物内的可能性确定移动设备在建筑物内或在车辆内。

专利名称：模型运行方法、装置、终端及存储介质

专利号：CN110458294A

发明人：蒋燚

单位：OPPO 广东移动通信有限公司

年份：2019

概述：

现如今，手机、电脑、多媒体设备等终端，可以运用机器学习模型实现不同的功能，例如，人脸检测、语音识别、图像识别等。一般来说，终端使用固定的配置信息对机器学习模型进行配置，使得完成配置的机器学习模型包括的算子是固定的。然而不同处理器（如：NPU、DSP、GPU）支持的算子（如：卷积算子、池化算子、激励函数算子）不同，当处理器不支持机器学习模型中的某些算子时，则该模型无法在该处理器上正常运行。因此，为了保证模型在不同处理器上的正常运行，OPPO 提出了一种机器学习模型运行方法。首先，该方法按算子顺序确定第一处理器不支持运行的算子（第一算子），并基于第一算子对机器学习模型进行调整，调整后的模型包含可支持的算子（第二算子）；其次，针对第一算子，其输入数据为调整后的模型的输出数据，根据算子的运算时间以及其他处理器的状态信息，确定第二

处理器；再者，该方法还对第一算子的模型进行拆解，使大部分算子能够在第一处理器中运行，保证了模型的完整性。

专利名称：深度学习模型的鲁棒性评估方法、装置及存储介质

专利号：CN110222831A

发明人：刘焱、郝新、王洋

单位：百度在线网络技术（北京）有限公司

年份：2019

概述：

在深度学习模型应用于智能驾驶、人脸支付、智能安防等敏感领域时，若遭受对抗样本攻击，将会威胁驾驶安全、资金安全和公共安全。通常把深度学习模型抵御对抗样本的能力称为深度学习模型的鲁棒性。目前评估深度学习模型的鲁棒性主要依赖白盒攻击算法，需要提供深度学习模型的具体网络结构定义以及具体参数，不符合企业知识产权保护的要求。而现有的黑盒攻击算法都依赖于一定的遍历策略，需要频繁地远程调用 API，其评估效率较低。

因此，百度公司提出了一种深度学习模型的鲁棒性评估方法，该方法包括：获取与待评估的深度学习模型对应的开源模型和数据集；将数据集中的原始图像输入到开源模型中，生成与原始图像对应的对抗样本；调用待评估的深度学习模型，使用对抗样本对待评估的深度学习模型进行攻击；统计数据集中的原始图像对应的对抗样本对待评估的深度学习模型的攻击成功率；利用攻击成功率确定待评估的深度学习模型的鲁棒性指标。该发明的优势在于：不用提供深度学习模型的网络结构定义和参数，属于黑盒评估方式，仅需调用该模型即可达到接近白盒攻击算法的评估效果，且大大减少了攻击次数，提升了评估效率。

专利名称：视频识别方法和识别装置、存储介质

专利号：CN109871828A

发明人：贾红红、崔延镇

单位：京东方科技集团股份有限公司

年份：2019

概述：

在相关技术中，仅针对视频帧中的图像进行识别，并未考虑相邻帧之间的变化情况，无法有效提升视频识别准确率。因此，京东方提出了基于图像和光流图的视频识别方法。

该专利的方法为：视频识别装置从视频中提取出图像和光流图（相邻帧之间的变化情况），利用第一机器学习模型对图像进行分类处理，以得到第一分类结果，利用第二机器学习模型对光流图进行分类处理，以得到第二分类结果，其中第一机器学习模型的深度大于第二机器学习模型的深度，对第一分类结果和第二分类结果进行融合，以得到视频的识别结果。由于第一机器学习模型的深度大于第二机器学习模型的深度，因此能够从图像中提取出更多的特征信息，此外，将两个互不相同的机器学习模型的分类结果进行融合，从而能够在识别视频的过程中，不仅借助图像自身的特征信息，还借助相邻帧之间的变化情况，从而提升视频识别的准确度。

专利名称：一种基于众包的多源融合全景建模方法

专利号：CN109523499A

发明人：孙善宝、谭强、于治楼

单位：济南浪潮高新科技投资发展有限公司

年份：2018

概述：

全景图像是利用图像处理技术模拟构建出的三维空间场景，其可以真实、全面、直观的表现现实场景，让人们在计算机虚拟世界中更好的重现场景，使人们产生更加真实的现实体验。图像识别分析需要海量数据的支持，诸如全景地图也需要海量的场景数据，场景图片与拍摄地点、拍摄时间、拍摄角度都有关系，全景地图中的同一地点也需要不同季节、不同天气的图片，这就需要海量实景图片的收集。如何有效的利用智能移动设备，采用众包模式采集全景图像，并利用深度学习算法基于多源图像数据融合进行全景建模成为亟需解决的问题。

该专利通过云端众包平台发布全景图片众包任务，由众包任务接受者根据任务要求，通过移动图像采集设备获取图像，统一汇集到云端，再利用云端聚集的大量计算资源，采用机器学习、深度学习等算法将海量图像及其元数据进行评估、分类、选取、拼接、图像脱敏等处理，实现实景场景的全景建模。提升了全景图像的覆盖率，实现了任务并行处理，提高了全景建模的效率；保护了用户隐私。

专利名称：System and method for generating real-time, event and user-based responses and analytics（生成实时、事件和基于用户的响应和分析的系统和方法）

专利号：US10477271B1

发明人：Joseph Higbee

发明单位：Opine Inc.

年份：2017

概述：

用户响应和分析系统（“URA 系统”），可用于各种环境，如体育赛事、政治辩论、电视节目、电影和其他活动，当用户在消费媒体或现场活动时，有兴趣实时或接近实时地分享他们的观点并消费他人的观点。该方法包括：为个人计算设备提供用户界面，使得用户能够发布语句并提供对事件的实时响应，其中用户界面从用户接收作为非结构化文本、图像、GIF 或视频形式的或选定响应的实时响应；接收用户的实时响应；记录用户实时响应的响内容、响应时间、生物数据和用户位置；然后将用户的实时响应与用户组中的其他用户的实时响应一起编译，生成聚合的响应数据；将聚合响应数据分发给用户组中的用户；为用户生成实时情感数据，并发送基于实时情感数据与用户进行有针对性的通信。

该系统提供三个主要功能：（1）即时收集和向用户显示实时游戏玩法、投票陈述或问题的系统；(2)收集、分析、反馈用户请求的实时用户数据的系统；(3)利用实时用户输入数据和实时游戏数据向目标用户提供实时、逻辑化购买广告的广告平台。

专利名称：GENERATING AND DEPLOYING PACKAGES FOR MACHINE LEARNING AT EDGE DEVICES（在边缘设备上生成和部署机器学习包）

专利号：US2019/0156246A1

发明人：Calvin Yue-Ren Kuo; Jiazhen Chen; Jingwei Sun; Haiyang Liu

单位：Amazon Technologies, Inc.

年份：2018 年

概述：

边缘计算设备部署在许多环境中以实现各种应用。无论是在我们的家中，还是嵌入汽车和工厂中，边缘设备可能使用了各种传感器来监测周围环境，做出预测，并根据预测采取行动。在许多应用场景下（如监控摄像机、自动驾驶汽车、工业机械），设备在很短的时间内收集大量数据，并根据收集到的数据进行实时决策。因此，在许多情况下，机器学习推理都在本地设备上进行。在使用机器学习模型生成预测之前，必须对其进行训练。训练机器学习模型可能需要大量的计算资源；而且，要使机器学习模型能够在边缘设备上运行的过程可能非常复杂、耗时且容易出错。

因此，该专利实现了在边缘设备上生成和部署机器学习包。提供商网络的机器学习部署服务可以接收（例如，来自客户端的用户）推理应用的指示、推理应用要使用的机器学习框

架、推理应用要使用的机器学习模型以及运行推理应用的边缘设备。然后，机器学习部署服务可以基于推理应用、机器学习框架和机器学习模型生成包。然后，机器学习部署服务可以将包部署到边缘设备进行安装并启用，从而使所有边缘设备以最优的方式工作，减少边缘设备计算资源的损耗或生成推理模型所需要的时间。

专利名称：MULTI-TASK LEARNING USING KNOWLEDGE DISTILLATION（利用知识蒸馏进行多任务学习）

专利号：US2019/0325308A1

发明人：Junyoung Chung; Melvin Jose Johnson Premkumar; Michael Schuster; Wolfgang Macherey

单位：Google LLC

年份：2019 年

概述：

知识蒸馏是一种模型压缩方法，模型压缩指的是在 teacher-student 框架中，将复杂、学习能力强的网络学到的表征“知识”蒸馏出来，传递给参数量小、学习能力弱的网络。

该专利使用知识蒸馏技术执行多任务学习。首先获取多个机器学习任务相应的训练数据集，针对每个机器学习任务，配置相应的教师机器学习模型来执行相应的机器学习任务；然后利用从教师机器学习模型中提取的知识以及数据集，训练学生机器学习模型来执行多个机器学习任务。与教师机器学习模型相比，学生机器学习模型的规模较小，因此比教师机器学习模型具有更快的运行速度，更易于在硬件中部署。

专利名称：EVOLVED MACHINE LEARNING MODELS（进化的机器学习模型）

专利号：US2019/0295000A1

发明人：Arno Candel; Dmitry Larko; SriSatish Ambati; Prithvi Prabhu; Mark Landry; Jonathan C. McKinney

单位：H2O.ai Inc.

年份：2019 年

概述：

一个机器学习模型可以被训练来实现一个复杂的功能，如：根据一组输入来生成一个或多个预测。然而，基于模型的特殊性和包含在输入集合中的初始特征，其预测的准确性是有限的。该专利提出一种进化的机器学习模型方法：利用原始特征数据的子集训练多个初始机

器学习模型以提供预测。基于验证数据，将初始机器学习模型的预测特征标签与数据的实际特征值进行比较生成验证评分。初始机器学习模型的多样性可以根据验证评分进行排序，并基于排序筛选幸存的机器学习模型。再者，从幸存模型中确定出重要特征（一个或多个重要特征可以根据一个特征用于分割决策树的次数来确定），将重要特征进行转换操作以生成新的特征，并使用一个或多个新特征和原始特征的一个子集来生成进化的机器学习模型。运用验证数据，比较一个或多个进化的机器学习模型相关的验证分数和一个或多个幸存的机器学习模型相关的验证分数，并基于验证分数，至少选择一个或多个进化的机器学习模型或一个或多个幸存的机器学习模型作为新的幸存的机器学习模型。

专利名称：IDENTIFYING ENTITIES USING A DEEP-LEARNING MODEL（使用深度学习模型识别实体）

专利号：US10402750B2

发明人：Jason E. Weston; Keith Adams; Sumit Chopra

单位：Facebook, Inc.

年份：2019 年

概述：

深度学习是一种机器学习，它可以在有监督或无监督的环境中训练模型来学习数据的表示，在该专利中，社交网络系统可以使用深度学习模型来预测与用户相关的实体，其中，训练后的深度学习模型可将实体映射到向量表示（强度值），从而确定出相关的实体。该专利的方法为：通过获取社交网络系统的用户在社交网络系统中与之交互的第一组实体，以及社交网络系统中的第二组实体（可能是用户未交互过的实体或者随机选择的实体等），使用深度学习模型确定第一组实体的向量表示，从第一组实体中选择目标实体（可随机选择），将其矢量表示从第一组实体中移除，合并第一组向量表示中的其余向量表示以确定用户的向量表示，并使用深度学习模型确定第二组实体的向量表示。通过比较用户的矢量表示和目标实体的矢量表示，计算目标实体和用户之间的相似度得分；在第二组实体中，将用户的矢量表示与第二组实体的矢量表示进行比较，计算用户和第二实体之间的相似度得分。然后使用深度学习模型，根据以上的相似度得分更新第二组实体中一个或多个实体的矢量表示。

5 人才篇

本篇通过 AMiner 大数据平台挖掘机器学习领域顶级学术会议 ICML、NeurIPS 近 10 年的论文，提取论文中所有学者信息，从中选出 h-index 排名最靠前的 2000 位领域活跃学者，分析了学者的分布等情况，介绍了部分该领域国内外知名度较高的活跃学者。

5.1 学者情况概览

- 全球人才分布

学者地图用于描述特定领域学者的分布情况，对于进行学者调查、分析各地区竞争力现况尤为重要，下图为机器学习领域全球学者分布情况：

图 5-1 机器学习领域全球学者分布

地图根据学者当前就职机构地理位置进行绘制，其中颜色越深表示学者越集中。从该地图可以看出，美国的人才数量遥遥领先且主要分布在其东西海岸；欧洲中西部也有较多的人才分布；亚洲的人才主要分布于我国东部及日韩地区；其他诸如非洲、南美洲等地区的学者非常稀少；机器学习领域的人才分布与各地区的科技、经济实力情况大体一致。此外，在性别比例方面，机器学习领域中男性学者占比 89.8%，女性学者占比 10.2%，男性学者占比远高于女性学者。

- h-index 分布

机器学习学者的 h-index 分布如下图所示，大部分学者的 h-index 都在 30 以上，其中 h-index 小于 30 的人数最多，有 591 人，占比 29.1%。

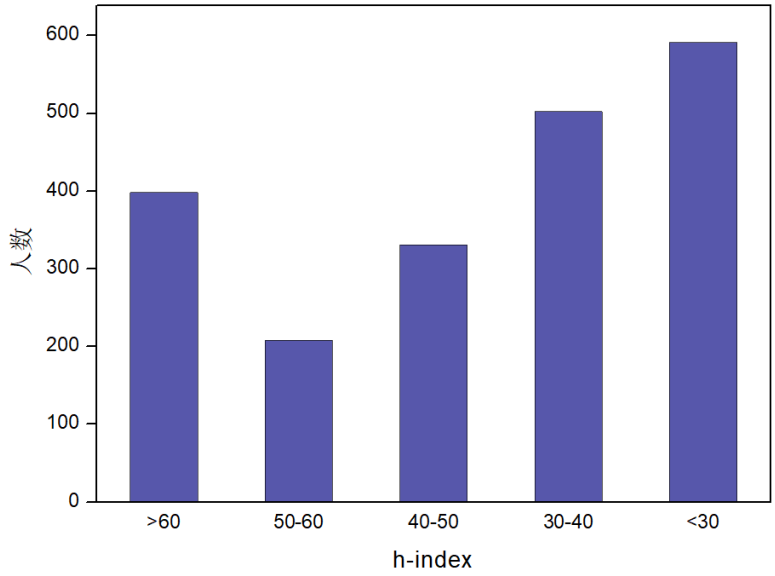


图 5-2 机器学习领域学者 h-index 分布

- 中国人才分布

图 5-3 机器学习领域中国学者分布

我国专家学者在机器学习领域的分布如上图所示。通过上图我们可以发现，京津地区在本领域的人才数量最多，其次是长三角和珠三角地区，相比之下，内陆地区的人才较为匮乏，这种分布与区位因素和经济水平情况不无关系。同时，通过观察中国周边国家的学者数量情况，特别是与日韩、东南亚等亚洲国家相比，中国在机器学习领域学者数量较多。

中国与其他国家在机器学习的合作情况可以根据 AMiner 数据平台分析得到，通过统计论文中作者的单位信息，将作者映射到各个国家中，进而统计中国与各国之间合作论文的数量，并按照合作论文发表数量从高到低进行了排序，如下表所示。

表 5-1 机器学习领域中国与各国合作论文情况

序号	合作国家	论文数	引用数	平均引用数	总的学者数
1	中国-美国	511	26694	52	819
2	中国-英国	44	1398	32	73
3	中国-新加坡	36	1189	33	56
4	中国-澳大利亚	31	744	24	42
5	中国-印度	22	1123	51	19
6	中国-德国	17	419	25	39
7	中国-瑞士	11	233	21	22
8	中国-荷兰	6	93	16	10
9	中国-巴基斯坦	4	82	21	3
10	中国-以色列	3	23	8	6

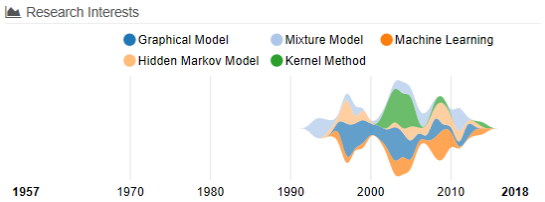
从上表数据可以看出，中美合作的论文数、引用数、平均引用数、学者数遥遥领先，表明中美间在机器学习领域合作之密切；从地域角度看，中国与欧洲的合作非常广泛，前 10 名合作关系里中欧合作共占 4 席；中国与印度合作的论文数虽然不是最多，但是平均引用数依然位列第二，说明在合作质量上中印合作也达到了较高的水平。

5.2 代表性学者简介

综合 h-index 以及领域知名度与活跃度，我们收集整理了国内外机器学习领域的高水平学者，其中，国际代表性学者如：Michael I. Jordan、Yann Lecun、Geoffrey E. Hinton、Yoshua Bengio、Andrew Y Ng、Jurgen Schmidhuber、Fei-Fei Li、Daphne Koller、John D. Lafferty、Peter L. Bartlett、Michael Collins、Ian Goodfellow、David Sliver、Zoubin Ghahramani、David J.C. MacKay、Christopher Bishop、Tony Jebara、Max Welling 等；国内代表性学者如：张钹、周志华、李航、朱军、颜水成、杨强、唐杰、刘铁岩、王海峰、何晓飞、戴文渊、黄高、王立威、张长水、孙剑、林宙辰等。下面我们将对国内外机器学习领域代表性学者进行简要介绍，排名不分先后。此外，限于报告篇幅，我们对所有学者不能逐一罗列，如有疏漏，还请与 AMiner 编者联系，或者登录 https://www.aminer.cn/获取更多资料。

5.2.1 国际代表性学者

- Michael I. Jordan



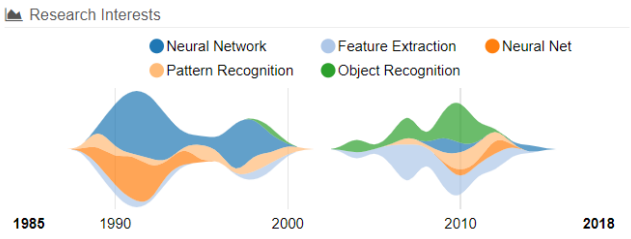
Michael I. Jordan，美国三院（美国国家科学院、美国国家工程院、美国艺术与科学院）院士，机器学习泰斗，被誉为人工智能领域的“根目录”之一，伯克利大学机器学习实验室 AMP Lab 联合主任，IEEE Fellow，ACM Fellow。

Michael I. Jordan 是美国科学家，加州大学伯克利分校电子工程系、计算机科学和统计系杰出教授，机器学习、统计学和人工智能研究员。他是机器学习领域的领军人物之一，并且在 2016 年被 *Semantic Scholar* 称为世界上最有影响力的计算机科学家。同年也被 AMiner 评为机器学习最有影响力学者。

他于 1985 年获得加利福尼亚大学圣地亚哥分校博士学位。自 1988 年至 1998 年，Michael I. Jordan 任麻省理工学院教授，他的研究方向包括了计算学、统计学、认知科学以及生物科学。近年来，他的研究兴趣集中在贝叶斯非参数分析、概率图模型、谱方法、核方法、分布式计算系统、自然语言处理、信号处理和统计遗传学等问题的应用上。深度学习领域的权威 Yoshua Bengio，贝叶斯学习领域权威 Zoubin Ghahramani 及前百度首席科学家吴恩达等人都是其门下学生。

他曾获得众多奖项，在 2016 年获得 IJCAI 研究卓越奖（IJCAI Research Excellence Award），2015 年获得了 David E. Rumelhart 奖，2009 年获得了 ACM / AAAI Allen Newell 奖，2004 年获得 ICML 最佳学生论文奖。同时，他是 AAAI、ACM、ASA、CSS、IEEE、IMS、ISBA 和 SIAM 成员。

- Yann LeCun



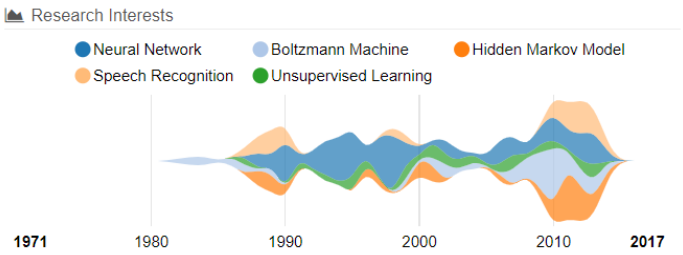
Yann LeCun，人工智能领域三大奠基人之一，被称为“卷积网络之父”。

Yann LeCun 是美国工程院院士，Facebook 人工智能研究院院长，纽约大学 Sliver 教授，同时还兼职于科学数据中心，数学科学交流学院，神经科学中心，以及电子工程计算机系。他以使用卷积神经网络（CNN）进行光学字符识别和计算机视觉方面的工作而闻名，并且是卷积网络的创始人。

他获得巴黎第六大学（Pierre et Marie Curie）的计算机科学博士学位，1987 年至 1988 年，是多伦多大学 Geoffrey Hinton 实验室的博士后研究员。他于 2003 年加入纽约大学，之后还在普林斯顿的 NEC 研究院短暂任职。在 2012 年，他创建了纽约大学数据科学中心，并担任主任。2013 年底，他被任命为 Facebook 人工智能研究总监，并继续在纽约大学做兼职教授。2015-2016 年，他在巴黎法兰西工学院做客座教授。

他曾获得的荣誉有：2014 年 IEEE 神经网络先驱奖、2015 年 IEEE PAMI 杰出研究员奖、2016 年墨西哥 IPN 荣誉博士，2018 年图灵奖。

- Geoffrey E. Hinton



Geoffrey E. Hinton，人工智能领域三大奠基人之一，被称为“神经网络之父”，“深度学习鼻祖”。

Geoffrey E. Hinton 是英国计算机科学家，担任多伦多大学计算机科学系教授，多伦多大学向量学院（Vector Institute）首席科学顾问。人工智能三大奠基人之一 Yann LeCun，以及谷歌大脑研究科学家 Hugo LaRochelle 都是其博士后。

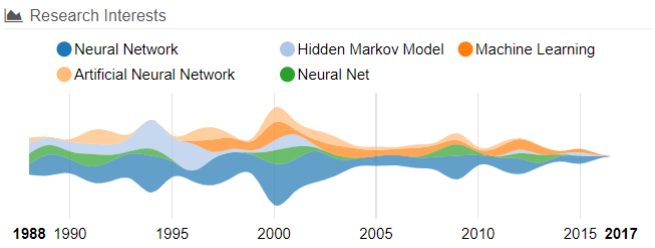
他于 1975 年获得爱丁堡大学人工智能方向博士学位，神经网络是他的研究重点。

2013 年，他加入谷歌并带领 AI 团队，将神经网络带入到研究与应用的热潮，将“深度学习”从边缘课题变成了谷歌等互联网公司的依赖的核心技术，并将 Backpropagation（反向传播）算法应用到神经网络与深度学习。

Geoffrey E. Hinton 获得诸多项荣誉。2005 年获得 JICAI 卓越研究奖项；2011 年获得苏赛克斯大学理学博士荣誉学位；2012 年，获得了加拿大基廉奖（Killam Prizes，有“加拿大诺贝尔奖”之称的国家最高科学奖）；2013 年获得 Doctorat honorifique, University of

Sherbrooke；2014 年获得 IEEE Frank Rosenblatt Medal；2016 年获得 NEC C&C Award，IEEE/RSE James Clerk Maxwell Medal；2018 年图灵奖。

- Yoshua Bengio

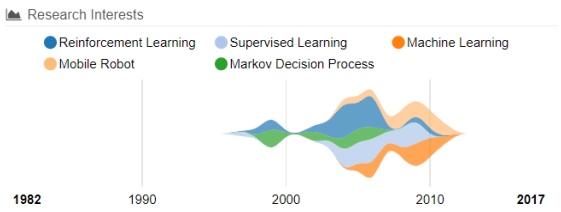


Yoshua Bengio，加拿大计算机科学家，与 Geoffrey Hinton、Yann LeCun 一起，被称为人工智能三大奠基人。根据 MILA 的数据，在 *h* 指数至少为 100 的计算机科学家中，Yoshua Bengio 是每天都有被引用的一个。他在人工神经网络和深度学习方面做出了突出贡献。Yoshua Bengio 于 1991 年获得加拿大麦吉尔大学计算机科学博学位，并是麻省理工学院和贝尔实验室的博士后。他自 1993 年以来担任蒙特利尔大学教授，担任计算机科学与运筹学系主任。他撰写了三本书，超过 500 种出版物，经常被引用在深度学习、复现神经网络、概率学习算法、自然语言处理和多元学习领域，其中，*Deep Learning* 是他于 GAN 之父 Ian Goodfellow 等人合著的入门深度学习必读经典教程。

他是加拿大最受欢迎的计算机科学家之一。自 2000 年起，他在统计学习算法中担任加拿大研究主席，自 2006 年成为 NSERC 工业主席，自 2005 年以来，他是加拿大高级研究所高级研究员，自 2014 年以来，他一直致力于深度学习。他是 NEURIPS 基金会的董事会成员，也是 NEURIPS 的课程主席和总裁。他参与组织了 14 年的学习研讨会，以及新的国际学习代表会议。他目前的兴趣集中于通过机器学习对 AI 的追求，并且包括关于深度学习和表征学习的基本问题，高维空间中的泛化几何，多元学习，生物学启发式学习算法以及统计机器学习的具有挑战性的应用。2016 年 10 月，Yoshua Bengio 联合创立了 Element AI，这是一家位于蒙特利尔的企业孵化器，致力于将人工智能（AI）研究转化为实际的商业应用。2017 年 5 月，Bengio 宣布他将加入蒙特利尔的法律创业公司 Botler AI，担任战略顾问。他是 CIFAR 高级研究员并共同指导其在机器和大脑学习计划。此外，他还是 MILA（蒙特利尔大学学习算法学院）的创始人们兼科学主任。Yoshua Bengio 的论文“*A neural probabilistic language model*”开创了神经网络 language model（语言模型）的先河。该论文的思路影响、启发了之后的很多基于神经网络做 NLP（自然语言处理）的文章。

Yoshua Bengio 获得荣誉有：2009 年 ACFAS Urgel-Archambault 奖、2017 年加拿大勋章官员、2017 加拿大皇家学会会员、2018 加拿大 AI 协会终身成就奖、2018 年图灵奖、2019 年 Killam 计算机科学奖、2019IEEE CIS 神经网络先锋奖，IEEE 计算智能学会

- Andrew Y. Ng



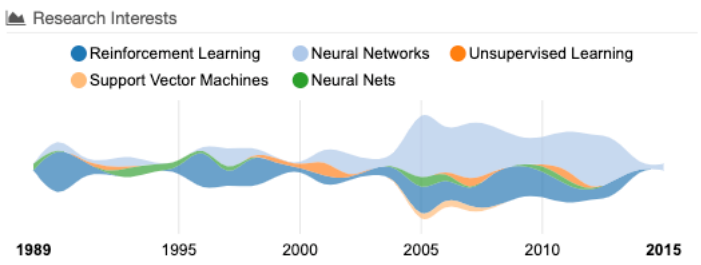
Andrew Y. Ng（吴恩达）于 2002 年获得了加州大学伯克利分校的博士学位，并从这年开始在斯坦福大学工作。他是前文介绍的 Michael I Jordan 的弟子。他的主要兴趣领域在机器学习、深度学习、机器人、人工智能和计算机视觉等方面。2010 年，时任斯坦福大学教授的 Andrew Y. Ng 加入谷歌开发团队 XLab，这个团队已先后为谷歌开发无人驾驶汽车和谷歌眼镜两个知名项目，Andrew Y. Ng 加入后开始“谷歌大脑”项目。2014 年 5 月，吴恩达加入百度，担任百度公司首席科学家，负责百度研究院的领导工作，尤其是 Baidu Brain 计划。2017 年 10 月，吴恩达出任 Woebot 公司新任董事长，该公司拥有一款同名聊天机器人

Andrew Y. Ng 最知名的事情是，他所开发的人工神经网络通过观看一周 YouTube 视频，自主学会识别哪些是关于猫的视频。这个案例为人工智能领域翻开崭新一页。

他 2007 年获得了斯隆奖（Sloan Fellowship），2008 年入选“the MIT Technology Review TR35”，即《麻省理工科技创业》杂志评选出的科技创新 35 俊杰，以及计算机思维奖（Computers and Thought Award），并在 2013 年入选《Time》杂志年度全球最有影响力的 100 人之一，其中共 16 位科技界人物。他也是“计算机和思想奖”的获得者。

他现在的兴趣主要是深度学习。他在 2013 年前共有 128 项学术著作，如 *Deep Learning with COTS HPC Systems*（Adam Coates,Brody Huval,Tao Wang,David J.Wu,Bryan Catanzaro and Andrew Y.Ng 等人在 ICML 2013 上发表）、*Parsing with Compositional Vector Grammars* 等，限于篇幅，本报告不一一列举。他所著 *Machine Learning Yearning* 于 2018 年出版，该书面向的用户群体为机器学习从业者，主要介绍机器学习实际使用时的一些策略和技巧，以便为开发指明方向，提升开发效率。

- Jürgen Schmidhuber

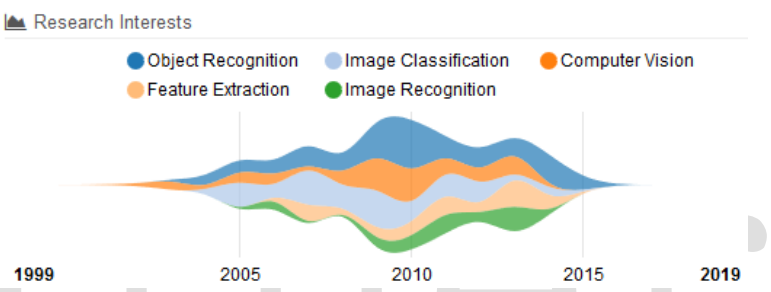


Jürgen Schmidhuber 是瑞士人工智能实验室（IDSIA）的研发主任，同时任教于卢加诺大学和瑞士南部应用科学与艺术学院。他还是欧洲科学与艺术院的成员。他于 1987 年和 1991 年在慕尼黑工业大学先后获得计算机科学的学士和博士学位。他在人工智能、深度学习和人工神经网络领域的成就有很深的造诣。

他是长短期记忆网络 LSTM 的发明人、深度学习元老，被称为递归神经网络之父。Schmidhuber 本人创立的公司 Nnaisense 正专注于人工智能技术研发，致力于在金融、重工业和自动驾驶汽车等领域开展人工智能的商业应用。此前，他开发的算法让人类能够与计算机对话，还能让智能手机将普通话翻译成英语。

他获得的其他奖项包括 2013 年国际神经网络协会的亥姆霍兹奖，2016 年电气与电子工程师协会的神经网络先锋奖等。

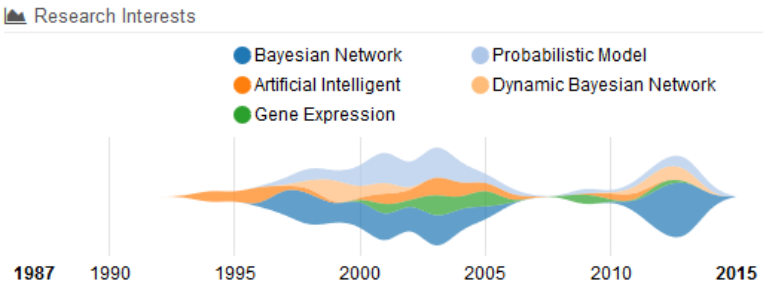
- Fei-Fei Li（李飞飞）



Fei-Fei Li（李飞飞），美国斯坦福大学红杉讲席教授，以人为本人工智能研究院（HAI）院长，AI4ALL 联合创始人及主席。

李飞飞在 2005 年获得加州理工学院电子工程博士学位。主要研究领域为机器学习、深度学习、计算机视觉、认知与计算、神经科学。她在顶级期刊和会议上发表了近 200 篇科学论文。李飞飞是 ImageNet 和 lmageNet 挑战的发明者，lmageNet 挑战是一个重要的大型数据集和基准测试，除了她的技术贡献外，还为深度学习和 Al 的最新发展做出了贡献。她是倡导 STEM 和 Al 多样性的主要声音，她是美国非盈利组织 Al4ALL 的联合创始人和主席，旨在提高 Al 教育的包容性和多样性。她曾在世界经济论坛、the Grace Hopper Conference 2017、TED2015 年大会等学术或有影响力的会议上发表主旨演讲。她是 ACM 的研究员，曾获得 2006 年微软研究院新教员奖学金，2009 年 NSF 终身成就奖，2011 年 Alfred Sloan 教员奖，2012 年雅虎实验室 FREP 奖，2014 年 IBM 教员奖，2016 年 IEEE PAMI Mark Everingham 奖，2017 年雅典娜学术领导奖，2019 IEEE PAMI Longuet-Higgins Prize，2019 年国家地理学会进步奖等。

- Daphne Koller

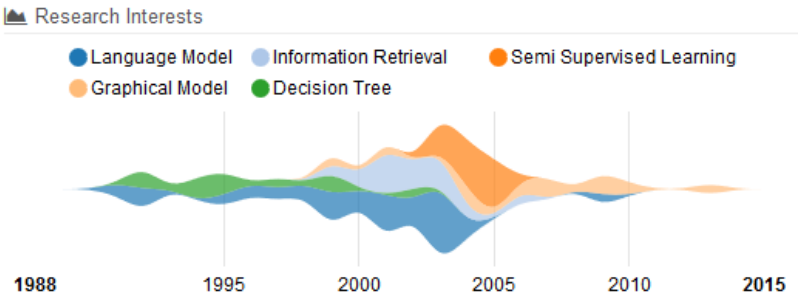


Daphne Koller 教授于 1993 年在斯坦福大学获得博士学位，1995 年加入斯坦福大学，现在是该校工程学院的 Rajeev Motwani 教授。她的研究重点是使用概率模型和机器学习来理解包含大量不确定性的复杂领域。她目前的研究项目包括计算生物学、计算医学和从传感器数据对物理世界的语义理解。

Daphne Koller 是斯坦福大学计算机科学本科生暑期研究项目 CURIS 的创始人和负责人。该项目成立十年来已经培训了 500 多名学生。2010 年，她在斯坦福大学的课堂上开创并试验了一种在线教育模式，这种模式促进了斯坦福大学向公众提供的在线课程的形成。

她曾获得 1994 年亚瑟论文奖，斯隆基金会 1996 年学院奖学金，1998 年总统早期职业科学家和工程师奖（PECASE），1999 年 ICAl 电脑和思想奖，2001 年考克斯奖章、2004 年麦克阿瑟基金会奖学金、2008 年 ACM/Infosys 奖，于 2011 年当选为美国国家工程院院士。

- John D. Lafferty

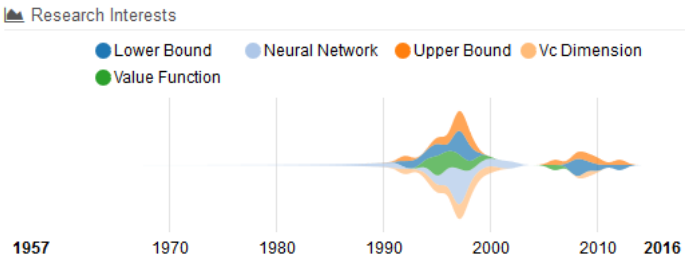


John D. Lafferty，1986 年于普林斯顿大学获得数学博士。他是芝加哥大学的教授，研究方向是机器学习，目前主要集中在非参数方法、高维数据、图形模型、文档和文本分析的计算和统计方面，是芝加哥大学计算与应用数学计划（CAMI）的成员。

在 2011 年进入芝加哥大学之前，他从 1994 年开始在卡内基梅隆大学任教，在那里他帮助建立了世界上第一个机器学习系。在 CMU 之前，他是 IBM Thomas J. Watson 研究中心的一名研究人员。在加入 IBM 之前，他是哈佛大学数学系的助理教授。

他在 2007 年获选为 IEEE 院士，以表彰他对统计模式识别和统计语言处理的贡献。他担任过许多著名的职位，包括：神经信息处理系统（NIPS）基金会会议的项目联席主席和总联席主席、CMU 新博士机器学习博士项目联合主任、JMLR 副主编、国家研究委员会应用与理论统计委员会（CATS）委员等。

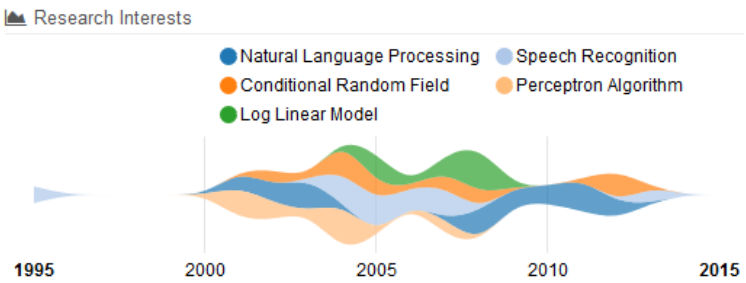
- Peter L. Bartlett



Peter L. Bartlett ，1992 年于澳大利亚昆士兰大学获得信息技术与电气工程博士。他是加州大学伯克利分校米勒研究所统计和计算机科学客座教授，澳大利亚国立大学高级研究所信息科学与工程研究学院研究员、高级研究员和教授。他也是昆士兰大学计算机科学和电子工程学院的荣誉教授。他的研究兴趣包括：机器学习、统计学习理论和强化学习；确定性博弈论背景下的预测方法分析；大规模顺序决策问题方法的设计等。

他是《神经网络学习：理论基础》一书的合著者。他曾担任《机器学习》、《控制信号与系统数学》、《机器学习研究》、《人工智能研究》和《IEEE 信息论汇刊》的副主编。2001 年，他因在统计学习理论方面的研究而获得马尔科姆·麦金托什澳大利亚年度物理科学家奖，2008 年被选为数理统计研究所奖章讲师，2015 年当选为澳大利亚科学院院士。

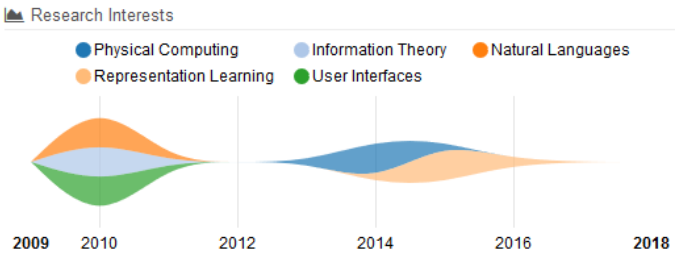
- Michael Collins



Michael Collins，哥伦比亚大学计算机科学教授，研究兴趣是自然语言处理和机器学习，在统计分析和统计机器学习方面做出了重要贡献。1998 年在宾夕法尼亚大学获得了计算机科学博士学位。1999 年到 2002 年，Michael Collins 在美国电话电报公司做实验室研究，从 2003 年到 2010 年 12 月，他在哥伦比亚大学做副教授，也是谷歌 NYC 的一名研究科学家

在他的研究中涵盖了广泛的主题，如解析重新排序，树核，半监督学习，机器翻译和指数梯度算法，一般重点区别模型和结构化预测。曾为《宾州华尔街日报》语料库提供的最先进的解析器。最近研究方向为前馈神经网络和计算图形和反向传播。他曾获得美国国家科学基金会终身成就奖，阿尔弗雷德·p·斯隆研究奖学金，ACL 研究员，2012 年布拉瓦特尼克奖的最终入围教师。

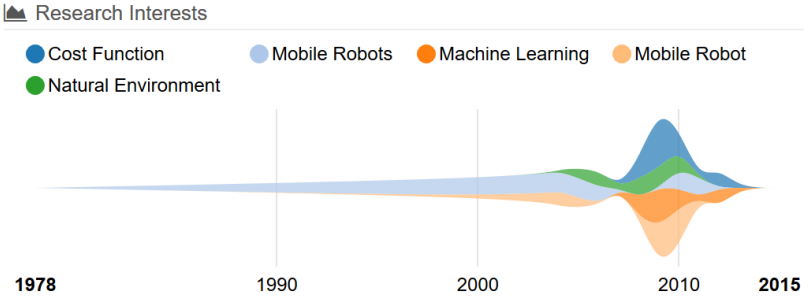
- Ian Goodfellow



Ian Goodfellow，是机器学习领域备受关注的年轻学者之一，本科与硕士就读于斯坦福大学，师从吴恩达，博士阶段则跟随 Yoshua Bengio 研究机器学习。他因提出了生成对抗网络（GANs）而闻名，被誉为“GANs 之父”，

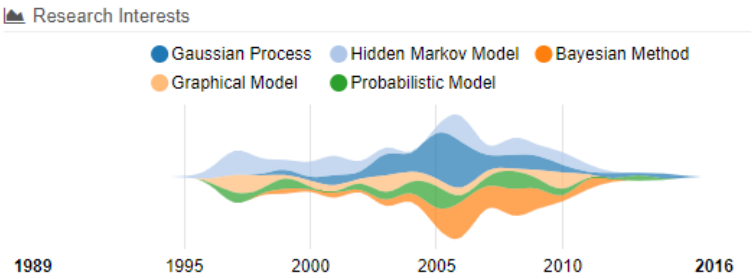
毕业后，Goodfellow 加入 Google，成为 Google Brain 研究团队的一员。然后他离开谷歌加入新成立的 OpenAI 研究所，在 2017 年 3 月他又回到谷歌研究院。2019 年，Ian Goodfellow 加入苹果公司，领导机器学习特殊项目组。

- David Silver



David Silver，AlphaGo 的首席研究员和 AlphaStar 的共同负责人。2004 年，他在阿尔伯塔大学攻读强化学习博士学位。2011 年，西尔弗获得英国皇家学会大学研究奖学金，随后成为伦敦大学学院的讲师，目前是该校的一名教授。他最近的工作集中在强化学习和深度学习的结合上。David Sliver 领导了 AlphaGo 项目，并在第一个项目中击败了顶级专业棋手，AlphaGo 随后获得了荣誉 9 段专业认证：并获得了戛纳狮子奖，然后领导了 Alphazero 的发展。随后，他领导了 AlphaZero 的开发，AlphaZero 使用同样的人工智能从头开始学习围棋，然后再以同样的方式学习国际象棋和围棋，达到了比任何其他计算机程序更高的水平。Silver 是 DeepMind 发表论文最多的员工之一。

- Zoubin Ghahramani



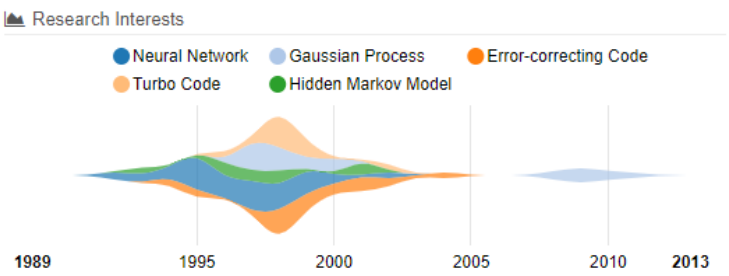
Zoubin Ghahramani，是剑桥大学信息工程教授，他领导了由大约 30 名研究人员组成的机器学习小组，并担任了 Uber-AI 实验室的首席科学家。他曾担任英国国家数据科学研究所阿兰图灵研究所（Alan Turing Institute）的创始剑桥主任，勒沃胡姆未来情报中心（Leverhulme Centre for the Future of Intelligence）副学术主任，剑桥圣约翰学院（St John's College Cambridge）院士。

他在宾夕法尼亚大学学习计算机科学和认知科学，1995 年从麻省理工学院获得博士学位，并在多伦多大学做博士后。他的学术生涯包括同时被任命为伦敦盖茨比计算神经科学部门的创始成员之一，以及 CMU 机器学习部门的教员超过 10 年。

他目前的研究兴趣包括统计机器学习、贝叶斯非参数、可伸缩推理、概率规划等。他发表了 250 多篇论文，获得 38000 多条引文（h 指数 84）。他的工作得到了 EPSRC、DARPA、微软、谷歌、Infosys、Facebook、亚马逊、FX Concepts、NTT 和其他一些工业合作伙伴的资助和捐赠。

2013 年，他获得了 75 万美元的谷歌奖，用于研究如何建立自动统计师。他曾担任微软剑桥研究院（Microsoft Research Cambridge）、VocalIQ（被苹果收购）、剑桥资本管理公司（Cambridge Capital Management）、Echobox、Informetis、Opera Solutions 和其他几家公司的顾问。他还担任过一些领导职务，担任机器学习领域主要国际会议的项目和总主席：AISTATS（2005 年）、ICML（2007 年、2011 年）和 NIPS（2013 年、2014 年）。2015 年，他被选为皇家学会会员，2016 年，他被评为机器学习领域十大最具影响力的学者之一。

- David J.C. MacKay



David J.C. MacKay，曾任剑桥大学卡文迪什实验室物理系自然哲学教授，现为剑桥大学工程系教授，能源和气候变化部首席科学顾问。

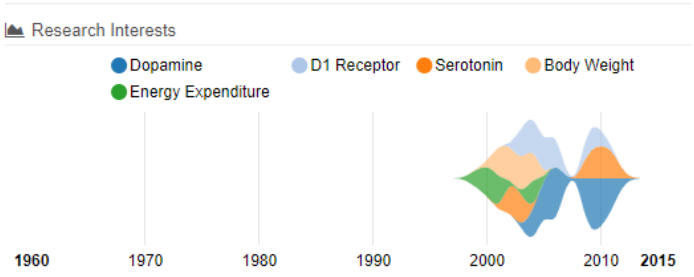
1967 年 4 月 22 日出生于英国特伦特的斯托克。在纽卡斯尔接受莱姆学校和剑桥三一学院的教育后，他于 1991 年在加州理工学院完成了计算和神经系统博士学位。

他的兴趣包括构建和实现发现数据模式的分层贝叶斯模型，开发神经网络的概率方法，以及纠错码的设计和解码。

他在机器学习、信息理论和通信系统方面的研究在国际上享有盛名，其中包括 Dasher 的发明，Dasher 是一种软件接口，可以用任何肌肉在任何语言中进行有效的通信。他从 1995 年开始在剑桥教物理。自 2005 年以来，他将越来越多的时间用于能源方面的公共教学。他是世界经济论坛全球气候变化议程理事会成员。

1985 年南斯拉夫国际物理奥林匹克运动会：银牌；一等奖，1999 年通信学会 Leonard G.Abraham 奖论文奖（与 R.J.McEliece 一起以及 J.﹣F.Cheng），2001 年、1999 年 IBM 合作伙伴奖，2009 年当选物理研究所院士、皇家学会会员，2010 年当选土木工程师学会会员，2013 年获梅尔切特奖。

- Christopher Bishop



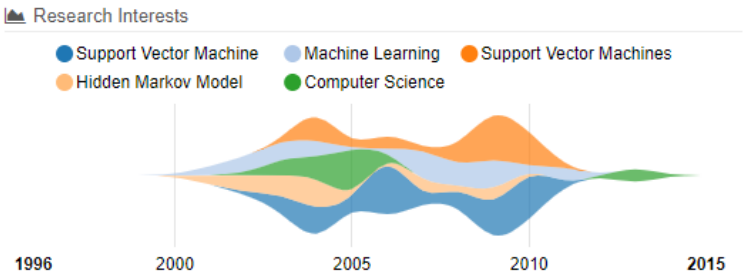
Christopher Bishop，微软剑桥研究院技术研究员兼实验室主任，爱丁堡大学计算机科学教授，剑桥达尔文学院院士。

Chris 在牛津大学获得物理学学士学位，在爱丁堡大学获得理论物理学博士学位，并发表了一篇关于量子场论的论文。从那时起，他对模式识别产生了兴趣，并成为 AEA 技术应用神经计算中心的负责人。随后，他被选为阿斯顿大学计算机科学和应用数学系的主席，并在那里成立和领导了神经计算研究小组。

克里斯是两本被广泛引用的机器学习教科书的作者：《神经网络模式识别》（1995）和《模式识别与机器学习》（2006）。他还致力于机器学习在从计算机视觉到医疗保健等领域的广泛应用。克里斯是公众参与科学的积极倡导者，2008 年，他发表了著名的皇家学会圣诞讲座，1825 年由迈克尔法拉第创立，并在国家电视台播出。

他于 2004 年当选皇家工程院院士，2007 年当选爱丁堡皇家学会院士，2017 年当选皇家学会院士。

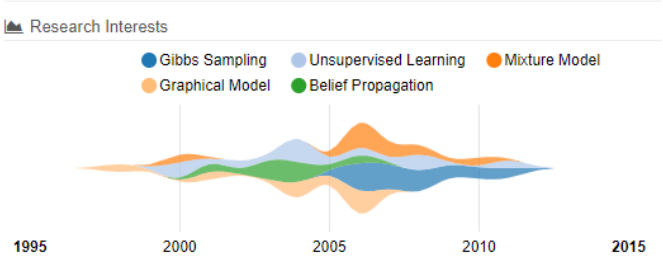
- Tony Jebara



Tony Jebara，哥伦比亚大学计算机科学系副教授，哥伦比亚大学机器学习实验室负责人。主要研究方向为计算机科学和统计学的交叉融合，在视觉、学习和时空建模等方面成就很高。他于 2002 获得麻省理工学院博士学位。他指导哥伦比亚机器学习实验室（Columbia Machine Learning Laboratory），该实验室的研究与计算机科学和统计学交叉，开发新的数据学习框架，并将其应用于视觉、网络、时空数据和文本。Tony Jebara 已经创立了包括 Sense Networks、Agolo、Ninoh 和 Bookt 在内的几家初创公司，并为其提供咨询服务。他在会议、研讨会和期刊上发表了 100 多篇同行评议论文，包括 NIPS、ICML、UAI、COLT、JMLR、CVPR、ICCV 和 AISTAT。他是《机器学习：辨别与生成》一书的作者，也是视觉、学习和时空建模领域多项专利的共同发明人。

他的作品在第 26 届机器学习国际会议上获得最佳论文奖，在第 20 届机器学习国际会议上获得最佳学生论文奖，并在 2001 年获得模式识别学会的杰出贡献奖。2004 年，Tony Jebara 获得了国家科学基金会的职业奖。他还是《机器学习研究》杂志和《机器学习》编辑委员会的副主编。2007 年至 2011 年，Jebara 任机器学习副主编，2010 年至 2012 年任 IEEE 模式分析和机器智能事务副主编。2006 年，他与人共同创立了 NYAS 机器学习研讨会，并从那时起一直担任该研讨会的指导委员会成员。Tony Jebara 还担任了 2014 年第 31 届机器学习国际会议（ICML）的项目主席。

- Max Welling



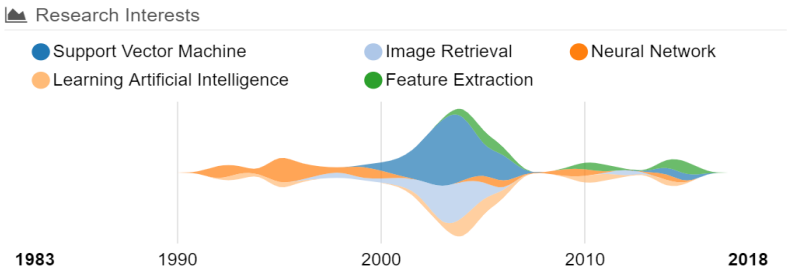
Max Welling，阿姆斯特丹大学的“研究主席”，加州大学欧文分校（UCI）计算机科学与统计学教授，加拿大高级研究所（CIFAR）副研究员，Scyfer BV 联合创始人。

在过去，他曾在加州理工学院（Caltech）（1998-2000）、加州大学洛杉矶分校（UCL）（2000-2001）和多伦多大学（U.Toronto）（2001-2003）担任博士后。1998 年，他在诺贝尔奖获得者霍夫特教授的指导下获得了博士学位。

Max Welling 从 2011 年至 2015 年担任 IEEE TPAMI 的副主编。他自 2015 以来担任 NIPS 基金会的董事会成员（在机器学习方面规模最大的会议），分别担任 2013 和 2014 年度 NIPS 的计划主席和总主席。2009 年，他还是 AISTATS 和 2016 年 ECCV 的项目主席，2018 年 MIDL 的总主席。他曾在 JMLR 和 JML 的编辑委员会任职，并担任神经计算、JCGS 和 TPAMI 的副主编。他从谷歌、Facebook、雅虎、NSF、NIH、NWO 和 ONR-MURI 获得了多项资助，其中一项是 2005 年的 NSF 职业资助。他是 2010 年 ECCV Koenderink 奖的获得者。Welling 是阿姆斯特丹数据科学研究中心的董事会成员，他领导阿姆斯特丹机器学习实验室（AMLAB），并共同领导高通公司的 UvA 深度学习实验室（QUVA）和博世公司的 UvA 深度学习实验室（DELTA）。

5.2.2 国内知名学者

- 张钹



张钹，中国科学院院士，清华大学计算机科学与技术系教授，清华大学人工智能研究院院长。

张钹于 1958 年毕业于清华大学自动控制系，是国家第一批自动控制专业的毕业生。1995 年他当选为中国科学院院士。

他早期从事自动控制理论与系统研究，1979 年开始计算机科学与技术研究。从事人工智能理论、人工神经网络、遗传算法、分形和小波等理论研究；以及把上述理论应用于模式识别、知识工程、智能机器人与智能控制等领域的应用技术研究。

他针对人工智能问题求解计算复杂性、指数爆炸的主要困难，提出了问题分层求解的商空间理论，解决了不同粒度空间的描述、它们之间相互转换、复杂性分析等理论问题。在此

基础上提出统计启发式搜索算法，基于拓扑的空间规划方法和关系矩阵的规划算法，对克服计算量的指数爆炸很有成效。还提出了研究不确定性处理、定性推理、模糊分析、证据合成等新原理。指导并参加建成了陆地自主车、图像与视频检索等实验平台。

张钹和同期同事成了国内最早接触到人工智能的研究者，并成为我国在这方面的首批专家。

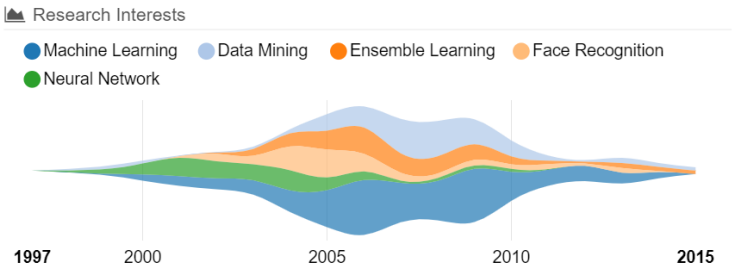
在学术研究上的主要贡献是提出问题分层求解的商空间理论，通过代数的方法，系统地解决了不同层次求解空间的问题表达、复杂性分析、不同层次空间之间信息、算子及推理机制等的相互转换关系。在上述理论基础上，他进一步提出了统计启发式搜索算法，基于拓扑的空间规划方法以及基于关系矩阵的时间规划算法等，极大降低了计算复杂性，具有重要的应用价值。其专著《问题求解理论及应用》全面总结了他在人工智能理论研究中的成果，其英文版于 1992 年由 Elsevier Science Publishers B.V.(Nortn-Holland)出版，中文版获国家教委颁发的高校出版社优秀学术专著特等奖。澳大利亚专家 Ronald Walts 在计算机杂志 *The Australian Computer Journal*（1995）对《问题求解理论及应用》（英文版）的评论为“这是一部在重要研究领域的优秀著作”。美国学者 Harold S.Stone 认为，张钹等在统计启发式搜索等方面的工作，是“最近几年中国学者作出的很有意义的贡献”，“将新一代计算技术的前沿向前推进了”。

他在国内外共发表论文 100 多篇，中英文专著有《问题求解理论及应用》（中英版）以及《人工神经网络理论及应用》等。

他于 1994 年当选为俄罗斯自然科学院外籍院士；1995 年当选为中国科学院院士；2011 年德国汉堡大学授予自然科学名誉博士；2015 年 1 月 31 日，张钹获得 2014 CCF 终身成就奖。

他的社会任职有：智能技术与系统国家重点实验室主任、校学位委员会副主任、信息科学与技术学院学术委员会主任；中国自动化学会机器人专业委员会副主任及智能控制专业委员会副主任；《计算机学报》副主编；国家高技术“863”计划智能机器人主题专家组成员；河南科技大学兼职院士；计算机学术委员会主任。

- 周志华



周志华，南京大学教授，博士生导师；教育部长江学者特聘教授，国家杰出青年基金获得者；南京大学计算机科学与技术系副主任、软件新技术国家重点实验室常务副主任，机器学习与数据挖掘研究所（LAMDA）所长，校学术委员会委员、南京大学人工智能学院院长（兼）。

周志华于 2000 年获得南京大学计算机科学与技术系博士学位，2001 年 1 月起留校任教，2002 年 3 月被破格聘任为副教授，2003 年，在他 29 岁时获得国家杰出青年科学基金，随后被聘为教授。

他于 2006 年入选教育部长江学者特聘教授，2012 年当选 IEEE Fellow 和 IAPR Fellow（国际模式识别学会会士），2013 年当选 ACM Distinguished Scientist（ACM 杰出科学家）和中国计算机学会（CCF）会士，成为大陆高校首位当选 ACM 杰出科学家的学者。2007 年创建南京大学机器学习与数据挖掘研究所（LAMDA），2010 年 11 月任软件新技术国家重点实验室常务副主任，2013 年 5 月任计算机系副主任。

2016 年，他当选 AAAI Fellow（国际人工智能学会），成为我国大陆第一位，也是此次入选的唯一来自美欧之外的学者，并且是唯一在中国大陆取得博士学位的 AAAI Fellow。2016 年 11 月，当选美国科学促进会会士（AAAS Fellow）。2016 年 12 月，当选 ACM Fellow，成为第一位在中国大陆取得全部学位的 ACM Fellow。

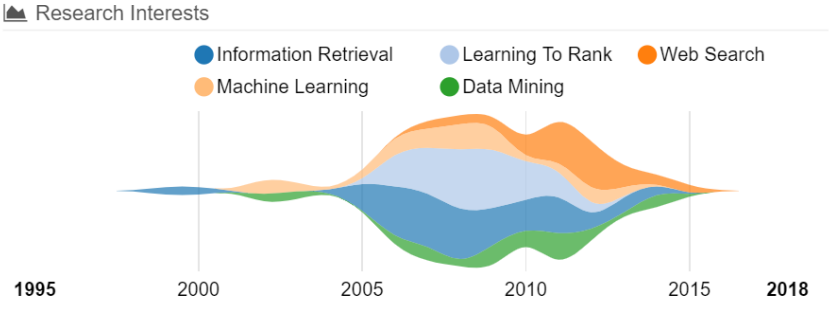
2017 年 2 月，当选人工智能领域顶级学术会议 AAAI 2019 程序委员会主席，是该会议自 1980 年成立以来首位华人主席、也是首次由美欧之外国家的学者出任主席。

兼任 AAAI Fellow，IEEE Fellow，IAPR Fellow，ACM Fellow 和 AAAS Fellow，周志华成为国际上与人工智能相关的重要学会“大满贯”Fellow 华人第一人。

此外，他还担任 IJCAI 程序委员会主席，是中国内地首位任此职位学者。

周志华主要从事人工智能、机器学习、数据挖掘等领域的研究工作。他著有机器学习入门书籍《机器学习》。

- 李航



李航，北京大学、南京大学兼职教授。

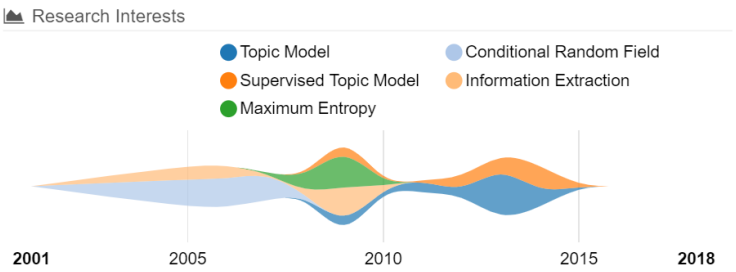
李航毕业于日本京都大学电气电子工程系，于 1998 年获得日本东京大学计算机科学博士学位。曾任日本 NEC 公司中央研究所研究员，微软亚洲研究院高级研究员与主任研究员、华为技术有限公司诺亚方舟实验室主任。现任今日头条人工智能实验室主任。

他的研究方向包括信息检索、自然语言处理、统计机器学习及数据挖掘。他一直活跃在相关学术领域，曾出版过三部学术专著，并在顶级国际学术会议和国际学术期刊上发表过上百篇学术论文，拥有 42 项授权美国专利。

他出版的三本技术书籍其中最广为人知的是 2012 年出版的《统计学习方法》，他发表超过 120 项技术论文，包括 SIGIR、WWW、WSDM、ACL、EMNLP、ICML、NeurIPS、SIGKDD、AAAI、IJCAI 等顶级国际会议以及包括 CL、NLE、JMLR、TOIS、IRJ、IPM、TKDE、TWEB、TIST。他和他同事的论文收到了 SIGKDD'08 最佳应用论文奖，SIGIR'08 最佳学生论文奖，ACL'12 最佳学生论文奖。

他是 ACM 杰出科学家。他的社会任职包括 AIRS-2008 程序委员会主席，SIGIR-2008 Poster & Demo 委员会主席，KDD-2009 宣传主席，EMNLP-2009 领域主席，ACM Transaction on Asian Language Information Processing 副主编，Journal of Computer Science and Technology 编委等。

- 朱军



朱军，清华大学计算机科学系教授，智能技术与系统国家重点实验室副主任，卡内基梅隆大学兼职教授。2013 年，入选 IEEE Intelligent Systems 的“人工智能 10 大新星”（AI’s 10 to Watch）。

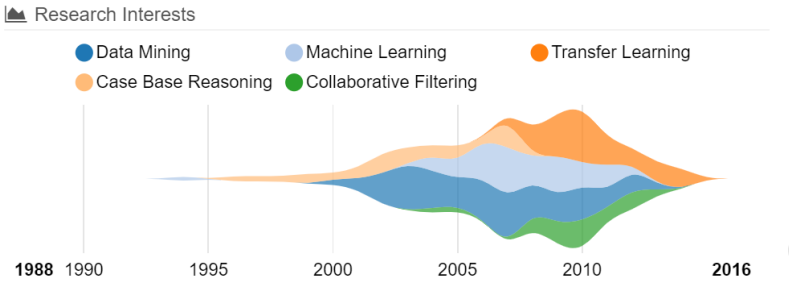
朱军于 2009 年获得清华大学计算机博士学位，主要从事机器学习研究。

他在国际重要期刊与会议发表学术论文 80 余篇，他开源了 ZhuSuan，一个用于贝叶斯深度学习（贝叶斯方法和深度学习的结合）的 GPU 库，可以在 TensorFlow 上使用

他是 AAAI 2019，NeurIPS 2018，ICML 2018，UAI 2018，IJCAI 2018 的区域主席，担任国际期刊 IEEE TPAMI 和 Artificial Intelligence 的编委、国际会议 ICML 2014 地区联合主席、以及 ICML、NEURIPS 等国际会议的领域主席。

他于 2006 年被评为微软学者，2009 年入选卡内基梅隆大学 Innovation Fellow；中国计算机学会优秀博士论文奖获得者（2009）；清华大学 221 基础研究计划入选者（2012）；中国计算机学会青年科学家（2013）；IEEE Intelligent Systems 杂志评选的“AI’s 10 to Watch”（2013）；国家优秀青年科学基金获得者（2013），同年获得、中国计算机联合会（CCF）颁发的“CCF 青年科学家”奖；2014 年，他获得清华-MSRA 联合研究实验室颁发的最佳协作奖；2015 年获得全国青年顶尖人才支持计划的支持，同年收到了“CVIC SE 人才”奖；2017 年，他被麻省理工学院 TR35 中国选为“先驱者”之一。

- 杨强



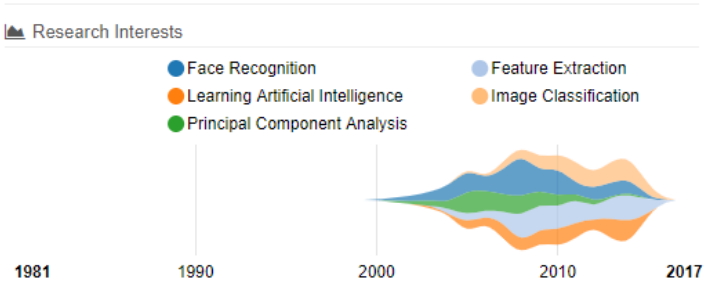
杨强，香港科技大学新明工程学讲席教授，计算机科学和工程学系主任，大数据研究所所长。IEEE Fellow，IAPR Fellow，AAAS Fellow，ACM 杰出科学家，KDD 中国主席。

杨强于 1989 年获得马里兰大学计算机科学博士学位，之后直到 1995 年，任加拿大滑铁卢大学计算机系任助理教授及副教授。其主要研究领域为机器学习、数据挖掘和自动规划。他是人工智能研究的国际专家和领军人物，在学术界和工业界做出了杰出的服务和贡献，尤其近些年为中国人工智能（AI）和数据挖掘（KDD）的发展起了重要引导和推动作用。迄今为止，杨强已发表逾 400 篇关于人工智能和数据挖掘方面的论文，引用超过 20000 次。

2009 年，他创建了 ACM 刊物 *Transactions on Intelligent Systems and Technology（TIST）* 并任首届主编。2012 年至 2015 年，出任华为诺亚方舟实验室创始主任；2015 年，任香港科技大学计算机与工程学系主任；2016 年，在香港科技大学创建大数据研究所。

他的社会兼职有：2013 年 7 月当选为国际人工智能协会（AAAI）院士，是第一位获此殊荣的华人，之后又于 2016 年 5 月当选为 AAAI 执行委员会委员，是首位也是至今为止唯一的 AAAI 华人执委，同年，任 ACM 数据挖掘中国分会（KDD China）主席。2017 年 8 月他当选为国际人工智能联合会（IJCAI，国际人工智能领域创立最早的顶级国际会议）理事会主席，是第一位担任 IJCAI 理事会主席的华人科学家。

- 颜水成



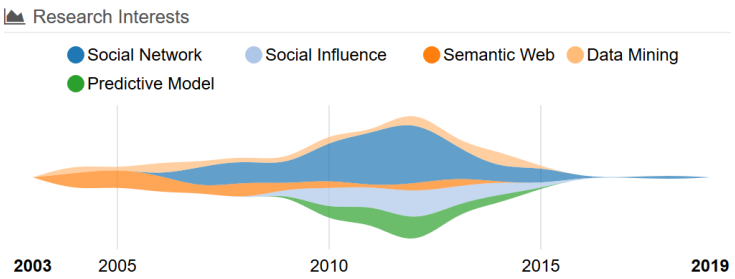
颜水成，新加坡国立大学副教授、360 集团副总裁、人工智能研究院院长、第十三批国家“千人计划”专家。

主要研究兴趣是为计算机视觉、多媒体和信息检索应用开发机器学习理论。

他在众多研究课题上撰写/合著了数百篇技术论文，其中谷歌学者引文 2 万余次。他是 2014 年、2015 年和 2016 年 ISI 被高度引用的研究员。颜水成博士率领的团队共获得了 10 次计算机视觉领域两大核心竞赛 Pascal VOC 和 ImageNet 大规模视觉识别（ILSVRC）冠军和荣誉奖，10 余次最佳（学生）论文奖。他的团队还曾获得多媒体领域顶会 ACM MM 最佳论文奖、最佳学生论文奖和最佳技术演示奖的大满贯。

颜水成博士团队提出的“Network in Network”（NIN）网络结构的核心 1x1 卷积是近年来几乎所有计算机视觉深度学习模型的标准模块，在学术界和工业界影响深远，其思想也被后期的 GoogleNet、残差网络（ResNet）等模型所采用。

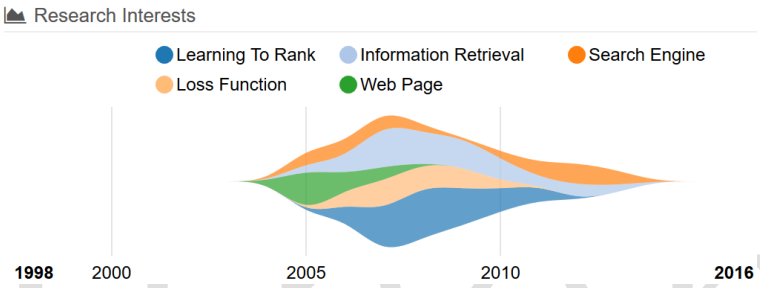
- 唐杰



唐杰，清华大学计算机科学与技术系长聘教授，计算机系副主任、清华工程院知识智能联合实验室主任。研究兴趣包括人工智能、数据挖掘、社交网络、机器学习和知识图谱，研究重点是设计挖掘社交和知识网络的新算法。发表论文 200 余篇，拥有专利 20 余项。曾担任国际期刊 ACM TKDD 的执行主编和国际会议 CIKM’16、WSDM’15 的程序委员会主席、KDD’18 大会副主席以及 IEEE TKDE、ACM TIST、IEEE TBD 等期刊编委。他曾获英国皇家学会-牛顿高级奖学金、CCF 青年科学家奖、国家自然科学基金委员会杰出青年学者、北京市科技进步一等奖、中国人工智能学会科技进步一等奖、KDD’18 杰出贡献奖。主要创新

性研究包括：1）社会影响力分析：提出基于话题的社会网络影响力模型，针对大规模社会网络进行用户级别的微观建模，自动计算用户之间基于不同话题层次的影响力强度，为定量化、细粒度的网络影响力分析给出理论基础，部分解决了影响力最大传播模型的输入假设问题。2）社会网络用户行为建模：将社会网络的基础理论（结构平衡理论、两阶段传播理论、结构洞理论等）融入概率因子图模型中对社会网络关系和强度进行定量描述，实现了社会网络关系挖掘的统一学习算法。3）网络行为建模和影响力分析，提出了针对社会网络的微观动态分析方法，并首次提出了社会影响力的量化分析方法，以及社会网络行为和社会影响力关联关系的分析方法。4）应用上述研究成果，研发了完全自主知识产权的科技情报大数据挖掘与服务平台 AMiner。系统 2006 年上线以来，吸引了来自全球 220 个国家/地区的 1000 多万次独立 IP 访问。

- 刘铁岩

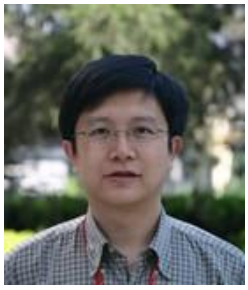


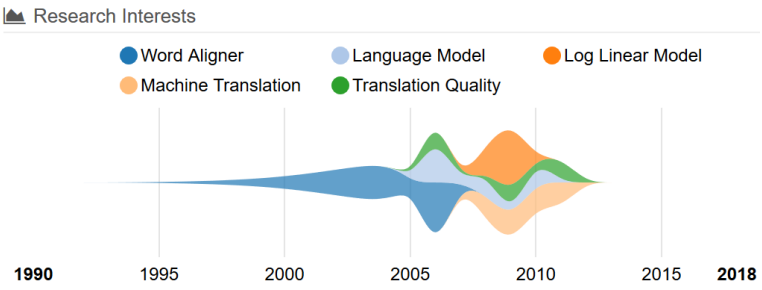
刘铁岩，博士毕业于清华大学电子工程系。现任微软亚洲研究院主任研究员，互联网经济与计算广告学研究组负责人。他是美国计算机学会(ACM)、国际电子电气工程师学会(IEEE)、和中国计算机学会（CCF）的高级会员。中国科技大学和南开大学的客座教授。

刘铁岩博士是机器学习和信息检索领域的知名专家，尤其在排序学习方面取得了国际领先的研究成果。他著有《排序学习及其在信息检索中的应用》等学术专著。他在国际顶级期刊和会议上发表相关论文 70 余篇。他持有 40 余项美国和国际专利。他的论文曾获得国际信息检索大会(SIGIR)最佳学生论文奖，和国际期刊《视觉通信和图像表示》的最高引用论文奖。他是国际计算机辅助搜索会议（RIAO）2010 年度的程序委员会主席，国际信息检索大会(SIGIR)2008-2011 年度的领域主席(Area Chair)，亚洲信息检索会议（AIRS）2009-2011 年度的领域主席，国际数据挖掘大会（KDD）2012 年度的展览和演示主席，国际互联网大会（WWW）2011 年度的领域主席。他担任美国计算机学会会刊《信息系统（TOIS）》的副主编，国际期刊《信息检索》和《人工智能》的编委，和数十个国际期刊的审稿专家。他是包括 WWW、SIGIR、ICML、ACL、ICIP 等在内的三十几个国际会议的程序委员会成员，是国际排序学习研讨会（LR4IR）2007-2009 年度的联合主席，和 2010 年排序学习竞赛的联合组织者。他曾经在 WWW、SIGIR、KDD 等国际会议上做关于排序学习的主题讲座，并受邀作为 KDD 2011 年度的大会主题辩论嘉宾。他受邀为亚太多媒体大会（PCM 2010）和中国

信息检索大会（CCIR 2011）做大会特邀报告。他还受邀为包括卡耐基梅隆大学在内的十余所国内外高校讲授《排序学习》和《机器学习》的课程。

- 王海峰

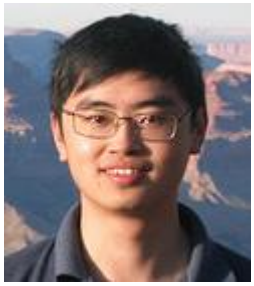


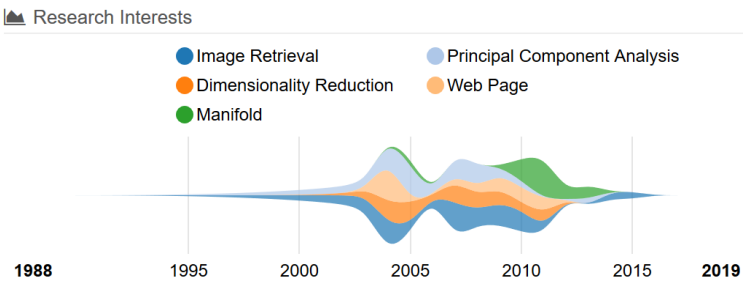


王海峰，博士，百度首席技术官。主要研究领域包括机器翻译、自然语言处理、搜索技术、语音技术、机器学习与数据挖掘、推荐及个性化等。曾主持及参与了多个产品的研发，已申请中国、美国及日本专利 30 余项，主持开发的系统还在国际评测中获得多项第一。已发表包括一流国际期刊论文及顶级国际会议论文在内的学术论文 70 余篇。

王海峰于 2010 年加入百度，2013 年晋升为公司副总裁。2014 年，转岗至搜索业务群组任副总经理，先后负责了百度搜索、手机百度等用户产品。2017 年 3 月 22 日，百度宣布组成百度 AI 技术平台体系（AIG），任命百度副总裁王海峰为 AI 技术平台体系（AIG）总负责人，同时晋升为 Estaff 成员。2018 年，晋升百度高级副总裁。王海峰是是唯一来自中国大陆的 ACL 会士，是首个吴文俊人工智能杰出贡献奖获得者。2019 年 3 月，任北京百度投资管理有限公司董事。2019 年 5 月，百度宣布晋升高级副总裁王海峰为百度集团首席技术官，同时他将继续担任 AI 技术平台体系（AIG）和基础技术体系（TG）总负责人。2019 年 9 月，百度 CTO 王海峰出任东软控股董事。

- 何晓飞





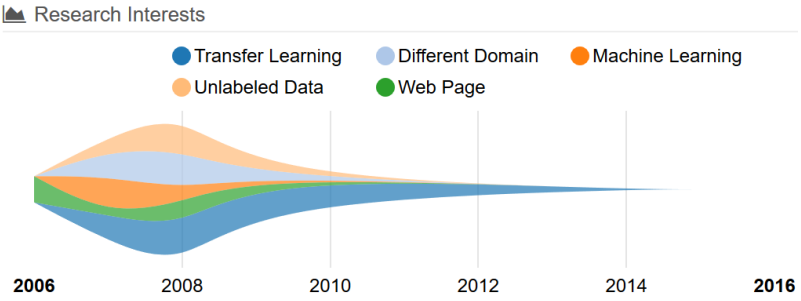
何晓飞，中国浙江大学计算机学院的教授。2005 年在芝加哥大学获得计算机科学的博士学位，博士毕业后，他在雅虎做了一名研究科学家。2007 年加入浙江大学。

何晓飞的研究兴趣是模式识别、机器学习和计算机视觉。他与流形学习奠基人 Partha Niyogi 教授共同提出的保局投影算法是世界上第一个线性流形算法，在国际上掀起了基于

图论的线性降维算法研究热潮。他与微软亚洲研究院合作提出的基于块结构的链接分析算法被誉为下一代互联网搜索引擎的核心算法，被国际上数十家 IT 专业媒体报道。在雅虎研究院曾领导关于查询语句分类、海量网页分类、广告关键字建议等项目的研究开发工作。

滴滴研究院成立后，同时宣布 AI 科学家何晓飞任首届院长。何晓飞正式加盟后，负责滴滴出行平台核心交易引擎建设。后来滴滴出行中不可或缺的拼车、动态调价、订单分配、运力调度、供需预测，路径规划等项目，均出自交易引擎。后来，何晓飞离职创业，2017 年 8 月创立建立逐影科技公司，主打无人货运。

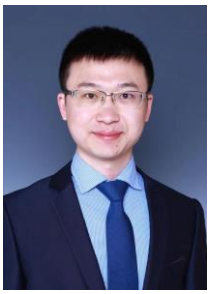
- 戴文渊

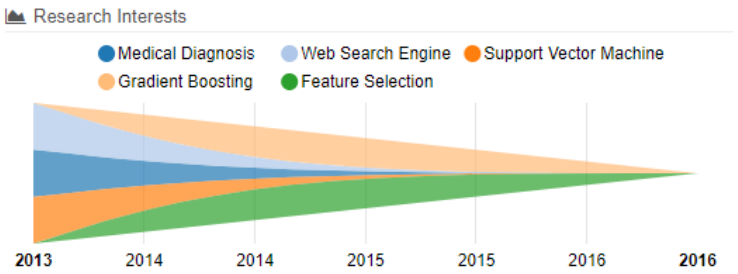


戴文渊，毕业于上海交通大学，现供职于华为诺亚方舟研究员，担任主任研究院。戴文渊在 ACM 大学生程序设计竞赛中屡获佳绩，先后获得 ACM 国际大学生程序设计竞赛亚洲区预选赛冠军 3 次。2005 年 4 月，以队长身份在全球总决赛中夺得世界冠军。其学术论文多次被国际顶级学术会议 NIPS、ICML、AAAI、KDD 等收录，并获得 PKDD 2007 最佳学生论文奖。2009 年，戴文渊放弃继续攻读博士学位，入职百度，先后任百度商务搜索部资深研发工程师、主任研发架构师（T10）。2013 年 6 月，他加入华为诺亚方舟实验室，担任主任研究员。目前任第四范式创始人、首席执行官，是人工智能研究领域“迁移学习”全球领军学者，机器学习全球商业领军人物，国际大学生程序设计竞赛（ACM-ICPC）世界冠军，中国智能最高奖“吴文俊人工智能科学技术”一等奖获得者。

他曾帮助百度建立了中国最大的机器学习系统，获“百度最高百万美元奖”，任百度最年轻的高级科学家（技术排名第 3）。曾任华为诺亚方舟实验室主任科学家，帮助 AI 技术应用于电信、金融、手机等产业，创造数十亿的利润提升。其学术论文多次被 NIPS、ICML、AAAI、KDD 等国际顶级学术会议收录，2007 年发表的论文 Boosting for Transfer Learning 在迁移学习领域论文引用数至今仍排名世界第三。从机器学习少年天才到百度高级科学家，再到人工智能行业应用创业者，戴文渊始终致力于将人工智能技术应用到行业中去，降低人工智能技术的使用成本和门槛，让更多的人能够享受到人工智能技术带来的红利。

- 黄高





黄高，清华大学助理教授，博士生导师。

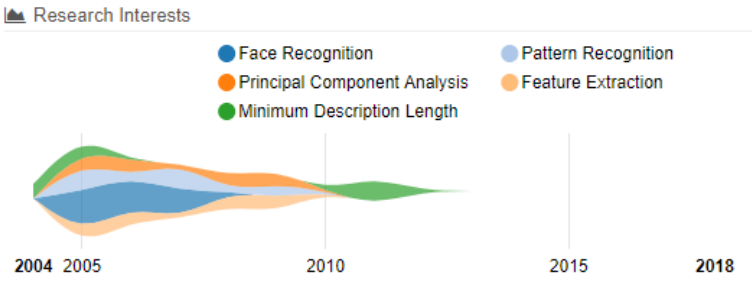
主要研究领域为深度神经网络的结构设计与优化算法，以及深度学习在计算机视觉中的应用。

2009 年本科毕业于北京航空航天大学，2015 年获得清华大学控制科学与工程博士学位，2015 年至 2018 年为美国康奈尔大学计算机系博士后。其博士论文获选中国自动化学会优秀博士学位论文以及清华大学优秀博士论文一等奖。该获奖论文的主要贡献是提出了一种全新的卷积神经网络架构“密集链接卷积网络”（DenseNet），显著地提升了模型在图片识别任务上的准确率。

目前在 NIPS、ICML、CVPR 等国际顶级会议及 IEEE 多个汇刊共计发表学术论文 30 余篇。2016 年曾获得全国百篇最具国际影响学术论文、2017 年国际计算机视觉顶级会议 CVPR 最佳论文奖、2018 年世界人工智能创新大赛 SAIL 先锋奖和吴文俊人工智能自然科学一等奖等奖励和荣誉。

他是 AAAI 2018 高级程序委员，担任 NeurIPS、ICML、CVPR、ICCV、ECCV、ICLR、AAAI 等国际学术会议和 JMLR、TPAMI、TIP、TNNLS 等国际期刊审稿人。

- 王立威



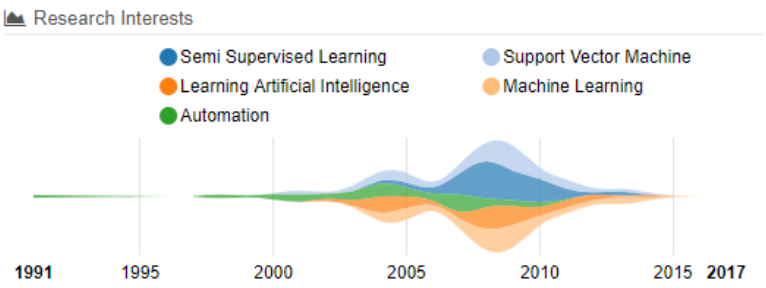
王立威，1999 年获清华大学学士学位，2002 年获清华大学硕士学位，2005 年获北京大学博士学位。现为北京大学信息科学技术学院教授。

长期从事机器学习相关研究，目前主要致力于机器学习基础理论，即泛化理论的研究，差分隐私算法的设计与分析以及医疗影像诊断算法与系统的开发。自 2002 年以来，在 PAMI、

CVPR、ICML 等国际顶级期刊和和会议上发表论文 60 余篇，并参与编写《机器学习及其应用》2009 版“关于 Boosting 算法的 Margin 解释”及 2015 版“差分隐私保护的机器学习”相关章节。

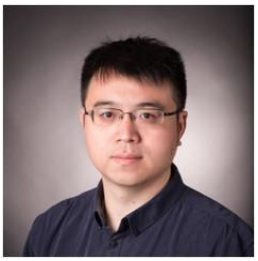
曾获得第 11 届 Meeting on Image Recognition and Understanding 会议最佳论文奖，2010 年获得 *Pattern Recognition Letters* 期刊最高引用论文奖（2005-2010），2010 年入选 AI's 10 to Watch，是首位获得该奖项的亚洲学者。2012 年获得首届国家自然科学基金优秀青年基金，新世纪优秀人才。任 NIPS 等权威会议 Area Chair，以及多家学术期刊编委。

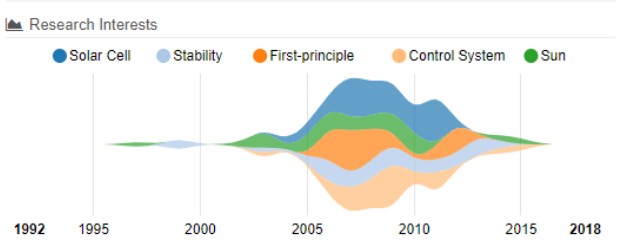
- 张长水



张长水，男，1965 年生，河北人。智能技术与系统国家重点实验室学术委员会委员，清华大学自动化系教授、博士生导师，智能技术与系统国家重点实验室副主任，自动化系主任。主要从事图像处理、信号处理、模式识别与人工智能、进化计算等研究领域以及和工业界的合作。1986 年 7 月毕业于北京大学数学系，获得理学学士学位。1992 年 7 月毕业于清华大学自动化系，获得博士学位。1992 年 7 月至 1994 年 12 月，在清华大学自动化系任讲师；1995 年 1 月—2000 年 8 月，在清华大学自动化系任副教授；2000 年 9 月起，在清华大学自动化系任教授；2001 年起，任清华大学博士生导师。近几年在国际期刊和会议上发表学术论文超过 100 篇，其中包括国际权威期刊 Pattern Recognition、TNN、TKDE、IEEE Transaction on Multimedia 以及国际顶级会议 IJCAI、AAAI、NIPS、ICML、ECML、SIGIR、CVPR 等。他还是国际权威期刊 Pattern Recognition 编委。

- 孙剑

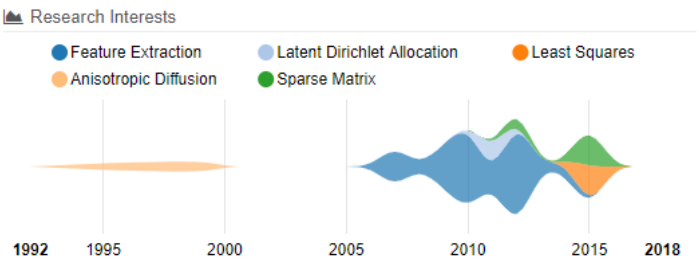




孙剑，男，前微软亚研院首席研究员，现就职于北京旷视科技有限公司，任旷视首席科学家、旷视研究院院长。其主要研究方向是计算机视觉和深度学习。2003 年在西安交通大学模式识别与智能控制专业研究生毕业，获得工学博士学位，2003 年加入微软亚洲研究院。孙剑自 2002 年以来在 CVPR、ICCV、SIGGRAPH、PAMI 等顶级学术会议和期刊上发表学术论文 100 余篇，拥有超过 40 项美国或国际专利。

2009 年孙剑带领团队发表的论文 *Single Image Haze Removal Using Dark Channel Prior* 赢得了国际计算机视觉与模式识别会议（CVPR）的最佳论文奖（CVPR Best Paper），这是亚洲人第一次获得该奖；2010 年，他被美国科技评论期刊《麻省理工科技评论》（*MIT Technology Review*）评选为“全球 35 岁以下杰出青年创新者”。2012 年至 2014 年，他加入法国国家信息与自动化研究院(INRIA)/巴黎高等师范学院 Willow 组。2016 年，孙剑带领的团队凭借 *Deep Residual Learning for Image Recognition* 再次获得了国际计算机视觉与模式识别会议（CVPR）的最佳论文奖（CVPR Best Paper）。2016 年 7 月，孙剑正式加入旷视任首席科学家、旷视研究院院长。2017 年 8 月，他担任中国自动化学会(Chinese Association of Automation, CAA)混合智能专委会副主任。2018 年 5 月，2018 年第一批国家重点研发计划公示孙剑博士担任变革性技术关键科学问题专项项目负责人。2019 年 1 月，孙剑出任西安交通大学人工智能学院首任院长。

- 林宙辰



林宙辰，北京大学信息科学技术学院机器感知与智能教育部重点实验室教授，主要研究领域为机器学习、模式识别、计算机视觉、图像处理、数值优化。NeurIPS 2019 在加拿大温哥华正式拉开帷幕 NeurIPS 2019 在加拿大温哥华正式拉开帷幕 2000 年于北京大学获得理学博士学位。2007 年荣获 Microsoft SPOT Award，2015 年 ImageNet 大规模视觉识别竞赛（ILSVRC）场景分类项目冠军，2016 年获国家自然科学杰出青年基金资助。他是 CVPR 2014/2016、ICCV 2015、NIPS 2015 的领域主席和 AAAI 2016/2017、IJCAI 2016 的高级程序委员。他也是 IEEE Transactions on Pattern Analysis And Machine Intelligence 和 International Journal of Computer Vision 的编委。

5.3 NeurIPS 十年高引学者

2019 年 12 月，NeurIPS 2019 在加拿大温哥华正式拉开帷幕。作为机器学习领域最重要的顶会，NeurIPS 一直有着很强的影响力和排名，被认为是神经计算方面最好的会议之一。随着近几年深度学习的崛起，NeurIPS 不仅成为了学术界的新星，也引起了工业界的高度关注，注册人数从数年前的几百人跃升到今年的近万人。根据 AMiner 数据平台的统计分析，NeurIPS 的 H5 指数为 149，10H 值为 34641，在人工智能方向会议中排名第二。通过对 NeurIPS 近十年（2009 至 2019）接收论文引用量的统计分析，我们获得了 NeurIPS 高引学者 TOP100 榜单。

表 5-2 NeurIPS（2009-2019）高引学者 TOP100

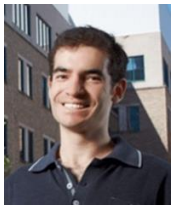
序号	姓名	单位	总引用量
1	Ilya Sutskever	OpenAI	67457
2	Geoffrey E. Hinton	多伦多大学	47482
3	Alex Krizhevsky	Google	44218
4	Yoshua Bengio	蒙特利尔大学	18714
5	Greg Corrado	Google	17218
6	Jeffrey Dean	Google	17218
7	Kai Chen	Google	16139
8	Tomas Mikolov	Facebook	15166
9	Ian Goodfellow	Apple	13480
10	Kaiming He	Facebook AI	12605
11	Jian Sun	旷视科技	12601
12	Aaron Courville	蒙特利尔大学	12407
13	Ross B. Girshick	Facebook AI	11495
14	Shaoqing Ren	Momenta	11093
15	Mehdi Mirza	DeepMind	10713
16	Jean Pouget-Abadie	Google	10618
17	Bing Xu	布兰迪斯大学	10618
18	David Warde-Farley	DeepMind	10618
19	Sherjil Ozair	蒙特利尔大学	10618
20	Quoc V. Le	Google	10180
21	Oriol Vinyals	DeepMind	9663
22	Andrew Y. Ng	斯坦福大学	6632
23	Andrew Zisserman	牛津大学	5570
24	Koray Kavukcuoglu	DeepMind	5223
25	Karen Simonyan	DeepMind	4883
26	Ruslan Salakhutdinov	苹果 AI	4456
27	Antonio Torralba	麻省理工学院	4249
28	Ryan P. Adams	普林斯顿大学	4116
29	Francis Bach	法国国家信息与自动化研究所	3350

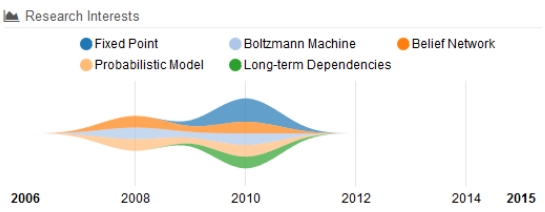
30	Xi Chen	纽约大学	3257
31	Honglak Lee	Google Brain	3248
32	David M. Blei	哥伦比亚大学	3191
33	Lukasz Kaiser	Google AI	3146
34	Jason Yosinski	Uber 人工智能实验室	3042
35	Hugo Larochelle	Google Brain	2992
36	Jeff Clune	Uber 人工智能实验室	2989
37	Tong Zhang	香港大学	2889
38	Marc' Aurelio Ranzato	Facebook AI	2844
39	Hod Lipson	哥伦比亚大学	2802
40	Pieter Abbeel	加州大学伯克利分校	2761
41	Jasper Snoek	Google Brain	2734
42	Jakob Uszkoreit	Google	2710
43	Wojciech Zaremba	OpenAI	2669
44	Yann LeCun	Facebook	2616
45	Tim Salimans	OpenAI	2566
46	Pradeep D. Ravikumar	卡内基梅隆大学	2541
47	Jason Weston	Facebook	2539
48	Rob Fergus	纽约大学	2441
49	Michael I. Jordan	加州大学伯克利分校	2427
50	Samy Bengio	Google	2354
51	Richard Socher	Salesforce	2332
52	Eric Poe Xing	卡内基梅隆大学	2303
53	Christopher D. Manning	斯坦福大学	2248
54	Martin J. Wainwright	加州大学伯克利分校	2176
55	Aude Oliva	麻省理工人工智能实验室	2113
56	Jurgen Schmidhuber	慕尼黑工业大学	2082
57	Jianxiong Xiao	普林斯顿大学计算机科学系	2079
58	Rajat Monga	Google	2052
59	Matthieu Devin	Google	2052
60	Mark Z. Mao	Google	2052
61	Andrew Senior	纽约州立大学帕切斯学院	2052
62	Paul A. Tucker	北卡罗莱纳州立大学	2052
63	Ke Yang	耶鲁大学	2052
64	Bolei Zhou	香港中文大学	1914
65	Agata Lapedriza	西班牙巴塞罗那自治大学	1914
66	Richard Zemel	多伦多大学	1897
67	Nathan Srebro	丰田工业大学芝加哥分校	1848
68	Vladlen Koltun	Intel Labs	1829
69	Inderjit S. Dhillon	德克萨斯大学奥斯汀分校	1826
70	Razvan Pascanu	加拿大蒙特利尔大学	1811
71	Alexander J Smola	亚马逊	1754
72	Benjamin Recht	加州大学伯克利分校	1719

73	Antoine Bordes	Facebook	1689
74	Nicolas Usunier	Facebook	1631
75	Joshua B. Tenenbaum	麻省理工学院	1628
76	Kyunghyun Cho	纽约大学	1626
77	Hao Su	加州大学圣地亚哥分校	1589
78	Jure Leskovec	斯坦福大学	1569
79	Faruk Ahmed	加州大学伯克利分校	1554
80	Vincent Dumoulin	Google	1554
81	Jifeng Dai	商汤科技	1508
82	Philipp Krahenbuhl	斯坦福大学	1503
83	Trevor Darrell	加州大学伯克利分校	1499
84	John Schulman	OpenAI	1488
85	Yan Duan	加拿大蒙特利尔算法研究所	1470
86	Chong Wang	微软研究院	1439
87	Volodymyr Mnih	DeepMind	1428
88	Song Han	麻省理工学院	1427
89	William J. Dally	斯坦福大学	1427
90	Prateek Jain	微软研究院	1413
91	Stephen J. Wright	威斯康星大学	1412
92	Sewoong Oh	韩国首尔延世大学	1409
93	Xiaoou Tang	香港中文大学	1405
94	Dit-Yan Yeung	香港科技大学	1400
95	John Wright	哥伦比亚大学	1374
96	Arvind Ganesh	伊利诺伊大学香槟分校	1374
97	Shankar Rao	伊利诺伊大学香槟分校	1374
98	Yigang Peng	商汤科技	1374
99	Yi Ma	加州大学伯克利分校	1374
100	Rein Houthooft	乐元素	1359

下面是本榜单 TOP10 学者的简介，其中 Geoffrey E. Hinton、Yoshua Bengio、Ian Goodfellow 已在上节中进行了介绍，本节不再重复。

- Ilya Sutskever

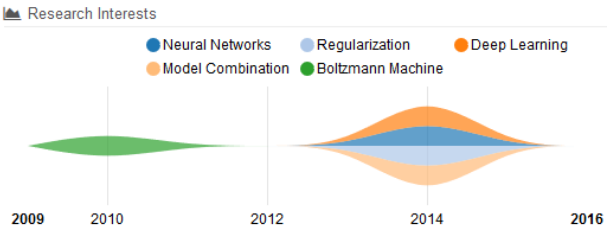




Ilya Sutskever，目前担任 OpenAI 的首席科学家。他对深度学习领域做出了几项重大贡献。他是卷积神经网络 AlexNet 的联合创始人。他与 Oriol Vinyals 和 Quoc Le 一起发明了从序列到序列的学习方法。Sutskever 也是 AlphaGo 和 TensorFlow 的共同发明人。

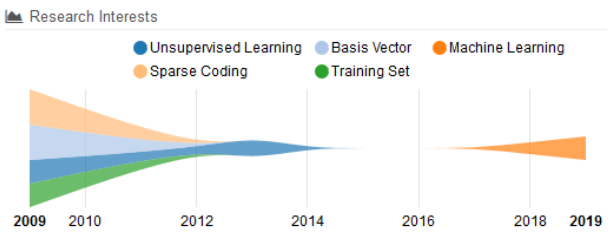
他获得了多伦多大学计算机科学系的计算机科学学士学位和博士学位。2012 年毕业后，Sutskever 在斯坦福大学跟随 Andrew Ng 做了两个月的博士后。然后他回到多伦多大学，加入了欣顿的新研究公司 DNNResearch，这是欣顿研究小组的一个分支。四个月后谷歌收购了 DNNResearch，并聘请 Sutskever 为谷歌 Brain 的研究科学家。在谷歌大脑中，Sutskever 与 Oriol Vinyals 和 Quoc Le 一起创建了序列到序列的学习算法。2015 年，Sutskever 被麻省理工学院技术评论评为 35 岁以下的 35 名创新者。2015 年底，他离开谷歌，成为新成立的 OpenAI 研究所的所长。Sutskever 是 NVIDIA NTECH 2018 和 AI Frontiers Conference 2018 的主题演讲者

- Alex Krizhevsky



Alex Krizhevsky，生于乌克兰长于加拿大，是一名计算机科学家，以其在人工神经网络和深度学习方面的研究而闻名，尤其是一种名为 AlexNet 的深度卷积神经网络。Krizhevsky 使用他的 AlexNet 在 ImageNet 挑战赛 2012 年中实现了一个图像识别的里程碑，这彻底改变了计算机视觉领域，并导致了当前的人工智能热潮。Krizhevsky 曾就读于多伦多大学，师从 Geoffrey E. Hinton 教授。在赢得 2012 年的 ImageNet 挑战赛后不久，他和他的同事将他们的初创公司 DNN Research Inc.卖给了谷歌。他的许多关于机器学习和计算机视觉的论文经常被其他研究人员引用。

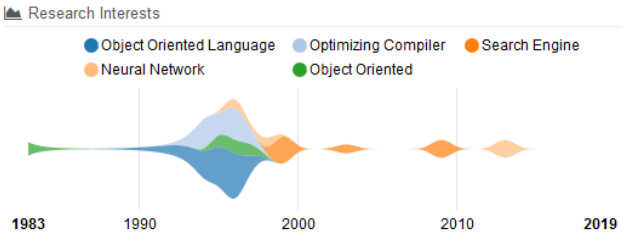
- Greg Corrado



Greg Corrado 是谷歌研究中心的首席科学家，也是谷歌大脑团队的联合创始人，主要从事人工智能、计算神经科学和可伸缩机器学习领域工作，发表过从行为经济学到粒子物理学再到深度学习等领域的论文。在谷歌工作期间，他致力于通过 RankBrain 和 SmartReply 等产品将人工智能直接交到用户手中，并通过 TensorFlow 和 Word2vec 等开源软件版本将其交到开发人员手中。在加入谷歌之前，他曾在 IBM 研究神经形态硅器件和大型神经模拟。

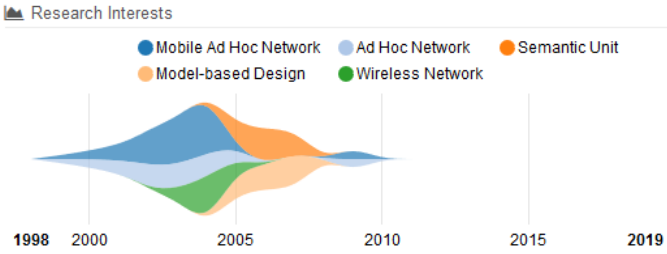
他在斯坦福大学完成了神经科学和计算机科学的研究生学业，在普林斯顿大学完成了物理学的本科学业。

- Jeffrey Dean



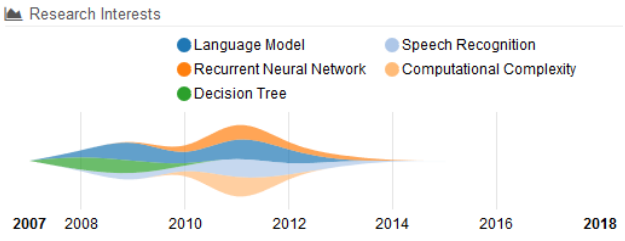
Jeffrey Dean，美国计算机科学家和软件工程师。他目前是谷歌 AI 的负责人。他在华盛顿大学获得了计算机科学博士学位，1996 年在 Craig Chambers 的指导下研究面向对象编程语言的编译器和全程序优化技术。他于 2009 年入选美国国家工程学院，该学院表彰他在“大型分布式计算机系统的科学与工程”方面的工作。在谷歌期间，他设计并实现了公司的大部分广告、爬行、索引和查询服务系统，以及构成谷歌大部分产品基础的各种分布式计算基础设施。他还致力于提高搜索质量、统计机器翻译和各种内部软件开发工具，并在工程招聘过程中有重要的参与。在加入谷歌之前，他曾在 DEC/Compaq 的西部研究实验室从事分析工具、微处理器体系结构和信息检索方面的工作。

- Kai Chen



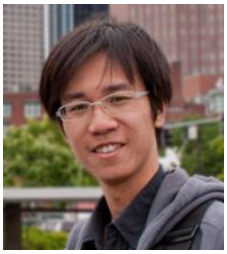
Kai Chen（陈楷），谷歌工程师，主要研究方向包括机器学习、深度学习、在线广告等，目前致力于医疗保健和自然语言处理的应用机器学习。陈楷在 1990 就读于清华大学计算机科学专业，1996-1998 年就读于特拉华大学计算机科学专业，2004 年于伊利诺伊大学香槟分校获得计算机科学博士学位。

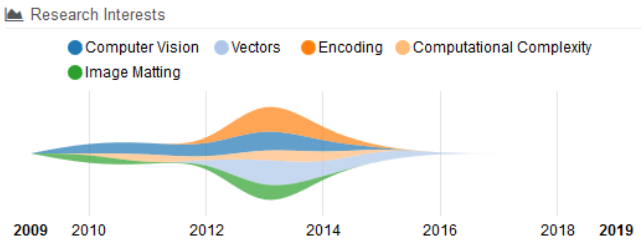
- Tomas Mikolov



Tomas Mikolov 是捷克的计算机科学家，主要从事机器学习领域的研究，目前是 Facebook 的一名研究科学家。Tomas Mikolov 在深度学习和自然语言处理领域做出了许多贡献，最著名的是发明了著名的单词嵌入方法 word2vec。在布尔诺理工大学获得计算机科学博士学位，从事基于递归神经网络的语言模型研究。在 2014 年加入 Facebook 之前，Tomas Mikolov 曾在约翰霍普金斯大学、蒙特利尔大学、微软和谷歌担任访问研究员。Tomas Mikolov 认为，如果不发展人工智能，人类将面临更大的风险，从而降低了人工智能带来的生存风险。

- Kaiming He





Kaiming He（何恺明），Facebook AI Research（FAIR）研究科学家。2011 年，何恺明博士毕业于香港中文大学多媒体实验室，导师为汤晓鸥。博士毕业后，何恺明正式加入微软亚洲研究院工作（MSRA）。他的研究兴趣是计算机视觉和深度学习。他获得了 2018 年 PAMI 青年研究员奖、2009 年 CVPR 最佳论文奖、2016 年 CVPR 最佳论文奖、2017 年 ICCV 最佳学生论文奖、2018 年 ECCV 最佳论文荣誉奖，其关于残差网络（ResNets）的论文是谷歌 Scholar Metrics 2019 中所有领域被引用最多的论文。ResNet 目前是计算机视觉领域的流行架构，也被用于机器翻译、语音合成、语音识别和 AlphaGo 的研发上。

6 应用篇

机器学习是人工智能研究的核心内容，它的应用已遍及人工智能的各个分支，随着机器学习能力的增强和技术的发展，其应用前景也十分广泛，近年来我们看到机器学习与自动驾驶、制造、金融、零售等行业产生更为紧密的融合，并开始实现大规模的商业应用。本篇将介绍机器学习算法的应用场景以及在各行业、企业中的应用。

6.1 算法应用场景

6.1.1 分类算法应用场景实例

（1） O2O 优惠券使用预测

以优惠券盘活老用户或吸引新客户进店消费是 O2O 的一种重要营销方式。然而随机投放的优惠券对多数用户造成无意义的干扰。对商家而言，滥发的优惠券可能降低品牌声誉，同时难以估算营销成本。个性化投放是提高优惠券核销率的重要技术，它可以让具有一定偏好的消费者得到真正的实惠，同时赋予商家更强的营销能力。

现有 O2O 场景相关的丰富数据，希望通过分析建模，精准预测用户是否会在规定时间内使用相应优惠券。

（2） 市民出行选乘公交预测

基于海量公交数据记录，希望挖掘市民在公共交通中的行为模式。以市民出行公交线路选乘预测为方向，期望通过分析广东省部分公交线路的历史公交卡交易数据，挖掘固定人群在公共交通中的行为模式，分析推测乘客的出行习惯和偏好，从而建立模型预测人们在未来一周内将会搭乘哪些公交线路，为广大乘客提供信息对称、安全舒适的出行环境，用数据引领未来城市智慧出行。

（3） 商品图片分类

电商网站含有数以百万计的商品图片，“拍照购”、“找同款”等应用必须对用户提供的商品图片进行分类。同时，提取商品图像特征，可以提供给推荐、广告等系统，提高推荐/广告的效果。希望通过对图像数据进行学习，以达到对图像进行分类划分的目的。

（4） 广告点击行为预测

用户在上网浏览过程中，可能产生广告曝光或点击行为。对广告点击进行预测，可以指导广告主进行定向广告投放和优化，使广告投入产生最大回报。

希望基于 100 万名随机用户在六个月的时间范围内广告曝光和点击日志，包括广告监测点数据，预测每个用户在 8 天内是否会在各监测点上发生点击行为。

6.1.2 回归算法应用场景实例

（1） 机场客流量分布预测

为了有效利用机场资源，机场正利用大数据技术，提升生产运营的效率。机场内需要不断提升运行效率的资源有航站楼内的各类灯光电梯设施设备、值机柜台、商铺、广告位、安检通道、登机口，航站楼外的停机位、廊桥、车辆（摆渡车、清洁车、物流车、能源车），要想提升这些资源的利用率，首先需要知道未来一段时间将会有多少旅客或航班会使用这些资源，其次需要精准的调度系统来调配这些资源和安排服务人员，帮助机场提升资源利用效率，保障机场安全与服务提升。

以海量机场 WiFi 数据及安检登机值机数据，希望通过数据算法实现机场航站楼客流分析与预测。

（2） 新浪微博互动量预测

新浪微博作为中国最大的社交媒体平台，旨在帮助用户发布的公开内容提供快速传播互动的通道，提升内容和用户的影响力。希望能够最快找到有价值的微博的方法，然后应用于平台的内容分发控制策略，对于有价值的内容可以增加曝光量，提高内容的传播互动量。对于一条原创博文而言，转发、评论、赞等互动行为能够体现出用户对于博文内容的兴趣程度，也是对博文进行分发控制的重要参考指标。

希望根据抽样用户的原创博文在发表一天后的转发、评论、赞总数，建立博文的互动模型，并预测用户后续在博文发表一天后的互动情况。

（3） 电影票房预测

中国是全球第二大电影市场，同时也是增长最快的市场之一；随着市场的成熟，影响电影票房的因素也越来越多，包括题材、内容、导演、演员、编辑和发行方等等。因此对电影制作公司而言，依靠主观经验制作一部高票房的电影也越来越困难，而随着大数据技术的发展，借助大数据分析对电影市场进行分析，指导电影制作成为可能。

希望依据历史票房数据、影评数据、舆情数据等互联网公众数据，对电影票房进行预测。

6.1.3 聚类算法应用场景实例

（1） 基于用户位置信息的商业选址

随着信息技术的快速发展，移动设备和移动互联网已经普及到千家万户。在用户使用移动网络时，会自然的留下用户的位置信息。随着近年来 GIS 地理信息技术的不断完善普及，结合用户位置和 GIS 地理信息将带来创新应用。如百度与万达进行合作，通过定位用户的位置，结合万达的商户信息，向用户推送位置营销服务，提升商户效益。

商户希望通过大量移动设备用户的位置信息，为某连锁餐饮机构提供新店选址。

（2） 中文地址标准化处理

地址是一个涵盖丰富信息的变量，但长期以来由于中文处理的复杂性、国内中文地址命名的不规范性，使地址中蕴含的丰富信息不能被深度分析挖掘。通过对地址进行标准化的处理，使基于地址的多维度量化挖掘分析成为可能，为不同场景模式下的电子商务应用挖掘提供了更加丰富的方法和手段，因此具有重要的现实意义。

（3） 国家电网用户画像

随着电力体制改革向纵深推进，售电侧逐步向社会资本放开，当下的粗放式经营和统一式客户服务内容及模式，难以应对日益增长的个性化、精准化客户服务体验要求。如何充分利用现有数据资源，深入挖掘客户潜在需求，改善供电服务质量，增强客户黏性，对公司未来发展至关重要。

对电力服务具有较强敏感度的客户对于电费计量、供电质量、电力营销等各方面服务的质量及方式上往往具备更高的要求，成为各级电力公司关注的重点客户。经过多年的发展与沉淀，目前国家电网积累了全网 4 亿多客户档案数据和海量供电服务信息，以及公司营销、电网生产等数据，可以有效的支撑海量电力数据分析。

因此，国家电网公司希望通过大数据分析技术，科学的开展电力敏感客户分析，以准确地识别敏感客户，并量化敏感程度，进而支撑有针对性的精细化客户服务策略，控制电力服务人工成本、提升企业公众形象。

6.1.4 关联规则应用场景实例

（1） 依据用户轨迹的商户精准营销

随着访问移动互联网的用户量逐渐增长，随着移动终端的大力发展，越来越多的用户选择使用移动终端访问网络，根据用户访问网络的偏好，也形成了相当丰富的用户网络标签和画像等。如何根据用户的画像对用户进行精准营销成为了很多互联网和非互联网企业的新发展方向。如何利用已有的用户画像对用户进行分类，并针对不同分类进行业务推荐，特别是在用户身处特定的地点、商户，如何根据用户画像进行商户和用户的匹配，并将相应的优惠和广告信息通过不同渠道进行推送。

希望根据商户位置及分类数据、用户标签画像数据提取用户标签和商户分类的关联关系，然后根据用户在某一段时间内的位置数据，判断用户进入该商户地位范围 300 米内，则对用户推送符合该用户画像的商户位置和其他优惠信息。

（2） 基于兴趣的实时新闻推荐

随着近年来互联网的飞速发展，个性化推荐已成为各大主流网站的一项必不可少服务。提供各类新闻的门户网站是互联网上的传统服务，但是与当今蓬勃发展的电子商务网站相比，新闻的个性化推荐服务水平仍存在较大差距。一个互联网用户可能不会在线购物，但是绝大部分的互联网用户都会在线阅读新闻。因此资讯类网站的用户覆盖面更广，如果能够更好的挖掘用户的潜在兴趣并进行相应的新闻推荐，就能够产生更大的社会和经济价值。初步研究发现，同一个用户浏览的不同新闻的内容之间会存在一定的相似性和关联，物理世界完全不相关的用户也有可能拥有类似的新闻浏览兴趣。此外，用户浏览新闻的兴趣也会随着时间变化，这给推荐系统带来了新的机会和挑战。

因此，希望通过对带有时间标记的用户浏览行为和新闻文本内容进行分析，挖掘用户的新闻浏览模式和变化规律，设计及时准确的推荐系统预测用户未来可能感兴趣的新闻[68]。

实际上，如今随着机器学习开始进入商业化阶段，机器学习在自动驾驶、制造业、金融业、零售业等行业领域得到了极为广泛的应用。其应用场景往往相对复杂，需要多种机器学习的方法，甚至多个学科的方法相结合才能得到较好的解决。后面的章节，本报告将详细介绍其在不同行业的应用。

6.2 行业应用

作为人工智能的核心技术，过去机器学习的应用更多是企业测试性的行动，近年来机器学习与自动驾驶、制造、金融、零售等行业开始有了更紧密的融合，并开始实现大规模的商业应用。下面我们分行业对机器学习的应用案例进行介绍。

6.2.1 金融行业应用

- 欺诈检测

使用机器学习进行欺诈检测时，先收集历史数据并将数据分割成三个不同的部分，然后用训练集对机器学习模型进行训练，以预测欺诈概率。最后建立模型，预测数据集中的欺诈或异常情况。与传统检测相比，这种欺诈检测方法所用的时间更少。由于目前机器学习的应用量还很小，仍然处于成长期，所以它会在几年内进一步发展，从而检测出复杂的欺诈行为。

- 股票市场预测

当今，股票市场俨然已成为大家关注的热点，但是，如果不了解股票运作方式和当前趋势，要想击败市场则非常困难。随着机器学习的使用，股票预测变得相当简单。这些机器学习算法会利用公司的历史数据，如资产负债表、损益表等，对它们进行分析，并找出关系到公司未来发展的有意义的迹象。此外，该算法还可以搜索有关该公司的新闻，并通过世界各地的消息源来了解市场对公司的看法。此外，通过自然语言处理技术，它可以通过浏览新闻频道和社交媒体的视频库来搜索更多有关该公司的数据。这项技术还在发展中，虽然目前还不够准确，但可以肯定的是，在不久的将来，它将能够做出非常准确的股市预测。

- 财资部（Treasury）/客户关系管理（CRM）/现货交易（Spot Transactions）

客户关系管理（CRM）在小额银行业务中占有十分突出的地位，但在银行内部的财资空间却没什么作用。因为财资部有自己的产品群，如外汇、期权、掉期交易（Swaps）、远期交易（Forwards）以及更为重要的现货交易（Spots）。线上交易需要结合这些产品的复杂程度、客户风险、市场与经济行为以及信用记录信息，这对银行来说几乎是一个遥远的梦想。

- 聊天机器人/私人财务助理

聊天机器人可以担当财务顾问，成为个人财务指南，可以跟踪开支，提供从财产投资到新车消费方面的建议。财务机器人还可以把复杂的金融术语转换成通俗易懂的语言，更易于沟通。一家名为 Kasisto 的公司的聊天机器人就能处理各种客户请求，如客户通知、转账、支票存款、查询、常见问题解答与搜索、内容分发渠道、客户支持、优惠提醒等。通过长期记录用户的可扣除费用，还能提供潜在节流账单[69]。

- 摩根大通

摩根大通推出了一个智能合约（COiN）平台，该平台利用自然语言处理技术，它解决了从法律文件中提取重要数据的问题。对 12,000 份年度商业信贷协议进行人工审查通常需要约 360,000 个工时。然而，机器学习允许在短短几个小时内审查相同数量的合同。

- BNY Mello

将流程自动化集成到他们的银行生态系统中。这项创新每年可节省 30 万美元，并带来了极大的改善了运营情况。

- Privatbank

一家乌克兰银行，通过其移动和网络平台实施聊天机器人助理。Chatbots 加快了一般客户查询的解决速度，并减少人工助理的数量[70]。

摩根大通量化投资和金融衍生品战略团队的Marko Kolanovic和Rajesh T.Krishnamachari最近刚刚发布了一份在金融服务领域机器学习和大数据最为全面的一份报告。这份报告名为“大数据和AI战略”，副标题是“机器学习和其它投资数据分析方法”，该报告指出，机器学习将会在未来对市场运作至关重要。分析师、投资经理、交易预案和投资总监都需要了解机器学习技术。如果不这样做，他们就会落伍——像月收益和GDP数字这样的常规数据源正在变得与投资策略越来越不相关，因为使用新数据集和方法的投资者可以预测这些数字，并在它们发布前预先做出行动[71]。

6.2.2 自动驾驶

将汽车内外传感器的数据进行融合，借此评估驾驶员情况、进行驾驶场景分类，都要用到机器学习。自动驾驶汽车的设计制造面临着诸多挑战，如今，各大公司已经广泛采用机器学习寻找相应的解决方案。汽车中的ECU（电子控制单元）已经整合了传感器数据处理，如何充分利用机器学习完成新的任务，变得至关重要。潜在的应用包括将汽车内外传感器的数据进行融合，借此评估驾驶员情况、进行驾驶场景分类。这些传感器包括像激光雷达，雷达，摄像头或者是物联网。

车载信息娱乐系统所运行的应用，能从传感器数据融合系统中获取数据。举个例子，如果系统察觉驾驶员发生状况，有能力把车开到医院。基于机器学习的应用，还包括对驾驶员的语言和手势识别以及语言翻译。相关的算法被分类为非监督和监督算法。它们两者的区别在于学习的方式。

在自动驾驶汽车上，机器学习算法的一个主要任务是持续渲染周围的环境，以及预测可能发生的变化。这些任务可以分为四个子任务：目标检测、目标识别或分类、目标定位、运动预测。

机器学习算法可以简单地分为4类：决策矩阵算法、聚类算法、模式识别算法和回归算法。可以利用一类机器学习算法来完成两个以上的子任务。例如，回归算法能够用于物体定位和目标识别或者是运动预测[72]。

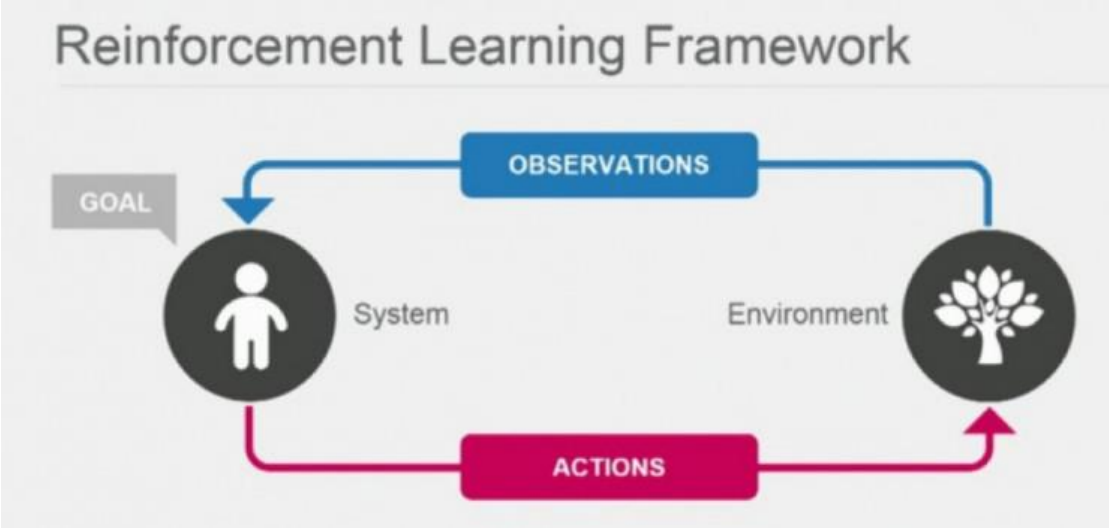


图 6-1 自动驾驶目标识别、运动预测

6.2.3 健康和医疗

为了更好地了解人工智能和机器学习正如何改变医疗保健行业，我们通过一些具体案例，并且这些案例可以有力证明这些前沿技术的实用价值。

- 判断发展中国家的结核病情况

识别图像中的模式（Pattern）是现有人工智能系统中最强有力的一点，研究人员现在正在训练人工智能检查胸部 x 光片，识别结核病。这项技术可以为缺乏放射学家的结核病流行地区带来有效的筛查和评估手段。

- 一种治疗退伍军人创伤后应激障碍（PTSD）的人工智能

退伍军人创伤后成长计划与 IBM Watson 合作使用人工智能和分析技术，以确保更多患有创伤后应激障碍的退伍军人能够完成心理治疗。使用这些技术，他们的完成率从不到 10%上升到 73%。根据退伍军人事务部的统计，80%的患有创伤后应激障碍的退伍军人在确诊后一年内完成治疗计划，然后康复。在 300 万阿富汗和伊拉克战争老兵中，大约五分之一患有创伤后应激障碍。

- 检测脑出血

以色列医疗技术公司 MedyMatch 和 IBM Watson Health 正在使用人工智能，通过检测颅内出血，帮助医院急诊室的医生更有效地治疗中风和头部外伤患者。AI 系统使用临床洞察力（clinical insight）、深度学习、患者数据和机器视觉来自动标记潜在的脑出血，以供医生检查。

- 优化管理工作流程并消除等待时间

行政和助理工作是 AI 起作用的主要领域。埃森哲表示，语音到文本转录等省时的工作流功能有可能替代为医疗专业人员订购测试和处方以及在图表中写笔记等任务--任何涉及非患者护理的任务。这相当于节省了 17%的医生工作时间和 51%的注册护士工作时间。

人工智能还可以优先处理医生的电子邮件，并帮助患者解决简单的医疗问题，而无需医生的帮助，优化双方的时间表。例如，启动 Scanadu 的 doc.ai 自然语言处理程序允许患者通过应用程序向他们解释实验室结果，从而节省了患者和医生的时间和金钱。Nuance Communication 推出了一款类似虚拟助手的产品，可以解释测试结果并处理患者的基本问题。首先实施这些技术的医疗保健组织将会从中获利，因为他们将有最多的时间来构建知识库。

- 检测阿尔茨海默病

现在，人工智能机器人只需要不到一分钟的时间，就可以根据语音模式和声音来诊断阿尔茨海默氏病，准确率达到 82%，而且这种准确率还在不断提高。人工智能系统可以处理单词之间的停顿长度、处理代词优于专有名词的任何偏好、处理过于简单的描述以及语音频率和幅度的变化。所有这些因素对于人类听众来说都很难高精度地记录和检测，但人工智能系统却能够进行客观和可量化的分析。

- 癌症诊断

用于检测和诊断癌症的传统方法包括计算机断层扫描（CT）、磁共振成像（MRI）、超声和 X 射线。不幸的是，许多癌症无法通过这些技术得到足够准确的诊断，从而可靠地挽救生命。微阵列基因图谱的分析是一种替代方法，但这项技术需要计算很多小时，除非这项技术可以使用 AI 替换。现在已经被证明，斯坦福大学的人工智能诊断算法与由 21 名经委员会认证的皮肤科医生的团队一样有效地从图像中检测潜在的皮肤癌。Startup Enlitic 正在使用深度学习来检测 CT 图像中的肺癌结节，其算法比作为一个团队工作的专家胸科医生的准确率高 50%。

在人工智能的帮助下，其他医疗保健公司正在经历诊断、治疗甚至治愈的过程。Insilico Medicine 正在用深度学习算法寻找新药和治疗方法，包括新的免疫疗法。这些基因疗法使用每个病人的细胞来模拟他们自己的生物学和免疫系统。

人工智能之所以能使这些疗法奏效，是因为它能设计出组合疗法，并以闪电般的速度，以模拟的形式进行数百万次实验来识别令人难以置信的复杂的生物标记物。

- 机器人辅助手术

在价值潜力方面，机器人辅助手术是人工智能辅助方向的佼佼者。AI-enabled 机器人技术可以通过集成实时操作矩阵、来自实际手术医生的数据以及来自手术前病历的信息来提高和指导手术器械的精度。事实上，埃森哲报告说，人工智能机器人技术带来的进步缩短了 21%的停留时间[73]。

6.2.4 零售业

IDC 副总裁 Ivano Ortis 最近分享了他的观点“人工智能将把分析带到一个新的水平，并将成为零售创新的基础，这已经得到了全球半数零售商的认可。人工智能可以实现规模化、自动化和前所未有的精度，当适用于超细微客户细分和上下文交互的时候，可推动客户体验”。

鉴于人工智能和机器学习的能力，很容易看到人工智能和机器学习是如何成为零售商强大的工具。现在，计算机可以读取、倾听和了解数据，从数据中进行学习，立即且准确地推荐下一个最佳动作，而不需要明确的编程。这对那些希望能够准确预测需求、预期客户行为、优化和个性化客户体验的零售商来说是一个福音。

例如，它可以用于自动化：

- 基于关于每个客户独特性和购买倾向的个性化产品建议
  - 选择额外的加售和交叉销售选择，推动更大的客户价值
  - 聊天机器人可以推动与客户进行智能的、有意义的交互
  - 根据过去和现在的采购数据和客户数据推荐额外服务和产品
  - 平面图分析，支持店内产品销售，告诉人们还缺些什么，将销售情况与货架空间进行对比，通过自动重新订货加速货架补充
  - 定价引擎，做定制化的、适合情境的定价决策

特别是在英国，零售商们已经可以收集大量来自客户的交易数据和行为数据。而且随着数据量的增长，处理能力的提升，机器学习已经更广泛地应用于零售行业，进一步优化业务流程，推动更有影响力的个性化、上下文消费者体验和产品。

零售业已经开始感受到人工智能和机器学习的影响了，例如：

- 零售商正在通过机器学习结合物联网技术来预测需求，优化商店业务并减轻员工负担。

- 基于店内摄像头检测提供个性化的广告，承担店员部分的半手动的、通过在平板电脑或者触屏终端设备查看客户的消费记录。
- 零售商可以监控排队结账的等候时间，以了解个别店面的流量和商店销售效率，然后进行分类和调整店面布局来实现购物篮、满意度和销售的最大化。
- 系统现在可以通过把计划调整为按需活动，来识别和预测客户行为，改善员工生产效率。
- 摄像头系统可以在店内员工之前检测易腐产品的新鲜状态。
- 实体店正在实现很多操作任务的自动化，例如设置货架定价，确定产品分类和混合，优化促销等。
- 店内应用可以显示客户在特定通道停留了多长时间，根据个人消费记录和偏好数据，提供有针对性的优惠和建议（通过他/她的移动设备）。

麦肯锡最近的一项研究提供了很多例子，量化了这些技术如何改变零售商运营和竞争方式所带来的潜在价值，例如：

采用数据和数据分析的美国零售商供应链业务已经看到，过去 5 年运营利润率增长了 19%。使用数据和分析来改善商品销售，包括定价、分类和展示位置优化，使得运营利润率又提高了 16%。

个性化广告是当前机器学习最强大的用例之一。其他具有较高潜力的零售用例还包括优化定价、根据旅行和物流的实时数据优化编排计划，还有优化商品销售策略。

微薄的利润（尤其是在杂货行业）以及来自行业领先早期采用者的压力——例如亚马逊和沃尔玛——使得利用客户数据降低整个价值链成本的动力越来越强。但是麦肯锡分析师在 2011 年估计，美国零售行业仅实现了 30% ~ 40%的潜在利润提升和生产效率的增长——这一增长中有很大一部分是通过降低价格实现的。所以到目前为止，人工智能和机器学习只发挥了很小一部分的潜在价值。

据福布斯称，美国零售商有潜力实现净利润 60%的增长和年生产力 0.5% ~ 1%的增长。但是，实现这一价值还存在着障碍，例如缺乏分析人才，企业内的数据孤岛。

这时候就需要机器学习和人工智能了。人工智能和机器学习可以帮助减轻推动利用可用数据所需的分析任务。当部署了一个全公司范围的、实施的分析平台时，这将成为所有公司职能优化决策所依赖的事实来源[74]。

6.2.5 制造业

与自动驾驶汽车一样，随着物联网的发展，制造业企业可以从安置在生产线各环节的传感器收集大量的生产数据。

然而，这些数据并没有被充分利用。随着从复杂系统收集到众多参数的数据，数据分析变成了一项艰巨的任务。机器学习在制造业中的最大应用将是异常检测。

据统计，到 2030 年，全球的淡水需求预计将超过供应近 40%。为协助各企业实现净零水循环使用的目标，美国水处理公司 Ecolab（艺康集团）正通过包括 Azure 和 Dynamics CRM Online 在内的微软云平台帮助全球企业实现可持续运营。

与全球各地数以千计传感器相连的云平台能收集实时用水数据，并通过机器学习和商业智能分析全球各地的生产用水运营解决方案，不仅提高效率，还能降低水、能源消耗及运营成本。

尽管在这个领域之前已经进行过一些分析尝试，未来将会有更多机器学习通过监督学习和建模来预测风险和失败。

此外，机器学习也将推动工业自动化的实现，通过观察生产线和数据流来学习，并能够精确优化生产过程，降低生产成本，加快生产周期，从而节省人工分析数据的时间成本和资金成本[75]。

6.3 企业应用

6.3.1 机器学习在国内企业的应用

- 百度机器学习云平台

百度机器学习云平台（Baidu Machine Learning，简称 BML）是基于百度公有云和私有云平台，由百度基础架构部自主研发的机器学习产品。面向百度公有云和私有云的机器学习/数据挖掘/数据分析的用户，致力于建设业界领先的机器学习云平台。BML 主要应用于大数据的统计与分析、数据挖掘、模型训练、商业智能、可视化等领域，包括百度公司内部的广告点击预估，搜索排序，推荐等重要应用都运行在 BML 上。BML 是百度公司多年以来大规模分布式机器学习方面的技术优势积累。不仅提供了丰富、高效、成熟的机器学习算法，还打通了机器学习的全流程，用户可以便捷的完成从原始数据格式化、统计、训练、评估、预测、发布模型服务等应用。

高效的分布式计算能力让用户即使在海量数据的情况下，也能轻松达成工作目标，几百 T 的样本训练一个模型在几个小时就能搞定。BML 还提供前沿的深度学习研发成果，从普通 DNN 到 Word2Vec 训练有全面的支持，帮助用户训练自己的神经网络并且对训练结果进行可视化，方便进行深度学习的训练过程以及结果的可视化。

BML 还为公有云的企业级用户提供了成套的解决方案，快速接入解决企业的实际问题，帮助用户挖掘大数据的价值[76]。

- 阿里云发布机器学习平台

阿里云机器学习平台是构建在阿里云 MaxCompute（原 ODPS）计算平台之上，集数据处理、建模、离线预测、在线预测为一体的机器学习平台。阿里云机器学习封装了阿里巴巴集团内成熟的算法，向机器学习用户提供了更简易的操作体验。

机器学习平台 PAI 3.0 推出了全新的算法模型市场，涵盖电商、社交、广告、金融等多个行业，数十种场景的算法模型。同时还新增了流式算法组件、图神经网络、增强学习组件等平台工具。作为机器学习平台的内核，PAI 的智能计算引擎进行了全面升级，通过编译技术优化通用计算引擎，训练性能提升 400%。PAI 团队研发了深度学习编译器 TAO（Tensor Accelerator and Optimizer），以通用化、平台化的方式有效解决上层 Workload 与底层硬件计算单元之间高效映射的问题。

此外，在深度学习优化分布式引擎方面，PAI 3.0 可以实现单任务支持上千 worker 并发训练，并支持 5k+超大规模异构计算集群。PAI 希望实现‘用更少的硬件，支持更多业务更快完成业务迭代’。为了完成这个目标，团队有针对性地研发了 GPU 分时复用技术。整套技术实现遵循了数据驱动的思想，包括实时在线性能数据反馈通路、细粒度 GPU 资源复用、虚拟显存以及基于历史数据的资源预估策略这几个关键模块。

此外，PAI 3.0 还发布了大规模图神经网络，缓存机制效率提升 40%，算子速度提升 12 倍，系统端建图时间从数小时降至 5 分钟。据了解，从 PAI1.0 开始，该机器学习平台已经在阿里巴巴内部使用了 2 年。基于该平台，在淘宝搜索中，搜索结果会基于商品和用户的特征进行排序。通过使用参数服务器，淘宝可以把百亿个特征的模型，分散到数十个乃至于上百个参数服务器上，打破了规模的瓶颈[77]。

- 腾讯智能钛机器学习

智能钛机器学习（TI Machine Learning, TI-ML）是基于腾讯云强大计算能力的一站式机器学习生态服务平台。它能够对各种数据源、组件、算法、模型和评估模块进行组合，使得算法工程师和数据科学家在其之上能够方便地进行模型训练、评估和预测。智能钛系列产品支持公有云访问、私有化部署以及专属云部署。腾讯智能钛机器学习具有多种应用场景：

- 金融

金融行业的客户具备多样性，如何根据客户历史数据，对相关客户进行针对性理财产品推荐，是提高工作效率，提升金融机构效益，和提升用户体验的关键。机器学习平台可以辅助金融机构建立用户购买行为预测模型，预测用户行为，从而对用户进行针对性理财产品推荐。

- 工业

传统的工业质检依赖大量人力，成本高且漏检率难以提升。TI 机器学习平台基于设备参数与生产图像对产品进行缺陷检测与缺陷分类，大大降低人力成本、提升缺陷检出率的同时帮助企业进行质量控制数字化管理。

- 教育

随着行业的兴起，各类 AI 算法大赛不断，如何提供满足各参赛队伍的使用习惯的工具，同时又能支撑数千人的高并发一直是各举办单位的痛点，TI 机器学习平台内置的丰富算法与框架组件满足不同用户的使用习惯，高性能集群稳定性可以支持大批量的训练任务[78]。

- 第四范式

第四范式在上海发布了基于“机器学习圈”理论的最新产品化成果——AI Prophet AutoML 平台（下简称“AutoML 平台”）与 AI Prophet AutoCV 平台（下简称“AutoCV 平台”）。两款产品以人工智能通用平台“第四范式先知”为基础能力，结合企业 AI 应用的场景需求以及第四范式 “让 AI 做 AI”的 AutoML 技术，逐步扩大“第四范式先知”的生态系统，为 AI 规模化、产业化落地提供了新的借鉴模式。

第四范式 AutoML 平台旨在帮助企业基于历史的数据、业务的实时反馈做迭代，充分挖掘特征做出精准决策。AutoML 平台友好交互界面大幅降低了 AI 应用门槛，企业只需“收集行为数据、收集反馈数据、模型训练、模型应用”4 步，无需大量编码工作，即可使企业业务专家升级为 AI 开发者、完成 AI 应用，将 AI 的开发周期从以半年为单位缩短至周级别。

第四范式 AutoCV 平台则秉承了“第四范式先知”企业级、低门槛、低总拥有成本（TCO）、端到端全流程覆盖等 DNA，赋予企业自主可控、高效率的智能视觉构建能力。据了解，按照以往流程，企业构建一个智能视觉应用需要历经 9 个必要过程，约需 20 人专家团队近 60 天时间；采用 AutoCV 平台只需耗费 1 名业务人员 1 天的时间，不仅生产效率提升 120 倍，TCO 成本也呈现数量级下降[79]。

6.3.2 机器学习在国外企业的应用

机器学习是与人工智能一同急剧发展的领域，这两种新兴技术催生了新的商业活动，不乏机器学习初创公司或人工智能公司。下面介绍了国外若干顶尖的机器学习公司[80]。

- 亚马逊

机器学习用于亚马逊的全部消费者服务，从在线商店到 Kindle 和 Echo 设备，不一而足。机器学习用于确定用户喜好(比如产品购买)，还用于 Alexa 引擎、Alexa 智能家居设备、亚马逊 JHIM、亚马逊 Rekognition、亚马逊音乐及其他功能。此外，该公司基于从消费级产品方面获得的体验，通过 AWS 提供机器学习服务。

Amazon SageMaker 是一项完全托管的服务，可以帮助开发人员和数据科学家快速构建、训练和部署机器学习（ML）模型。SageMaker 完全消除了机器学习过程中每个步骤的繁重工作，让开发高质量模型变得更加轻松。

传统的 ML 开发是一个复杂、昂贵、迭代的过程，而且没有任何集成工具可用于整个机器学习工作流程，这让它难上加难。您需要将工具和工作流程拼接在一起，这既耗时又容易出错。SageMaker 在单个工具集中提供了用于机器学习的所有组件，让这一难题迎刃而解，因此模型将可以通过更少的工作量和更低的成本更快地投入生产。

- 苹果

苹果借助机器学习大大改善了 Siri，因此它不仅仅可以呼叫联系人列表的某个人。还可以识别谁最近向你发送了电子邮件，但不在你的联系人列表中；还有面部识别功能，识别 30000 多个中文字符，或者告诉你车子泊在哪里。在全球开发者大会（WWDC）上，苹果面向 iOS 开发者推出了最新版的机器学习模型框架 Core ML 3，将机器智能引入智能手机 app。

Core ML 3 将首次能够为设备上的（on-device）机器学习提供训练，以提供 iOS app 的个性化体验。利用不同的数据集训练多个模型的能力也将成为 macOS 上新的 Create ML app 的一部分，用于目标检测和识别声音等 app。需机器学习的专业知识，使用 Core ML 3 和新的 Create ML app，轻松创建、训练并部署机器学习模型。

其主要特点如下：

- 设备模型个性化

Core ML 模型被捆绑到 app 中，帮助驱动像在照片中搜索或对象识别这样的智能功能。现在，这些模型可以通过设备上的用户数据进行更新，帮助模型在不违背隐私的情况下了解用户行为。

- 支持高级神经网络

现在最复杂的机器学习模型可以在带有 Core ML 3 的设备上运行。可以使用并运行最新的模型，如用于理解图像、视频、声音和其他富媒体的尖端神经网络。

- 构建计算机视觉机器学习功能

在 app 中轻松构建计算机视觉机器学习功能。利用人脸检测、跟踪和捕获以及文本识别、图像显著性和分类，以及图像相似性识别。其他功能包括提高地标检测、矩形检测、条形码检测、目标跟踪和图像配准。使用新的 Document Camera API 通过相机检测和捕获文档。

- 训练和部署 NLP 模型

对自然语言文本进行分析，推导出其语言特有的元数据，以供深入理解。你可以使用这个框架和 Create ML 来训练和部署定制的 NLP 模型。功能包括 Create ML 文本模型的迁移学习、词嵌入向量（WordEmbedding）、情感分类和文本目录。可用于英语、法语、德语、意大利语、简体中文和西班牙语。

- 演讲

利用设备上 10 种语言的语音识别以及语音显著性功能，如语音信息、streaming confidence、语音检测和声学功能。你的 app 可以通过访问语音识别信息来消除同音词的歧义。这些功能现在也可用于 Mac app[81]。

- Ayasdi

Ayasdi 最初是 DARPA（美国国防部高级研究项目组）资助的一家初创公司，诞生于斯坦福大学数学系。其核心技术“拓扑数据分析”可以找到复杂数据中的细微模式，尤其是能够找到所谓“暗数据”中的洞察力，这种数据常常被认为无用，但实际上大有价值。为我们的平台提供动力的引擎称为拓扑数据分析（Topological Data Analysis, TDA）。TDA 被认为是 DARPA 资助的最重要的技术进步之一，并获得了广泛的奖项和认可。

TDA 基于拓扑学的数学原理。拓扑学研究数据的形状。TDA 指的是对这一学科的适应，以分析高度复杂的数据。它借鉴了这样一种理念，即所有数据都有一个基本的形状，而这个形状是有意义的。Symphony AyasdiAI 的 TDA 方法借鉴了广泛的机器学习、统计和几何算法，结合和综合他们的数据。分析创建所有数据点的摘要或压缩表示，以帮助快速发现数据中的关键模式和关系。通过识别数据点之间存在的几何关系，Symphony AyasdiAIi 的 TDA 方法提供了一种极其简单的数据查询方法，以了解数据中片段和子片段的基本属性。通过减少对机器学习专家选择正确算法的依赖，TDA 减少了遗漏关键见解的可能性。它经常使用

当前的机器学习技术作为输入来发现本地数据中的微妙模式和洞察力。通常，TDA 增强了与之配对的任何算法[82]。

事实上，Ayasdi 一直在美国与各个顶级医院和药厂合作。医院和制药公司可以从公开的信息源获得很多数据，和他们自己的数据结合起来，进行一些新的研究[83]。

- Digital Reasoning

Digital Reasoning 擅长认知计算，运用机器学习来识别沟通数据中有意思的人类行为。它利用人工智能积累上下文，填补任何来源的认知空白，明确什么有价值、什么没价值，并通过揭露隐藏的关系、风险和机会来得出结论。

Digital Reasoning 公司研发出的这种机器学习平台，能够建立一种语言学习模式，而不只是单纯地识别关键字。它能比传统的工具更加智能地识别出银行的内幕交易及价格操纵行为，在知识图谱的基础上真正理解用户的请求，不再拘泥于用户所输入请求语句的字面本身，而是透过现象看本质，准确地捕捉到用户所输入语句后面的真正意图，并以此来进行搜索与挖掘，从而更准确地向用户反馈结果。该智能平台甚至被训练成能够识别出交易滥用、官商勾结、市场操控等现象。

Digital Reasoning 的首次亮相是在 911 事件中。当时，该公司正在帮助政府抓捕网络上的恐怖分子。这些网络上的信息几乎都是用一些代码来掩盖其真正意义，因此迫使 Digital Reasoning 要运用更加智能的语言。

近日，Digital Reasoning 公司还与美国纳斯达克（Nasdaq）进行了合作，协助其建设监测资本市场的工具。Nasdaq 在今年 5 月份对其投资了 4000 万美元[84]。

- Darktrace

Darktrace 使用人工智能和机器学习来提供名为“企业免疫系统”的网络安全系统，该系统模拟人体免疫系统：了解什么是所有设备和用户的“正常行为”，环境变化后更新洞察的信息，然后寻找表明存在安全问题的异常情况。因此，它不需要传统防病毒软件所使用的病毒特征数据库；一旦发现新威胁，就会更新。

企业免疫系统是世界上最先进的网络防御机器学习技术。受到人体免疫系统自我学习智能的启发，这种新技术在复杂和普遍的网络威胁的新时代中，使组织自我保护方式发生了根本转变。

人体免疫系统非常复杂，并且不断适应新形式的威胁，例如不断变异的病毒 DNA。它的工作原理是了解身体的正常情况，识别和消除那些不符合正常发展模式的异常值。

Darktrace 将相同的逻辑应用于企业和工业环境。在机器学习和人工智能算法的支持下，企业免疫系统技术迭代地为网络中的每个设备和用户学习提供独特的“生活模式”(“自我”)，并将这些见解联系起来，以发现新出现的威胁，否则这些威胁将被忽视。

从一开始，Darktrace 就拒绝了与历史攻击相关的数据可以预测未来数据的假设。相反，Darktrace 的网络 AI 平台使用无监督的机器学习来大规模地分析网络数据，并根据它所看到的证据进行数十亿次基于概率的计算。它不依赖于过去威胁的知识，而是独立地对数据进行分类并检测引人注目的模式[85]。

- Facebook

Facebook 的 20 亿用户每天都在使用机器学习，但他们没意识到这一点。它用于 Facebook、Messenger 和 Instagram 的朋友标记建议、个性化新闻源、共同朋友分析和社群推荐。该公司在全球有四个人工智能研究园区，表明它专注于用人工智能来运行网站。

使用机器学习的主要服务：

- 消息推送

消息推送排名算法能够使用户在每次访问 Facebook 时，最先看到对他们来讲最重要的事情。一般模型会通过训练来确定影响内容排序的各种用户和环境因素。之后，当用户访问 Facebook 时，该模型会从数千个候选中生成一个最佳推送，它是一个图像和其他内容的个性化集合，以及所选内容的最佳排序。

- 广告

广告系统利用机器学习来确定向特定用户显示什么样的广告。通过对广告模型进行训练，我们可以了解用户特征，用户上下文，以前的互动和广告属性，进而学习预测用户在网站上最可能点击的广告。之后，当用户访问 Facebook 时，我们将输入传递进训练好的模型运行，就能立马确定要显示哪些广告。

- 搜索

搜索会针对各种垂直类型（例如视频、照片、人物、活动等）启动一系列特定的子搜索进程。分类器层在各类垂直类型的搜索之前运行，以预测要搜索的是垂直类型中的哪一个，否则这样的垂直类型搜索将是无效的。分类器本身和各种垂直搜索都包含一个训练的离线阶段，和一个运行模型并执行分类和搜索功能的在线阶段。

- Sigma

Sigma 是一个分类和异常检测通用框架，用于监测各种内部应用，包括站点的完整性，垃圾邮件检测，支付，注册，未经授权的员工访问以及事件推荐。Sigma 包含了在生产中每

天都要运行的数百个不同的模型，并且每个模型都会被训练来检测异常或更一般地分类内容。

- Lumos

Lumos 能够从图像及其内容中提取出高级属性和映射关系，使算法能够自动理解它们。这些数据可以用作其他产品和服务的输入，比如通过文本的形式。

- Facer

Facer 是 Facebook 的人脸检测和识别框架。给定一张图像，它首先会寻找该图像中所有的人脸。然后通过运行针对特定用户的人脸识别算法，来确定图中的人脸是否是该用户的好友。Facebook 通过该服务为用户推荐想要在照片中标记的好友。

- 语言翻译

语言翻译是涉及 Facebook 内容的国际化交流的服务。Facebook 支持超过 45 种语言之间的源语言或目标语言翻译，这意味着 Facebook 支持 2000 多个翻译方向，比如英语到西班牙语，阿拉伯语到英语。通过这 2000 多个翻译通道，Facebook 每天提供 4.5B 字的翻译服务，通过翻译用户的消息推送，Facebook 每天可为全球 6 亿人减轻语言障碍。

- 语音识别

语音识别是将音频流转换成文本的服务。它可以为视频自动填补字幕。目前，大部分流媒体都是英文的，但在未来其他语言的识别也将得到支持。另外，非语言的音频文件也可以用类似的系统（更简单的模型）来检测。

除了上面提到的主要产品之外，还有更多的长尾服务也利用了各种形式的机器学习。Facebook 产品和服务的长尾数量达数百个[86]。

- 谷歌

谷歌在过去五年先后收购了 13 家公司，以加强视觉处理、图像处理、谷歌语言、搜索引擎排名、语音识别和搜索预测等功能。此外，它还为其谷歌云服务客户提供 Cloud AI 服务，让客户可以将机器学习添加到其应用程序中。

2018 年 1 月 18 日，Google Cloud AI 首席科学家李飞飞连发三条 Twitter，通过一篇博客文章发布了谷歌最新 AI 产品—AutoML，该产品可以自动设计机器学习模型，通过 Google 最先进的传输学习和神经架构搜索技术，帮助机器学习专业知识薄弱的企业或个人用户构建自己的高质量自定义模型；另一方面，Cloud AutoML 能使 AI 专家们更加高效，帮助其构建更强大 AI 系统的同时，帮助其拓展新的领域。

当前，Google 发布了第一个产品 AutoML Vision，并已将它作为云服务开放出来，提供了一种简单，安全和灵活的 ML 服务，可让用户为自己的数据训练自定义视觉模型。同时，谷歌也表示稍后会支持其他标准机器学习模型，包括语音、翻译、视频、自然语言处理等。

作为谷歌产品，AutoMLVision 具有以下三个特点：

- 更精准：Cloud AutoML Vision 基于谷歌领先的图像识别方法，包括传输学习和神经架构搜索技术。这意味着即使企业不具备足够的机器学习专业知识，也可以获得更准确的模型。
- 更快：使用 Cloud AutoML 可以在几分钟内创建一个简单的模型，用以调试你想用 AI 支持的应用程序，可以在一天内构建能用于生产的完整模型。
- 操作简单：AutoML Vision 提供了一个简单的图形用户界面，可让你指定数据，然后将数据转换为一个针对特定需求的高质量模型。

产品使用

Cloud AutoML Vision 可以更快、更轻松地创建用于图像识别的自定义机器学习模型。凭借其拖放式界面可轻松上传图像，训练和管理模型，然后直接在 GoogleCloud 上部署这些训练的模型。使用者只需要将图片上传并点击训练，便能选择想要建立的定制化模型或是谷歌提供的模型。如果希望定制化模型，谷歌建议理想的情况是，每个标签至少要有 100 张训练图片。如果选择通过 Vision API 使用谷歌提供的模型，则只能标识一些常见的物件，像是脸部、标志、地标等。

谷歌 Cloud AutoML Vision 系统基于监督式学习，所以需要提供一系列带有标签的数据。具体来说，开发者只需要上传一组图片，然后导入标签或者通过 App 创建，随后谷歌的系统就会自动生成一个定制化的机器学习模型。整个过程，从导入数据到打标签到训练模型，所有的操作都是通过拖拽完成。在这个模型生成以及训练的过程中，除了训练样本时需要人工打标签外，其他的步骤就不需要人为的干预。据说，模型会在一天之内训练完成[87]。

- IBM Watson

Watson 问世已有几年，但机器学习方面去年刚推出。它让数据科学家可以转换数据，并运用机器学习算法来训练预测模型，构建利用机器学习模型所作的预测的智能应用程序。开发人员还可以运用算法从数据集中学习，生成可基于数据集进行预测的模型。它还为客户提供数据模型构建功能，客户可以从 IBM 提供的算法中进行选择，或者让 IBM 决定哪种算法最适合自己。

Watson Machine Learning 经过集成，能够与 Watson Studio 协同工作，支持您的跨职能团队快速轻松地部署、监控和优化模型。自动生成 API，帮助开发人员在几分钟内将 AI 注入其应用程序。Watson Machine Learning 的直观仪表板让您的团队能够轻松管理生产中的模型，并且其无缝工作流程支持持续的再训练，从而保持并提高模型准确性。

优势：

支持轻松且经济高效地在公共云、私有云、混合云或多云环境中部署 AI 和机器学习资产。无缝扩展您的 AI 计划，无需大量前期投资，即可将试点项目扩展为业务关键型企业部署。通过简化模型训练和部署流程，让 AI 资产更快进入市场。Watson Machine Learning 自动执行模型训练的多个环节，同时，多平台硬件优化通过最大限度利用资源来加速训练计划。利用一系列预先训练的模型和开放式数据集来减少技能短缺。利用自动化的性能监控和连续反馈，简化生命周期管理，并通过开放式模块化架构轻松地与其他数据科学工具进行互操作。

特点：

借助 Apache Spark，使用结构化和非结构化数据（无论是在关系数据库、Hadoop 还是对象存储中）对机器学习和深度学习模型进行训练，使模型训练分散化。端到端管理和治理 AI 和机器学习生命周期，构建可部署在云端或内部的便携式模型。从其他数据科学工具导入模型，并将模型作为服务、应用或脚本，为各种平台和工具持续训练和部署。

自动执行超参数优化和功能部件工程，实现快速训练。利用 A/B 测试和性能监控，为再训练创建反馈循环，以保持尽可能高的准确性[88]。

- QBurst

堪称机器学习公司和人工智能公司中的先驱。应用机器学习以业务所需的速度做出数据驱动的决策。人类大脑无法轻易分析的多维问题可以通过广泛的机器学习技术来解决。通过识别数据中的潜在结构，揭示新的见解，并从数据中做出准确的预测，机器学习算法可以将大数据集中包含的信息上下文化。利用机器学习，您可以优化以信息为中心的业务流程，根据客户需求定制解决方案，提高生产力，预测需求，以及其他许多可能性。

- 能源需求预测

机器学习预测系统可以利用过去的能源消耗数据和天气参数来预测未来的能源需求。将经过时间考验的 SARIMA 模型与新的机器学习技术相结合的混合预测模型也在不断发展。电力公司现在可以控制发电和优化调度，从而降低成本和能源浪费。

- 欺诈识别

建立在合法和欺诈交易已知案例上的模型可以为新交易分配怀疑分数，从而帮助识别信用卡欺诈。大量的算法包括决策树、神经网络、回归、k-均值聚类、支持向量机等。利用决策树和贝叶斯网络对保险索赔中的欺诈行为进行预测和标记。

- 预见性维护

在地理上分散的位置对机器进行持续的监控对于机器的顺利运行至关重要。检测算法可以根据历史数据分析实时机器参数，从而识别设备的恶化状态。因此，运营商可以启动预测性维护，防止对资产造成不可逆转的损害。

- 病历注释

虽然电子健康记录是患者数据的丰富来源，但由于其高度非结构化，不适合进行分析。在 NLP 中使用机器学习，可以对症状、疾病和治疗等实体进行分析和标记，使它们在临床决策时很容易检索。

- 卫生信息学

医学研究创造的知识超出了从业者所能应付的范围。将 NLP 与语义知识处理和机器学习相结合的智能系统可以帮助从业者更快地查找特定问题的研究文献。

- 医学图像分析

监督机器学习技术应用于医学图像分析，以计算机辅助诊断某些脑部疾病。基于大量标记图像（如 CT 和 MRI 扫描）训练的模型可以自动检测疾病指标并帮助医生做出预后判断。

- 智能广告牌

通过使用实时图像识别应用程序，零售商可以根据客户的性别、年龄和种族对客户进行分类。他们可以利用这种智能，在数字广告牌上展示有针对性的广告，以提高品牌知名度。

- 推荐产品

基于内容和协同过滤的算法可用于生成特定于用户的推荐。这些推荐可能包括一组基于用户选择的具有共同特性的相似项目，以及相似用户喜欢的项目。

- 情感分析

从选民到消费者，衡量人们的情绪对于政治和零售等各个领域的竞选活动至关重要。运用自然语言处理，情感可以被挖掘，以帮助建立更有响应性的活动和修改品牌定位[89]。

- 高通

骁龙平台凭借终端侧人工智能，创造了机器学习驱动端到端的解决方案，更点燃了语音交互的革命。支持多种语言的深度学习，提升性能表现，达到更个性化的互动从而打造出真正的虚拟助理。高通向骁龙 820 处理器支持的终端提供首个深度学习软件开发包（SDK）。名为“Qualcomm 骁龙神经处理引擎”的这款 SDK 由 Qualcomm® Zeroth™机器智能平台支持，并且经过优化，可利用骁龙异构计算功能向 OEM 厂商提供强大节能的平台，从而在终端上提供直观且颇具吸引力的、由深度学习驱动的体验。该 SDK 是骁龙 820 的最新软件增加项，将通过为我们的客户提升骁龙产品组合的价值，展现 Qualcomm Technologies 的持续领导力。

随着骁龙神经处理引擎的发布，Qualcomm Technologies 将成为首个提供专为移动领域优化的深度学习工具包的移动系统处理器（SOC）供应商。该 SDK 将使 OEM 厂商能在诸如智能手机、安全摄像头、汽车以及无人机等搭载骁龙 820 的终端上，运行它们自己的神经网络模型，且完全无须与云端相连。该 SDK 可实现的普通深度学习用户体验包括场景侦测、文本识别、物体跟踪与避障、手势、人脸识别和自然语言处理[90]。

- Skytree

如果你打算自称是“机器学习公司”，最好有点干货。Skytree 提供企业级机器学习平台，可帮助客户发现深层分析洞察力、预测未来趋势、提出建议，并揭示未开发的市场和客户。Skytree 机器学习平台旨在持续搜索最精确的模型，从而不断提升模型的性能。

Skytree 是一家大数据分析公司，让组织和公司客户执行机器学习和其他针对大量数据的高级分析。Skytree 独特的服务器为客户提供了高级绩效、灵活性和准确性。Skytree 服务器部署简单，可以针对高级分析提供实时的回复。Skytree 公司的总部位于美国硅谷。其团队可以为客户提供世界上需求最大和数据密集型环境相关的建议与指导，如美国国家航空航天局官方网站，Sloan Digital Sky Survey 等。Skytree 雄心勃勃，希望主流公司能够利用其出色的机器学习技术。

Skytree 的 PowerPacks 是一系列的模块，主要用来接入 Skytree 的服务器基层。这款工具将为 Skytree 服务器基层添加大量的功能，提高绩效。除了创新的传统机器学习优化方式之外，Skytree 还会为用户提供极度准确的模块管理。Skytree 公司的专家与客户合作，确保客户可以有效地解决机器学习的挑战。Skytree 的咨询服务为客户提供了任何与大数据机器学习部署所需的支持。Skytree 的专家会对你的统计方法学进行评估，定制化机器学习模式和计算方法。Skytree 还会为你提供概念项目的证据，进行大数据管道设计，通过最终的微调来进行最初的展示，依据分析需求指数进行可伸缩性计划，执行基础设施和集成，部署和运作分析引擎等[91]。

- 优步

对于外界来说，优步是一家拼车公司。其背后是 Michelangelo，这个机器学习即服务平台让内部团队能够在优步的大规模环境下无缝构建、部署和运行机器学习解决方案。它涵盖了端到端的机器学习工作流程，比如管理数据，训练、评估和部署模型，进行预测，监管预测（比如叫的车多久后到达）。优步计划最终向公众提供这种机器学习即服务。

Uber 工程师们一直致力于开发各种新技术，以让客户得到有效、无缝的用户体验。现在，他们正在加大对人工智能、机器学习领域的投入来实现这个愿景。在 Uber，工程师们开发出了一个名为“米开朗基罗”（Michelangelo）的机器学习平台，它是一个内部的“MLaaS”（机器学习即服务）平台，用以降低机器学习开发的门槛，并能根据不同的商业需求对 AI 进行拓展与缩放，就有如客户使用 Uber 打车一样方便。

米开朗基罗平台可以让公司内部团队无缝构建、部署与运行 Uber 规模的机器学习解决方案。它旨在覆盖全部的端到端机器学习工作流，包括：数据管理、训练模型、评估模型、部署模型、进行预测、预测监控。此系统不仅支持传统的机器学习模型，还支持时间序列预测以及深度学习。

米开朗基罗已经成为了 Uber 工程师、数据科学家真正意义上的“平台”，现在有数十个团队在此平台上构建、部署模型。实际上，米开朗基罗平台现在部署于多个 Uber 数据中心并使用专用硬件，用于为公司内最高负载的在线服务提供预测功能[92]。

Uber 的机器学习用例：

- Uber Eats

Uber Eats 使用基于 Michelangelo 的多个模型来做预测，以便食客每次打开 APP 都可以有更好的体验。基于机器学习的排名模型会根据历史数据和用户当前的进程信息，来推荐合适的餐馆和菜品。基于 Michelangelo，优食也会根据预测到达时间、历史数据以及餐馆的实时信息，来估算餐食的送达时间。

- 市场预测

Uber 的市场团队利用了各种时空预测模型，这些模型能够预测未来各个地点和时间乘坐者的需求，以及司机是否有空。根据所预测的供需不平衡情况，Uber 系统可以提醒司机提前去往最有机会接客的地点。

- 客户支持

在 Uber 平台，每天约有 1500 万次出行记录。人们经常把钱包或手机遗忘在车内，或通过 Uber 的帮助系统提交各种问题。这些问题单将被提交至客服代表。基于 Michelangelo 的机器学习模型被应用于此，使问题的解决过程更加自动化，并大大提升了速度。

- 乘车检查

自 2010 年的第一条 Uber 乘坐记录以来，每次出行时地图都会使用 GPS 数据。所以我们知道自己何时处于何地，以及是谁在驾驶。但 Uber 希望可以做得更多。利用 GPS 的力量和司机的智能手机中的其他传感器，Uber 的技术可以检测到可能发生的车祸。例如，如果在一次旅程中出现长时间的意外停车，乘客和司机都会收到一条提醒，可提供交通事件援助。

- 预计到达时间（ETAs）

对公司来说，最重要的指标之一就是各种预估时间。精确的预估时间对好的用户体验至关重要，这些指标被输入无数其他的内部系统中，来协助判定价格和路线。

Uber 的地图服务团队开发了一个复杂的分段路线系统，用来计算基本的预估时间值。这些基本的预估时间具有相同类型的错误。地图服务团队发现他们可以使用机器学习模型来预测这些错误，并用预测的错误来进行修正。由于这个模型正逐个应用在各个城市，Uber 团队发现预估到达时间的准确性大幅提升，在某些情况下，平均预估到达时间的误差减小了 50% 以上。

- 一键聊天

一键聊天的功能基于自然语言处理模型，模型可以预测并展示最有可能的回复，使乘客与司机之间的交流更加高效。司机只需按一下按钮，即可回复乘客的消息，从而避免分心。

- 自动驾驶车辆

Uber 的自动驾驶汽车系统使用深度学习模型来实现各种功能，包括物体检测和路线规划。建模人员用 Michelangelo 的 Horovod 在大量 GPU 机器上进行高效的分布式训练[93]。

6.4 北京智谱华章科技有限公司介绍

北京智谱华章科技有限公司由清华大学科研团队、清华控股、中科创星联合创立。公司源自清华大学 10 余年知识图谱和人工智能研究的积累，致力于打造可解释性、鲁棒性、安全可靠、具有推理能力的新一代认知引擎，用 AI 赋能政府与企业。公司主力产品及服务包括科技信息咨询、人才评价/培养、专家推荐、技术趋势分析、技术及产业分析报告等专业知识服务。公司拥有自主知识产权的科技情报大数据挖掘与服务平台——AMiner。

科技情报大数据挖掘与服务平台 AMiner 由清华大学知识工程实验室团队研发，在国家 863、973 及自然科学基金等多个项目支持下，以学者、论文文献、专利、期刊/会议、科技新闻、学术活动等数据为基础，构建数据之间的关联关系，深入分析挖掘，提供如技术发展

趋势分析、前沿技术预见、学术评价、专家搜索/推荐、学者地图、学者关系网络分析等专业知识服务。

AMiner 平台 2006 年上线，经过十多年的建设发展，已建立运作良好的数据采集及集成更新机制，收录论文文献超 3 亿，专利 1 亿，学者 1.3 亿，其中超过 50 万专家经过了人工标注与审核，建立了如各国院士、大奖获得者、领域知名学者、知名高校教师、优秀青年人才等特色专家子库超过 800 个。同时平台在学者命名排歧、隐含关联关系挖掘、科技知识图谱构建等核心关键技术方面进行深入研究，发表相关论文 200 余篇、申请专利 40 余项，获得 2013 年中国人工智能学会科技进步一等奖和 2017 年北京市科学技术奖（进步）一等奖等荣誉。

AMiner 系统平台免费为全球科研人员提供科技信息资源检索及分析挖掘服务，吸引了全球 220 个国家/地区 1000 多万独立 IP 的访问，年度访问量 1800 万次，为科技部组织的第六次国家信息领域技术预测提供文献数据分析报告，为先进计算、人工智能、网络与通信、网络安全、光电子与微电子等 5 大技术领域提供论文趋势、各国技术力量对比、领先机构对比、各国合作关系对比、领域热点技术分析等专业分析；为科技部人才中心提供科技人才评价及评审专家推荐；同时为中国工程院、国家自然基金委、中国科协、北京市科委、以及搜狗、华为、腾讯等 20 余家企事业单位提供技术支持及特色知识服务。

AMiner 系统平台（https://www.aminer.cn/）典型的知识服务包括：

1、学者档案管理及分析挖掘

学者档案管理及分析挖掘是 AMiner 平台的核心功能服务之一。其特色在于除了提供专家学者如姓名、单位、地址、联系方式、个人简介、教育经历等个人基本信息之外，还利用团队多年的命名排岐相关技术基础，建立了较为完全的学者-论文映射关系，提供学者学术评价、研究兴趣发展趋势分析、学者合作者关系网络等分析挖掘信息，同时支持用户交互，通过众包方式丰富专家学者的相关信息。

学者档案信息对公众开放，注册用户可免费查询专家档案信息，年度用户访问量超过 1100 万。

2、专家学者搜索及推荐

AMiner 平台中专家学者搜索界面如图 2 所示，搜索支持 H-index、地域、语种、性别等多种过滤条件，搜索结果可以按相关性、H-index、活跃度等多种方式排序，同时还支持利用知识图谱进行扩展搜索、搜索关键词自动提示、相似专家推荐等多种搜索方式，以满足不同的用户需求。

AMiner 平台搜索功能免费对公众开放，同时基于系统平台的学者库资源，提供面向机构的专家学者推荐服务，可以根据实际应用需求推荐合适的专家学者。如为科技部及国家自然基金委推荐项目评审专家，为中国工程院院刊《Engineering》、清华大学出版社《视觉多媒体》等 10 多家期刊推荐读者等。

3、技术发展趋势分析

技术发展趋势分析是当前的一个研究热点。项目团队基于 AMiner 多年积累的数据资源及技术基础，能自动分析挖掘不同技术领域的发展趋势，标出分支技术及技术发展历程中的重要人物及事件（代表论文）。同时支持发现领域技术热点及进行技术前沿分析等知识服务。下图展示了 AMiner 对人工智能技术的技术发展趋势分析。技术发展趋势分析在华为、科技部、中国工程院等单位都已有应用，对于企业或科研管理部门明确科研方向、制定科研计划具有重要意义。

4、全球学者分布地图

全球学者分布地图直观的展示特定技术领域专家学者在全球的分布情况，可以快速定位技术研究热点地区及区域内的权威专家，展示特定区域的专家统计分析情况，方便进行不同区域不同专家之间的对比分析。下图展示了“机器学习”领域全球学者的分布情况。全球学者分布地图对于企业或科研管理部门寻找合作区域专家、实现全球布局具有重要意义。

5、全球学者迁徙图

全球学者迁徙图直观的展示特定技术领域专家学者在全球随时间的分布变化情况，可以快速定位不同历史时期的技术研究热点地区及代表性专家。同时也支持对特定专家的迁徙情况进行专门分析展示，以及某特定时期内全球热点区域的统计分析等。下图展示了 2016 年“机器学习”领域全球最有影响力学者在 2007 年的迁徙图。全球学者迁徙图对于企业或科研管理部门用全球战略眼光发现技术前沿、制定人才战略、实现全球布局具有重要意义。

6、开放平台

AMiner 自研发之处，一直强调开放共享。提供平台学者及论文等数据的访问 API 接口，可以直接调用查询平台相关学术数据。同时提供学术资源下载，开放共享学术数据超过 2 亿条，累计数据下载超过 230 万次。近期联合微软学术发布了开放学术图谱，提供超过 3 亿的论文文献原数据下载。

平台主要技术创新点如下：

1）跨媒体科技知识图谱构建技术。针对科技信息资源分布广、多模态、碎片化的特点，提出多维依赖的概率图标注模型，将信息语义化的识别错误率降低 40-56%；提出基于最小

风险的多源语义集成方法，支持结构感知的集成策略动态选择，将学者画像的精度提高到90%，建立了亿级节点规模的跨语言科技知识图谱。

2）科技情报网络的隐含关联挖掘方法。针对科技情报网络语义关联挖掘难题，提出基于话题的多维影响力分析模型，攻克了大网络关键节点挖掘的高计算复杂度问题，挖掘精度比传统方法提高 50%，实现了科技情报网络的对象评价和趋势分析。

3）基于立体画像的多维科技情报快速匹配技术。针对大规模网络匹配效率低的问题，提出跨媒体情报查询意图理解方法，将意图理解的正确率提高到 97.9%，实现了基于随机采样的情报快速匹配算法，将网络相似度匹配的复杂度由原来的 O(N2)降为 O(N)，在 10 亿条边规模的情报网络上比最优的对比方法快 300 倍。

4）知识驱动的智能型科技情报挖掘平台 AMiner。研发了具有自主知识产权的以知识和科研人员为核心的新一代智能型科技情报挖掘和服务平台 AMiner，建成了超过 2.3 亿学术论文/专利和 1.36 亿学者的科技图谱，提供学者评价、专家发现、智能指派、学术地图等科技情报专业化服务。

7 趋势篇

领域技术分析系统（http://trend.aminer.cn）可以基于 AMiner 超过 2 亿篇论文的数据进行深入挖掘，对技术趋势、国际趋势、机构趋势及学者趋势等方面进行分析。机器学习是一门多领域交叉学科，设计概率论、统计学、逼近论、凸分析、算法复杂度理论等多门学科。在下面的各种趋势分析中，研究基础是期刊/会议 *Journal of Machine Learning Research*、*Machine Learning*、*International Conference on Machine Learning*、*Conference and Workshop on Neural Information Processing Systems* 近 20 年的论文。

- 技术趋势

技术趋势分析如下图所示。技术趋势分析描述了技术的出现、变迁和消亡的全过程，可以帮助研究人员理解领域的研究历史和现状，快速识别研究的前沿热点问题。图中每条色带表示一个话题，其宽度表示该术语在当年的热度，与当年该话题的论文数量呈正相关，每一年份中按照其热度由高到低进行进行排序。通过技术趋势分析可以发现当前该领域的热点研究话题 Top10 是：Neural Network、Machine Learning、Deep Neural Networks、Deep Learning、Support Vector Machine、Reinforcement Learning、Feature Selection、Deci Tree、Data Mining、Artificial Neural Network。

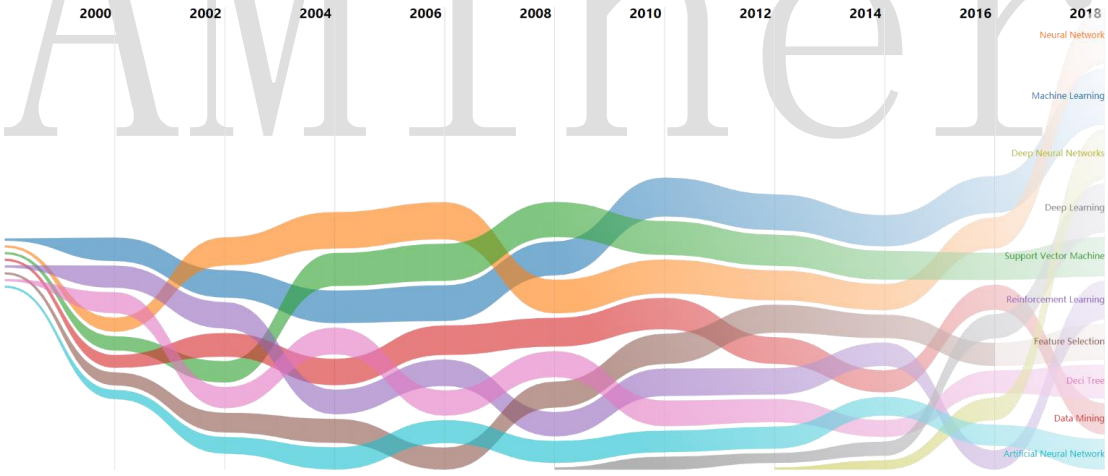


图 7-1 机器学习技术趋势

根据技术趋势分析我们可以发现，该领域当前最热门的话题是 Neural Network，从全局热度来看，Neural Network 一直保持着较高的话题热度，2002-2006 年期间保持着最高的热度并于 2018 年重登榜首。

该系统还会在趋势图右侧列出本领域的推荐论文，引用量前五的论文如下：

1. 论文标题：*Scikit-learn: Machine Learning in Python*

论文作者：Fabian Pedregosa, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg

引用量：13600

2. 论文标题：*Natural Language Processing (Almost) from Scratch*

   论文作者：Ronan Collobert, Jason Weston, Léon Bottou, Michael Karlen, Koray Kavukcuoglu, Pavel Kuksa

   引用量：4094

3. 论文标题：*Ensemble methods in machine learning*

   论文作者：T. G Dietrich

   引用量：4624

4. 论文标题：*Manifold Regularization: A Geometric Framework for Learning from Labeled and Unlabeled Examples*

   论文作者：Mikhail Belkin, Partha Niyogi, Vikas Sindhwani

   引用量：2857

5. 论文标题：*Support Vector Machine Active Learning with Application sto Text Classification*

   论文作者：Thomas G. Dietterich

   引用量：2428

- 国家趋势

国家趋势分析如下图所示。图中每条色带表示一个国家，其宽度表示该国家在当年的研究热度，与当年该国论文数量呈正相关，每一年份中按照其热度由高到低进行进行排序。通过国家趋势分析可以发现当前机器学习领域研究热度 Top10 的国家分别是：United States、China、United Kingdom、Canada、France、Germany、India、Japan、Australia、Italy。

根据国家趋势分析我们可以发现，该领域当前研究热度最高的国家是美国，从全局热度来看，美国早期就有着领先优势并一直保持着较高的热度，在 2012 年前后重新登顶榜首并延续至今。同时可以看出，中国在机器学习领域的研究热度与美国不相上下，在 2002-2010 年期间中国超过美国位居第一，随后虽被美国超越也仍然保持着第二的位置。可以说机器学习领域长期都是中美争霸的状态。

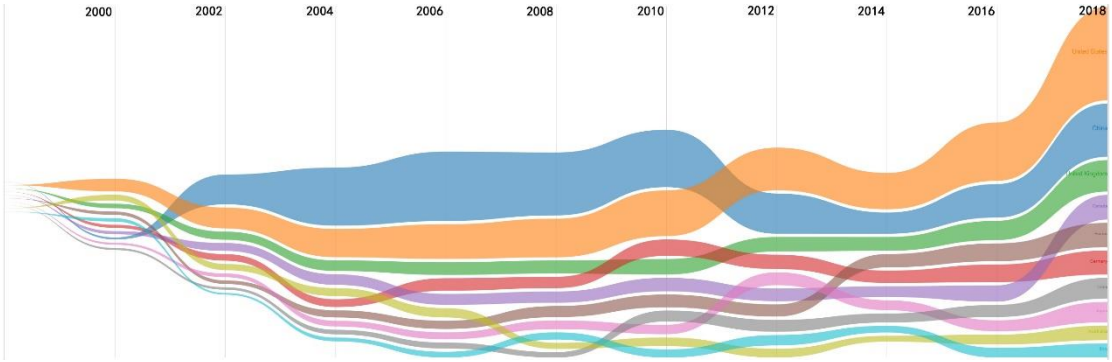
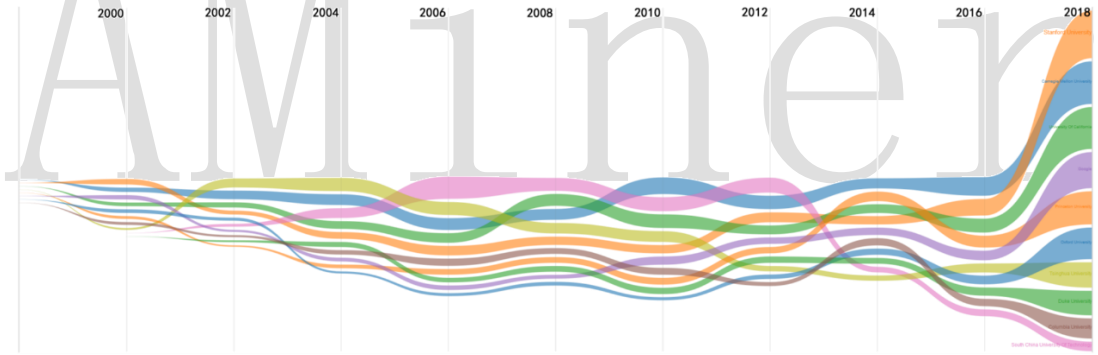


图 7-2 机器学习国家趋势

- 机构趋势

机构趋势分析如下图所示。图中每条色带表示一个机构，其宽度表示该机构在当年的研究热度，与当年该机构论文数量呈正相关，每一年份中按照其热度由高到低进行进行排序。通过机构趋势分析可以发现当前机器学习领域研究热度 Top10 的机构分别是：Stanford University、Carnegie Mellon University、University of California、Google、Princeton University、Oxford University、Tsinghua University、Duke University、Columbia University、South China University of Technology。

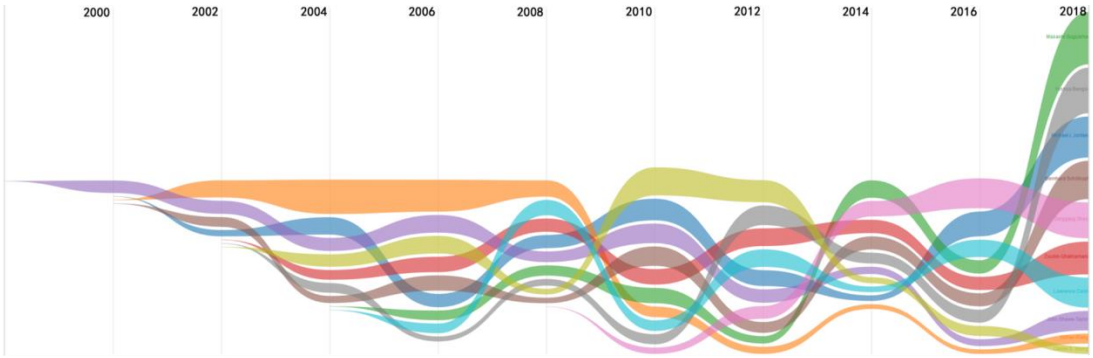


根据机构趋势分析我们可以发现，该领域当前研究热度最高的是斯坦福大学，斯坦福大学早期在很长一段时间内并没有特别的优势，而是在 2018 年强势崛起并登顶榜首。从全局角度来看，卡耐基梅隆大学在各时期内都保持了较高的热度排名，基本都在三甲范围，体现出卡耐基梅隆大学的强大实力。同时可以看出，中国在机器学习领域也有部分上榜机构，如清华大学等。

- 学者趋势

学者趋势分析如下图所示。图中每条色带表示一个学者，其宽度表示该学者在当年的研究热度，与当年该学者论文数量呈正相关，每一年份中按照其热度由高到低进行进行排序。通过学者趋势分析可以发现当前机器学习领域研究热度 Top10 的学者分别是：Masashi

Sugiyama、Yoshua Bengio、Michael I. Jordan、Bernhard Schölkopf、Dinggang Shen、Zoubin Ghahramani、Lawrence Carin、John Shawe-Taylor、Xizhao Wang、Daniel S. Yeung。



8 资源篇

本篇中我们搜集整理了机器学习领域的若干资源，希望能对读者朋友更好地了解机器学习有所帮助，同时也欢迎大家补充。

8.1 开源代码

1）深度学习框架 Pytorch

https://github.com/pytorch/pytorch

2）深度学习框架 Tensorflow

https://github.com/tensorflow/tensorflow

3）机器学习库 scikit-learn

https://github.com/scikit-learn/scikit-learn

4）自然语言处理时下最流行的 Transformer 库

https://github.com/huggingface/transformers

5）自然语言处理工业级别库 spaCy

https://github.com/explosion/spaCy

6）自然语言处理 Toolkit NLTK

https://github.com/nltk/nltk

7）自然语言处理经典模型库 Gensim

https://github.com/RaRe-Technologies/gensim

8）图计算库 NetworkX

https://github.com/networkx/networkx

9）XGBoost

https://github.com/dmlc/xgboost

10）深度学习 FastAI

https://github.com/fastai/fastai

8.2 预训练

1）Glove

https://nlp.stanford.edu/projects/glove/

2）FastText

https://fasttext.cc/

3）MUSE

https://github.com/facebookresearch/MUSE

4）ELMo

https://allennlp.org/elmo

5）BERT

https://github.com/google-research/bert

6）XLNet

https://github.com/zihangdai/xlnet

7）XLM

https://github.com/facebookresearch/XLM

8）OpenAI-GPT2

https://github.com/openai/gpt-2-output-dataset

9）ResNet, VGG

https://keras.io/applications/

10）YOLOv2

https://github.com/experiencor/keras-yolo2

8.3 课程

1）stanford cs231n ML

http://cs231n.stanford.edu/

2）FastAI ML

https://www.fast.ai/2018/09/26/ml-launch/

3）OpenAI RL

https://gym.openai.com/

4）stanford cs234 RL

https://web.stanford.edu/class/cs234/index.html

5）CMU 10701 ML

https://www.cs.cmu.edu/~lwehbe/10701_S19/

6）CMU 11747 NN4NLP

http://www.phontron.com/class/nn4nlp2019/description.html

7）Coursera ML

https://www.coursera.org/learn/machine-learning

8）edX

https://www.edx.org/course/machine-learning

9）udacity

https://www.udacity.com/course/intro-to-machine-learning-nanodegree--nd229

10）deeplearning.ai

https://www.coursera.org/specializations/deep-learning

8.4 数据集

1）[CV] ImageNet

http://www.image-net.org/

2）[CV] CoCo

http://cocodataset.org/

3）[CV] PASCAL VOC

http://host.robots.ox.ac.uk/pascal/VOC/index.html

4）MNIST

http://yann.lecun.com/exdb/mnist/

5）[NLP] GLUE

https://gluebenchmark.com/

6）[NLP] XNLI

https://github.com/facebookresearch/XNLI

7）[Recommendation] MovieLens

https://grouplens.org/datasets/movielens/

8）[NLP] WikiText

https://blog.einstein.ai/the-wikitext-long-term-dependency-language-modeling-dataset/

9）[NLP] SQuAD

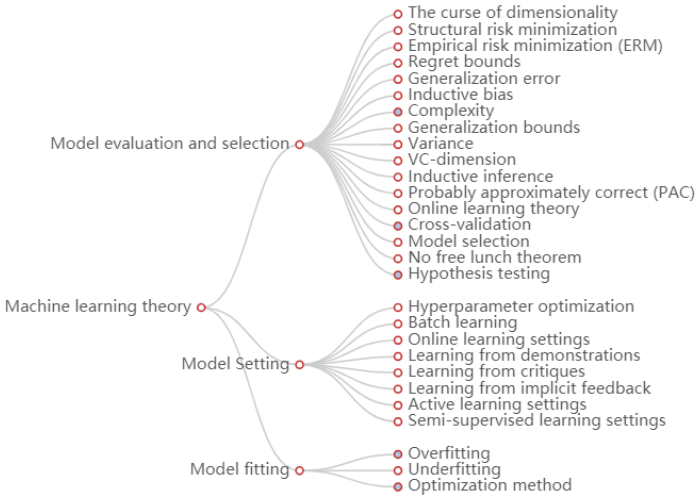
https://rajpurkar.github.io/SQuAD-explorer/

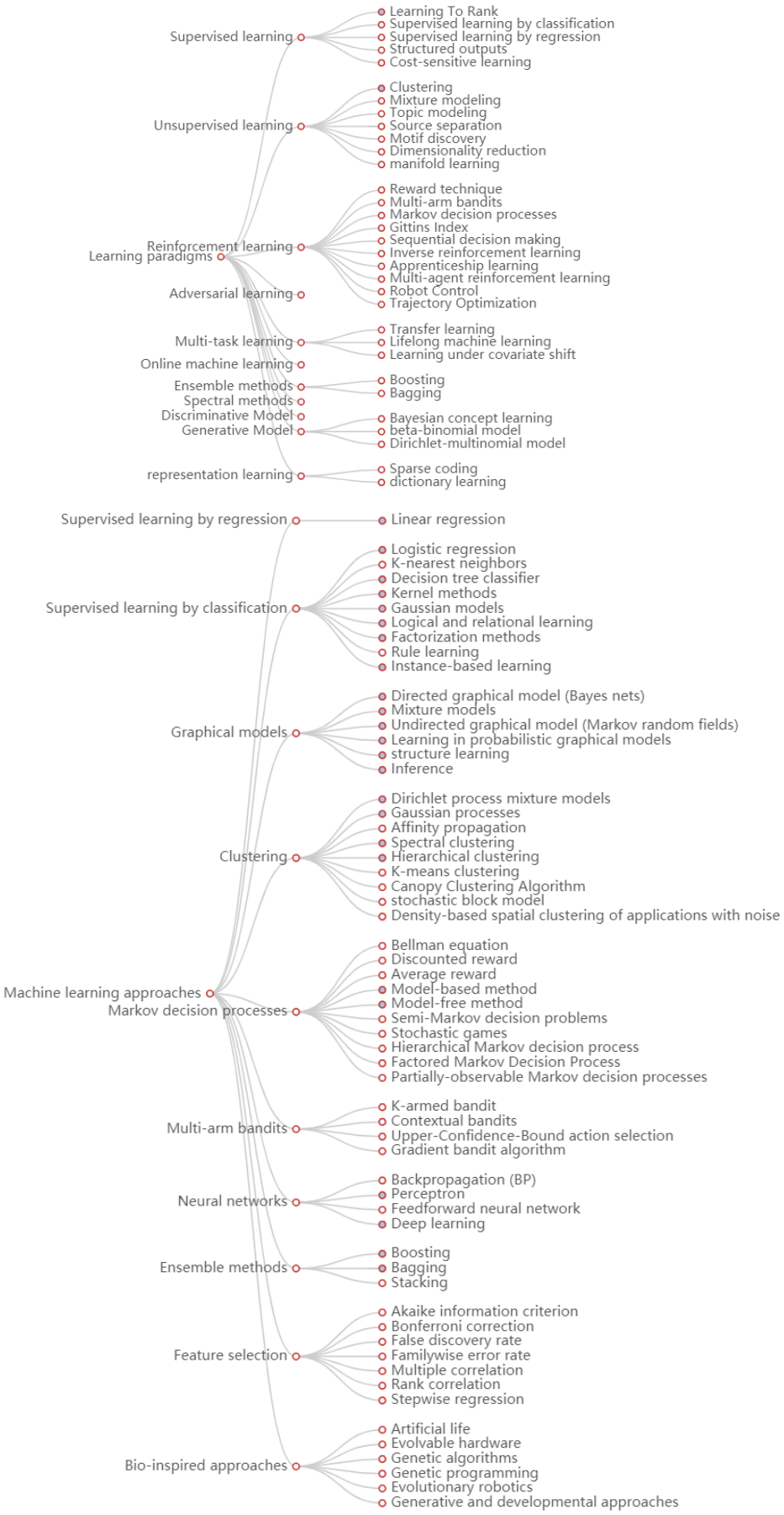
10）[CV] CIFAR

https://www.cs.toronto.edu/~kriz/cifar.html

8.5 机器学习知识树

本报告分析了近年来机器学习领域的高水平学术论文，挖掘出了相关关键词，结合知识图谱技术整理了机器学习八级知识树，详细数据可联系 https://www.aminer.cn/data 下载原始数据，鉴于自动分析技术和论文采集的局限性，图谱还可以进一步完善，欢迎读者批评指正，我们会根据根据读者的反馈定期更新。Machine learning 的二级分类包括 Machine learning theory、Learning paradigms 以及 Machine learning approaches，它们的知识树展示如下：




Learning paradigms
Supervised learning
Learning To Rank
Supervised learning by classification
Supervised learning by regression
Structured outputs
Cost-sensitive learning
Unsupervised learning
Clustering
Mixture modeling
Topic modeling
Source separation
Motif discovery
Dimensionality reduction
manifold learning
Reinforcement learning
Reward technique
Multi-arm bandits
Markov decision processes
Gittins Index
Sequential decision making
Inverse reinforcement learning
Apprenticeship learning
Multi-agent reinforcement learning
Robot Control
Trajectory Optimization
Adversarial learning
Multi-task learning
Transfer learning
Lifelong machine learning
Learning under covariate shift
Online machine learning
Ensemble methods
Boosting
Bagging
Spectral methods
Discriminative Model
Generative Model
Bayesian concept learning
beta-binomial model
Dirichlet-multinomial model
representation learning
Sparse coding
dictionary learning
Machine learning approaches
Supervised learning by regression
Linear regression
Supervised learning by classification
Logistic regression
K-nearest neighbors
Decision tree classifier
Kernel methods
Gaussian models
Logical and relational learning
Factorization methods
Rule learning
Instance-based learning
Graphical models
Directed graphical model (Bayes nets)
Mixture models
Undirected graphical model (Markov random fields)
Learning in probabilistic graphical models
structure learning
Inference
Clustering
Dirichlet process mixture models
Gaussian processes
Affinity propagation
Spectral clustering
Hierarchical clustering
K-means clustering
Canopy Clustering Algorithm
stochastic block model
Density-based spatial clustering of applications with noise
Markov decision processes
Bellman equation
Discounted reward
Average reward
Model-based method
Model-free method
Semi-Markov decision problems
Stochastic games
Hierarchical Markov decision process
Factored Markov Decision Process
Partially-observable Markov decision processes
Multi-arm bandits
K-armed bandit
Contextual bandits
Upper-Confidence-Bound action selection
Gradient bandit algorithm
Neural networks
Backpropagation (BP)
Perceptron
Feedforward neural network
Deep learning
Ensemble methods
Boosting
Bagging
Stacking
Feature selection
Akaike information criterion
Bonferroni correction
False discovery rate
Familywise error rate
Multiple correlation
Rank correlation
Stepwise regression
Bio-inspired approaches
Artificial life
Evolvable hardware
Genetic algorithms
Genetic programming
Evolutionary robotics
Generative and developmental approaches

参考文献

[1] Samuel, A. L. (1959). Some studies in machine learning using the game of checkers. *IBM Journal of research and development*, 3(3): 210-229.

[2] Top 10 Machine Learning Projects; https://www.pantechsolutions.net/blog/machine-learning-projects-and-ideas/.

[3] Deep Dive Into Machine Learning; https://mc.ai/deep-dive-into-machine-learning/.

[4] Cooley, J. W., & Tukey, J. W. (1965). An algorithm for the machine calculation of complex Fourier series. *Mathematics of computation*, 19(90): 297-301.

[5] Fukushima, K. (1980). Neocognitron: A self-organizing neural network model for a mechanism of pattern recognition unaffected by shift in position. *Biological Cybernetics*, 36, 193-202.

[6] Holmes, G., Donkin, A., & Witten, I. H. (1994). Weka: A machine learning workbench. *Intelligent Information Systems*, 357-361.

[7] Ho, T. K., Hull, J. J., & Srihari, S. N. (1994). Decision combination in multiple classifier systems. *IEEE transactions on pattern analysis and machine intelligence*, 16(1): 66-75.

[8] Ferrucci, D. A., Brown, E. W., Chucarroll, J., Fan, J., Gondek, D. C., Kalyanpur, A., ... & Welty, C. (2010). Building Watson: An overview of the DeepQA project. *AI magazine*, 31(3): 59-79.

[9] Le, Q. V. (2013). Building high-level features using large scale unsupervised learning. *Acoustics, Speech and Signal Processing (ICASSP)*, 8595-8598.

[10] Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Den Driessche, G. V., ... & Hassabis, D. (2016). Mastering the game of Go with deep neural networks and tree search. *Nature*, 529(7587): 484.

[11] Machine Learning Types. https://towardsdatascience.com/machine-learning-types-2-c1291d4f04b1.

[12] Sabharwal, A., & Selman, B. (2011). S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, Third Edition. *Artificial Intelligence*, 935-937.

[13] 监督式学习. https://zh.wikipedia.org/wiki/監督式學習.

[14] 机器学习三兄弟概念大揭秘. http://imgtec.eetrend.com/blog/2019/100043763.html.

[15] 无监督学习. https://zh.wikipedia.org/wiki/無監督學習.

[16] 史上最全机器学习经典算法详解. https://zhuanlan.zhihu.com/p/95135478.

[17] 强化学习. https://zh.wikipedia.org/wiki/强化学习.

[18] Sutton R S, Barto A G. (2011). Reinforcement learning: An introduction.

[19] 袁莎，白朔天，唐杰. 强化学习原理与实战. https://doc-14-00-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/5bdgohivkgo3jcecrs0mcv800bi52o61/

1575979200000/16548294868625771876/*/1j1z-DhW3-uoh_KfafwcPf8Ggx5fiUtO_?e=download.

[20] Goodfellow, I., Pougetabadie, J., Mirza, M., Xu, B., Wardefarley, D., Ozair, S., ... & Bengio, Y. (2014). Generative Adversarial Nets. *Advances in neural information processing systems*, *2672-2680*.

[21] 一文看懂 GAN 演进图谱. https://www.infoq.cn/article/GCGIboPIfTpBe9dEqF3m.

[22] Radford, A., Metz, L., & Chintala, S. (2015). Radford A, Metz L, Chintala S. Unsupervised Rrepresentation Llearning with Ddeep Cconvolutional Ggenerative Aadversarial Nnetworks. *arXiv preprint arXiv*,1511.06434, 2015.

[23] Karras, T., Laine, S., & Aila, T. (2018). A Style-Based Generator Architecture for Generative Adversarial Networks. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 4401-4410.

[24] Zhang, H., Xu, T., & Li, H. (2017). StackGAN: Text to Photo-Realistic Image Synthesis with Stacked Generative Adversarial Networks. *Proceedings of the IEEE International Conference on Computer Vision*, 5907-5915.

[25] Zhu, J., Park, T., Isola, P., & Efros, A. A. (2017). Unpaired Image-to-Image Translation Using Cycle-Consistent Adversarial Networks. *Proceedings of the IEEE international conference on computer vision*, 2223-2232.

[26] Isola, P., Zhu, J., Zhou, T., & Efros, A. A. (2017). Image-to-Image Translation with Conditional Adversarial Networks. *Proceedings of the IEEE conference on computer vision and pattern recognition*, 1125-1134.

[27] Antipov, G., Baccouche, M., & Dugelay, J. (2017). Face aging with conditional generative adversarial networks. *International Conference on Image Processing (ICIP)*, 2089-2093.

[28] AI 换脸技术-DeepFakes. http://baijiahao.baidu.com/s?id=1596785142340985604&wfr=spider&for=pc.

[29] 生成对抗网络(GAN)的发展史. https://zhuanlan.zhihu.com/p/63428113.

[30] 997 篇-历史最全生成对抗网络（GAN）论文串烧. https://zhuanlan.zhihu.com/p/38533823.

[31] 对抗机器学习. https://www.jiqizhixin.com/graph/technologies/a1490c68-7868-4b6a-a775-097d458c64c1.

[32] 深入浅出对抗性机器学习. https://zhuanlan.zhihu.com/p/52561355.

[33] Kearns, M., & Li, M. (1993). Learning in the presence of malicious errors. *SIAM Journal on Computing*, 22(4): 807-837.

[34] Biggio, B., Nelson, B., & Laskov, P. (2011). Support vector machines under adversarial label noise. *Asian Conference on Machine Learning*, 97-112.

[35] Kloft, M., & Laskov, P. (2010). Online anomaly detection under adversarial impact. *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics*, 405-412.

[36] Biggio, B., Corona, I., Maiorca, D., Nelson, B., Srndic, N., Laskov, P., ... & Roli, F. (2013). Evasion attacks against machine learning at test time. *Joint European conference on machine learning and knowledge discovery in databases*, 387-402.

[37] Liu, D. C., & Nocedal, J. (1989). On the limited memory BFGS method for large scale optimization. *Mathematical programming*, 45(1-3): 503-528.

[38] Papernot, N., Mcdaniel, P., Jha, S., Fredrikson, M., Celik, Z. B., & Swami, A. (2016). The limitations of deep learning in adversarial settings. *IEEE European Symposium on Security and Privacy (EuroS&P)*, 372-387.

[39] Ateniese, G., Mancini, L. V., Spognardi, A., Villani, A., Vitali, D., & Felici, G. (2015). Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers. *arXiv preprint arXiv*:1306.4447, 2013.

[40] 什么是自动机器学习，它有哪些用处. https://www.boxuegu.com/news/1359.html.

[41] 自动机器学习 AutoML 和神经架构搜索 NAS 简介. https://zhuanlan.zhihu.com/p/75747814.

[42] 自动机器学习简述. https://my.oschina.net/taogang/blog/3011686.

[43] Wang, Q., Ming, Y., Jin, Z., Shen, Q., Liu, D., Smith, M. J., ... & Qu, H. (2019). Atmseer: Increasing transparency and controllability in automated machine learning. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 681.

[44] Cracking open the black box of automated machine learning. https://techxplore.com/news/2019-06-black-automated-machine.html.

[45] 机器学习模型可解释性的详尽介绍. https://www.jiqizhixin.com/articles/2019-10-30-9.

[46] 人工智能之机器学习篇——在线学习. https://baijiahao.baidu.com/s?id=1594337146635999109&wfr=spider&for=pc.

[47] FTRL(Follow The Regularized Leader)学习总结. https://www.cnblogs.com/arachis/p/FTRL.html.

[48] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, 5998-6008.

[49] Taylor, W. L. (1953). Cloze procedure: A new tool for measuring readability. *Journalism Bulletin*, 30(4):415–433.

[50] Alec Radford, Karthik Narasimhan, Tim Salimans, and Ilya Sutskever. (2018). Improving language understanding with unsupervised learning. *Technical report, OpenAI*.

[51] Peters, M. E., Ammar, W., Bhagavatula, C., & Power, R. (2017). Semi-supervised sequence tagging with bidirectional language models. *In ACL*.

[52] Wu, Y., Schuster, M., Chen, Z., Le, Q. V., Norouzi, M., Macherey, W., ... & Dean, J. (2016). Google's neural machine translation system: Bridging the gap between human and machine translation. *arXiv:1609.08144*.

[53] BERT 详解. https://zhuanlan.zhihu.com/p/48612853.

[54] Yang, Z., Dai, Z., Yang, Y., Carbonell, J. G., Salakhutdinov, R., & Le, Q. V. (2019). XLNet: Generalized Autoregressive Pretraining for Language Understanding. *arXiv preprint arXiv*:1906.08237, 2019.

[55] Dai, Z., Yang, Z., Yang, Y., Carbonell, J. G., Le, Q. V., & Salakhutdinov, R. (2019). Transformer-xl: Attentive language models beyond a fixed-length context. *arXiv preprint arXiv*:1901.02860, 2019.

[56] Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., ... & Stoyanov, V. (2019). Roberta: A robustly optimized bert pretraining approach. *arXiv preprint arXiv*:1907.11692, 2019.

[57] Joshi, M., Chen, D., Liu, Y., Weld, D. S., Zettlemoyer, L., & Levy, O. (2019). Span bert: Improving pre-training by representing and predicting spans. *arXiv preprint arXiv*: 1907.10529, 2019.

[58] Liu, X., He, P., Chen, W., & Gao, J. (2019). Multi-task deep neural networks for natural language understanding. *arXiv preprint arXiv*:1901.11504, 2019.

[59] Liu, X., He, P., Chen, W., & Gao, J. (2019). Improving Multi-Task Deep Neural Net works via Knowledge Distillation for Natural Language Understanding. *arXiv preprint arXiv*:1904.09482.

[60] 8 篇论文梳理 BERT 相关模型进展与反思. https://www.msra.cn/zh-cn/news/features/bert.

[61] 如何通俗易懂地解释卷积. https://www.zhihu.com/question/22298352/answer/637156871.

[62] 一文读懂图卷积 GCN. https://mp.weixin.qq.com/s/Rd-MBAgq_i-PsaopzNmACQ.

[63] 图神经网络. https://www.jiqizhixin.com/graph/technologies/c39cf57b-df95-4c9e-9a8a-0d8e a330d625.

[64] 2018 年深度学习的主要进步. https://blog.csdn.net/weixin_42137700/article/details/857546 04.

[65] 图网络模型原理详解. https://blog.csdn.net/weixin_40871455/article/details/86515934.

[66] Momentum Contrast for Unsupervised Visual Representation Learning 无监督胜有监督，刷新检测分割任务. https://blog.csdn.net/weixin_43876801/article/details/103148773.

[67] Ding M, Zhou C, Chen Q, et al. (2019). Cognitive Graph for Multi-Hop Reading Co mprehension at Scale. *arXiv preprint arXiv*:1905.05460.

[68] 机器学习算法应用场景. https://blog.csdn.net/abc52shenghuo/article/details/77990579.

[69] 机器学习是在金融领域的应用，离不开大数据. https://www.jianshu.com/p/0f3b638a4a74.

[70] 三问（why?what?how?）金融领域的机器学习. https://www.jianshu.com/p/ddc8c54fc355.

[71] 摩根大通报告 12 个亮点总结：金融领域的机器学习工具有哪些.

[72] 机器学习算法在自动驾驶领域的应用大盘点. https://blog.csdn.net/weixin_34050005/artic le/details/90434845.

[73] 人工智能与机器学习技术在医疗保健行业中的应用. https://zhuanlan.zhihu.com/p/34918 987.

[74] 当人工智能和机器学习遇到零售. http://www.cniteyes.com/archives/32001.

[75] 2017 年机器学习将在这四大行业得到全面应用. https://baijiahao.baidu.com/s?id=1567230473301588&wfr=spider&for=pc.

[76] word2vec 神经模型. http://www.51sjk.com/b1b47639/.https://blog.csdn.net/amds123/article/details/72860400/.

[77] 阿里云发布机器学习平台 PAI v3.0. https://baijiahao.baidu.com/s?id=1628657591620076285&wfr=spider&for=pc.

[78] 腾讯智能钛机器学习 TI-ML. https://cloud.tencent.com/product/ti.

[79] 第四范式发布两大机器学习通用平台. http://news.sciencenet.cn/sbhtmlnews/2018/9/339532.shtm?id=339532.

[80] 全球机器学习领域顶尖的 16 家公司. https://blog.csdn.net/cf2SudS8x8F0v/article/details/80088355.

[81] 苹果 Core ML 3 给开发者惊喜，机器学习训练从未这么简单. http://www.sohu.com/a/318815747_473283.

[82] Enterprise AI Goes to Market Through Applications. https://www.ayasdi.com/platform/applications/.

[83] 大数据“显影”：Ayasdi 用拓扑数据分析癌症. https://www.ctocio.com/ccnews/11043.html.

[84] 这家公司打击过 911 恐怖分子，现在又来给银行抓内鬼. https://www.leiphone.com/news/201609/ef4V7YVCEqDP4UhX.html.

[85] darktrace 亮点. https://blog.csdn.net/weixin_34337265/article/details/86020998.

[86] Facebook 如何运用机器学习进行十亿级用户数据处理. https://blog.csdn.net/qq_40027052/article/details/79139612.

[87] 谷歌 Cloud AutoML 自动机器学习平台初步研究. https://blog.csdn.net/eason_oracle/article/details/79929445.

[88] Watson Machine Learning. https://www.ibm.com/cn-zh/cloud/machine-learning.

[89] Machine Learning for Intelligent Decision Support. https://www.qburst.com/machine-learning-services/.

[90] Qualcomm 通过全新骁龙机器学习软件开发包让移动终端更加智能. https://www.qualcomm.cn/news/releases-2016-05-02.

[91] 网站简介-Skytre. http://www.0430.com/us/web77897/.

[92] Meet Michelangelo: Uber’s Machine Learning Platform. https://eng.uber.com/michelangelo/.

[93] 如何高效推进 ML 模型开发和部署？Uber 机器学习平台 Michelangelo 实践. https://blog.csdn.net/dQCFKyQDXYm3F8rB0/article/details/84207671.

顾问：朱军、唐杰

编辑：景晨、刘佳、邵洲、殷达、赵杨奥

数据：赵慧军

关注“学术头条”并回复“机器学习”下载报告