人工智能机理解释与数学方法探讨

郭田德, 韩丛英*

中国科学院大学数学科学学院, 北京 100049

E-mail: tdguo@ucas.ac.cn, hancy@ucas.ac.cn

收稿日期: 2020-02-10; 接受日期: 2020-03-23; 网络出版日期: 2020-05-26; * 通信作者
国家自然科学基金 (批准号: 11731013, 11991022 和 U19B2040) 资助项目

摘要 人工智能是一门交叉学科, 融合了脑认知科学、心理学、数学 (包括统计学)、信息科学、计算机科学等诸多学科. 目前, 以大数据驱动的深度学习为代表的人工智能发展迅速, 在许多领域有广泛的应用. 但是, 人工智能现在最大的缺陷是没有理论, 基本上还处于实验科学阶段. 探讨人工智能的机理, 进行其理论研究, 对人工智能的进一步发展至关重要. 为了揭示人工智能的本质, 进一步促进人工智能的理论研究, 本文从认知生物学和认知心理学两个层面, 探讨现有的三个主要的人工智能学派—联结主义、符号主义和行为主义—所蕴含的机理和具体实现的数学理论和方法, 试图解释人工智能的本质, 给出未来可解释的和具有创造性的人工智能的一些可能的基础研究方法和研究方向.

关键词 人工智能 数学 认知生物学 认知心理学

MSC (2010) 主题分类 00A71, 68T01

1 引言

计算机问世之后, 特别是第二次世界大战之后, 就出现了执行困难智力任务的计算机程序, 再通过这些程序, 可以构建通用工具, 解决各种各样的日常问题. 1943 年, McCulloch 和 Pitts^[1] 发表了《神经活动内在性的逻辑计算》, 其突出贡献是将生物神经系统归纳为“M-P 神经元模型”. 1950 年, Turing^[2] 发表了《计算机器与智能》, 引入了图灵测试的概念. 1949 年, Hebb^[3] 提出的赫布理论解释了学习过程中大脑神经元所发生的变化, 标志着机器学习领域迈出了第一步. 1959 年, Samuel^[4] 创造了“机器学习”一词. Samuel 基于其理论研究成果所编制的下跳棋程序是世界上第一个有自主学习功能的游戏程序, 并用这个跳棋程序击败了人类的跳棋冠军. 1997 年 5 月, IBM 的深蓝击败了国际象棋世界冠军卡斯帕罗夫, 标志着计算机程序可以彻底解决类似于国际象棋这样复杂的游戏. 2006 年, Hinton 和 Salakhutdinov^[5] 提出的带“深度结构”自编码网络的方法取得了巨大的成功, 开启了

英文引用格式: Guo T D, Han C Y. Artificial intelligence mechanism and mathematics implementation methods (in Chinese). Sci Sin Math, 2020, 50: 1541–1578, doi: 10.1360/SSM-2020-0031

深度学习的时代. 围棋人工智能程序 AlphaGo 的出现, 让人们人工智能的期待再次提升到前所未有的高度, 带动人工智能迎来了新的发展时代. 人工智能从提出到 20 世纪的初级发展阶段, 经过了曲折的历程^[6-10], 发展到今天, 进入了一个最好的时代.

人工智能, 简单地说, 就是机器能做人类智能能做的事情. 其核心就是根据人们对人脑工作机制和人类认知方式的研究成果, 通过了解人的智能的实质, 建立相应的数学模型, 利用一定的数据, 设计训练和求解算法, 并用计算机软硬件实现, 从而生产出一种新的智能机器, 能以人类智能相似的方式做出反应, 胜任一些通常需要人类智能才能完成的复杂工作. 人工智能学科研究的主要内容包括知识表示、知识获取、知识处理、自动推理、自动搜索、机器学习、自然语言理解、计算机视觉、智能机器人、自动程序设计等方面, 其中机器学习是人工智能的核心研究内容之一. 特别地, 机器学习的进步, 似乎正在不断接近人们心中的人工智能目标, 例如基于机器学习的语音识别、机器翻译、图像检测和图像识别等技术已经在我们的实际生活中开始得到了应用. 机器学习的发展还在继续, 甚至被认为有可能彻底改变人类文明的发展方向乃至人类自身.

虽然现在人工智能取得了一些进步, 但与真正的智能还相去甚远. 人工智能现在最大的缺陷是没有理论, 基本上还处在实验科学阶段, 其进一步发展的瓶颈也就是缺乏理论指导. 探讨人工智能的机理, 进行其理论研究, 对人工智能的进一步发展至关重要. 在过去二十多年的研究和开发中, 虽然国内外对人工智能理论的研究已经有了一些进步, 但还没有达到真正的突破. 既然人工智能的理论和方法主要是模仿人脑工作机制和人类的认知方式, “大脑的生物结构特性”和“人类的认知心理学”必然是人工智能首先需要研究和借鉴的方向. 迄今为止, 人工智能的发展有符号主义、联结主义和行为主义三个学派, 本文将从认知生物学和认知心理学两个层面探讨这三个学派的人工智能机理解释以及实现的数学理论和方法, 试图解释人工智能的本质, 给出未来可解释的和具有创造性的人工智能的一些可能的基础研究方法和研究方向.

2 基于认知生物学的联结主义人工智能机理解释与数学方法

认知生物学就是分析有机体生命和认知手段之间在功能上的类似性, 也就是认知神经科学的主要研究内容. 认知神经科学^[11]是认知生物学在 20 世纪 80 年代末出现的一种主要研究趋势, 它是脑科学、认知科学、神经科学等多个学科的融合, 主要研究和探讨人类心理及其活动的脑基础, 以便揭示出人类心理和大脑之间的关系. 认知神经科学认为脑结构与脑功能具有多层次性的特点, 虽然人脑的结构是脑功能的基础, 但在结构和功能之间并不是简单的一一对应关系.

2.1 人脑的构成与工作模式简介

大脑是人体中一个非常复杂的器官, 人类的思想和意识都来源于此. 人脑由大脑、小脑、间脑、脑干组成, 其中大脑是脑的主要部分, 是中枢神经系统的最高级部分. 大脑分为左右两个大脑半球, 二者由神经纤维构成的胼胝体相连, 协调工作.

人类为了适应环境的变化, 需要随时随地处理各种信息, 并依次做出决策来指导行动. 大脑就是人类的信息处理中心, 负责处理各种信息. 人们的听觉、视觉、触觉等各种感官收集到的信息都要传递给大脑进行处理, 根据大脑的处理结果, 人们做出不同的决策和反应. 除此之外, 大脑还是人类的

图 1 (网络版彩图) 典型的单个神经元结构^[12] 图 2 (网络版彩图) 神经元之间信息传递方式^[12]

认知中心, 人类的意识、思维、情感和记忆等所有更高级的认知也都是由大脑产生并保持。所以, 我们可以说, 所谓智能就是人类大脑的能力。

人类大脑的智能主要依赖于神经系统完成。人类的大脑神经系统包含大约一百四十亿 (超过 10^{10}) 个计算单元, 它们之间通过大约一百万亿 (超过 10^{15}) 个连接, 时刻进行着广泛而复杂的联系, 是高级神经活动的中枢^[13]。智能就是依靠这些巨大的计算单元和连接组成的复杂系统而实现。这些计算单元是一类特殊的细胞, 被称为神经元, 而它们之间的连接被称为突触。神经元除了拥有一般细胞的结构外, 还从细胞体上长出许多小触手, 这些突起的小触手被称为“神经突起”。神经突起有两种, 一种突起长度较短、但数量较多, 被称为“树突”, 其主要功能是负责接收信息。另一种突起只有一根, 并且与其他突起明显不同, 被称为“轴突”, 轴突的主要功能是负责发送信息。一个神经元的轴突和另一个神经元的树突接触的地方被称为“突触”, 就像我们身体上的关节, 肘关节连接着大臂和小臂, 膝关节连接着大腿和小腿, 而突触就连接着一个神经元和另一个神经元, 如图 1。

神经元之间传递信息有两种通道。第一种传递通道如图 2(a): 神经元 A 接收到信息—神经元 A 的轴突末端—神经元 B 的树突—神经元 B 接收到信息。即, 一个神经元接收到了信息, 传递给其轴突, 到达轴突的末端之后, 再通过一种特殊的方式传递给另一个神经元的树突, 树突接收到信息后, 传递给其神经元中心的部分, 也就是细胞体, 至此便完成了一次神经元间的信息传递。第二种传递通道如图 2(b): 通过轴突之间直接传递信息。在这个传递过程中, 突触有两个重要组成部分: 一部分是

图 3 (网络版彩图) 大脑对视觉信息的分层处理机制^[12]

传出信息的轴突末端, 称为突触前; 另一部分是接收信息的树突或者胞体本身, 称为突触后. 突触前和突触后共同组成突触, 它就是神经元间信息传递的桥梁.

2.2 人类大脑的工作机制

大脑进行工作时, 首先是感受器细胞将刺激 (如光量子) 转换成电信号, 处理后经化学突触传递到神经元细胞, 每个神经元的计算依靠电流进行, 这些电流由突触电信号引发, 并在神经元中央部分 (细胞体) 进行整合, 只有当电信号超过兴奋阈值时才将电脉冲传递给其他神经元. 单一的神经元是一个简单的计算单元, 对于其输入, 计算一个简单的标量积, 接着再经过一个 S 型函数, 然后进行输出. 由于计算是基于电信号的, 而这个电信号又受到人体当前的化学物质、压力、血液供应、血糖水平等因素的影响, 所以这个计算伴随着很多噪声. 神经系统的智能是按照互联的强度编码的, 并且通过改变连接来进行学习, 只有超过兴奋阈值才会有连接, 并有信号传递. 显然, 这种模式与“标准”串行计算机不同, 串行计算机以周期的方式执行, 即先从存储器中取出内容, 进行运算, 然后再将结果写回存储器. 但是, 人的神经网络不区分存储器和处理过程, 而是通过网络中的信号流同步操作.

人类收集信息的方式有多种, 包括听觉、视觉、触觉等各种感官; 收集信息的方式也都不一样, 类似于不同的传感器. 但是, 信息处理中心, 即大脑, 对信息的处理方式是相似的. 视觉是人类感知外部世界获取信息的最重要途径之一. 接下来我们以大脑对视觉信息的处理为例说明其处理的方式. 图 3 中, 在初级视觉皮层之后有两条通路, 往大脑上方走的通路, 分析的是视觉信号所带来的“Where”信息, 也就是位置; 而往下方走的通路, 分析的是关于“What”的信息, 也就是去识别和描述看到的是什么物体^[14]. 1981 年诺贝尔医学和生理学奖获得者 Hubel 和 Wiese 的研究表明, 大脑对视觉信息的处理是等级制的 (参见文献 [12]). 我们称负责接受信号的神经通道为上行通路, 而视网膜

到视觉皮层是最主要的视觉上行通路,但也不是唯一的.从视网膜上收集到了视觉信号,由两眼的视觉神经,传输给像交叉路口似的视交叉,然后将信号发到大脑的一个叫外侧膝状核的区域中,再将视觉信号层层分类整理,传递到初级视觉皮层 V_1 . V_1 处理简单视觉, V_2 是处理图形与物体轮廓(空间内大小的识别就是在 V_2 处理), V_3 更多的是传递信息, V_4 对颜色觉有关, V_5 (MT, 中央颞区) 传递运动立体视觉信息.

总之,大脑的工作机制可以描述为: (1) 大量的神经元形成网络,对于从其他多个神经元传递过来的信号,如果它们的和不超过某个阈值,则神经元不做出任何反应; (2) 对于从其他多个神经元传递过来的信号,如果它们的和超过某个阈值,则神经元做出反应,处理成固定强度的信号后向另外的神经元传递; (3) 从其他多个神经元传递过来的信号之和,每个信号对应的权重不同; (4) 大脑对视觉信息的处理是等级制的(分层),从低级的 V_1 区提取边缘特征,到 V_2 区的形状或者目标的部分等,再到更高层、整个目标、或者目标的行为等.

如果我们能把大脑的活动转换成电能,就相当于一只 20 瓦灯泡的功率.人的大脑中进行着 10 万种/秒不同的化学反应.人体五种感觉器官不断接受的信息中,大约仅有 1% 左右的信息经过大脑处理,其余 99% 左右的信息均被过滤掉.人的大脑平均为人体总体重的 2%; 大脑神经细胞间信号在神经或肌肉纤维中的最快的神经冲动传导速度为 400 多千米/小时,而人体内有超过 72 千米的神经;人的大脑每天可处理 8,600 万条信息.但是,迄今为止,人们对大脑的研究还有许多待解之谜.比如,许多简单的连结产生的系统,为什么可以产生诸如物体识别、说话、倾听、吃饭、喝咖啡等复杂的智能活动? 人们为什么能够为了兴趣或为了养家糊口而勤奋工作? 研究者普遍认为这是由于涌现行为产生的结果.所谓“涌现”是指一个系统中个体间预设的简单互动行为所造就的无法预知的复杂样态的现象^[15]. 大脑的工作机制表明,许多十分简单的互联计算单元能够形成复杂的智能系统.由于单个神经元的功能十分简单,它只是用一个超平面将输入空间分成两个区域,因此复杂性必然来自参与一个复杂行为的更多层的神经元.

2.3 人工神经网络模型

将上述大脑神经元的工作模式在数学上抽象化,形成人工神经元,并以其为单位人工地形成网络,这样的网络就是人工神经网络.将构成大脑的神经元的集合体抽象为数学模型,这是神经网络的出发点,即用人工神经网络实现人工智能,也是基于认知生物学的人工智能的建模与解释,即所谓的联结主义人工智能的实现思路,也称之为平行分布式加工系统.简单地说,该系统包含许多相互连接的模块,每个模块由一些简单的相互连接的加工单元构成,每个加工单元的功能是接收来自其他给定单元的输入,通过简单的加工,然后输出给其他单元.几组模块可以组成通路,每条通路包括一组相互连接的模块.对于给定的任务,平行分布式加工系统进行操作时,就会选择一条通路,通路上的加工单元进行输入和输出的加工,通路中的连接确定了这条通路的强度,从而通路的选择也确定了任务加工的结果、速度和准确性.

2.3.1 单层感知器模型

生物神经元以化学突触进行通信,突触专门将信号传递给各个靶细胞.触发突触进行信号传递的基本过程是利用传播的电信号,当且仅当兴奋性和抑制性突触的输入信号的结合超过某个给定的阈

图4 (网络版彩图) 单层感知器模型

值时, 这个电信号才会产生, 此时神经元的输出才被打开. 根据这一工作原理, 我们首先建立平行分布式加工系统的加工单元, 即单层感知器模型, 如图4所示.

单层感知器模型的输入和输出之间的关系用简单的非线性变换实现:

$$y = \sigma(W^T x + b). \quad (2.1)$$

仿照生物神经元的工作模式, (2.1) 式中简单的非线性变换由一个参数化的线性变换 (加权求和) 与一个简单的非线性变换 (挤压函数) 复合而成. 此处的挤压函数, 在生物神经元中就是一个二值函数, 而在人工神经元中, 为了处理方便, 替换成具有较好性质 (连续性、平滑性) 的形状相似的函数, 也就是通常所取的激活函数. 将 S 型挤压函数 (或者称为传递函数) 应用到无限制的线性模型输出上, 是添加 “最小限度的非线性” 的简单方法.

2.3.2 多层感知器模型

两个线性变换的复合仍然是线性变换, 如果将第一个线性变换的输出进行非线性函数变换, 然后再进行第二个线性变换, 依次下去, 能够逼近任意的光滑函数^[16]. 第一个线性变换将提供第一个 “隐藏层”, 第二个变换将从隐藏层中产生可见的输出. 多层感知器神经网络是由大量的互联单元 (神经元) 构成的, 它们平行工作, 用于解决特定的问题, 图5是多层感知器模型构成的一个平行分布式加工系统.

多层感知器的体系结构组织方式是信号从输入层依次流过不同的层, 最后到达输出层, 中间层称为隐藏层, 因为它们在输入端和输出端是不可见的.

2.4 具体实现中的数学方法

多层感知器模型实现的是多层的非线性变换^[17]:

$$y^{(k+1)} = \sigma_k(W_k^T y^{(k)} + b^{(k)}) \quad (k = 1, 2, \dots, K), \quad (2.2)$$

其中 $y^{(1)} = x$, K 为多层感知器模型的层数. 即最终的输出 $y^{(K+1)}$ 由输入

$$y^{(1)} = x$$

图 5 (网络版彩图) 多层感知器模型

经过 K 次参数化的简单非线性变换复合而成:

$$\begin{aligned} y^{(K+1)} &= \sigma_K(W_K^T y^{(K)} + b^{(K)}) = f^K(y^{(K)}) \\ &= f^K(f^{K-1}(y^{(K-1)})) = \dots = f^K(f^{K-1}(\dots f^{(1)}(y^{(1)}) \dots)). \end{aligned} \quad (2.3)$$

具体的实现就是要建立相应的数学模型, 设计求解算法, 得到 (2.3) 式中每一次非线性变换的权重参数和偏置参数

$$(W_k, b^{(k)}) \quad (k = 1, 2, \dots, K).$$

此类模型本质上是一类数据再表达的自编码方法, 其中的参数求解一般是根据样本数据训练而得, 所以是数据驱动的, 因此又称之为数据驱动的数据再表达方法^[18]. 数据再表达中的栈式自编码网络方法就是该类方法的具体数学实现.

自编码网络^[19]就是在保持输入与输出尽可能一致(通过信息损失判定)的前提下, 实现无监督方式下的隐层特征提取的数据再表达和参数学习的体系结构. 其实, 自编码网络的概念在 20 世纪 80 年代就被 Rumelhart 等^[20]引入, 它可以对数据进行压缩, 从而实现对数据的降维. 下面我们首先重点介绍单隐藏层的自编码网络的实现方法, 然后讨论多隐藏层的自编码网络的实现方法, 再讨论由多个单隐藏层的自编码网络堆积而成的栈式自编码网络的实现方法.

一般来说, 单隐藏层的自编码网络都具备三层网络结构, 分别为输入层、一个隐藏层和输出层, 其中输入层的输入是原始数据, 隐藏层的输出是数据的一种再表达, 输出层的输出是为了恢复原始数据, 使丢失的信息尽可能地少. 2006 年, Hinton 和 Salakhutdinov^[5]提出的带“深度结构”自编码网络的方法取得了巨大的成功. 该文章中的自编码网络是以受限玻尔兹曼机(restricted Boltzmann machine, RBM)为基础, 由带有多个单隐藏层的自编码网络堆积而成, 自下而上逐层进行训练, 最后根据后端任务再微调整个网络, 使得深度网络的训练变得可行. Hinton 等人的工作开启了深度学习时代(参见文献[21]). 所以说, Hinton 等人提出的深度学习, 本质上主要是一种逐层数据再表达的自编码方法.

图 6 (网络版彩图) 单隐藏层自编码网络的结构图

通常来说, 一个单隐藏层的自编码网络的结构如图 6 所示. 图 6 中, 虚线框中是一个单隐藏层的自编码网络模型, 它由单个的编码器和单个的解码器两部分构成. 编码器将输入数据 $x \in \mathbb{R}^n$ 变换成编码数据 $y \in \mathbb{R}^m$, 解码器将编码数据 y 重建成数据 $\tilde{x} \in \mathbb{R}^n$. 单隐层自编码网络的优化模型如下:

$$\begin{aligned} \min \quad & J(x, \tilde{x}) \\ \text{s.t.} \quad & \begin{cases} y = f(x), \\ \tilde{x} = g(y), \end{cases} \end{aligned} \quad (2.4)$$

其中,

$$J: \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$$

为一个衡量 x 和 $\tilde{x}$ 之间误差的函数或者称之为损失函数, n 是输入数据的维度.

2.4.1 单隐藏层全连接自编码网络算法

为了得到编码变换 f 和解码变换 g , 上述单隐藏层自编码网络的结构可以用多种方法实现. 如果采用神经网络的实现方法, 则编码变换 f 和解码变换 g 都采用线性变换和一个简单的非线性变换的复合得到, 即

$$y = f(x) := \sigma_f(Wx + b^{(1)}), \quad (2.5)$$

$$\tilde{x} = g(y) := \sigma_g(W^T y + b^{(2)}), \quad (2.6)$$

其中, $W \in \mathbb{R}^{m \times n}$ 为输入层和隐藏层之间的权值矩阵, $W^T \in \mathbb{R}^{n \times m}$ (W^T 表示 W 的转置) 为隐藏层和输出层之间的权值矩阵 (当然这个权值矩阵可以是任意的, 为了简单起见, 取 W 的转置); $b^{(1)} \in \mathbb{R}^m$ 和 $b^{(2)} \in \mathbb{R}^n$ 分别为隐藏层和输出层的偏置向量; σ_f 和 σ_g 为激活函数, 一般可取为 sigmoid 函数, 即

$$\sigma_f(z) = \sigma_g(z) = \frac{1}{1 + e^{-z}}. \quad (2.7)$$

对于一个样本的损失函数 $J(x, \tilde{x})$, 可以取为平方误差函数 $L(x, \tilde{x})$,

$$L(x, \tilde{x}) = \|x - \tilde{x}\|^2, \quad (2.8)$$

或者交叉熵函数

$$L(x, \tilde{x}) = - \sum_{i=1}^n [x_i \log(\tilde{x}_i) + (1 - x_i) \log(1 - \tilde{x}_i)], \quad (2.9)$$

等等. 因为最终是要让解码层重构出原始的输入, 也就是让训练样本集合中的所有数据丢失的信息之和尽可能少, 因此, 最终归结为如下形式的最优化问题:

$$\min_{W, b^{(1)}, b^{(2)}} J(W, b^{(1)}, b^{(2)}) = \frac{1}{M} \sum_{i=1}^M L(W, b^{(1)}, b^{(2)}; x^{(i)}, \tilde{x}^{(i)}), \quad (2.10)$$

其中, $W, b^{(1)}, b^{(2)}$ 为需要优化的参数; $x^{(i)}, \tilde{x}^{(i)}$ 分别为第 i 个输入数据和第 i 个输入数据的重建数据, $i = 1, 2, \dots, M$, M 为数据集的大小, 即训练样本的数量.

算法 1 给出单隐藏层全连接自编码网络算法框架.

算法 1 单隐藏层全连接自编码网络算法框架

第 1 步 输入: 样本数据 $x^{(i)} \in \mathbb{R}^n$ ($i = 1, 2, \dots, M$), 激活函数 σ_f 和 σ_g (一般可以取为 sigmoid 函数), 选取损失函数 $L(x, \tilde{x})$ (一般可以取为平方误差函数或者交叉熵函数).

第 2 步 令

$$\begin{aligned} y^{(i)} &= f(x^{(i)}) := \sigma_f(Wx^{(i)} + b^{(1)}) \quad (i = 1, 2, \dots, M), \\ \tilde{x}^{(i)} &= g(y^{(i)}) := \sigma_g(W^T y^{(i)} + b^{(2)}) \quad (i = 1, 2, \dots, M). \end{aligned}$$

选择一种合适的优化方法, 如随机梯度类算法或者随机拟牛顿算法等, 求解最优化问题:

$$\min_{W, b^{(1)}, b^{(2)}} J(W, b^{(1)}, b^{(2)}) = \frac{1}{M} \sum_{i=1}^M L(W, b^{(1)}, b^{(2)}; x^{(i)}, \tilde{x}^{(i)}).$$

第 3 步 输出: 输入层和隐藏层之间的权值矩阵 W , 隐藏层和输出层的偏置向量 $b^{(1)}$ 和 $b^{(2)}$.

根据第 3 节将要讲述的认知心理学的“相似性、接近性、闭合性、连续性”等简单性原则, 大脑知觉中物体的组织不是一个偶然的或是随意的活动, 而是受一些经济而又简单的原则控制的有规律的程序, 它能使结果具有很大限度的稳定性和不变性. 体现在网络结构中, 典型的是卷积神经网络, 或者体现在最优化问题 (2.10) 中, 就是在优化的目标函数中加上不同的正则项, 从而得到“卷积自编码”^[22]、“稀疏自编码”^[23]、“降噪自编码”^[24]和“可收缩自编码”^[25]等其他自编码模型.

2.4.2 单隐藏层卷积自编码网络算法

卷积自编码网络利用了传统自编码网络的无监督的学习方式, 改变了一般自编码网络中的全连接模式, 改用卷积神经网络的卷积操作, 选择局部连接, 实现了局部连接、参数共享的数据再表达的特征提取.

在叙述卷积自编码网络^[22]之前, 我们先简单介绍卷积神经网络^[26–29]的主要结构. 卷积神经网络模型主要是卷积层和池化层交替使用, 这和大脑初级视觉皮层的简单与复杂细胞接受外界刺激的处理方式类似, 也与认知心理学的“相似性、接近性”等简单性原则相关, 它的一种较常见的结构由卷积层、池化层 (也是一种下采样层) 和分类层堆叠而成.

因为图像数据有着特殊的空间局部结构, 图像的一部分的统计特性与其他部分是相似的. 一般的神经网络的全连接自编码网络会忽视这种结构. 除了这个问题, 还会引入参数上的冗余等问题. 卷积神经网络的设计充分考虑了图像的局部结构. 卷积就是一种特征提取方式, 卷积计算充分保持图像的局部结构, 即一部分学习的特征也能用到另一部分上; 池化本质是图像的下采样 (把原始图像的窗口像素变成一个像素), 是对不同位置的特征进行聚合统计, 常用的池化方法有最大池化、平均池

化和最大概率池化等. 像卷积神经网络那样, 卷积自编码网络在输入图像中的所有局部位置共享参数, 保持空间的局部性.

对于单通道的输入 x , 一个隐藏层的卷积自编码网络的第 k 个特征图的表示为

$$y^{(k)} = \sigma(x * W^{(k)} + b^{(k)}), \quad (2.11)$$

其中, $W^{(k)}$ 和 $b^{(k)}$ 是参数, 偏置 $b^{(k)}$ 对于第 k 个特征图来说是相同的, σ 是激活函数 (这里一般采取双曲正切函数), $*$ 表示二维的卷积. 重构 (解码过程) 可以如下计算:

$$\tilde{x} = \sigma\left(\sum_{k \in H} y^{(k)} * \tilde{W}^{(k)} + c\right), \quad (2.12)$$

其中, 每个输入通道对应一个偏置 c , $\tilde{W}^{(k)}$ 是参数, H 表示特征图的集合. 一个样本的损失函数可以选择平方误差函数

$$L(x, \tilde{x}; \theta) = \sum_{i=1}^n (x_i - \tilde{x}_i)^2, \quad (2.13)$$

其中参数为 $\theta = (W^{(k)}, b^{(k)}, \tilde{W}^{(k)}, c)$, 求解类似于一般的神经网络.

算法 2 给出单隐藏层卷积自编码网络算法框架.

算法 2 单隐藏层卷积自编码网络算法框架

第 1 步 输入: 样本数据 $x^{(i)} \in \mathbb{R}^n$ ($i = 1, 2, \dots, M$), 激活函数 σ (一般采取双曲正切函数), 选取损失函数 $L(x, \tilde{x})$ (一般可以取为平方误差函数).

第 2 步 令

$$\begin{aligned} y^{(k)} &= \sigma(x * W^{(k)} + b^{(k)}) \quad (k \in H), \\ \tilde{x}^{(k)} &= \sigma\left(\sum_{k \in H} y^{(k)} * \tilde{W}^{(k)} + c\right). \end{aligned}$$

选择一种合适的优化方法, 如随机梯度法或者随机拟牛顿法, 求解最优化问题:

$$\min J(x, \tilde{x}; \theta) = \frac{1}{M} \sum_{j=1}^M \sum_{i=1}^n (x_i^{(j)} - \tilde{x}_i^{(j)})^2.$$

第 3 步 输出: 输入层和隐藏层之间的权值矩阵 $W^{(k)}$, $b^{(k)}$, 隐藏层和输出层的偏置向量 $\tilde{W}^{(k)}$ 和 c .

其实, 在解码的过程中可以采用最大池化的操作. 实验表明, 采取了这种操作后就没有必要对隐藏神经元或者权重施加 L_1 或者 L_2 正则化. 如果用池化代替的正则化, 那么这个正则化项建模的意义就是聚合统计的效果 (聚类、降维、稀疏等), 因此从某种意义上说这也可以视为正则化的作用.

2.4.3 单隐藏层稀疏自编码网络算法

通常聪明人的大脑往往体积更大, 较大体积的大脑内富含更多的神经元, 具备更强的计算能力. 然而, Genc 等^[30] 的研究表明, 尽管聪明人神经元数量相对较多, 但在测试中, 智商高的人的大脑神经元活动明显比智商较低的人少, 也就是说 “智商高的人的大脑具备非常精简但极为高效的神经元连接”. 因此, 他们虽然神经元活动较少, 却表现出更强的智慧表现. 这种稀疏性也符合格式塔认知心理学认知的简单性原则. 在大脑的工作过程中, 如果当神经元的输出接近于 1 时认为是被激活, 输出接近于 0 时认为是被抑制, 使得神经元大部分时间被抑制的限制称作稀疏性限制 (这里假设神经元

的激活函数是 sigmoid 函数, 如果使用 tanh 函数作为激活函数的话, 则输出接近于 -1 时认为是抑制的).

稀疏自编码网络背后的思想是认为高维而稀疏的特征有利于解决学习任务. 在这个网络中不会特意去指定哪些隐藏节点被抑制了, 而是指定了一个稀疏性常数 ρ , 表示的是隐藏层神经元的平均活跃程度. 为了实现这一目标, 需要引入一个度量来衡量实际的激活度与期望的激活度之间的差别, 并且将之作为正则项. 在下面的模型介绍中, 不妨引入 KL 散度作为这个度量. 其实, KL 散度是信息论中的一个概念, 它的计算公式如下所述:

如果 P 和 Q 是两个离散随机变量, 则它们之间的 KL 散度定义为

$$D_{KL}(P \parallel Q) = \sum_i P(i) \log \frac{P(i)}{Q(i)}. \quad (2.14)$$

如果 P 和 Q 是两个连续随机变量, 则它们之间的 KL 散度定义为

$$D_{KL}(P \parallel Q) = \int_{-\infty}^{+\infty} P(x) \log \frac{P(x)}{Q(x)} dx. \quad (2.15)$$

设样本集合的大小为 M , 隐藏层的节点数目为 s_2 . 令 $a_j^{(2)}$ 表示在给定输入是 x 的情况下, 隐藏层神经元 j 的激活度 (角标 “2” 表示自编码网络中的第 2 层, 也就是表示第 1 个隐藏层). 那么在隐藏层中神经元 j 对所有样本的平均激活度为

$$\bar{\rho}_j = \frac{1}{M} \sum_{i=1}^M a_j^{(2)}(x^{(i)}).$$

因此根据 KL 散度的定义, ρ 和 $\bar{\rho}_j$ 之间的 KL 散度为

$$D_{KL}(\rho \parallel \bar{\rho}_j) = \rho \log \frac{\rho}{\bar{\rho}_j} + (1 - \rho) \log \frac{1 - \rho}{1 - \bar{\rho}_j}. \quad (2.16)$$

于是稀疏自编码网络模型的目标函数的正则项, 即隐藏层的所有 s_2 个节点的散度和为

$$\sum_{j=1}^{s_2} D_{KL}(\rho \parallel \bar{\rho}_j) = \sum_{j=1}^{s_2} \left(\rho \log \frac{\rho}{\bar{\rho}_j} + (1 - \rho) \log \frac{1 - \rho}{1 - \bar{\rho}_j} \right). \quad (2.17)$$

这样, 单隐藏层网络的损失函数为

$$J_{\text{sparse}}(W, b^{(1)}, b^{(2)}) = J(W, b^{(1)}, b^{(2)}) + \beta \sum_{j=1}^{s_2} D_{KL}(\rho \parallel \bar{\rho}_j), \quad (2.18)$$

其中, β 是一个超参数, $J(W, b^{(1)}, b^{(2)})$ 由 (2.10) 给出. 除了稀疏约束项之外, 为了防止过拟合, 还可以加入权重衰减项, 所以最后的损失函数就是

$$\min J_{\text{SAE}}(W, b) = J(W, b^{(1)}, b^{(2)}) + \beta D_{KL}(\rho \parallel \bar{\rho}_j) + \frac{\lambda}{2} \sum_{i=1}^M \sum_{j=1}^{s_2} (w_{ij})^2. \quad (2.19)$$

这就是单隐藏层稀疏自编码网络训练时需要优化的目标函数, 也是一个单隐藏层网络的误差后传播模型.

算法 3 给出单隐层稀疏自编码网络算法框架.

算法 3 单隐层稀疏自编码网络算法框架

第 1 步 输入: 样本数据 $x^{(i)} \in \mathbb{R}^n$ ($i = 1, 2, \dots, M$), 激活函数 σ_f 和 σ_g (一般可以取为 sigmoid 函数), 选取损失函数 $L(x, \tilde{x})$ (一般可以取为平方误差函数) 和超参数 λ, β .

第 2 步 令

$$\begin{aligned} y^{(i)} &= f(x^{(i)}) = \sigma_f(Wx^{(i)} + b^{(1)}) \quad (i = 1, 2, \dots, M), \\ \tilde{x}^{(i)} &= g(y^{(i)}) = \sigma_g(W^T y^{(i)} + b^{(2)}) \quad (i = 1, 2, \dots, M). \end{aligned}$$

选择一种合适的优化方法, 如随机梯度法或者随机拟牛顿法, 求解最优化问题:

$$\min J_{\text{SAE}}(W, b) = J(W, b^{(1)}, b^{(2)}) + \beta D_{KL}(\rho \parallel \bar{\rho}_j) + \frac{\lambda}{2} \sum_{i=1}^M \sum_{j=1}^{s_2} (w_{ij})^2.$$

第 3 步 输出: 输入层和隐藏层之间的权值矩阵 W , 隐藏层和输出层的偏置向量 $b^{(1)}$ 和 $b^{(2)}$.

2.4.4 单隐藏层降噪自编码网络算法

基本的自编码网络能够恢复出原始数据的特征未必是最好的. 降噪自编码网络^[24]的思想是对于加了噪声的数据进行编码、解码, 最后还能恢复出原始数据的鲁棒特征. 具体来说, 将原始数据 x 通过一个随机映射 $\hat{x} \sim q_D(\hat{x} | x)$ “污染”成 $\hat{x}$, 然后通过基本的自编码网络得到隐藏层的表示 $y \sim f_\theta(\hat{x}) = s(W\hat{x} + b^{(1)})$, 并从中重构出 $\tilde{x} = g_{\theta'}(y)$.

算法 4 给出单隐藏层降噪自编码网络算法框架.

算法 4 单隐藏层降噪自编码网络算法框架

第 1 步 输入: $x^{(i)} \in \mathbb{R}^n$ ($i = 1, 2, \dots, M$), 激活函数 σ_f 和 σ_g (一般可以取为 sigmoid 函数), 选取损失函数 $L(x, \tilde{x})$ (一般可以取为平方误差函数) 和超参数 λ, β .

第 2 步 将数据 $x^{(i)} \in \mathbb{R}^n$ ($i = 1, 2, \dots, M$) 通过一个随机映射得到:

$$\hat{x}^{(i)} \sim q_D(\hat{x}^{(i)} | x^{(i)}).$$

第 3 步 令

$$\begin{aligned} y^{(i)} &= f(\hat{x}^{(i)}) = \sigma_f(W\hat{x}^{(i)} + b^{(1)}) \quad (i = 1, 2, \dots, M), \\ \tilde{x}^{(i)} &= g(y^{(i)}) = \sigma_g(W^T y^{(i)} + b^{(2)}) \quad (i = 1, 2, \dots, M), \\ J(W, b^{(1)}, b^{(2)}) &= \sum_{i=1}^M L(W, b^{(1)}, b^{(2)}; x^{(i)}, \tilde{x}^{(i)}). \end{aligned}$$

选择一种合适的优化方法, 如随机梯度法或者随机拟牛顿法, 求解最优化问题:

$$\min J_{\text{DAE}}(W, b^{(1)}, b^{(2)}) = J(W, b^{(1)}, b^{(2)}) + \beta J_{KL}(\rho \parallel \bar{\rho}) + \frac{\lambda}{2} \sum_{i=1}^M \sum_{j=1}^{s_2} (w_{ij})^2.$$

第 4 步 输出: 输入层和隐藏层之间的权值矩阵 W , 隐藏层和输出层的偏置向量 $b^{(1)}$ 和 $b^{(2)}$.

注意, 虽然降噪自编码网络算法与稀疏自编码网络算法中建立的优化模型的目标函数在形式上看起来是相同的, 但是其中的第一项 $J(W, b^{(1)}, b^{(2)})$, 含义是不同的.

2.4.5 单隐藏层可收缩自编码算法

可收缩自编码网络^[25]也是一种正则化的自编码网络, 即它的损失函数是由经典的重构误差函数和一个惩罚项组合而成. 这种网络希望得到的特征数据再表达对训练样本周围数据的小扰动是鲁棒的, 这可以通过使惩罚项是非线性映射的雅可比 (Jacobi) 矩阵的 Frobenius 范数实现. 具体来说, 如

果原始数据 x 经过编码函数 f 映射到隐藏层的表示 $y = f(x)$ 或者

$$y_i = f_i(x), \quad x \in \mathbb{R}^n \quad (i = 1, 2, \dots, m),$$

记此变换的雅可比矩阵为 $J_f(x) = (J_{ij}) \in \mathbb{R}^{m \times n}$, 其中

$$J_{ij} = \frac{\partial f_i}{\partial x_j} \quad (i = 1, 2, \dots, m; j = 1, 2, \dots, n).$$

惩罚项就是对所有样本的特征关于输入数据变换的偏导数求平方和. 记

$$\|J_f(x^{(k)})\|_F^2 = \sum_{i=1}^m \sum_{j=1}^n [J_{ij}(x^{(k)})]^2 \quad (k = 1, 2, \dots, M). \quad (2.20)$$

从几何上看, 惩罚项 $\|J_f(x)\|_F^2$ 使得到特征空间的映射在训练数据附近是收缩的. 直观上看, 一阶导数的值较低, 这导致隐藏层的表示对输入数据小变动的鲁棒性或者不变性, 这也与第 3 节将要讲到的认知心理学中的平滑性原则一致. 所以单隐藏层可收缩自编码网络中需要优化的目标函数是

$$J_{\text{CAE}}(W, b^{(1)}, b^{(2)}) = \sum_{i=1}^M (L(x^{(i)}, g(f(x^{(i)}))) + \lambda \|J_f(x^{(i)})\|_F^2), \quad (2.21)$$

其中, M 是训练数据的个数, f 是编码函数, g 是解码函数, L 是损失函数, λ 是一个超参数.

算法 5 给出单隐藏层可收缩自编码网络算法框架.

算法 5 单隐藏层可收缩自编码网络算法框架

第 1 步 输入: $x^{(i)} \in \mathbb{R}^n$ ($i = 1, 2, \dots, M$), 激活函数 σ_f 和 σ_g (一般可以取为 sigmoid 函数), 选取损失函数 $L(x, \tilde{x})$ (一般可以取为平方误差函数) 和超参数 λ .

第 2 步 令

$$\begin{aligned} y^{(i)} &= f(x^{(i)}) = \sigma_f(Wx^{(i)} + b^{(1)}) \quad (i = 1, 2, \dots, M), \\ \tilde{x}^{(i)} &= g(y^{(i)}) = \sigma_g(W^T y^{(i)} + b^{(2)}) \quad (i = 1, 2, \dots, M), \\ J_{ij} &= \frac{\partial f_i}{\partial x_j} \quad (i = 1, 2, \dots, m; j = 1, 2, \dots, n), \\ \|J_f(x^{(k)})\|_F^2 &= \sum_{i=1}^m \sum_{j=1}^n [J_{ij}(x^{(k)})]^2 \quad (k = 1, 2, \dots, M), \\ J_{\text{CAE}}(W, b^{(1)}, b^{(2)}) &= \frac{1}{M} \sum_{i=1}^M (L(x^{(i)}, g(f(x^{(i)}))) + \lambda \|J_f(x^{(i)})\|_F^2). \end{aligned}$$

选择一种合适的优化方法, 如随机梯度法或者随机拟牛顿法, 求解最优化问题:

$$\min J_{\text{CAE}}(W, b^{(1)}, b^{(2)}) = \frac{1}{M} \sum_{i=1}^M (L(x^{(i)}, g(f(x^{(i)}))) + \lambda \|J_f(x^{(i)})\|_F^2).$$

第 3 步 输出: 输入层和隐藏层之间的权值矩阵 W , 隐藏层和输出层的偏置向量 $b^{(1)}$ 和 $b^{(2)}$.

2.4.6 多隐藏层自编码网络方法

上面讨论的都是单隐藏层自编码网络, 数据经过单隐藏层自编码网络, 相当于进行了一次简单的非线性变换, 往往表达能力不够. 研究表明, 人脑对数据的表示是逐层进行的. 因此, 一般神经网络

算法 6 多隐藏层自编码网络算法框架

第 1 步 输入: 样本数据 $x^{(i)} \in \mathbb{R}^n$ ($i = 1, 2, \dots, M$), 激活函数 σ_f 和 σ_g (一般可以取为 sigmoid 函数), 选取损失函数 $L(x, \tilde{x})$ (一般可以取为平方误差函数或者交叉熵函数).

第 2 步 令

$$y^{(k+1,i)} = f^{(k)}(y^{(k,i)}) = \sigma_f(W^{(k)}y^{(k,i)} + b^{(k,1)}) \quad (k = 1, 2, \dots, K; i = 1, 2, \dots, M),$$

其中 $y^{(1,i)} = x^{(i)}$, K 为网络层数, $y^{(K+1,i)}$ 是 $x^{(i)}$ 最终的再表达数据; 令

$$\tilde{y}^{(k,i)} = g^{(k)}(\tilde{y}^{(k+1,i)}) = \sigma_g((W^{(k)})^T \tilde{y}^{(k+1,i)} + b^{(k,2)}) \quad (k = K, K-1, \dots, 1; i = 1, 2, \dots, M),$$

其中 $\tilde{y}^{(k,i)} = y^{(k+1,i)}$. $x^{(i)}$ 的重建数据为 $\tilde{x}^{(i)} = \tilde{y}^{(1,i)}$. 那么损失函数为:

$$J(W, b^{(1)}, b^{(2)}) = \frac{1}{M} \sum_{i=1}^M L(x^{(i)}, \tilde{x}^{(i)}),$$

其中 $(W, b^{(1)}, b^{(2)}) = \{(W^{(k)}, b^{(k,1)}, b^{(k,2)}) \mid (k = 1, 2, \dots, K)\}$. 选择一种合适的优化方法, 如随机梯度法或者随机拟牛顿法, 求解最优化问题:

$$\min_{W, b^{(1)}, b^{(2)}} J(W, b^{(1)}, b^{(2)}).$$

第 3 步 输出: 输入层和各个隐藏层之间的权值矩阵、各个隐藏层和输出层之间的偏置向量:

$$(W, b^{(1)}, b^{(2)}) = \{(W^{(k)}, b^{(k,1)}, b^{(k,2)}) \mid (k = 1, 2, \dots, K)\}.$$

也都是多层的. 自然地, 自编码网络也可以有多个隐藏层, 以实现输入数据的一种多层数据再表达. 下面我们给出多隐藏层自编码网络算法框架 (见算法 6).

上述卷积自编码网、稀疏自编码、降噪自编码和可收缩自编码网络都可以建成类似的多隐藏层自编码网络的形式, 在此不再赘述. 多隐藏层自编码网络模型中, 目标函数包含了所有的参数 $(W^{(k)}, b^{(k,1)}, b^{(k,2)})$ ($k = 1, 2, \dots, K$), 用梯度下降等传统算法训练参数, 计算量巨大, 一般与神经元数目的平方成正比. 虽然在神经科学中, 关于对等反向传播的“大脑皮质内从高阶区域向低阶区域的反馈信号”结论还存在争论, 但是 Rumelhart 等^[20]提出了具有范式转移的反向传播机制, 利用链式法则求梯度的方法训练参数, 在此基础上提出了反向传播算法, 把计算量下降到与神经元数目成正比. 通过在神经网络里增加多个隐层, 反向传播算法同时也解决了感知器无法解决的异或门难题. 反向传播算法迭代地处理训练元组数据集, 将每个元组的网络预测与实际知道的类标号相比较进行学习, 对于每个训练样本, 修改权重使得网络预测和实际类之间的均方误差最小. 这种修改“反向”进行, 即由输出层, 经由每个隐藏层, 到第一个隐藏层 (所以称作反向传播). Rumelhart 等^[20]认为, 这种方法似乎并不是大脑学习的一种合理模型. 然而, 将这个方法应用在各种各样的任务上后, 通过权重空间的梯度下降, 可以构建出很有趣的内部表征. 这表明, 很值得在神经网络中找出更有生理可行性的方法来进行梯度下降. Hinton 的博士后 LeCun 等^[31]用美国邮政系统提供的近万个手写数字的样本, 通过反向传播算法训练神经网络系统, 在独立的测试样本中错误率低至 5%, 达到实用水准.

2.4.7 深度栈式 (多层) 自编码方法

另外一种多层的实现方法是上述多个独立的单隐藏层的自编码网络串联在一起, 独立完成每一步编码和解码过程后, 再去掉中间的重建层, 得到深度栈式 (多层) 自编码方法, 如图 7 所示.

图 7 中, x 是输入层的数据, $y^{(1)}$ 是第一个单隐藏层自编码网络的输出, 以此类推, $y^{(K)}$ 是第 K 个单隐藏层自编码网络的输出, 也就是最终适合后端学习任务的数据再表达或者说是特征. 多隐藏层自编码方法只包含一个自编码网络 (含多个隐藏层), 而深度栈式自编码方法包含了多个独立的单

图 7 (网络版彩图) 深度自编码网络结构图

隐藏层的自编码网络. 要实现这种多层的数据再表达, 也要求出每一个独立的自编码网络输入层和隐藏层之间的权值矩阵 $W^{(k)}$ 、隐藏层和输出层的偏置向量 $b^{(k,1)}$ 和 $b^{(k,2)}$, 其中 K 是串联的自编码网络的层数, 深度栈式自编码方法是分别建立优化模型求解这些参数. 但是, 直接用反向传播的算法训练这样的深度栈式自编码网络同样易出现“梯度消失”或者“梯度爆炸”等现象. 为了解决这样的问题, Hinton 和 Salakhutdinov^[5] 提出了一种新的训练方式, 这种训练方式分为两个阶段: 逐层预训练和微调. 简单地说, 逐层预训练就是一层一层 (layer by layer) 独立训练, 且每一层都只关心自己的效果, 让当前层误差最小 (greedy). 这相当于每一层求解一个优化模型, 大大降低了计算量, 并在一定程度上消除了“梯度消失”或者“梯度爆炸”带来的问题, 这也就是深度栈式自编码方法与多隐藏层自编码方法的重要区别. 微调就是根据后端的任务, 再对参数进行一些微调. 正是这种训练方式的提出, 才导致深度学习的第三次兴起.

从以上的讨论可以看出, 由多层感知器模型建立的人工神经网络模型, 是一种平行分布式加工系统, 它直接模仿大脑生物神经元的信息传递和逐层处理的机制, 实现人工智能. 但是, 此类模型中的参数求解一般是数据驱动 (或者称为资料驱动) 的, 对于更复杂的“序列”信息处理, 例如逻辑推理, 需要有反馈回路, 上述简单的模型无法模拟. 视觉皮层中就存在着大量的反馈连接, 卷积神经网络实际上只描述了在视觉腹侧通路在 0–100 毫秒左右的前馈处理机制. 但是整个视觉感知的过程还需要注意力、期望等反馈机制, 并且这样的前馈和反馈共同作用的方式也符合贝叶斯推断 (Bayesian inference) 和预测编码的框架.

对于计算机来说简单的任务, 比如解方程或者数值计算, 对人脑来说是困难的; 然而对于人脑来说很简单的任务, 如认出你的父母、老师、同学和朋友, 对计算机来说是困难的. 原因是神经系统是动物在进化过程中寻找到的对特定任务的一种最优实现, 其中“突触”就是一个简单完美的设计, 神经元巧妙地利用其自身的物理特性实现某个特定的计算任务. 从硬件设计的角度来看, 通用的电路在特定任务上的性能或功耗肯定比特定任务设计的专有电路差. 但是, 大多数人工神经网络却运行在标准计算机上, 相当于将神经元一般化, 而非对特定任务进行最优实现. 所以对于硬件电路的设计者来说, 应该设计能够实现特定任务特性的单个神经元. 另外, 现在的计算水平, 很难真正模拟大脑如此多的计算单元和连接 (一百四十亿个以上的计算单元和一百万亿个以上的连接). 所以, 我们认为, 当前建立在多层感知器模型上的人工神经网络模型, 很难真正实现人脑的“智能”.

3 基于认知心理学的人工智机理解释与数学方法

上一节我们从人脑的生物结构和工作机制研究了人类的认知过程, 并通过直接模仿, 建立了多层人工神经网络模型. 实际上, 从认知心理学的角度研究人类的认知过程, 对实现真正意义下的“智能”可能更为重要.

认知心理学是 20 世纪 50 年代心理学的一个重要研究方向. 从广义说, 认知心理学主要研究人类

的高级心理过程, 这种心理过程一般是指人们的认识过程, 主要包括注意、知觉、表象、记忆、创造性、问题解决、言语和思维等. 从狭义说, 认知心理学相当于当代的信息加工心理学, 也就是采用信息加工论的观点对认知过程进行研究. 现代认知心理学发展到今天, 表现为信息加工论认知心理学、联结主义认知心理学和生态认知心理学三种理论形态.

信息加工论认知心理学在 20 世纪 50 年代中期被提出, 其主要代表人物有纽厄尔 (A. Newell)、西蒙 (H. A. Simon) 和奈瑟尔 (U. Neisser) 等人. 它以“心理活动像计算机”为隐喻, 用信息加工的观点看待人的认知过程, 认为人的认知过程是一个接受、加工、贮存和输出信息的过程. 由于这种观点以符号操作为基础, 通过符号的串行加工方式建立心理模型, 故又称之为符号论认知心理学.

20 世纪 80 年代以来, 联结主义认知心理学开始复兴. 在联结主义心理学看来, 人脑不能简单地等同于计算机, 符号加工与真实的人类心理加工存在很大差距. 它提出以大脑隐喻代替计算机隐喻, 把大脑视为生物的神经网络, 以平行分布加工代替串行加工. 联结主义认知心理学试图构建一个更接近于神经活动的认知模型, 它实质上是模仿生物认知的机理. 因此, 直接模仿生物认知机理的联结主义人工智能学派, 同时也可以通过联结主义认知心理学来解释.

生态认知心理学是 20 世纪中期在西方出现的一种心理学改造运动, 它对西方心理学的方法论和研究思路都产生了深刻的影响, 它提倡在真实环境中研究人 - 环境系统中的心理与行为的一种研究取向, 它认为心理学的研究对象应该是人 - 环境这个统一的系统, 而不是单纯从人的角度来研究人的心理和行为, 提倡在真实环境中研究的方法.

由此可以看出, 从认知心理学的角度解释, 联结主义认知心理学对应于联结主义人工智能学派, 人工神经网络是其具有代表性的一种实现方式; 信息加工论心理学对应于符号主义人工智能学派, 自动推理系统是该学派的一种具体实现方式; 人 - 环境系统中的心理与行为的生态认知心理学对应于行为主义人工智能学派, 而且强化学习是行为主义人工智能学派的一种重要的实现方式.

在 2.1 小节中我们给出了基于认知生物学的人工智能的建模与解释, 它实际上还可以看成是依据联结主义认知心理学, 对人工智能的建模与解释, 我们已经进行了讨论. 下面分别讨论信息加工论心理学对应的符号主义人工智能学派、人 - 环境系统中的心理与行为的生态认知心理学对应的行为主义人工智能学派, 给出这两个学派的机理解释与实现的数学方法.

3.1 信息加工论心理学与符号主义人工智能

信息加工论心理学是在人工智能之父图灵的工作基础上发展起来的一个心理学的学派. 反过来, 信息加工论心理学的发展又促进了人工智能的发展. 信息加工论心理学与符号主义人工智能密切相关. 符号主义人工智能的解释与实现的方法主要是逻辑学, 特别是数理逻辑. 人工智能的产生与发展初期与逻辑学的发展密不可分. 逻辑学为人工智能的研究提供了根本观点与方法, 而逻辑方法则是人工智能研究中的主要形式化工具^[32,33].

逻辑学是一门研究思维形式及思维规律的科学. 从 17 世纪莱布尼兹 (G. W. Leibniz) 提出数理逻辑以来, 随着人工智能发展的需求, 各种各样的逻辑也随之产生. 一般而言, 逻辑学可分为经典逻辑、非经典逻辑和现代逻辑. 经典逻辑与模态逻辑都是二值逻辑; 多值逻辑就是具有多个命题真值的逻辑, 是向模糊逻辑的一种逼近; 模糊逻辑是处理具有模糊性命题的逻辑; 概率逻辑是研究基于逻辑的概率推理^[34].

图 8 (网络版彩图) 概率图模型的有向和无向两种拓扑结构

人工智能诞生的初期, 逻辑推理占据了统治地位. 1963 年, 纽厄尔和西蒙等人编制的“逻辑理论机”, 是一个数学定理证明的程序. 在此基础上, 纽厄尔和西蒙编制了通用问题求解程序, 开拓了人工智能“问题求解”这一领域. 长期以来, 经典数理逻辑 (包括形式逻辑与数理逻辑) 的研究和应用在人工智能中一直处于主导地位. 经典数理逻辑只是数学化的形式逻辑, 只能满足人工智能的部分需要. 这两种逻辑都存在局限性, 无法解决面临的一些应用问题, 从而出现了一些新的逻辑学派. 人工智能发展了用数值的方法表示和处理不确定的信息, 即给系统中每个语句或公式赋一个数值, 用来表示语句的不确定性或确定性. 人们把这些新的逻辑学派称为非经典逻辑, 其相应的推理方法则叫作非经典推理^[35]. 与之相对应, 把传统的逻辑学派及其推理方法称为经典逻辑和经典推理. 贝叶斯公式就是非经典逻辑推理的代表: 设 $B_1, B_2, \dots, B_n$ 为样本空间 Ω 的一个划分, A 是一个事件, 且 $P(A) > 0, P(B_i) > 0, i = 1, 2, \dots, n$, 则有

$$P(B_i | A) = \frac{P(B_i)P(A | B_i)}{\sum_{j=1}^n P(B_j)P(A | B_j)} \quad (i = 1, 2, \dots, n). \quad (3.1)$$

概率图模型是一类用图的形式表示随机变量之间条件依赖关系的概率模型, 是概率论与图论的结合. 概率图模型如图 8, 主要分为两种, 即贝叶斯网络 (Bayesian network) 和 Markov 网络. 把 Markov 随机场映射到无向图中, 此无向图中的节点都与某个随机变量相关, 连接着节点的边代表与这两个节点有关的随机变量之间的关系. 无向图模型也叫 Markov 随机场或 Markov 网络, 有向图模型也叫贝叶斯网络或信念网络. 1985 年, J. Pearl 提出了贝叶斯网络, 即有向无环图模型, 它是一种模拟人类推理过程中因果关系的不确定性概率图模型, 其网络拓扑结构是一个有向无环图.

在人工智能的数据再表达中, 概率图模型可以很好地表示实体之间关系, 而且可以很容易导出相应的概率公式. 在人工智能的推理中, 当我们得到相关的信息和观测数据之后, 就可以很容易利用概率图导出的计算公式进行推理, 给出判别结果. 在人工智能的学习中, 可以利用专家经验和样本数据, 对概率图模型的相关参数进行估计, 效率更高并且不需要估计冗余的参数. 对于朴素贝叶斯模型来说, 特定的类别样本在不同的特征属性上具备不同的数据表征, 而且特征之间有着独立性假设, 即特征之间是无关联的. 对于隐 Markov 模型来说, 隐状态之间满足 Markov 性假设, 即当前状态只和前

一状态有关, 而与历史状态和后续状态无关; 另外, 还假设特征之间也是相互独立的, 且特征只由当前隐状态产生. 对于最大熵 Markov 模型来说, 与隐 Markov 模型相比, 每个隐状态只依赖前一状态和当前观测, 而且每组这样三者的组合都是独立的, 且采用最大熵模型建模. 对于条件随机场模型来说, 当前状态依赖于上下文状态和上下文观测, 所以没有独立性假设, 可以自由搭配特征以及标注.

人工智能仅靠贝叶斯网络是不够的, 因为它无法形成任意复杂的结构. 只有将逻辑判断与贝叶斯网络结合在一起, 概率推断才能发挥其真正的威力.

常识推理是一种非单调逻辑, 即人们基于不完全的信息推出某些结论, 当人们得到更完全的信息后, 可以改变甚至收回原来的结论. 非单调逻辑可处理信息不充分情况下的推理. 20 世纪 80 年代, 非单调逻辑系统主要包括赖特 (R. Reiter) 提出的缺省逻辑、麦卡锡 (J. McCarthy) 提出的限定逻辑、麦克德莫特 (D. McDermott) 和多伊尔 (J. Doyle) 建立的非单调逻辑推理系统、以及摩尔 (R. C. Moore) 提出的自认知逻辑. 常识推理也是一种可能出错的不精确的推理, 即容错推理^[36]. 在人工智能的发展中, 多值逻辑和模糊逻辑也已经被引入其中, 处理模糊性和不完全性信息的推理. 多值逻辑的三个典型系统是克林 (S. C. Kleene)、卢卡西维兹 (J. Lukasiewicz) 和波克万 (D. Bochvar) 的三值逻辑系统. 20 世纪 20 年代, 卢卡西维兹开创了模糊逻辑的研究, 1972 年, 扎德 (L. A. Zadeh) 提出了模糊推理的关系合成原则, 现有的绝大多数模糊推理方法都是扎德的关系合成规则的变形或扩充 (参见文献 [37]).

1977 年, 吴文俊 (参见文献 [38]) 在初等几何定理的机械化证明方面首先取得成功, 他提出了几何定理机器证明的吴方法. 此后, 吴文俊相继提出微分几何的定理机械化证明方法、方程组符号求解的吴消元法和全局优化的有限核定理, 建立了数学机械化体系. 他不仅建立了数学机械化的基础, 而且将这一理论应用于多个高技术领域, 解决了曲面拼接、机构设计、计算机视觉、机器人等高技术领域核心问题. 吴方法主要分两步, 第一步是问题代数化, 即引进坐标, 然后把需要证明定理中的假设与终结部分都用坐标间的代数关系来表示, 他所考虑的定理局限于这些代数关系是多项式等式关系的范围. 第二步是通过代数假设的多项式关系把终结多项式中的坐标逐个消去, 如果消去的结果为零, 则定理证明正确, 否则再进一步检查. 吴方法中的严格代数化是一个非常困难的问题, Gao 等^[39]突破的微分结式理论, 系统地将这种机器证明方法从代数范畴推广到微分范畴.

由于人工智能要模拟人的智能, 它的难点不在于人脑所进行的各种必然性推理, 而是最能体现人的智能特征的能动性、创造性思维, 这种思维活动中包括学习、抉择、尝试、修正、推理诸因素. 例如, 选择性地搜集相关的经验证据, 在不充分信息的基础上做出尝试性的判断或抉择, 不断根据环境反馈调整、修正自己的行为, 由此达到实践的成功. 于是, 逻辑学需要比较全面地研究人的思维活动, 并着重研究人的思维中最能体现其能动性特征的各种不确定性推理, 由此发展出的逻辑理论也将具有更强的可应用性.

3.2 基于生态认知心理学的行为主义人工智能

从另外一个角度, 人工智能可以不关心神经系统到底是如何实现某种功能的, 而只需要从行为的角度观察得到启发, 从而模仿并实现人工智能. 这就是行为主义人工智能学派的基本出发点. 该观点认为人工智能与神经科学更多的交叉是在于行为或计算层面以及算法层面, 而不是直接模仿和实现层面.

图 9 (网络版彩图) 强化学习的概念模型^[40]

信息加工论心理学和联结主义认知心理学都是以元素分析为基础, 而生态认知心理学的基本原则是交互作用原则, 强调心理、行为 and 环境的交互作用是认知的根本. 被传统心理学所分离的两个方面的东西, 如行为和心理、行为和环境, 在生态认知心理学的本体论上都认为是相互依赖和相互作用的对子, 因而在认识论和方法论上, 都不能对它们进行分离地研究和解释. 因此, 从方法论上, 生态认知心理学把交互作用原则作为首要原则运用到认知心理学中. 强化学习就是基于生态认知心理学的交互作用原则而设计的一种机器学习方法.

3.2.1 强化学习的人工智能建模与数学实现方法

强化学习强调如何基于环境选择行动, 以取得最大化的预期收益. 其思想来源于认知心理学中的行为主义理论, 即智能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. 其学习过程可以描述为^[40]: (1) 在每个时刻智能体与环境交互得到一个高维度的状态表示, 并利用深度学习等方法来感知观察, 以得到抽象或具体的状态特征表示; (2) 基于预期回报来评价各动作的价值函数, 并通过合适的策略将当前状态映射为相应的动作; (3) 环境对此动作做出反应, 并得到下一个观察. 通过不断循环以上过程, 最终就可以得到实现目标的最优策略. 图 9 描述了强化学习的概念模型.

强化学习通常可以建模为一个 Markov 决策过程^[41], Markov 决策过程可以用一个多元组 $(S; A; P; R; \gamma)$ 来表示, 其中 S 是决策过程中的状态集合; A 是决策过程中的动作集合; P 是状态之间的转移概率; R 是采取某一动作从当前状态到达下一状态后的回报值 (也可看作奖励); γ 是折扣因子. 下面我们给出一个例子来说明这个多元组的具体含义.

图 10 是一个机器人在网格世界中执行导航任务, 其中黑块代表一个障碍物. 假设我们期望机器人到达格子 $(4, 3)$, 但是又要避开格子 $(3, 1)$. 机器人可以到达 11 个网格中任何一个, 所以机器人共有 11 个状态, 即: $S = \{(1, 1), (2, 2), \dots, (4, 1), (4, 2), (4, 3)\}$; 机器人可做的动作有向上、向下、向左、向右, 即: $A = \{U, D, L, R\}$; 概率 P_{sa} 表示机器人在 s 格子上执行 a 动作到达另外一个格子上的转移概率, 如果机器人撞墙或者走到不是相邻的格子时, 其概率为 0. 假设机器人当前的状态是 $(3, 2)$, 则 $P_{(3,2)U}(3, 3) = 0.6$ 表示机器人执行向上的动作从状态 $(3, 2)$ 转移到状态 $(3, 3)$ 的概率是 0.6, $P_{(3,2)D}(3, 1) = 0.2$ 表示机器人执行向下的动作从状态 $(3, 2)$ 转移到状态 $(3, 1)$ 的概率是 0.2, $P_{(3,2)L}(2, 2) = 0.1$ 表示机器人执行向左的动作从状态 $(3, 2)$ 转移到状态 $(2, 2)$ 的概率是 0.1,

图 10 (网络版彩图) 机器人导航状态

$P_{(3,2)R}(4,2) = 0.1$ 表示机器人执行向右的动作从状态 $(3,2)$ 转移到状态 $(4,2)$ 的概率是 0.1, 且满足自当前的状态是 $(3,2)$ 出发到达其他所有状态的概率和为 1; 回报或者奖励函数 $R: S \times A \rightarrow \mathbb{R}$, 我们期望到达的状态给予奖励, $R(4,3) = +1$, 需要避开状态 $R(3,1) = -1$, 其他状态 $R(s) = -0.03$, 其他状态 s 设置为 -0.03 表示机器人消耗能量的付出, 目的提醒机器人节约时间, 尽快到达目的地.

强化学习关注的不仅仅是当前的回报, 状态 s_t 到 s_{t+1} 会有一个回报, s_{t+1} 到 s_{t+2} 同样会有一个回报, 以此类推. s_t 对 s_{t+1} 的影响很大, 但对于 $s_{t+2}, s_{t+3}, \dots, s_t$ 的影响会越来越小, 所以引入折扣因子 γ 减小后面状态的回报对当前状态衡量的影响, 提出了累计回报函数:

$$G_t = R_{t+1} + \gamma R_{t+2} + \dots = \sum_{k=0}^{\infty} \gamma^k R_{t+k+1}. \quad (3.2)$$

状态动作值函数 (action-value function) $Q(s, a)$ 表示智能体从状态 s 出发, 执行动作 a 后再使用策略 π 的累计奖赏:

$$Q(s, a) = E[G_t \mid S_t = s, A_t = a, \pi]. \quad (3.3)$$

状态动作值函数遵循 Bellman 方程:

$$Q(s, a) = E_{s' \sim s} \left[R + \gamma \max_{a'} Q(s', a') \mid s, a \right]. \quad (3.4)$$

最优状态动作值函数 $Q^*(s, a)$ 指的是在所有的策略中产生的状态动作价值函数中最大的那个函数:

$$Q^*(s, a) = \max_{\pi} E[G_t \mid S_t = s, A_t = a, \pi]. \quad (3.5)$$

强化学习通过 Q 值来选取能够获得最大收益的动作, 一般通过 Bellman 方程迭代求解:

$$Q_{i+1}(s, a) = E_{s' \sim s} \left[R + \gamma \max_{a'} Q_i(s', a') \mid s, a \right]. \quad (3.6)$$

从而得到最优策略

$$\pi^* = \arg \max_{a \in A} Q^*(s, a).$$

然而对于实际问题而言, 状态空间一般很大, 使用迭代方法求解 Q 值计算量太大, 一般不可行, 因此通常使用线性和非线性函数近似表示状态动作值函数.

求解算法有值函数学习 (Q-learning)^[42]、深度 Q- 网络 (deep Q-learning net)^[43]、行动者 - 评论家 (actor-critic) 框架^[44]、深度确定性策略梯度 (deep deterministic policy gradient, DDPG)^[45]、近似策略梯度 (proximal policy optimization algorithms, PPO)^[46]、信赖域策略优化 (trust region policy optimization, TRPO)^[47] 等, 而基本思路就是建立设计不同的优化算法进行求解.

图 11 多智能体系统的概念模型

3.2.2 行为主义人工智能中的多智能体建模与数学实现方法

多智能体系统是由一系列能够智能运行并相互作用的智能体构成, 内部的各个智能体之间通过相互通信、合作、竞争等方式, 完成单个智能体不能完成的、大量而又复杂的工作, 通过相应的组织规则和信息交互协议完成特定任务的一类复杂系统. 多智能体系统建模是一个由概念模型、数学模型和计算机模型组成地完整建模过程, 是一个复杂的过程, 往往要进行多期进化博弈. 微观层面是考虑单智能体个体成本收益 (并同时考虑全体博弈互动和部分博弈互动的交互), 宏观层面上考虑异构的整体收益 (且同时考虑全局信息交互和局部信息交互的更替), 并通过多智能体系统 (特别是交互意愿变量的引入) 实现微观互动 (博弈行为) 和宏观涌现 (网络结构) 之间的双向反馈和动态交互.

在图 11 中, 这些智能体可以是同种类型也可以是不同类型的, 智能体之间相互作用一般为合作关系的描述, 主要有完全合作、完全竞争和部分合作关系等. 智能体在各自的当前状态通过与外界环境的交互, 根据需要的合作关系获得各自的预期回报, 做出下一状态相应的行为反应. 对于整个系统来说是与环境交互考虑获得整体利益最大的情况下做出下一状态的宏观行为预测.

在多智能体系统中, 每个智能体通过与环境进行交互获取奖励回报值 (reward) 来学习改善自己的策略, 从而获得该环境下最优策略的过程就多智能体强化学习. 多智能体强化学习的数学模型可以刻画为一个 Markov 博弈模型^[48]:

$$(A, X, \{U_i\}_{i \in A}, f, \{\rho\}_{i \in A}), \quad (3.7)$$

其中 $A = \{1, 2, \dots, n\}$ 为 n 个智能体, X 是状态空间, $\{U_i\}$ 是动作空间, 联合动作集合 $U = \times_{i \in A} U_i$, $f: X \times U \times X \rightarrow [0, 1]$ 是转移概率分布, $\rho_i: X \times U \times X \rightarrow \mathbb{R}$, $i \in A$ 是智能体 i 的奖励函数.

定义 $V_i(\pi_1, \dots, \pi_i, \dots, \pi_n)$ 为智能体 i 在关联策略 $(\pi_1, \dots, \pi_i, \dots, \pi_n)$ 下的期望奖励. 例如, 如果将智能体之间的相互作用设为完全竞争型 (对抗), 则每一个智能体自己的目标是最大化其获得的奖励值、极小化其他智能体的收益; 但是 $\max V_1, \dots, \max V_i, \dots, \max V_n$ (某方智能体利益最大化) 并不能代表多智能体就能够完成复杂任务, 即: 局部最优不等于全局最优.

如果一个关联策略 $(\pi_1^*, \dots, \pi_i^*, \dots, \pi_n^*)$ 满足

$$V_i(\pi_1^*, \dots, \pi_i^*, \dots, \pi_n^*) \geq V_i(\pi_1^*, \dots, \pi_i, \dots, \pi_n^*), \quad \forall \pi_i \in \Pi_i, \quad i = 1, 2, \dots, n, \quad (3.8)$$

则为一个纳什均衡 (Nash equilibrium). 纳什均衡就是所有智能体的一个联结策略, 在纳什均衡处, 对于所有智能体而言都不能在仅改变自身策略的情况下, 来获得更大的奖励. 根据博弈论相关内容, 不管是静态博弈还是动态博弈, 纳什均衡不等同于全局最优. 因此对于多智能体而言, 如何让多智能体系统获得整体最优利益是研究的重点. 深度强化学习的多智能体算法是多智能体系统信息交互及求解的主要方法. 多智能体决策一般分为集中式决策和分布式决策. 集中式决策指的是控制算法通常把整个多智能体系统的协作机制看成一个整体, 通过一个全局性的中央单元对所有单元进行统一决策, 多智能体转变为单智能体, 如 CommNet^[49]; 分布式决策指的是分布式控制算法将各个智能体划分为单个主体, 每一个主体独立处理环境状态信息, 并做出行为决策, 极大化每一个智能体的回报, 如 MADDPG (multi-agent deep deterministic policy gradient)^[50]. 但是多智能体算法面临很多问题和挑战: 不完全信息问题 (时间和空间)、输出空间维度爆炸问题和动态环境博弈问题等, 我们可以从局部最优与全局最优、大规模多智能体的自适应通信机制、回报设计、数据采样效率和复杂决策层次分解等问题展开更深入的研究.

3.3 基于格式塔完形心理学的人工智能解释与数学实现方法

格式塔心理学 (Gestalt psychology)^[51] 又叫完形心理学, 是西方现代心理学的主要学派之一. 格式塔心理学的主要观点有三个: (1) 关于心理学研究的对象, 格式塔学派认为只有直接经验 (意识) 与行为; (2) 格式塔心理学强调整体性, 特别是重视经验和行为的整体性, 提出整体不等于甚至大于部分之和; (3) 格式塔心理学主张以整体的动力结构观, 观察研究学习、回忆、志向、情绪、思维、运动等各种心理现象. 格式塔心理学的理论体系反对美国构造主义心理学的元素分析, 注重完形的整体组织, 它与生态认知心理学有许多相似之处, 同时它也反对古典心理学派的行为.

格式塔心理学受到物理学中的“场论”的影响. 物理学中把某个物理量在空间的一个区域内的分布称为场, 如温度场、密度场、引力场、电场、磁场等, 场论是物理学发现的一种全新结构, 而不是分子间引力和斥力的简单相加. 物理学上经典场论还包括量子场论, 主要是量子力学场的理论. 格式塔心理学借鉴“场论”, 对人类的心理现象和机制做出创新性的诠释. 根据场论的研究成果, 格式塔心理学认为心理是一个整体, 整体并不是部分的简单相加. 每个整体都具有自身独特的意义, 整体的性质决定部分的性质, 部分的性质则有赖于它在整体中的关系、位置和作用. “整体观”^[52] 贯穿于格式塔心理学体系之中. 格式塔心理学体系中的知觉以“整体观”、“部分的性质依赖于在整体中的关系、位置和作用”作为理论指导, 通过经验和环境, 根据相似性、接近性、闭合性、连续性等原则组织成了有意义的完形. 有意义的完形是格式塔心理学理论体系的概念模型, 此模型的构成, 包括经验、环境和原则是上述理论观点的具体表现.

格式塔心理学中的学习理论是西方学习理论中最重要的学说之一, 它弥补了行为主义和联结主义学习理论的不足与缺陷, 逐渐得到了心理学界的认可, 并在机器学习领域得到应用. 格式塔心理学关于创造性思维的研究用计算机实现, 可以模拟人类解决问题, 引起了人们的关注. 格式塔心理学对现代认知心理学发展起到了重要的作用, 被认为是现代认知心理学的先驱. 格式塔学派对认知心理学的产生和发展的促进作用主要表现在以下几个方面^[51]: (1) 格式塔学派的一些实验及其思想观点

图 12 低维流形示意图^[53]

构成了现代认知心理学产生与发展的基础, 有些已经成为现代认知心理学的基本观点和重要组成部分, 比如格式塔学派经典的知觉研究、在知觉组织原则指导下的记忆研究、富有开创性的问题解决领域等. (2) 格式塔学派重视对人的内部高级心理过程的研究, 强调认知活动的积极性和能动性, 促进了行为主义向认知方面的转化, 为现代认知心理学打破行为主义“环境决定论”的牢笼提供了有力武器. (3) 格式塔心理学强调经验和行为的整体性, 主张从整体的动力结构观来研究心理现象. 现代认知心理学受格式塔心理学整体观的影响, 也强调对人的认知过程进行整体的综合分析. (4) 在研究方法上, 认知心理学也受到格式塔心理学的影响. 认知心理学既继承了实验心理学定量研究的传统, 吸收了计算机科学的研究成果, 又充分吸收了格式塔心理学以现象学为基础的研究, 由此形成了一套比较完整的研究方法, 即实验、模拟、理论分析相结合的研究方法. 格式塔心理学的研究成果在人工智能领域有一些成功的应用, 比如本文将要讨论的流形学习, 但是总的来说, 成功的应用还比较少. 这也是未来人工智能发展的一个重要方向, 比如在人工智能, 特别是机器学习的优化模型中, 正则项可以解释为格式塔完形中相似性、接近性、闭合性、连续性这几大原则的数学实现方法, 如何构造更适合上述原则的数学模型就是人工智能一个重要研究内容.

3.3.1 流形学习的解释与数学实现方法

格式塔心理学家做过一个实验^[51]: 放一个形状不规则的积木, 同时给出几个不同旋转角度的形状, 其中有一个或多个是该积木旋转后的真实图像, 也有不是该积木旋转后的真实图像. 然后, 让儿童自己去判断和识别哪些是原来的积木旋转过来的. 儿童慢慢都能学会如何处理这种旋转, 并能做出准确判断. 该现象说明人的大脑能对每一个见到的物品进行自动的旋转. 认知心理学对记忆给了一种原型说的可能解释, 即某个概念都会以原型的形式存储在记忆中. 2000 年, Seung 和 Lee 发表在 *Science* 上的论文^[53]认为: 人是以流形方式完成记忆的. 另外, 我们也可以从空间张成的角度解释这种现象. 人眼里有上亿个视神经元, 客观世界的内在维度可以张成的空间比上亿维神经元张成的空间要小得多, 而输入进来的信息是通过视神经元识别, 就是高维度空间中一个超曲面, 也称为低维流形, 称其为嵌套在高维空间 (视神经元空间) 的低维流形^[54], 见图 12. 格式塔心理学与经典的原型学说的主要不同之处在于, 格式塔心理学假设用于记忆的离散吸引子能被替换成连续吸引子, 于是存储在大脑里的原型便不再是一个点, 如图 12(a), 而可能是一条曲线、一个曲面甚至超曲面, 如图 12(b).

视觉看到的任何内容, 都会从不同途径收敛到这个连续吸引子上, 并在此吸引子上实现对不同角度和不同内在维度的外推. 这在某种意义上不但解释了记忆的方式, 而且还解释了自动旋转问题. 因

图 13 (网络版彩图) 流形维数简约和数据可视化的流形示意图^[55]

此, 流形学习可以解决格式塔心理学中的“旋转不变性”问题.

让计算机实现类似的自我旋转或推理能力, 也许就往人工智能方向迈进了一大步. 自然图像中的内在控制变量是比较少的, 如果希望计算机能对不同角度的图像有合理的推测功能, 还原格式塔心理学中的旋转不变性, 找到高维空间中的流形结构, 并依照它的规则来推测, 就能够比较简单地完成这个能力. 数据形成的流形可能具有各种各样复杂结构, 要想利用经典的欧氏距离来解决问题, 可行的方案之一就是把它摊平或拉平, 这样待分析的数据所处的空间就是欧氏空间, 从而就引出了流形建模和学习的概念.

流形学习方法^[53], 自 2000 年被首次提出以来, 已成为信息科学领域的研究热点. 无论是理论还是应用, 流形学习方法都具有重要的研究意义. 假设数据是均匀采样于一个高维欧氏空间中的低维流形, 流形学习就是从高维采样数据中恢复低维流形结构, 即找到高维空间中的低维流形, 并求出相应的嵌入映射, 以实现维数简约或者数据可视化, 见图 12. 流形学习是从观测到的现象中寻找事物的本质, 找到产生数据的内在规律. 流形学习算法的主要思想是能够学习高维空间中样本的局部邻域结构, 并寻找一种子空间能够保留这种流形结构, 使得样本在投影到低维空间后, 得到比较好的局部近邻关系.

事实上, 基于统计的深度学习之所以取得了很大的成功, 其中最主要的原因是有如下基于流形的两个数据分布规律: (1) 流形分布律 (law of manifold distribution): 在高维背景空间中, 特定类的真实数据分布靠近某个低维流形; (2) 聚类分布律 (law of cluster distribution): 同一类数据中的不同子类, 对应于流形上不同的概率分布, 并且这些概率分布之间的距离足够远, 使得这些子类可以被区分.

流形学习首先要构造流形上样本点的局部邻域结构, 然后用这些局部邻域结构将样本点全局地映射到一个低维空间, 即流形嵌入. 各种方法之间的不同之处主要是构造的局部邻域结构不同以及利用这些局部邻域结构来构造全局低维嵌入方法的不同. 流形嵌入问题, 即如何来描绘这个流形、如何获取这个流形、如何保证逼近的精度, 这些也正是深度学习的第一个主要任务: 学习流形的结构, 计算流形嵌入. 数学上, 假设给定嵌入在背景空间中的流形, 我们将流形上的一个开邻域同胚映射到参数空间, 这一过程被称为是流形的局部参数化. 用深度学习的语言来讲, 就是学习编码映射和解码映射, 其中参数域被称为隐空间或者特征空间. 数据流形上的每个点被映射成参数域上的一个点, 如

每张人脸图片被映射成隐空间中的一个点, 称之为这张图片的特征, 或者编码.

给定嵌入在高维欧氏空间中的一个流形, 在流形上稠密采样, 通过采样点, 可以重构分片线性流形, 用以逼近初始流形, 如图 13 中的 (a) 和 (b). 如在数字几何中, 用三维扫描仪扫描一张人脸曲面, 得到的是稠密点云, 然后我们对点云计算三维背景空间的 Delaunay 三角剖分, 得到一张分片线性的曲面 (三角网格), 这张分片线性的曲面就是真实光滑人脸曲面的离散逼近. 逼近的精度, 取决于采样的密度, 理论上我们一般采用网格采样. 采样条件如下: 曲面上任意一个半径为给定阈值的测地圆盘内部, 至少有一个采样点; 任意两个采样点之间的距离不小于给定的阈值. 根据采样定理, 合适采样可以保证重构的离散曲面收敛于原来光滑曲面, 这里收敛是指 Hausdorff 距离收敛、测地距离收敛、曲率测度收敛和 Laplace-Beltrami 算子收敛.

深度学习也采取了同样的方法, 在数据流形上进行稠密采样, 然后重构分片线性流形, 用以逼近数据流形. 理论上的采样条件同样适用于深度学习理论, 但是我们目前几乎没有看到这方面的研究工作. 在深度学习模型之中, 用流形的参数表示来描绘流形, 这种参数表示就是解码映射, 一般由一个卷积神经网络来表示. 通常我们用 ReLU 卷积神经网络, 因此参数表示实际上就是分片线性映射.

另外, 流形学习还可以看成是非线性的主成分分析. 主成分分析得到的是一个线性子空间而舍弃了正交于子空间外的信息, 而流形学习得到的是一个非线性子空间而舍弃了流形外的信息. 流形学习的目的是维数缩减, 从而寻找到数据更本质的内在规律, 即数据分布的低维流形. 和一般的降维学习一样, 流形学习是把一组在高维空间中的数据在低维空间中再表达. 不同之处是, 在流形学习中假设所处理的数据采样在一个潜在的流形上, 或者说对于这组数据存在一个潜在的流形.

流形学习可以建成如下一般形式的流形上的优化模型:

$$\begin{aligned} \min \quad & f(Y) + h(Y) \\ \text{s.t.} \quad & \frac{1}{m} Y^T Y = I, \\ & Y \in \mathbb{R}^{n \times d}, \end{aligned} \quad (3.9)$$

其中 $f(Y)$ 为损失函数, 一般是光滑函数; $h(Y)$ 为正则项, 一般是非光滑函数. 例如, 在局部线性嵌入 (local linear embedding, LLE) 算法^[56–58] 和 Laplace 特征映射 (Laplacian eigenmaps, LE) 算法^[59] 中, $f(Y)$ 都可以归结为 $f(Y) = \text{tr}(Y^T M Y)$ 的形式. 下面以 LLE 为例说明. LLE 寻找保持局部线性几何的映射, 并假设这样的小块彼此重叠从而能够重建出整个流形, 并且流形在局部可以近似等价于欧氏空间. 假设有 m 个 n 维样本 $(x^{(1)}, x^{(2)}, \dots, x^{(m)})$, 其中第 i 个样本为 $x^{(i)} = (x_{j1}, x_{j2}, \dots, x_{jn})$, 这 m 个样本组成样本矩阵 $X = (x^{(1)}, x^{(2)}, \dots, x^{(m)}) \in \mathbb{R}^{m \times n}$. 对于第 i 个样本 $x^{(i)}$, 假设其 k 个最近邻样本集合为 $(x^{(i_1)}, x^{(i_2)}, \dots, x^{(i_k)})$. 需要找到 $x^{(i)}$ 与这 k 个最近邻样本集合 $(x^{(i_1)}, x^{(i_2)}, \dots, x^{(i_k)})$ 之间的线性关系, 即求出对应的权重系数矩阵:

$$W = (w^{(1)}, w^{(2)}, \dots, w^{(m)}) = \begin{pmatrix} w_{11} & w_{21} & \cdots & w_{m1} \\ w_{12} & w_{22} & \cdots & w_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ w_{1k} & w_{2k} & \cdots & w_{mk} \end{pmatrix} \in \mathbb{R}^{k \times m}$$

且满足 $\sum_{j=1}^k w_{ij} = 1$ ($i = 1, 2, \dots, m$). 为了求出最好的近似线性表示, 即要求解下述优化问题:

$$\begin{aligned} \min \quad & J(W) = \sum_{i=1}^m \left\| x^{(i)} - \sum_{j=1}^k w_{ij} x^{(i_j)} \right\|_2^2 \\ \text{s.t.} \quad & \sum_{j=1}^k w_{ij} = 1 \quad (i = 1, 2, \dots, m). \end{aligned} \quad (3.10)$$

记 $X^{(i)} = (x^{(i)}, x^{(i)}, \dots, x^{(i)}) \in \mathbb{R}^{n \times k}$, $N^{(i)} = (x^{(i_1)}, x^{(i_2)}, \dots, x^{(i_k)}) \in \mathbb{R}^{n \times k}$, 局部协方差矩阵为 $Z^{(i)} = (X^{(i)} - N^{(i)})^T (X^{(i)} - N^{(i)})$, 则 (3.10) 等价于

$$\begin{aligned} \min \quad & J(W) = \sum_{i=1}^m [(w^{(i)})^T Z^{(i)} w^{(i)}] \\ \text{s.t.} \quad & (e^{(k)})^T w^{(i)} = 1 \quad (i = 1, 2, \dots, m), \end{aligned} \quad (3.11)$$

其中, $e^{(k)} = (1, 1, \dots, 1)^T \in \mathbb{R}^k$. 运用拉格朗日乘子法^[17] 可以求得 (3.11) 的解为

$$w^{(i)} = \frac{(Z^{(i)})^{-1} e^{(k)}}{(e^{(k)})^T (Z^{(i)})^{-1} e^{(k)}} \quad (i = 1, 2, \dots, m). \quad (3.12)$$

设样本矩阵 X 降维后的数据为样本矩阵 $Y \in \mathbb{R}^{m \times d}$ ($d \ll n$), 则需要最小化损失函数

$$\Phi(Y) = \sum_{i=1}^m \left\| y^{(i)} - \sum_{j=1}^k w_{ij} y^{(i_j)} \right\|_2^2.$$

为了得到标准化的低维数据, 一般加入标准化约束条件

$$\frac{1}{m} \sum_{i=1}^m y^{(i)} (y^{(i)})^T = I.$$

为了得到降维后的数据 Y , 即要求解下述优化问题:

$$\begin{aligned} \Phi(Y) = \sum_{i=1}^m \left\| y^{(i)} - \sum_{j=1}^k w_{ij} y^{(i_j)} \right\|_2^2 \\ \text{s.t.} \quad \frac{1}{m} \sum_{i=1}^m y^{(i)} (y^{(i)})^T = I. \end{aligned}$$

将 $W \in \mathbb{R}^{k \times m}$ 扩展成稀疏方阵

$$W^s = (\hat{w}^{(1)}, \hat{w}^{(2)}, \dots, \hat{w}^{(m)}) = (w_{ij}^s) \in \mathbb{R}^{m \times n},$$

令 W^s 第 j 列 $\hat{w}^{(j)}$ 的元素中, 对 $x^{(j)}$ 进行近似线性表示时, 不在 $x^{(j)}$ 的近 k 邻域 $(x^{(i_1)}, x^{(i_2)}, \dots, x^{(i_k)})$ 中的向量对应的系数置为 0, 即

$$w_{ij}^s = \begin{cases} w_{ij}, & i = i_l \quad (i = 1, 2, \dots, m; l = 1, 2, \dots, k; j = 1, 2, \dots, k), \\ 0, & \text{否则.} \end{cases}$$

即要求解优化问题

$$\begin{aligned} \min \quad & \|Y - YW^s\| \\ \text{s.t.} \quad & \frac{1}{m}YY^T = I, \end{aligned} \quad (3.13)$$

其中 $\|Y - YW^s\|$ 是某种矩阵范数, 是数据进行局部线性表示的损失, 这种损失可以是所有样本线性表示的损失的和. 对 (3.13) 进一步整理就可以得到下述等价形式:

$$\begin{aligned} \min \quad & \Phi(Y) = \text{tr}(YMY^T) \\ \text{s.t.} \quad & \frac{1}{m}YY^T = I, \end{aligned} \quad (3.14)$$

其中 $M = (I^{(i)} - \hat{W}^{(i)})^T(I^{(i)} - \hat{W}^{(i)})$, $\hat{W}^{(i)} = \text{diag}(w_{i1}^s, w_{i2}^s, \dots, w_{im}^s)$, 决策变量矩阵 Y 是降维后的数据矩阵.

另外, LE 算法建立的优化模型为

$$\begin{aligned} \min \quad & \text{tr}(Y^TLY) \\ \text{s.t.} \quad & Y^TDY = I, \end{aligned} \quad (3.15)$$

其中决策变量矩阵 Y 是降维后的数据矩阵, L 为输入数据对应图的拉普拉斯矩阵, D 为图的度矩阵. 如果对降维后的数据矩阵 Y 再加上一些其他的限制, 相当于目标函数中加上适当的正则项 $h(Y)$, 就可以得到 (3.9) 一般形式流形优化问题, 其他流形学习的方法也可以推导出 (3.9) 的形式的流形上的优化模型, 只是对应的目标矩阵函数的形式不同.

3.3.2 迁移学习的解释与数学实现方法

动物心理学的开创者、联结主义心理学的建立者和教育心理学体系的创始人爱德华·桑代克设想出一种“相同要素”迁移学习理论^[60], 也就是说, 假如在涉及的两种学习情境中间有共同的要素就会发生迁移, 他把相同要素作为保证迁移的唯一手段. 不同情境下的零样本学习模型和图嵌入模型都属于“相同要素”迁移学习理论的具体实现.

(1) 具有相同特征的零样本学习模型

零样本学习 (zero-shot learning, ZSL) 是人工智能识别方法之一, 是一种基于迁移学习范式的学习方法, 是一类特殊的迁移学习. 简单来说, 零样本学习就是识别从未见过的数据类别, 即训练的分类器不仅仅能够识别出训练集中已有的数据类别, 还可以对于来自未见过的类别的数据进行区分, 见图 14. 零样本学习中, 不管是同类迁移学习 (特征空间和标签空间相同) 还是异类迁移学习 (特征空间和标签空间不同), 它们的一个重要理论基础就是, 存在多个不同空间均能对可区分样本类别的关键特征进行表达, 且多个空间可通过相同要素 (相同要素存在于不同领域, 例如视觉领域 - 特征空间、语义领域 - 语义空间等) 建立映射关系. 因此, 当获取到存在于某个空间的“要素”后, 便可获取其他空间对于“要素”的表示向量, 从而使得训练出来的模型具有迁移性.

为了方便描述零样本学习^[61], 引入以下记号: $\mathcal{S} = \{c_i^s \mid i = 1, 2, \dots, N_s\}$ 为可见类数据集合, 每一个 c_i^s 是一个可见类; 记 $\mathcal{U} = \{c_i^u \mid i = 1, 2, \dots, N_u\}$ 是不可见类数据集合, c_i^u 是一个不可见类, 且满足 $\mathcal{S} \cap \mathcal{U} = \emptyset$; 记 $\mathcal{X} \in \mathbb{R}^D$ 为特征空间, $D^{\text{tr}} = \{(x_i^{\text{tr}}, y_i^{\text{tr}}) \in \mathcal{X} \times \mathcal{S}\}_{i=1}^{N_{\text{tr}}}$ 为可见类标注标签的训练样本集合, $(x_i^{\text{tr}}, y_i^{\text{tr}})$ 为每一个标签样本, x_i^{tr} 为特征空间中的样本, y_i^{tr} 为与 x_i^{tr} 相对应的类标签;

图 14 零样本学习概念示意图

$C = \{x_i^{\text{te}} \in \mathcal{X}\}_{i=1}^{N_{\text{te}}}$, x_i^{te} 是特征空间的测试样本; $Y^{\text{te}} = \{y_i^{\text{te}} \in \mathcal{U}\}_{i=1}^{N_{\text{te}}}$ 为与 x_i^{te} 相对应的标签集合, 即需要被预测出的结果. 零样本学习的目的就是学习到一个分类函数 $f^u(\cdot) : \mathcal{X} \rightarrow \mathcal{U}$ 用来对测试样本 X^{te} 进行分类得到预测类别 Y^{te} . $\mathcal{T} \in \mathbb{R}^M$ 为语义空间, $t_i^s \in \mathcal{T}$ 对应于可见类 c_i^s , $t_i^u \in \mathcal{T}$ 对应于不可见类 c_i^u , $T^s = \{t_i^s\}_{i=1}^{N_s}$ 作为可见类的原型集合, $T^u = \{t_i^u\}_{i=1}^{N_u}$ 作为不可见类的原型集合; $\pi(\cdot) : \mathcal{S} \cup \mathcal{U} \rightarrow \mathcal{T}$ 是原型类函数, 能够获得输入、输出与原型类对应的类标签.

零样本学习的研究分为三种模式^[61], 一种是 CIII (class-inductive instance-inductive setting), 指的是只使用训练实例和可见数据标签集合来训练模型; 一种是 CTII (class-transductive instance-inductive setting), 指的是使用训练实例和可见数据标签集合, 外加不可见数据标签集合来训练模型; 另外一种是 CTIT (class-transductive instance-transductive setting), 指的是使用训练实例和可见数据标签集合, 外加不可见数据标签集合, 对应未标注的测试集合来训练模型. 上述三种模式是对应三种数据选择操作模式, 每种模式下根据映射的语义空间和具体选用基于模型还是实例又有多种实现方法来构建模型. 典型的实现方法有基于语义的嵌入方法—DeViSE 方法^[62], 这是一个基于度量学习解决 ZSL 问题的基线方法; 有基于语义的自编码方法—SAE (semantic autoencoder)^[63], 此自编码方法为解决因为不同域对应于不同特征空间, 会造成严重问题而提出的, 即: 自实例空间学习至语义空间, 再从语义空间学回至实例空间, 缓解了两种不同特征空间的差异性; 另外, Li 等^[64] 提出了基于构建属性语义空间 (attribute semantic space) 的方法, 通过人工构建一个描述图像的属性集合来构建属性语义空间. 下面以 CIII 模式为例, 给出构建语义空间的一个优化模型:

$$\min_w \frac{1}{N_{\text{tr}}} \sum_{i=1}^{N_{\text{tr}}} l_{c_j^s \in \mathcal{S}}(\phi(y_i^{\text{tr}}, c_j^s), \theta(x_i^{\text{tr}}, \pi(c_i^s); w)) + \lambda \mathbb{R}(w), \quad (3.16)$$

其中 $\phi(\cdot, \cdot)$ 是 y_i^{tr} 与 c_j^s 的关系函数, l 是损失函数, $\mathbb{R}(w)$ 是正则项, 对 w 参数进行约束, 可以实现格式塔构建有意义完形的原则, λ 是正则平衡系数. $\theta(\cdot, \cdot; w) : \mathbb{R}^D \times \mathbb{R}^M \rightarrow \mathbb{R}$ 是一个兼容性函数, 其将样本 x_i 与类原型特征 t_i 作为输入, 然后输出样本 x_i 属于 c_j 的概率或者匹配分数. 公式中 l 的优化

目标是最大化样本和与其所属的原型特征间的匹配分数, 同时最小化与其他可见类原型特征间的相似度得分.

(2) 图嵌入模型

旅行商问题、最小顶点覆盖、最大割问题、车辆路径问题等是一类顶点离散的组合优化问题, 除此之外, 我们还会经常遇到社交网络、交通网络等基于图结构的优化问题. 此类问题尽管实例不同, 但是他们的“相同要素”都可以转变为图模型, 通过一类图表示的组合优化问题的方法求解^[65]. 针对此类模型, Dai 等^[65] 提出将强化学习与图嵌入相结合的优化算法, 基于图嵌入方式设计网络, 依据当前时刻和历史时刻的输出决定下一时刻的输出, 直到遇到终止信号完成一次策略, 配合使用 Q-learning 算法^[41, 66], 可以随着局部变化对网络参数进行及时更新. 例如, 我们通过最小顶点覆盖问题的数据进行上述图嵌入模型和求解模型的训练, 可以得到其他最小顶点覆盖问题实例的解. 运用已经训练好的模型和参数, 直接代入旅行商问题的数据进行训练, 将之前获得的模型和参数作为新模型的预训练过程加入, 得到适用于求解旅行商问题的参数. 这种训练好的模型和参数能够在具备如下同类要素的问题中有条件的实现迁移, 这也是此类算法泛化性的评价指标之一.

记 $G(V, E, W)$ 表示带权重的图模型, W 表示顶点集合, $E = \{(u, v) \mid u \in V, v \in V\}$ 表示边集合, $W = \{w(u, v) \geq 0 \mid (u, v) \in E\}$ 表示边的权重集合. 图论中的图是一种抽象且具有较强表达能力的数据结构, 通过定义顶点和边描述实体和实体之间的关联关系. 图嵌入就是将图中的顶点基于关联信息映射成一个低维稠密向量表示, 保证在原始图中相似的顶点在低维表达空间也接近, 从而有利于构建机器学习模型, 进行后端的任务.

由于求解实例不同, 问题的目标函数和约束条件都不同, 为了方便叙述, 采用统一符号表示: S 代表当前局部解集合, $h(S)$ 判断当前局部解是否符合问题的约束条件; $t(h(S))$ 判断局部解是否满足终止条件; $c(h(S), G)$ 为问题的目标函数; $Q(h(S), v)$ 为估值函数, 用于更新局部策略.

图嵌入模型是基于当前局部解 S , 将点集 V 中的每一个顶点 v 映射为 p 维向量 μ_v . 首先将 μ_v 初始化为 0, 然后使用迭代方式更新向量表示:

$$\mu_v^{(t+1)} = F(x_v, \{\mu_u^{(t)}\}_{\mu \in N(v)}, \{w(u, v)\}_{\mu \in N(v)}; \theta), \quad (3.17)$$

其中, $N(v)$ 表示顶点 v 的邻点集合, F 表示非线性映射函数, 可以为神经网络或者其他类型的激活函数, x_v 为二值向量, 当 $v \in S$ 时, $x_v = 1$, 反之为 0. 在最小顶点覆盖问题中, 经过两次图嵌入网络模型迭代即可实现局部解的更新. 有了图嵌入的表示方式, 则后面可通过强化学习的一些算法进行求解^[40].

事实上, 上面讨论的“相同要素”的迁移学习是迁移学习中的简单情形. 格式塔心理学家苛勒 (W. Kohler) 提出了“情境关系理解”的迁移学习理论. 苛勒认为, 动物在一种情境中发现或理解的动力关系模式, 可以应用到另一种情境. 有机体在解决问题过程中习得的是原理或关系, 而非对特殊情境的特殊反应. 一旦有机体学会某一原理, 就会将其应用于相似的情境. 迁移学习也就是将学得的经验有变化地运用于另一情境. 产生学习迁移的原因, 是由于相似的功能所致, 也就是由于对整个情境中各部分的关系、目的和手段之间的关系的充分理解. 如果两个情境中包含了相同的要素, 保持这些相同的要素及其关系的学习实际上就是“相同要素”的迁移学习. 所以, 基于“相同要素”的迁移学习理论是基于“情境关系理解”的迁移学习理论的特殊情形. 人们要理解一个事物, 不仅要知道它的要素, 而且还要知道要素之间的相互关系, 也就是“情境关系”理解. 人工智能发展到今天, 类似于

模拟“人-环境”交互过程的强化学习模型及其数学实现方法,取得了很大成功,但是迄今为止尚没有建立基于苛勒“情境关系理解”的迁移学习理论的模型以及数学实现方法。

大脑处理信息的层级结构不但在视觉信息处理中有很重要的作用,而且还是一个非常广泛的利用组合性来处理复杂表示的方式。在决策、运动控制、执行功能等方面,层级结构可以使得复杂的行为建立在更小的控制单元上,不但可以很好地解决高维空间的扩展问题,也使得学习得到的经验具有很好的迁移特性。也就是说,层级结构一般更容易实现迁移学习。遗憾的是,人们还不知道大脑底层神经如何实现这种信息处理的层级结构,特别是不知道学习的机制是什么。如果能够建立“信息处理的层级结构”与“情境关系理解”相结合的迁移学习理论的模型和数学实现方法,将会向真正的智能迈进一大步。

4 人工智能中的数学理论与方法

人工智能技术是建立在数学模型之上的,从解释到实现都离不开数学,并且几乎用到了现代数学的各个分支。根据人类的思维过程,人工智能技术面临的首要问题是问题空间如何描述,即数据的再表达问题。数据的再表达要解决的问题,在通常意义下就是特征提取问题。该问题由环境与学习两部分组成:环境提供信息(数据),学习则实现数据再表达,用能够理解、便于识别的形式记忆下来。由此可见,数据再表达在人工智能技术中占有相当重要的地位,是机器学习成功的首要因素。人工智能技术要解决的第二个问题是推理策略问题。数学的各个分支在人工智能的数据再表达和推理策略两个方面的模型建立和算法实现中,都起到至关重要的作用,前面的内容已经有所体现,本节我们将简略综述。

4.1 人工智能中的代数

线性代数不仅仅是人工智能的基础,更是现代数学和以现代数学作为主要分析方法的众多学科的基础,从量子力学到图像处理都离不开向量和矩阵的使用。向量和矩阵是代数、特别是线性代数的主要工具。线性代数提供了现实世界的一种数学抽象方法,具体的事物和现象被抽象成某些特征的组合,并在由预先制定的规则定义的框架之下以静态和动态的方式加以观察,描述其静态和动态的特性。向量的实质是 n 维线性空间中的静止点;线性变换描述了向量或者作为参考系的坐标系的变化,可以用矩阵表示;矩阵的特征值和特征向量描述了变化的速度与方向。线性代数是人工智能技术的一个基础的工具集。另外,机器学习的主要研究内容—数据再表达中的主成分分析方法,包括K-L(Karhunen-Loeve)变换、主成分分析(可以看成是K-L变换的一个应用)、奇异值分解等都是线性代数的基本内容。代数表示论对表示学习 also 具有重要的指导意义。

4.2 人工智能中的最优化

人工智能在本质上是一个最优化过程,对于我们要实现的智能,即通过学习以求得最优解^[17],人工智能技术的最后几乎都是回到最优解问题上。不管是传统的机器学习还是深度学习,或是强化学习,它们的基础核心思想都可以归结为最优化问题。机器学习、深度学习的核心是模型和算法,而最优化的任务就是告诉模型应该学什么、怎么学、如何才能学得更好。模型学习往往都归结为求

一个带参数的映射函数, 需要运用大量数据学到这些参数, 并通过不断地测试运行, 才能发现模型中参数的优劣. 最优化的任务就是调整参数, 向着好的方面调整, 假如没有最优化, 模型就不知道该怎么学习而导致停滞不前. 深度神经网络拥有十分巨大的参数数量, 这些模型的学习需要一个目标函数, 目标函数的功能是让数据信息量损失最小、或者模型分类或识别的错误率尽量小. 为了达到此类目的, 模型的训练一般会给参数随机赋初值, 然后采用各种下降算法来寻找能让信息量损失或分类错误率更小的参数设置. 一阶算法, 如随机梯度下降法、共轭梯度法等, 以及二阶算法, 如基于 BFGS (Broyden-Fletcher-Goldfarb-Shanno) 或 L-BFGS (limited-memory BFGS), 截断牛顿法 (truncated-Newton method)、Hessian-free、Newton-CG (Newton-conjugate gradient) 等, 都是一些常用的算法.

4.3 人工智能中的统计

诺贝尔经济学奖获得者托马斯·萨金特 (Thomas J. Sargent) 在 2018 年 8 月的“共享全球智慧引领未来科技”世界科技创新论坛上表示: “人工智能其实就是统计学, 只不过用了一个很华丽的辞藻.” 虽然现在看来, 这种说法并不全面, 但是在人工智能的发展过程中, 统计学方法确实得到了广泛的应用. 机器学习从数据中自动分析获得规律, 并利用规律对未知数据进行预测. 因为学习算法中涉及了大量的统计学理论, 机器学习与推断统计学联系尤为密切, 也被称为统计学习理论. 数据挖掘就是要从大量的资料中自动搜索隐藏于其中的、有着特殊关联性的信息. 数据挖掘一般通过统计、在线分析处理、情报检索、专家系统 (依靠过去的经验法则) 和模式识别等诸多方法来实现目标. 人脸识别的应用非常广泛, 人脸识别将人脸看作一个眼睛、鼻子、嘴的特征及其位置的几何关系的二维像素矩阵, 从统计的角度, 通过分析大量人脸样本, 构造人脸模式空间, 然后再根据相似度识别不同人脸. 许多人工智能技术都建立在统计学基础上, 通过输入大量的数据, 对数据经过一系列筛选处理分析, 最终做出合理的推断. 人工智能中几乎用到了所有的统计学理论和方法. 统计学习理论主要是研究以下三个问题: (1) 学习的统计性能, 即通过有限样本能否学习得到其中的一些规律? (2) 学习算法的收敛性, 即学习过程是否收敛? 收敛的速度如何? (3) 学习过程的复杂性, 即学习器的复杂性、样本的复杂性、计算的复杂性如何? 当然, 统计学的问题往往最后又演变成一个优化问题, 统计与优化密不可分.

4.4 人工智能中的概率论

概率论是除线性代数之外, 人工智能的另一个理论基础, 多数机器学习模型采用的都是基于概率论的方法. 但由于实际任务中可供使用的训练数据有限, 因而需要对概率分布的参数进行估计, 这也是机器学习的核心任务. 概率的参数估计有两种方法: 最大似然估计法和最大后验概率法, 两者分别体现出频率学派和贝叶斯学派对概率的理解方式. 从理论的角度来说, 频率学派和贝叶斯学派各有千秋, 都发挥着不可替代的作用. 但具体到人工智能这一应用领域, 基于贝叶斯定理的各种方法与人类的心理认知机制吻合度更高, 在机器学习等领域中也扮演着更加重要的角色. 数据再表达的频率学派学习模型包括概率主成分分析、变分自编码网络和概率稀疏自编码网络. 数据再表达的贝叶斯学派学习模型中的概率图模型, 是用图结构来描述多元随机变量之间条件独立关系的概率模型, 可以借鉴统计物理的一些理论方法, 从而给研究高维空间中的概率模型带来了很大的便捷性. 图模型有三

个基本问题: (1) 表示问题, 即对于一个概率模型, 如何通过图结构来描述变量之间的依赖关系. (2) 推断问题, 即在已知部分变量时, 计算其他变量的后验概率分布. (3) 学习问题, 即图模型的学习包括图结构的学习和参数的学习. 很多机器学习模型都可以归结为概率模型, 即建模输入和输出之间的条件概率分布. 概率图模型提供了一种新的角度来解释机器学习模型, 并且这种角度有很多优点, 比如了解不同机器学习模型之间的联系、方便设计新模型等. 在机器学习中, 图模型越来越多地用来设计和分析各种学习算法.

概率论将是人工智能理论体系中的重要部分. 传统神经网络模型同人脑的神经网络的机理相差甚大, 脑神经元的刺激信号的原理不能完全体现在传统的神经网络中, 仅仅通过人为设定的海量加权重与阈值来充分体现. 人的头脑通过神经脉冲刺激的数量多少决定头脑兴奋程度的机理, 在目前的神经网络的模型中也不能体现; 输入数据往往是随机的, 传统的神经网络模型不擅长直接对随机变量数据的处理. 所以, 概率论与图论的交叉产生的图模型, 特别是随机图模型, 将会在未来的工智能理论中占有重要地位.

4.5 人工智能中的函数论

函数论是表示学习的主要工具之一. 空间映射理论的原理可以用来解决类似人脸识别、图像识别或文字识别等复杂系空间的模式识别问题. 由于复杂系空间的问题往往很难找到可以直接解决的算法, 因此不能像传统的智能系统一样, 直接通过传统的算法进行处理; 基于空间映射理论的处理方法就是把一个复杂系空间的问题映射到若干个简单系空间的问题. 虽然在每一个简单系空间中只能解决有限的问题, 但是根据组合理论, 若干个简单系空间的组合却能解决复杂系空间的问题 (相当于格式塔心理学中完形组织法则); 由复杂系空间问题映射到简单系空间, 是基于人的大脑的处理方式, 被称为人为介入的方法; 模型驱动的数据再表达学习方法^[18]: 围绕着一般的函数类 (一般的信号) 和一般的算子 (变换), 把注意力集中在这些一般函数 (信号) 的定量性质上, 并且研究当不同的算子作用于它们时, 这些定量性质是怎样变化的; 调和分析方法在分析一般函数 (信号) 时, 通过一些局部性质组合得到函数的整体性质, 如在分析一个函数时, 我们把它分解为一个和, 而这里的每个函数都是“局部化”了的, 即它的支集, 这种分解叫作空间变量的局部化. 基于熵编码的数据再表达方法、基于离散余弦变换 (discrete cosine transformation, DCT) 的数字图像数据的稀疏再表达方法、基于多分辨率分析的一般函数分解方法以及基于小波变换的数字图像处理方法都是模型驱动的数据的逐层再表达方法.

给定一个函数, 是否存在一个多层感知器网络和特定的权重, 使得这个多层感知器网络的输出能够很好地逼近这个函数? 研究表明, 如果有足够的隐藏节点, 拥有一个隐藏层的感知器网络就能够以任何精度逼近任何光滑函数. 这在某种意义下回答了“为什么许多简单的单位连结起来的系统, 可以产生如复杂的智能活动”这一疑问. 使用与神经网络类似的架构, 将简单的单元 (线性变换加一个简单的非线性变换) 以层的方式组织起来, 并且至少一个隐藏层, 就能模拟任何光滑函数输入 - 输出. 另一方面, 神经网络模型可以视作一个连续的动力系统的离散化^[67]. 最近的研究表明^[68], 残差网络是一种微分方程的解. 获得微分方程解法的反向传播梯度, 伴随系统除了描述初始的动态系统的过程外, 还通过链式法则 (反向传播法的关键所在), 描述了反向过程中每一点的导数状态. 正是通过伴随系统, 可以得到微分的初始状态, 并以类似的方式, 获得一个描述动态系统的函数 (“残差块” 或欧

图 15 (网络版彩图) 人工智能中的数学

拉法离散化过程) 的参数.

4.6 人工智能中的几何拓扑

传统特征学习的数据再表达方法中, 数据点和数据点之间的距离和映射函数都是定义在欧氏空间中的, 然而在实际情况中, 这些数据点可能不是分布在欧氏空间中的. 传统欧氏空间的度量难以用于真实世界的非线性数据, 从而需要对数据的分布引入新的假设. 因此无论是人工智能的解释或者建模, 几何观点下的人工智能具有大量的理论问题期待解决.

4.7 人工智能中的数理逻辑

符号主义, 又称为逻辑主义心理学派或计算机学派, 其原理主要为物理符号系统 (即符号操作系统) 假设和有限合理性原理. 符号主义认为人工智能源于数理逻辑. “人工智能”一词由麻省理工学院的约翰·麦卡锡等于 1956 年首先创造 (参见文献 [69]). 当时, 他大力提倡逻辑思考, 以发展能够进行推理的计算机系统. 这导致了一阶谓词逻辑的成熟应用, 用标准的数学语言及符号刻画真实世界. 一阶谓词逻辑用于描述一类物体及物体之间的联系, 可以对事实进行推理并得出有用的结论. 一阶谓词逻辑的最大成功之处在于, 它让人们找到了一种方法, 使用许多最简单的逻辑刻画愈发复杂的实际情况. 逻辑可以用最基础的概念形成极其复杂的结论.

综上所述, 人工智能中用到的各个数学分支及其发挥的作用如图 15 所示.

5 总结与展望

根据上述讨论, 建立在认知生物学和认知心理学基础上的人工智能, 发展成为联结主义人工智能、符号主义人工智能和行为主义人工智能三个学派, 并分别建立了一系列数学模型和求解方法, 如图 16 所示.

基于深度网络学习的联结主义人工智能近二十多年来发展迅速, 极大地推动了人工智能的研究与应用. 以深度强化学习为基础的围棋人工智能程序 AlphaGo/AlphaGoZero 的成功, 表明行为主义人工智能具有强大的生命力, 将会是人工智能未来发展的主流方向之一.

人工智能具有创造性思维的能力是人工智能成为真正“智能”的一个重要标志, 但现在的人工智能还不具备创造性思维的能力. 关于创造性思维有逻辑主义 (符号主义人工智能学派) 和联想主义 (联结主义人工智能学派) 两种传统观点. 传统的逻辑观点认为创造性思维追求真理、强调证明, 要求思维的每一个步骤都很严密, 并且发展了一套形式标准来检验和发现错误. 联想主义的观点认为思维是一连串的观念, 了解思维的途径就是研究支配观念连续的规律. 创造性思维在这里就成为只依赖回忆、靠过去操练过的机械信息、靠一系列盲目尝试中偶然的迸发. 这两种传统观点很难真正实现创造性思维.

创造性思维过程很复杂, 其中包括对整个问题情境的熟悉、对结构的了解, 进而发现问题, 转变情景中心, 将不完整的、不合适的结构转化为完整的、前后一致的, 有时是熟悉的或简单的结构, 最后实现问题的解决. 在这一过程中格式塔认知心理学着重强调个体对问题组成元素的结构重组, 其中决定结构重组的关键性因素是重定中心, 即问题结构中心的转变, 从片面的观点转变为从情景的客观结构所要求的中心出发, 这样就形成了一个新的结构, 各个部分根据在新的结构中的位置、作用、功能来改变各部分的含义. 由此可见, 结构中心的转变带来了根本性的变化, 各要素被看成新的、清

晰的结构的一部分, 其作用和功能不同, 获得了新的含义.

顿悟是获得创造性思维的重要途径之一. 顿悟就是顿然领悟, 若以一种新的角度来观察问题情境就会获致顿悟, 顿悟有助于问题的解决. 动物对于问题的解决不是来自于盲目的试误, 也不是出于各个部分偶然碰巧的凑合, 而是对有用的或适当的关系的突然知觉, 即顿悟. 一旦动物通过顿悟解决了问题, 就有一种对类似情境的高度迁移, 而且动物会表现出高水平的保持和理解. 动物在一种情境中发现或理解的动力关系模式, 可以应用到另一种情境. 有机体在解决问题过程中习得的是原理或关系, 而非对特殊情境的特殊反应. 一旦有机体学会某一原理, 就会将其应用于相似的情境.

我们认为, 可解释和创造性的人工智能的发展必须有现代数学理论的加入. 也许我们可以从如下几个具体问题的研究入手, 逐步向真正的智能靠近:

(1) 大脑不仅仅是由海量神经元构成的一个具有思维功能的连接器, 而且还是一个复杂的电场, 它是包含先于感觉刺激而存在的结构化的电化学力场, 感觉材料一旦进入这样的场, 立即更改这个场的结构, 同时又被该场所更改. 场论是一种动力学的研究方法, 是对环境作为一个整体的分析方法, 特别是规范场论在物理学上具有重要意义, 它为量子电动力学、弱相互作用和强相互作用提供了一个统一的数学形式化架构. 我们可以用数学的形式描述心理环境, 同时可以将规范场论 (如杨 - 米尔斯 (Yang-Mills) 理论) 引入到人工智能的研究中.

(2) 如何建立顿悟学习的理论模型和数学实现方法, 在构建优化模型时, 目标函数和约束条件能够实现学习过程中的自适应中心转换或中心重定, 将“试误训练学习”与“顿悟学习”有机结合, 最终实现顿悟学习的目标.

(3) 在实现顿悟学习的基础上, 如何构建“信息处理的层级结构”与“情境关系理解”相结合的迁移学习理论的模型和数学实现方法. “信息处理的层级结构”已经可以通过逐层数据再表达的方法实现, 关键是在模型中如何加入“情境关系理解”的因素, 创建统一的模型, 实现迁移学习.

(4) 将格式塔心理学中的“整体观”贯穿于人工智能实现的模型中, 特别是在模型中如何体现“相似性、接近性、闭合性、连续性”等简单性原则.

总之, 人工智能发展的路还很长, 需要认知、心理、数学、统计物理、信息、计算机、材料、元器件设计等诸多领域共同努力, 最终实现真正“智能”的目标.

致谢 本文是在袁亚湘主编的鼓励 and 帮助下完成的, 在此对袁亚湘主编表示衷心的感谢. 审稿专家对论文提出了一系列详细的修改意见, 其中既有叙述和打印方面的错误, 更有论述和逻辑上的不当之处, 使得该论文能够进一步完善并增色. 在此, 对评审专家的辛勤付出表示衷心的感谢.

参考文献

- 1 McCulloch W, Pitts W. A logical calculus of the ideas immanent in nervous activity (Reprinted from Bulletin of Mathematical Biophysics, 1943, 5: 115–133). Bull Math Biol, 1990, 52: 99–115
- 2 Turing A. Computing machinery and intelligence. Mind, 1950, 49: 433–460
- 3 Hebb D. The Organization of Behaviour. New York: John Wiley & Sons, 1949
- 4 Samuel A L. Some studies in machine learning using the game of checkers. IBM J Res Deve, 1959, 44: 210–229
- 5 Hinton G E, Salakhutdinov R R. Reducing the dimensionality of data with neural networks. Science, 2006, 313: 504–507
- 6 Buchanan B. A (very) brief history of artificial intelligence. AI Magazine, 2005, 26: 53–60
- 7 Cohen J. Human Robots in Myth and Science. New York: Barnes, 1967
- 8 Feigenbaum E, Feldman J, eds. Computers and Thought. New York: McGraw-Hill, 1963
- 9 Gardner M. Logic Machines and Diagrams. New York: McGraw-Hill, 1960

- 10 McCorduck P. *Machines Who Think*. San Francisco: Freeman, 1979
- 11 Gazzaniga M, Ivry R, Mangun G. *Cognitive Neuroscience: The Biology of the Mind*. New York: Norton, 2013
- 12 Kandel E, Schwartz J, Jessell T. *Principles of Neural Science*. New York: McGraw-Hill Medical, 2012
- 13 Sun J R. *Introduction to Brain Science* (in Chinese). Beijing: Peking University Press, 2001 [孙久荣. 脑科学导论. 北京: 北京大学出版社, 2001]
- 14 Ungerleider L, Haxby J. ‘What’ and ‘where’ in human brain. *Curr Opin Neurobiol*, 1994, 4: 157–165
- 15 Holland J, Chen Y, translated. *Emergence: From Chaos to Order* (in Chinese). Shanghai: Shanghai Science and Technology Press, 2006 [约翰·霍兰, 著. 陈禹, 译. 涌现: 从混沌到有序. 上海: 上海科学技术出版社, 2006]
- 16 Hornik K, Stinchcombe M, White H. Multilayer feedforward networks are universal approximators. *Neural Networks*, 1989, 2: 359–366
- 17 Guo T D, Han C Y. From numerical optimization method to learning optimization method (in Chinese). *Oper Res Trans*, 2019, 23: 1–12 [郭田德, 韩丛英. 从数值最优化方法到学习最优化方法. 运筹学学报, 2019, 23: 1–12]
- 18 Guo T D, Han C Y, Li M. Fusion of front-end and back-end learning based on layer-by-layer data re-representation (in Chinese). *Sci Sin-Inf*, 2019, 49: 739–759 [郭田德, 韩丛英, 李明强. 逐层数据再表达的前后端融合学习的理论及其模型和算法. 中国科学: 信息科学, 2019, 49: 739–759]
- 19 Baldi P. Autoencoders, unsupervised learning, and deep architectures. *J Mach Learn Res*, 2012, 27: 37–50
- 20 Rumelhart D E, Hinton G E, Williams R J. Learning representations by back-propagating errors. *Nature*, 1986, 323: 533–536
- 21 LeCun Y, Bengio Y, Hinton G E. Deep learning. *Nature*, 2015, 521: 436–444
- 22 Masci J, Meier U, Ciresan D, et al. Stacked convolutional auto-encoders for hierarchical feature extraction. In: *Proceedings of the 21st International Conference on Artificial Neural Networks*. Lecture Notes in Computer Science, vol. 6791. Berlin-Heidelberg: Springer-Verlag, 2011, 52–59
- 23 Hosseini-Asl E, Zurada J M, Nasraoui O. Deep learning of part-based representation of data using sparse autoencoders with nonnegativity constraints. *IEEE Trans Neural Netw Learning Syst*, 2016, 27: 2486–2498
- 24 Vincent P, Larochelle H, Bengio Y, et al. Extracting and composing robust features with denoising autoencoders. In: *Machine Learning. Proceedings of the 25th International Conference on Machine Learning (ICML 2008)*. Helsinki: ACM, 2008, 1096–1103
- 25 Rifai S, Vincent P, Muller X, et al. Contractive auto-encoders: Explicit invariance during feature extraction. In: *Proceedings of the 28th International Conference on Machine Learning (ICML 2011)*. Bellevue: ACM, 2011, 833–840
- 26 Ciresan D C, Meier U, Masci J, et al. Flexible, high performance convolutional neural networks for image classification. In: *Proceedings of the 22nd International Joint Conference on Artificial Intelligence (IJCAI 2011)*. Barcelona: DBLP, 2011, 1237–1242
- 27 LeCun Y, Bottou L, Bengio Y, et al. Gradient-based learning applied to document recognition. *Proc IEEE*, 1998, 86: 2278–2324
- 28 Simard P, Steinkraus D, Platt J. Best practices for convolutional neural networks applied to visual document analysis. In: *Proceedings of the Seventh International Conference on Document Analysis and Recognition*. Edinburgh: IEEE, 2003, 958–963
- 29 Behnke S. Hierarchical neural networks for image interpretation. *Lecture Notes Comput Sci (LNCS)*, 2003, 2766: 1345–1346
- 30 Genc E, Fraenz C, Schlüter C, et al. Diffusion markers of dendritic density and arborization in gray matter predict differences in intelligence. *Nat Commun*, 2018, 9: 1905
- 31 LeCun Y, Boser B, Decker J, et al. Backpropagation applied to handwritten zip code recognition. *Neural Computation*, 1989, 1: 541–551
- 32 He H C, He Z T. The development of artificial intelligence from the view of logic (in Chinese). In: Tu X Y, Han L Q, eds. *Artificial Intelligence: Review & Prospect*. Beijing: Science Press, 2006, 77–111 [何华灿, 何智涛. 从逻辑学观点看人工智能学科的发展. 见: 涂序彦, 韩力群, 主编. 人工智能: 回顾与展望. 北京: 科学出版社, 2006, 77–111]
- 33 Xiong L W. Artificial intelligence, philosophy and logic (in Chinese). *J Zhongshan Univ Social Sci*, 2003, 43: 226–230 [熊立文. 人工智能、哲学与逻辑. 中山大学学报, 2003, 43: 226–230]
- 34 Nilsson N J. Probabilistic logic. *Artif Intell*, 1986, 28: 71–87
- 35 Wang Y Q. *Principles and Methods of Artificial Intelligence* (in Chinese). Xi’an: Xi’an Jiaotong University Press, 2003 [王永庆. 人工智能原理与方法. 西安: 西安交通大学出版社, 2003]
- 36 Chen B. On the development of modern logic from the perspective of artificial intelligence (in Chinese). *Sun Yat-sen Univ Forum*, 2000, 2: 3–27 [陈波. 从人工智能看当代逻辑学的发展. 中山大学学报论丛, 2000, 2: 3–27]
- 37 He H C, Wang H, Liu Y H, et al. *Universal Logics Principle* (in Chinese). Beijing: Science Press, 2001 [何华灿, 王华, 刘永怀, 等. 泛逻辑学原理. 北京: 科学出版社, 2001]
- 38 Wu W T. *Mathematics Mechanization* (in Chinese). Beijing: Science Press, 2003 [吴文俊. 数学机械化. 北京: 科学出版

- 社, 2003]
- 39 Gao X S, Li W, Yuan C M. Intersection theory in differential algebraic geometry: Generic intersections and the differential Chow form. *Trans Amer Math Soc*, 2013, 365: 4575–4632
 - 40 Guo T D, Han C Y, Tang S Q. *Machine Learning Methods for Combinatorial Optimization* (in Chinese). Beijing: Science Press, 2019 [郭田德, 韩丛英, 唐思琦. 组合优化机器学习方法. 北京: 科学出版社, 2019]
 - 41 Sutton R, Barto A. *Reinforcement Learning: An Introduction*. Cambridge: MIT press, 2018
 - 42 Watkins C J C H, Dayan P. *Q-learning*. *Mach Learn*, 1992, 8: 279–292
 - 43 Vlad M, Koray K, Silver D, et al. Playing atari with deep reinforcement learning. In: *Proceedings of the Conference and Workshop on Neural Information Processing Systems (NIPS)*. arXiv:1312.5602, 2013
 - 44 Barto A G, Sutton R S, Anderson C W. Neuronlike adaptive elements that can solve difficult learning control-problems. *IEEE Trans Syst Man Cyber*, 1983, 13: 834–846
 - 45 Timothy P, Jonathan J, Alexander P, et al. Continuous control with deep reinforcement learning. arXiv:1509.02971, 2019
 - 46 Schulman J, Wolski F, Dhariwal P, et al. Proximal policy optimization algorithms. arXiv:1707.06347, 2019
 - 47 Schulman J, Levine S, Moritz P, et al. Trust region policy optimization. arXiv:1502.05477v5, 2017
 - 48 Buşoniu L, Babuška R, Schutter B. Multi-agent reinforcement learning: An overview. In: Srinivasan D, Jain L, eds. *Innovations in Multi-Agent Systems and Applications*, vol. 1. *Studies in Computational Intelligence*, vol. 310. Berlin-Heidelberg: Springer, 2010, 183–221
 - 49 Sukhbaatar S, Fergus R. Learning multiagent communication with backpropagation. *Adv Neural Inform Process Syst*, 2016, 29: 2244–2252
 - 50 Lowe R, Wu Y, Tamar A, et al. Multi-agent actor-critic for mixed cooperative-competitive environments. *Adv Neural Inform Process Syst*, 2017, 30: 6379–6390
 - 51 Koffka K. Li W, translated. *Principles of Gestalt Psychology* (in Chinese). Hangzhou: Zhejiang Education Press, 1997 [库尔特·考夫卡, 著. 黎炜, 译. 格式塔心理学原理. 杭州: 浙江教育出版社, 1997]
 - 52 Wang P, Pang G H, Gao F Q. *Gestalt Psychology, the Gestalt of Experience* (in Chinese). Ji'nan: Shandong Education Press, 2009 [王鹏, 潘光花, 高峰强. 经验的完形——格式塔心理学. 济南: 山东教育出版社, 2009]
 - 53 Seung H, Lee D. The manifold ways of perception. *Science*, 2000, 290: 2268–2269
 - 54 Zhang J P. *Errors Favor Intelligent Beings* (in Chinese). Beijing: Tsinghua University Press, 2019 [张军平. 爱犯错的智能体. 北京: 清华大学出版社, 2019]
 - 55 Weinberger K Q, Saul L K. Unsupervised learning of image manifolds by semidefinite programming. *Int J Comput Vision*, 2006, 70: 77–90
 - 56 Roweis S T, Saul L K. Nonlinear dimensionality reduction by locally linear embedding. *Science*, 2000, 290: 2323–2326
 - 57 Saul L K, Roweis S T. An introduction to locally linear embedding. <https://cs.nyu.edu/~roweis/lle/papers/lleintro.pdf>
 - 58 Saul L K, Roweis S T. Think globally, fit locally: Unsupervised learning of low dimensional manifolds. *J Mach Learn Res*, 2004, 4: 119–155
 - 59 Belkin M, Niyogi P. Laplacian eigenmaps and spectral techniques for embedding and clustering. *Adv Neural Inform Process Syst*, 2002, 15: 1585–592
 - 60 Thorndike E. Li W, translated. *Human Learning* (in Chinese). Beijing: Peking University Press, 2010 [爱德华·桑代克, 著. 李维, 译. 人类的学习. 北京: 北京大学出版社, 2010]
 - 61 Wang W, Zheng V, Yu H, et al. A survey of zero-shot learning: Settings, methods, and applications. *ACM Trans Intel Syst Tec*, 2019, 10: 13.1–13.37
 - 62 Frome A, Corrado G S, Shlens J, et al. DeViSE: A deep visual-semantic embedding model. *Adv Neural Inform Process Syst*, 2013, 26: 2121–2129
 - 63 Kodirov E, Xiang T, Gong S. Semantic autoencoder for zero-shot learning. In: *IEEE Conference on Computer Vision and Pattern Recognition*. Philadelphia: IEEE, 2017, 4447–4456
 - 64 Li Y, Zhang J, Zhang J, et al. Discriminative learning of latent features for zero-shot recognition. In: *IEEE Conference on Computer Vision and Pattern Recognition*. Philadelphia: IEEE, 2018, 7463–7471
 - 65 Dai H, Elias B, Zhang Y, et al. Learning combinatorial optimization algorithms over graphs. *Adv Neural Inform Process Syst*, 2017, 30: 6348–6358
 - 66 Riedmiller M. Neural fitted Q iteration—first experiences with a data efficient neural reinforcement learning method. In: *Proceedings of the 16th European Conference on Machine Learning*. *Lecture Notes in Artificial Intelligence*, vol. 3720. Berlin-Heidelberg: Springer-Verlag, 2005, 317–328
 - 67 E W. A proposal on machine learning via dynamical systems. *Comm Math Stat*, 2017, 5: 1–11
 - 68 Chen R, Rubanova Y, Bettencourt J, et al. Neural ordinary differential equations. arXiv:1806.07366v5, 2018
 - 69 McCarthy J, Minsky M, Rochester N, et al. A proposal for the dartmouth summer research project on artificial intelligence. *AI Magazine*, 2006, 27: 12–14

Artificial intelligence mechanism and mathematics implementation methods

Tiande Guo & Congying Han

Abstract Artificial intelligence is an interdisciplinary discipline that integrates many subjects, such as brain cognitive science, psychology, mathematics (including statistics), information science, and computer science. At present, artificial intelligence represented by big data-driven deep learning has developed rapidly and has been widely used in many fields. However, the biggest flaw in artificial intelligence right now is that it has no theory and is basically still in the experimental science stage. To explore the mechanism of artificial intelligence and carry out its theoretical research is of vital importance to the further development of artificial intelligence. To reveal the nature and promote the theoretical research of artificial intelligence, the mechanisms and concrete realizations of the three existing artificial intelligence schools are explored from the two levels of cognitive biology and cognitive psychology, such as symbolism, connectionism and behaviorism, trying to explain the nature of artificial intelligence. Some possible basic research methods and research directions of future interpretable and creative artificial intelligence are proposed.

Keywords artificial intelligence, mathematics, cognitive biology, cognitive psychology

MSC(2010) 00A71, 68T01

doi: 10.1360/SSM-2020-0031