AI营销培训 第一部分文案

# 一、内容纲领

## 1.1 关键词

原理

## 1.2 内容安排

1. 大模型发展背景 -> 基本概念原理概括

（简介）

1. 当前大模型发展现状，特别是国产模型状况以及其优势（ 智谱Qwen / 阿里Qwen / …… ）

（简介）

1. 语言大模型主流发展路线（ 注意力机制 / 循环神经网络 - RNNs ） -> 原理讲解

（略过）

1. 国产大模型介绍和 基本使用/本地部署 （针对不同基础，需求）讲解

（重点）

# 二、具体讲解内容

## 2.1 人工智能（大模型）沿革历史

### 2.1.1 起步发展期 [1943年—20世纪60年代]

人工智能概念的提出后，发展出了符号主义、联结主义(神经网络)等五种流派

前后相继取得了一批令人瞩目的研究成果，如机器定理证明、跳棋程序、人机对话等，掀起人工智能发展的第一个高潮。

1943年，美国神经科学家麦卡洛克（Warren McCulloch）和逻辑学家皮茨（Water Pitts）提出神经元的数学模型，这是现代人工智能学科的奠基石之一。

1950年，艾伦·麦席森·图灵（Alan Mathison Turing）提出“图灵测试”（测试机器是否能表现出与人无法区分的智能），让机器产生智能这一想法开始进入人们的视野。

图示

中度可信度描述已自动生成

1950年，克劳德·香农（Claude Shannon）提出计算机博弈。

1956年，达特茅斯学院人工智能夏季研讨会上正式使用了人工智能（artificial intelligence，AI）这一术语。这是人类历史上第一次人工智能研讨，标志着人工智能学科的诞生。

1957年,弗兰克·罗森布拉特（Frank Rosenblatt）在一台IBM-704计算机上模拟实现了一种他发明的叫做“感知机”（Perceptron）的神经网络模型。[感知机可以被视为一种最简单形式的前馈式人工神经网络，是一种二分类的线性分类判别模型，其输入为实例的特征向量想（x1,x2…），神经元的激活函数f为sign，输出为实例的类别（+1或者-1），模型的目标是要将输入实例通过超平面将正负二类分离。]

图示

描述已自动生成

1958年，David Cox提出了logistic regression[LR是类似于感知机结构的线性分类判别模型，主要不同在于神经元的激活函数f为sigmoid，模型的目标为(最大似然)极大化正确分类概率。]

图示

中度可信度描述已自动生成

1959年，Arthur Samuel给机器学习了一个明确概念：Field of study that gives computers the ability to learn without being explicitly programmed.（机器学习是研究如何让计算机不需要显式的程序也可以具备学习的能力）。

1961年，Leonard Merrick Uhr 和 Charles M Vossler发表了题目为A Pattern Recognition Program That Generates, Evaluates and Adjusts its Own Operators 的模式识别论文，该文章描述了一种利用机器学习或自组织过程设计的模式识别程序的尝试。

1965年，古德（I. J. Good）发表了一篇对人工智能未来可能对人类构成威胁的文章，可以算“AI威胁论”的先驱。他认为机器的超级智能和无法避免的智能爆炸最终将超出人类可控范畴。后来著名科学家霍金、发明家马斯克等人对人工智能的恐怖预言跟古德半个世界前的警告遥相呼应。

1966 年，麻省理工学院科学家Joseph Weizenbaum 在 ACM 上发表了题为《ELIZA-a computer program for the study of natural language communication between man and machine》文章描述了ELIZA 的程序如何使人与计算机在一定程度上进行自然语言对话成为可能，ELIZA 的实现技术是通过关键词匹配规则对输入进行分解，而后根据分解规则所对应的重组规则来生成回复。

1967年，Thomas等人提出K最近邻算法（The nearest neighbor algorithm）。[KNN的核心思想，即给定一个训练数据集，对新的输入实例Xu，在训练数据集中找到与该实例最邻近的K个实例，以这K个实例的最多数所属类别作为新实例Xu的类别。]

图示, 示意图

描述已自动生成

1968年，爱德华·费根鲍姆（Edward Feigenbaum）提出首个专家系统DENDRAL，并对知识库给出了初步的定义，这也孕育了后来的第二次人工智能浪潮。该系统具有非常丰富的化学知识，可根据质谱数据帮助化学家推断分子结构。[专家系统（Expert Systems）是AI的一个重要分支，同自然语言理解，机器人学并列为AI的三大研究方向。它的定义是使用人类专家推理的计算机模型来处理现实世界中需要专家作出解释的复杂问题，并得出与专家相同的结论，可视作“知识库(knowledge base)”和“推理机(inference machine)” 的结合。]

图示

描述已自动生成

1969年，“符号主义”代表人物马文·明斯基（Marvin Minsky）的著作《感知器》提出对XOR线性不可分的问题：单层感知器无法划分XOR原数据，解决这问题需要引入更高维非线性网络（MLP, 至少需要两层），但多层网络并无有效的训练算法。这些论点给神经网络研究以沉重的打击，神经网络的研究走向长达10年的低潮时期。

图表

描述已自动生成

### 2.1.2 反思低谷期 [20世纪70年代]

人工智能发展初期的突破性进展大大提升了人们对人工智能的期望，人们开始尝试更具挑战性的任务，然而计算力及理论等的匮乏使得不切实际目标的落空，人工智能的发展走入低谷。

1974年，哈佛大学沃伯斯(Paul Werbos)博士论文里，首次提出了通过误差的反向传播(BP)来训练人工神经网络，但在该时期未引起重视。[BP算法的基本思想不是（如感知器那样）用误差本身去调整权重，而是用误差的导数（梯度）调整。通过误差的梯度做反向传播，更新模型权重, 以下降学习的误差，拟合学习目标，实现网络的万能近似功能的过程。]

图示

描述已自动生成

1975年，马文·明斯基(Marvin Minsky)在论文《知识表示的框架》(A Framework for Representing Knowledge)中提出用于人工智能中的知识表示学习框架理论。

1976年，兰德尔·戴维斯（Randall Davis）构建和维护的大规模的知识库，提出使用集成的面向对象模型可以提高知识库（KB）开发、维护和使用的完整性。

1976年，斯坦福大学的肖特利夫(Edward H. Shortliffe)等人完成了第一个用于血液感染病的诊断、治疗和咨询服务的医疗专家系统MYCIN。

1976年，斯坦福大学的博士勒纳特发表论文《数学中发现的人工智能方法——启发式搜索》，描述了一个名为“AM”的程序，在大量启发式规则的指导下开发新概念数学，最终重新发现了数百个常见的概念和定理。

1977年，海斯·罗思(Hayes. Roth)等人的基于逻辑的机器学习系统取得较大的进展，但只能学习单一概念，也未能投入实际应用。

1979年，汉斯·贝利纳（Hans Berliner）打造的计算机程序战胜双陆棋世界冠军成为标志性事件。(随后，基于行为的机器人学在罗德尼·布鲁克斯和萨顿等人的推动下快速发展，成为人工智能一个重要的发展分支。格瑞·特索罗等人打造的自我学习双陆棋程序又为后来的强化学习的发展奠定了基础。)

### 2.1.3 应用发展期 [20世纪80年代]

人工智能走入应用发展的新高潮。专家系统模拟人类专家的知识和经验解决特定领域的问题，实现了人工智能从理论研究走向实际应用、从一般推理策略探讨转向运用专门知识的重大突破。而机器学习(特别是神经网络)探索不同的学习策略和各种学习方法，在大量的实际应用中也开始慢慢复苏。

1980年，在美国的卡内基梅隆大学(CMU)召开了第一届机器学习国际研讨会，标志着机器学习研究已在全世界兴起。

1980年，德鲁·麦狄蒙（Drew McDermott）和乔恩·多伊尔（Jon Doyle）提出非单调逻辑，以及后期的机器人系统。

1980年，卡耐基梅隆大学为DEC公司开发了一个名为XCON的专家系统，每年为公司节省四千万美元，取得巨大成功。

1981年，保罗（R.P.Paul）出版第一本机器人学课本，“Robot Manipulator：Mathematics，Programmings and Control”，标志着机器人学科走向成熟。

1982年，马尔（David Marr）发表代表作《视觉计算理论》提出计算机视觉（Computer Vision）的概念，并构建系统的视觉理论，对认知科学（CognitiveScience）也产生了很深远的影响。

1982年，约翰·霍普菲尔德（John Hopfield） 发明了霍普菲尔德网络，这是最早的RNN的雏形。霍普菲尔德神经网络模型是一种单层反馈神经网络（神经网络结构主要可分为前馈神经网络、反馈神经网络及图网络），从输出到输入有反馈连接。它的出现振奋了神经网络领域，在人工智能之机器学习、联想记忆、模式识别、优化计算、VLSI和光学设备的并行实现等方面有着广泛应用。

1983年，Terrence Sejnowski, Hinton等人发明了玻尔兹曼机（Boltzmann Machines），也称为随机霍普菲尔德网络，它本质是一种无监督模型，用于对输入数据进行重构以提取数据特征做预测分析。

图示

描述已自动生成

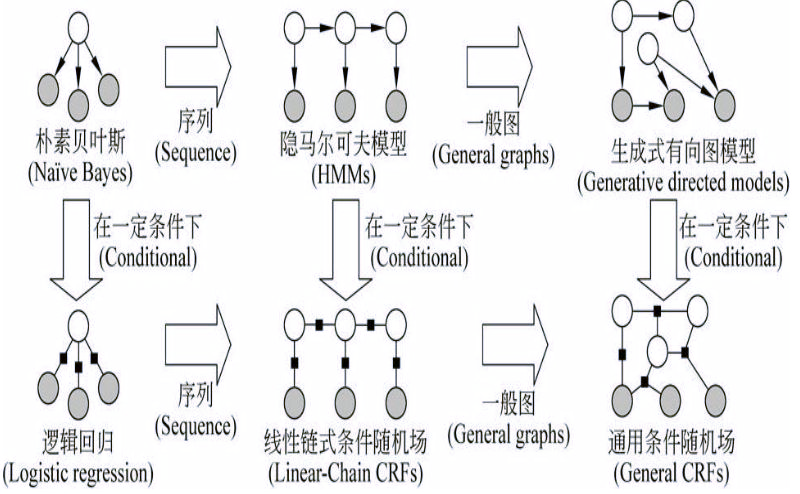
1985年，朱迪亚·珀尔提出贝叶斯网络(Bayesian network)，他以倡导人工智能的概率方法和发展贝叶斯网络而闻名，还因发展了一种基于结构模型的因果和反事实推理理论而受到赞誉。

[贝叶斯网络拓朴结构是一个有向无环图(DAG)，通过把某个研究系统中涉及的随机变量，根据是否条件独立绘制在一个有向图中，以描述随机变量之间的条件依赖，用圈表示随机变量(random variables)，用箭头表示条件依赖(conditional dependencies)就形成了贝叶斯网络。对于任意的随机变量，其联合概率可由各自的局部条件概率分布相乘而得出。如图中b依赖于a(即：a->b)，c依赖于a和b，a独立无依赖，根据贝叶斯定理有 P(a,b,c) = P(a)\*P(b|a)\*P(c|a,b)]

形状, 多边形

描述已自动生成

[贝叶斯网络是一种模拟人类推理过程中因果关系的不确定性处理模型，如常见的朴素贝叶斯分类算法就是贝叶斯网络最基本的应用。]



1986年，罗德尼·布鲁克斯(Brooks)发表论文《移动机器人鲁棒分层控制系统》，标志着基于行为的机器人学科的创立，机器人学界开始把注意力投向实际工程主题。

1986年，辛顿(Geoffrey Hinton)等人先后提出了多层感知器(MLP)与反向传播（BP）训练相结合的理念（该方法在当时计算力上还是有很多挑战，基本上都是和链式求导的梯度算法相关的），这也解决了单层感知器不能做非线性分类的问题，开启了神经网络新一轮的高潮。

图示

中度可信度描述已自动生成

1986年，昆兰（Ross Quinlan）提出ID3决策树算法。[决策树模型可视为多个规则(if, then)的组合，与神经网络黑盒模型截然不同是，它拥有良好的模型解释性。ID3算法核心的思想是通过自顶向下的贪心策略构建决策树：根据信息增益来选择特征进行划分（信息增益的含义是 引入属性A的信息后，数据D的不确定性减少程度。也就是信息增益越大，区分D的能力就越强)，依次递归地构建决策树。]

图示

描述已自动生成

1989年，George Cybenko证明了“万能近似定理”（universal approximation theorem）。简单来说，多层前馈网络可以近似任意函数，其表达力和图灵机等价。这就从根本上消除了Minsky对神经网络表达力的质疑。

[“万能近似定理”可视为神经网络的基本理论：⼀个前馈神经⽹络如果具有线性层和⾄少⼀层具有 “挤压” 性质的激活函数（如 sigmoid 等），给定⽹络⾜够数量的隐藏单元，它可以以任意精度来近似任何从⼀个有限维空间到另⼀个有限维空间的 borel 可测函数。]

图示, 多边形

描述已自动生成

1989年，LeCun (CNN之父) 结合反向传播算法与权值共享的卷积神经层发明了卷积神经网络（Convolutional Neural Network，CNN），并首次将卷积神经网络成功应用到美国邮局的手写字符识别系统中。

[卷积神经网络通常由输入层、卷积层、池化（Pooling）层和全连接层组成。卷积层负责提取图像中的局部特征，池化层用来大幅降低参数量级(降维)，全连接层类似传统神经网络的部分，用来输出想要的结果。]

图示

描述已自动生成

### 2.1.4 平稳发展期 [20世纪90年代—2010年]

由于互联网技术的迅速发展，加速了人工智能的创新研究，促使人工智能技术进一步走向实用化，人工智能相关的各个领域都取得长足进步。在2000年代初，由于专家系统的项目都需要编码太多的显式规则，这降低了效率并增加了成本，人工智能研究的重心从基于知识系统转向了机器学习方向。

1995年，Cortes和Vapnik提出联结主义经典的支持向量机(Support Vector Machine)，它在解决小样本、非线性及高维模式识别中表现出许多特有的优势，并能够推广应用到函数拟合等其他机器学习问题中。

[支持向量机（Support Vector Machine, SVM）可以视为在感知机基础上的改进，是建立在统计学习理论的VC维理论和结构风险最小原理基础上的广义线性分类器。与感知机主要差异在于：1、感知机目标是找到一个超平面将各样本尽可能分离正确(有无数个)，SVM目标是找到一个超平面不仅将各样本尽可能分离正确，还要使各样本离超平面距离最远(只有一个最大边距超平面)，SVM的泛化能力更强。2、对于线性不可分的问题，不同于感知机的增加非线性隐藏层，SVM利用核函数，本质上都是实现特征空间非线性变换，使可以被线性分类。]

感知器

图示

描述已自动生成

SVM

图表, 散点图

描述已自动生成

1995年， Freund和schapire提出了 AdaBoost (Adaptive Boosting)算法。AdaBoost采用的是Boosting集成学习方法——串行组合弱学习器以达到更好的泛化性能。另外一种重要集成方法是以随机森林为代表的Bagging并行组合的方式。以“偏差-方差分解”分析，Boosting方法主要优化偏差，Bagging主要优化方差

[Adaboost迭代算法基本思想主要是通过调节的每一轮各训练样本的权重(错误分类的样本权重更高)，串行训练出不同分类器。最终以各分类器的准确率作为其组合的权重，一起加权组合成强分类器。]

图示

描述已自动生成

1997年国际商业机器公司（简称IBM）深蓝超级计算机战胜了国际象棋世界冠军卡斯帕罗夫。深蓝是基于暴力穷举实现国际象棋领域的智能，通过生成所有可能的走法，然后执行尽可能深的搜索，并不断对局面进行评估，尝试找出最佳走法。

1997年，Sepp Hochreiter 和 Jürgen Schmidhuber提出了长短期记忆神经网络(LSTM)。

[LSTM是一种复杂结构的循环神经网络（RNN），结构上引入了遗忘门、输入门及输出门：输入门决定当前时刻网络的输入数据有多少需要保存到单元状态，遗忘门决定上一时刻的单元状态有多少需要保留到当前时刻，输出门控制当前单元状态有多少需要输出到当前的输出值。这样的结构设计可以解决长序列训练过程中的梯度消失问题。]

钟表的特写

低可信度描述已自动生成

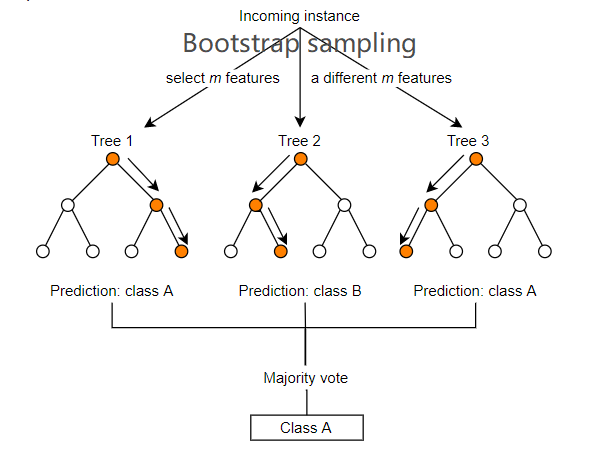
1998年，万维网联盟的蒂姆·伯纳斯·李(Tim Berners-Lee)提出语义网(Semantic Web)的概念。其核心思想是：通过给万维网上的文档（如HTML）添加能够被计算机所理解的语义(Meta data)，从而使整个互联网成为一个基于语义链接的通用信息交换媒介。换言之，就是构建一个能够实现人与电脑无障碍沟通的智能网络。

2001年，John Lafferty首次提出条件随机场模型（Conditional random field，CRF）。CRF是基于贝叶斯理论框架的判别式概率图模型，在给定条件随机场P ( Y ∣ X ) 和输入序列x，求条件概率最大的输出序列y \*。在许多自然语言处理任务中比如分词、命名实体识别等表现尤为出色。

2001年，布雷曼博士提出随机森林（Random Forest）。

随机森林是将多个有差异的弱学习器(决策树)Bagging并行组合，通过建立多个的拟合较好且有差异模型去组合决策，以优化泛化性能的一种集成学习方法。多样差异性可减少对某些特征噪声的依赖，降低方差（过拟合），组合决策可消除些学习器间的偏差。

[随机森林算法的基本思路是对于每一弱学习器(决策树)有放回的抽样构造其训练集，并随机抽取其可用特征子集，即以训练样本及特征空间的多样性训练出N个不同的弱学习器，最终结合N个弱学习器的预测（类别或者回归预测数值），取最多数类别或平均值作为最终结果。]



2003年，David Blei, Andrew Ng和 Michael I. Jordan于2003年提出LDA（Latent Dirichlet Allocation）。

[LDA是一种无监督方法，用来推测文档的主题分布，将文档集中每篇文档的主题以概率分布的形式给出，可以根据主题分布进行主题聚类或文本分类。]

图示

描述已自动生成

2003年，Google公布了3篇大数据奠基性论文，为大数据存储及分布式处理的核心问题提供了思路：非结构化文件分布式存储（GFS）、分布式计算（MapReduce）及结构化数据存储（BigTable），并奠定了现代大数据技术的理论基础。

图片包含 公司名称

描述已自动生成

2005 年，波士顿动力公司推出一款动力平衡四足机器狗，有较强的通用性，可适应较复杂的地形。

2006年，杰弗里·辛顿以及他的学生鲁斯兰·萨拉赫丁诺夫正式提出了深度学习的概念（Deeping Learning），开启了深度学习在学术界和工业界的浪潮。2006年也被称为深度学习元年，杰弗里·辛顿也因此被称为深度学习之父。

[深度学习的概念源于人工神经网络的研究，它的本质是使用多个隐藏层网络结构，通过大量的向量计算，学习数据内在信息的高阶表示。]

图表

描述已自动生成

2010年，Sinno Jialin Pan和 Qiang Yang发表文章《迁移学习的调查》。

[迁移学习(transfer learning)通俗来讲，就是运用已有的知识（如训练好的网络权重）来学习新的知识以适应特定目标任务，核心是找到已有知识和新知识之间的相似性。（知识蒸馏属于其中的特例）]

图示

描述已自动生成

### 2.1.5 蓬勃发展期 [2011年至今]

随着大数据、云计算、互联网、物联网等信息技术的发展，泛在感知数据和图形处理器等计算平台推动以深度神经网络为代表的人工智能技术飞速发展，大幅跨越了科学与应用之间的技术鸿沟，诸如图像分类、语音识别、知识问答、人机对弈、无人驾驶等人工智能技术实现了重大的技术突破，迎来爆发式增长的新高潮。

2011年，IBM Watson问答机器人参与Jeopardy回答测验比赛最终赢得了冠军。Waston是一个集自然语言处理、知识表示、自动推理及机器学习等技术实现的电脑问答（Q&A）系统。

2012年，Hinton和他的学生Alex Krizhevsky设计的AlexNet神经网络模型在ImageNet竞赛大获全胜，这是史上第一次有模型在 ImageNet 数据集表现如此出色，并引爆了神经网络的研究热情。

[AlexNet是一个经典的CNN模型，在数据、算法及算力层面均有较大改进，创新地应用了Data Augmentation、ReLU、Dropout和LRN等方法，并使用GPU加速网络训练。]

图示

描述已自动生成

2012年，谷歌正式发布谷歌知识图谱Google Knowledge Graph），它是Google的一个从多种信息来源汇集的知识库，通过Knowledge Graph来在普通的字串搜索上叠一层相互之间的关系，协助使用者更快找到所需的资料的同时，也可以知识为基础的搜索更近一步，以提高Google搜索的质量。

日程表

描述已自动生成

[知识图谱是结构化的语义知识库，是符号主义思想的代表方法，用于以符号形式描述物理世界中的概念及其相互关系。其通用的组成单位是RDF三元组(实体-关系-实体)，实体间通过关系相互联结，构成网状的知识结构。]

图片包含 图示

描述已自动生成

2013年，Durk Kingma和Max Welling在ICLR上以文章《Auto-Encoding Variational Bayes》提出变分自编码器（Variational Auto-Encoder，VAE）。

[VAE基本思路是将真实样本通过编码器网络变换成一个理想的数据分布，然后把数据分布再传递给解码器网络，构造出生成样本，模型训练学习的过程是使生成样本与真实样本足够接近。]

图示

描述已自动生成

2013年，Google的Tomas Mikolov 在《Efficient Estimation of Word Representation in Vector Space》提出经典的 Word2Vec模型用来学习单词分布式表示，因其简单高效引起了工业界和学术界极大的关注。

图示

描述已自动生成

[Word2Vec基本的思想是学习每个单词与邻近词的关系，从而将单词表示成低维稠密向量。通过这样的分布式表示可以学习到单词的语义信息，直观来看，语义相似的单词的距离相近。]

电脑合成图

中度可信度描述已自动生成

[Word2Vec网络结构是一个浅层神经网络（输入层-线性全连接隐藏层->输出层），按训练学习方式可分为CBOW模型(以一个词语作为输入，来预测它的邻近词)或Skip-gram模型 (以一个词语的邻近词作为输入，来预测这个词语)。]

图示

描述已自动生成

2014年，聊天程序“尤金·古斯特曼”（Eugene Goostman）在英国皇家学会举行的“2014图灵测试”大会上，首次“通过”了图灵测试。

2014年，Goodfellow及Bengio等人提出生成对抗网络（Generative Adversarial Network，GAN），被誉为近年来最酷炫的神经网络。

[GAN是基于强化学习(RL)思路设计的，由生成网络(Generator, G)和判别网络(Discriminator, D)两部分组成， 生成网络构成一个映射函数G: Z→X（输入噪声z, 输出生成的伪造数据x）, 判别网络判别输入是来自真实数据还是生成网络生成的数据。在这样训练的博弈过程中，提高两个模型的生成能力和判别能力。]

图示, 示意图

描述已自动生成

2015年，为纪念人工智能概念提出60周年，深度学习三巨头LeCun、Bengio和Hinton(他们于2018年共同获得了图灵奖)推出了深度学习的联合综述《Deep learning》。

[《Deep learning》文中指出深度学习就是一种特征学习方法，把原始数据通过一些简单的但是非线性的模型转变成为更高层次及抽象的表达，能够强化输入数据的区分能力。通过足够多的转换的组合，非常复杂的函数也可以被学习。]

图示

描述已自动生成

2015年，Microsoft Research的Kaiming He等人提出的残差网络（ResNet）在ImageNet大规模视觉识别竞赛中获得了图像分类和物体识别的优胜。

[残差网络的主要贡献是发现了网络不恒等变换导致的“退化现象（Degradation）”，并针对退化现象引入了 “快捷连接（Shortcut connection）”，缓解了在深度神经网络中增加深度带来的梯度消失问题。]

图示

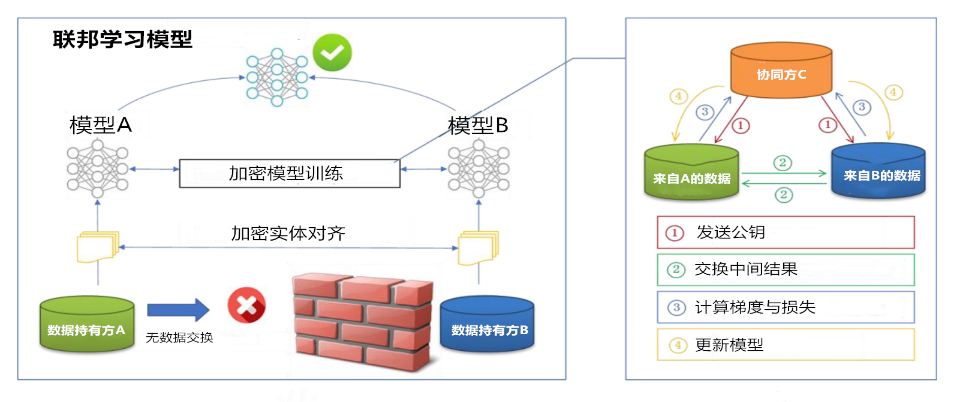
描述已自动生成

2015年，谷歌开源TensorFlow框架。它是一个基于数据流编程（dataflow programming）的符号数学系统，被广泛应用于各类机器学习（machine learning）算法的编程实现，其前身是谷歌的神经网络算法库DistBelief。

2015年，马斯克等人共同创建OpenAI。它是一个非营利的研究组织，使命是确保通用人工智能 (即一种高度自主且在大多数具有经济价值的工作上超越人类的系统）将为全人类带来福祉。其发布热门产品的如：OpenAI Gym，GPT等。

2016年，谷歌提出联邦学习方法，它在多个持有本地数据样本的分散式边缘设备或服务器上训练算法，而不交换其数据样本。

[联邦学习保护隐私方面最重要的三大技术分别是： 差分隐私 ( Differential Privacy )、同态加密 ( Homomorphic Encryption )和 隐私保护集合交集 ( Private Set Intersection )，能够使多个参与者在不共享数据的情况下建立一个共同的、强大的机器学习模型，从而解决数据隐私、数据安全、数据访问权限和异构数据的访问等关键问题。]



### 2.1.6 国产模型

！！！！！！！！！！！！！！！！！！！！！！！！！

## 2.2 大模型基本原理

人工智能研究目的

人工智能（Artificial Intelligence，AI）研究目的是通过探索智慧的实质，扩展人类智能——促使智能主体会听（语音识别、机器翻译等）、会看（图像识别、文字识别等）、会说（语音合成、人机对话等）、会思考（人机对弈、专家系统等）、会学习（知识表示，机器学习等）、会行动（机器人、自动驾驶汽车等）。一个经典的AI定义是：“ 智能主体可以理解数据及从中学习，并利用知识实现特定目标和任务的能力。

人工智能学派

主要思想

代表方法

联结主义

利用数学模型来研究人类认知的方法，用神经元的连接机制实现人工智能

神经网络、SVM等

符号主义

认知就是通过对有意义的表示符号进行推导计算，并将学习视为逆向演绎，主张用显式的公理和逻辑体系搭建人工智能系统

专家系统，知识图谱，决策树等

演化主义

对生物进化进行模拟，使用遗传算法和遗传编程

遗传算法等

贝叶斯主义

使用概率规则及其依赖关系进行推理

朴素贝叶斯等

行为主义

以控制论及感知-动作型控制系统原理模拟行为以复现人类智能

强化学习等

其中，**符号主义及联结主义**为主要的两大派系：

“符号主义”（Symbolicism），又称逻辑主义、计算机学派，认为认知就是通过对有意义的表示符号进行推导计算，并将学习视为逆向演绎，主张用显式的公理和逻辑体系搭建人工智能系统。如用决策树模型输入业务特征预测天气：

图示

描述已自动生成

“联结主义”（Connectionism），又叫仿生学派，笃信大脑的逆向工程，主张是利用数学模型来研究人类认知的方法，用神经元的连接机制实现人工智能。如用神经网络模型输入雷达图像数据预测天气：

图表

描述已自动生成

（语言大模型、多模态、LLM？）

## 2.3 大模型发展路线

### 2.3.1 要素

专家系统（Expert Systems）是AI的一个重要分支，同自然语言理解，机器人学并列为AI的三大研究方向

人工智能有三个要素：数据、算力及算法，数据即是知识原料

图示

描述已自动生成

#### 2.3.1.1 数据

数据是现实世界映射构建虚拟世界的基本要素，随着数据量以指数形式增长，开拓的虚拟世界的疆土也不断扩张。不同于AI算法开源，关键数据往往是不开放的，数据隐私化、私域化是一种趋势，数据之于AI应用，如同流量是互联网的护城河，有核心数据才有关键的AI能力。

图表

描述已自动生成

#### 2.3.1.2 算力

计算是AI的关键，自2010年代以来的深度学习浪潮，很大程度上归功于计算能力的进步。

量子计算发展

在计算芯片按摩尔定律发展越发失效的今天，计算能力进步的放慢会限制未来的AI技，量子计算提供了一条新量级的增强计算能力的思路。随着量子计算机的量子比特数量以指数形式增长，而它的计算能力是量子比特数量的指数级，这个增长速度将远远大于数据量的增长，为数据爆发时代的人工智能带来了强大的硬件基础。

边缘计算发展

边缘计算作为云计算的一种补充和优化，一部分的人工智能正在加快速度从云端走向边缘，进入到越来越小的物联网设备中。而这些物联网设备往往体积很小，为此轻量机器学习（TinyML）受到青睐，以满足功耗、延时以及精度等问题。

类脑计算发展

以类脑计算芯片为核心的各种类脑计算系统，在处理某些智能问题以及低功耗智能计算方面正逐步展露出优势。类脑计算芯片设计将从现有处理器的设计方法论及其发展历史中汲取灵感，在计算完备性理论基础上结合应用需求实现完备的硬件功能。同时类脑计算基础软件将整合已有类脑计算编程语言与框架，实现类脑计算系统从“专用”向“通用”的逐步演进。

人工智能计算中心成为智能化时代的关键基础设施

人工智能计算中心基于最新人工智能理论，采用领先的人工智能计算架构，是融合公共算力服务、数据开放共享、智能生态建设、产业创新聚集的“四位一体”综合平台，可提供算力、数据和算法等人工智能全栈能力，是人工智能快速发展和应用所依托的新型算力基础设施。未来，随着智能化社会的不断发展，人工智能计算中心将成为关键的信息基础设施，推动数字经济与传统产业深度融合，加速产业转型升级，促进经济高质量发展。

当前主流……（显卡NVIDIA）

#### 2.3.1.3 算法

机器学习自动化(AutoML)发展

自动化机器学习（AutoML）解决的核心问题是：在给定数据集上使用哪种机器学习算法、是否以及如何预处理其特征以及如何设置所有超参数。随着机器学习在许多应用领域取得了长足的进步，这促成了对机器学习系统的不断增长的需求，并希望机器学习应用可以自动化构建并使用。借助AutoMl、MLOps技术，将大大减少机器学习人工训练及部署过程，技术人员可以专注于核心解决方案。

图片包含 日程表

描述已自动生成

向分布式隐私保护方向演进

当前全球多个国家和地区已出台数据监管法规，如HIPAA（美国健康保险便利和责任法案）、GDPR（欧盟通用数据保护条例）等，通过严格的法规限制多机构间隐私数据的交互。分布式隐私保护机器学习(联邦学习)通过加密、分布式存储等方式保护机器学习模型训练的输入数据，是打破数据孤岛、完成多机构联合训练建模的可行方案。

数据和机理融合

AI模型的发展是符合简单而美的定律的。从数据出发的建模从数据中总结规律，追求在实践中的应用效果。从机理出发的建模以基本物理规律为出发点进行演绎，追求简洁与美的表达。一个好的、主流的的模型，通常是高度总结了数据规律并切合机理的，是“优雅”的，因为它触及了问题的本质。就和科学理论一样，往往简洁的，没有太多补丁，而这同时解决了收敛速度问题和泛化问题。

神经网络模型结构发展

神经网络的演进一直沿着模块化+层次化的方向，不断把多个承担相对简单任务的模块组合起来。神经网络结构通过较低层级模块侦测基本的特征，并在较高层级侦测更高阶的特征，无论是多层前馈网络，还是卷积神经网络，都体现了这种模块性(近年Hinton提出的“胶囊”（capsule）网络就是进一步模块化发展)。因为我们处理的问题（图像、语音、文字）往往都有天然的模块性，学习网络的模块性若匹配了问题本身内在的模块性，就能取得较好的效果。层次化并不仅仅是网络的拓扑叠加，更重要的是学习算法的升级，仅仅简单地加深层次可能会导致BP网络的梯度消失等问题。

多学派方法融合发展

通过多学派方法交融发展，得以互补算法之间的优势和弱点。如 1）贝叶斯派与神经网络融合，Neil Lawrence组的Deep Gaussian process, 用简单的概率分布替换神经网络层。2）符号主义、集成学习与神经网络的融合，周志华老师的深度随机森林。3) 符号主义与神经网络的融合：将知识库(KG)融入进神经网络，如GNN、知识图谱表示学习。4) 神经网络与强化学习的融合，如谷歌基于DNN+强化学习实现的Alpha Go 让AI的复杂任务表现逼近人类。

基于大规模无(自)监督预训练发展

“如果智能是一块蛋糕，那么蛋糕的大部分是无监督学习，蛋糕上的糖衣是监督学习，而蛋糕上的樱桃是强化学习（RL）——Yann Lecun”监督学习需要足够的带标签数据，然而人工标注大量数据既耗时又费力，在一些领域(如医学领域)上几乎不太可能获得足量的标注数据。通过大规模无(自)监督预训练方法利用现实中大量的无标签数据是一个研究的热点，如GPT-3的出现激发了对大规模自监督预训练方法继续开展探索和研究。未来，基于大规模图像、语音、视频等多模态数据的跨语言的自监督预训练模型将进一步发展，并不断提升模型的认知、推理能力。

基于因果学习方法发展

当前人工智能模型大多关注于数据特征间相关性，而相关性与更为本源的因果关系并不等价，可能导致预测结果的偏差，对抗攻击的能力不佳，且模型往往缺乏可解释性。另外，模型需要独立同分布(i.i.d.)假设(现实很多情况，i.i.d.的假设是不成立的)，若测试数据与训练数据来自不同的分布，统计学习模型往往效果不佳，而因果推断所研究的正是这样的情形：如何学习一个可以在不同分布下工作、蕴含因果机制的因果模型(Causal Model)，并使用因果模型进行干预或反事实推断。

可解释性AI (XAI)发展

可解释的人工智能有可能成为未来机器学习的核心，随着模型变得越来越复杂，确定简单的、可解释的规则就会变得越来越困难。一个可以解释的AI（Explainable AI, 简称XAI）意味着AI运作的透明，便于人类对于对AI监督及接纳，以保证算法的公平性、安全性及隐私性。

图形用户界面, 应用程序

描述已自动生成

## 2.4 国产大模型介绍

（阿里系 -> 通义千问、？系 -> 智谱清言、百度系 -> 文心一言、？系 -> Kimi、？系 -> 豆包、360×）

GitHub / GitLab ，Gitee （Gitcode×）

## 2.5 基本使用 / 本地部署

环境配置，基本技能要求