人工智能导论复习资料　　by 人工智能 2203 班何星奕

一、人工智能概述

1、智能的概念

（1）思维理论：智能的核心是思维，智能来自于大脑的思维活动；

（2）知识阈值理论：智能取决于知识的数量及一般化程度，智能就是在巨大搜索空间中迅速找到一个满意解的能力；

（3）进化理论：智能是复杂系统浮现的性质，用控制取代知识的表示。

2、智能的特征

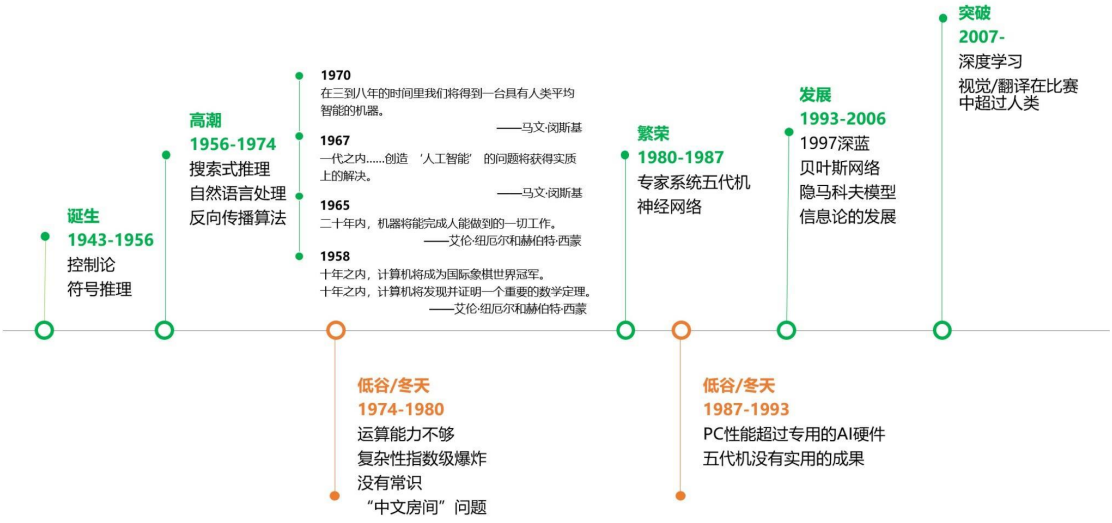
（1）具有感知能力；

（2）具有记忆与思维能力；

（3）具有学习能力；

（4）具有行为能力（表达能力）。

▲3、人工智能发展过程



起源于 1956.8 达特茅斯会议，首次提出“人工智能”概念；

1956 年为人工智能元年，约翰·麦卡锡为人工智能之父；

1970-1988——知识应用时期：以知识为中心；1986 至今——集成发展时期：计算智能。

▲强人工智能与弱人工智能：

弱人工智能：主要关注执行结果，是否模拟人类并不重要；

强人工智能：模拟人类、能够执行“通用任务”的人工智能；

▲4、人工智能主要学派

（1）符号主义（逻辑主义、心理学派或计算机学派）

原理：物理符号系统假设和有限合理性原理；

起源：数理逻辑；

认为人类认知和思维的基本单元是符号，而认知过程就是在符号表示上的一种运算；

致力于用计算机的符号操作来模拟人的认知过程。

（2）连接主义（仿生学派或生理学派）

原理：神经网络和神经网络间的连接机制和学习算法；

起源：仿生学和人脑模型的研究；

强调智能活动是由大量简单的单元通过复杂的相互连接后得到的结果。

（3）行为主义（进化主义或控制论学派）

原理：控制论及感知-动作型控制系统；

起源：控制论；

把神经系统的工作原理与信息理论、控制理论、逻辑以及计算机联系起来，模拟人在控制过程中的智能行为和作用。

二、搜索

1、基于算法的系统（物理规则）

任何有穷问题都有算法；

能用算法解决的问题，必须满足条件：可计算、有限长度（算法描述）、有限时间；

算法的局限：需要领域专业知识，缺乏全面认识；无明显规则约束，较难用显式算法建模。

2、基于搜索的系统（暴力主义）

通过探查和回溯的方法寻找解；

优势：可能利用部分知识解决问题；

缺陷：搜索状态爆炸<--固有矛盾-->规则集不完全。

3、基于实例的系统（经验主义）

给定一组输入和结果是一个问题的实例，就可能实现一个简单求解程序（死记硬背）；

推而广之：“归纳”或“学习”-->机器学习。

4、搜索方向

（1）数据驱动：从初始状态出发的正向搜索；

（2）目的驱动：从目的状态出发的逆向搜索；

（3）双向搜索：正、逆向同时进行，直到在中间某处汇合。

▲5、搜索策略

（1）盲目搜索：在不具有对特定问题的任何有关信息的条件下，按固定的步骤（依次或随机调用操作算子）进行搜索；

（2）启发式搜索：考虑特定问题领域可应用的知识，动态地确定调用操作算子的步骤，优先选择较适合的操作算子，尽量减少不必要的搜索，以求尽快达到结束状态。

▲6、状态空间表示方法

状态空间图：反映问题的实际结构，但空间复杂度高，仅用于小规模问题；

搜索树：展示起点至终点路径，直观表示问题解决过程，但可能造成搜索和计算冗余。

▲7、深度优先搜索

先子状态后兄弟状态搜索，无法保证搜索结果为最短路径。

▲8、宽度优先搜索

先兄弟状态后子状态搜索，逐层扩展，对于有解问题必能找到解。

▲9、统一代价搜索（在宽度优先基础上可以考虑权重影响）

以 g(n)=从根节点到节点 n 的代价为依据，选择 g(n)最小的节点扩展。

▲▲10、启发式搜索策略

启发式信息：用来简化搜索过程有关具体问题领域的特性信息；

适合采用启发式策略的基本情况：

（1）存在问题陈述和数据获取的模糊性，可能会使待求解问题没有一个确定解；

（2）状态空间特别大，搜索中生成扩展的状态数会随着搜索的深度呈指数级增长；

启发信息分类：

按运用的方法分类：

（1）陈述性启发信息：用于更准确、更精炼地描述状态；

（2）过程性启发信息：用于构造操作算子；

（3）控制性启发信息：表示控制策略的知识；

按作用分类：

（1）用于扩展节点的选择（决定扩展哪一节点）；

（2）用于生成节点的选择（决定生成哪些后继节点）；

（3）用于删除节点的选择（决定删除哪些无用节点）；

估价函数表达式：f (n) = g (n) + h (n)；

g (n)：从初始节点 S_0 到节点 n 的实际代价；

h (n)：从节点 n 到目标节点 S_g 的最优路径的估计代价，即启发函数；

h (n)比重小可降低搜索工作量，但可能无法找到最优解；

h (n)比重大则工作量加大，极端情况下变为盲目搜索，但可能可以找到最优解；

统一代价搜索：f (n) = g (n)，每次选择最小的实际代价进行遍历；

最佳优先搜索：f (n) = h (n)，每次选择最小的估计代价进行遍历；

A 搜索算法：f (n) = g (n) + h (n)，每次选择最小估价函数进行遍历；

A*搜索算法（最佳图搜索算法）：定义 h (n) <= h*(n)（最优路径代价），可找到最优解；

A*搜索的最优性条件：

（1）启发函数的可采纳性：h (n) <= h*(n)，有解问题存在最优解时必能找到；

（2）启发函数的一致性/单调性：h (n) <= c (n, n') + h (n')；

启发函数的信息性：h (n)越大，信息性越多，所搜索的状态越少。

11、贪心算法（寻找局部最优解，期望实现全局最优，无法保证得到全局最优解）

无后效性：某个状态以前的过程不会影响以后的状态，只与当前状态有关；

Dijkstra 算法：每次选择已有点位外最短距离的点，纳入已有点位，然后不断更新。

三、机器学习

▲1、机器学习的基本概念

特征 x、特征向量 X；

标签 y；

样本（示例）；

数据集：一组样本构成的集合，可分为训练集（训练模型）、测试集（测试模型）两种；

机器学习的内涵：希望从函数集合 F 中自动寻找一个“最优”的函数 f *(x)，以实现样本特征向量 x 和标签 y 之间的真实映射关系。

▲2、机器学习的三要素

（1）模型：类似于函数；

（2）学习准则

衡量模型好坏可以通过期望风险 $\mathcal{R}(\theta)$，期望风险未知时，通过经验风险近似；

经验风险最小化准则用来降低训练集训练的错误率，但可能造成过拟合；

正则化：引入参数的先验，使其不要过度地最小化经验风险；

（3）优化算法：找到最优模型（不考虑过拟合问题）；

▲▲3、机器学习方法与分类

（1）监督学习：已知输入输出，学习标记的训练样本来训练模型，但数据标注成本较高；

（2）无监督学习：已知输入，仅对输入数据分析，但学习过程困难、发展缓慢；

K-means 聚类：初始化集群中心，每个点选择距离最短的集群中心纳入集群，结束后按集群各点平均值重新确定集群中心，然后重复选点、改中心，直至完全收敛；

（3）强化学习：不断交互，调整策略，谋求最大奖励值；

（4）弱监督学习：数据标签允许是不完全的、不确切、不精确的；

（5）迁移学习：数据独立同分布不成立时，可将已学知识迁移至新问题中；

（6）更多……学习

其中，（1）、（2）、（3）为机器学习三大范式

4、常用定理

（1）没有免费午餐定理：不存在一种机器学习算法适合于任何领域或任务；

（2）丑小鸭定理：分类结果取决于选择的特征，特征的选择又依赖于任务的目的；

（3）奥卡姆剃刀原理：正则化思想：简单模型泛化能力更好，性能相近时选择简单模型；

▲归纳偏置：很多学习算法经常会对学习的问题做一些假设，这些假设就称为归纳偏置，可以理解为人为假设；

5、机器学习与人工智能

（1）模式识别（感知）：建立模型刻画已有的特征；

（2）机器学习（思考）：根据样本训练模型；

（3）深度学习：是一种实现机器学习的技术。

四、符号学派

1、符号主义

观点：“认知即计算”，知识是信息的一种形式，是构成智能的基础，知识表示、知识推理、知识运用是人工智能的核心；

具体做法：符号（表示）和逻辑（推理）的组合；

2、知识特性：相对正确性（一定条件和环境下）、不确定性、可表示性与可利用性；

3、推理方式及分类

（1）演绎推理（一般-->个别）、归纳推理（个别-->一般）、默认推理（默认假设成立）；

（2）确定性推理（条件确定，结论确定）、不确定性推理（条件不都确定，结论不确定）；

（3）单调推理（不断向前推进）、非单调推理（否定已推出的结论）；

（4）启发式推理、非启发式推理；

启发性知识：与问题有关且能加快推理过程、提高搜索效率的知识；

4、推理方向：正向、逆向、混合（正向逆向结合，交叉验证）、双向（正向逆向同时进行）；

5、一阶谓词逻辑表示法：基本同离散数学；

▲6、自然演绎推理：从一组已知为真的事实出发，运用经典逻辑推理规则推出结论；

（1）P 规则（前提引入）；

（2）T 规则（结论引用）；

（3）假言推理：（P , P→Q）--> Q；

充分条件：如果（前件），则（后件）-->承认前件就承认后件；否认后件就否认前件；

必要条件：只有（前件），才（后件）-->否认前件就否认后件；承认后件就承认前件；

充要条件：当且仅当-->承认/否认其中的一个，就必须承认/否认其中的另一个；

（4）拒取式推理：（P→Q，﹁Q）--> ﹁P；

▲7、归结演绎推理：是一种反驳方法（反证法）；

子句集的一些基本定义：

（1）原子谓词：不能再分解的命题；

（2）文字：原子谓词公式及其否定；

（3）子句：任何文字本身及其析取式；

（4）空子句：不包含任何文字的子句，是永假、不可满足的；

（5）子句集：由子句构成的集合（各子句是合取关系）；

8、鲁滨逊归结原理（消解原理，是机器定理证明的基础）

定理：谓词公式不可满足的充要条件是其子句集不可满足；

9、命题逻辑消解推理规则

（1）命题逻辑中的归结原理

（﹁P∨Q，﹁Q∨R）--> ﹁P∨R；

（2）谓词逻辑中的归结原理

子句中含有变元，不能直接消去互补文字，应当先对变元进行代换才能继续归结操作；

10、归结反演（应用归结原理证明定理，可以理解为反证法）

列写题干条件，将结论取反作为条件，最终推出空子句，则证明结论为真；

11、产生式

通常用于表示事实、规则以及它们的不确定性度量，适合于表示事实性知识和规则性知识；

（1）确定性规则知识的产生式表示：IF P THEN Q 或 P →Q；

（2）不确定性规则知识的产生式表示：IF P THEN Q（置信度）或 P →Q（置信度）；

（3）确定性事实性知识的产生式表示：（对象，属性，值）或（关系，对象 1，对象 2）；

（4）不确定性事实性知识的产生式表示：（对象，属性，值，置信度）或（关系，对象 1，对象 2，置信度）；

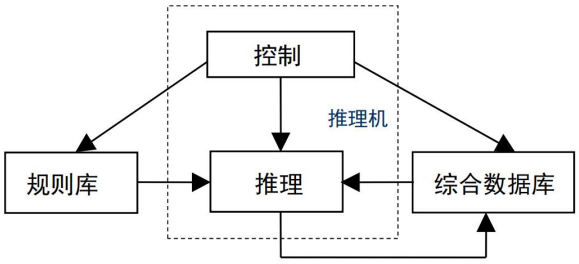
蕴含式是产生式的一种特殊情况，仅能表示精确知识；产生式可以表示不精确知识；

▲产生式系统的一些概念：

（1）规则库：用于描述相应领域内知识的产生式集合；

（2）综合数据库：用于存放问题求解过程中各种当前信息的数据结构；

（3）控制系统（推理机）：由一组程序组成，负责整个产生式系统运行，实现问题求解；



特点：将可用规则与已知事实匹配，成功匹配称为推理，是专家系统中的核心内容；

▲12、C-F 模型（基本方法）

可信度：根据经验对一个事物或现象为真的相信程度；

可信度方法带有较大的主观性和经验性，但直观、简单且有效；

（1）知识不确定性的表示：IF E THEN H (CF(H,E))

可信度因子 CF(H,E)：该条知识的可信度，在[-1, 1]上取值，由领域专家直接给出；

大于 0 为结论 H 为真的可信度，小于 0 为结论 H 为假的可信度，等于 0 则 H 与 E 无关；

（2）证据不确定性的表示：CF(E)＝0.6 则认为 E 的可信度为 0.6

CF(E)也在[-1, 1]上取值，取值意义与可信度因子一致；

（3）组合证据不确定性的算法

证据合取（与）则取最小可信度，证据析取（或）则取最大可信度；

（4）不确定性的传递算法

CF(H) = CF(H, E)×max{0,CF(E)}，即结论 H 的可信度 = 知识的可信度×证据的可信度；

（5）结论不确定性的合成算法

$$CF_{1,2}(H)=\begin{cases} CF_1(H)+CF_2(H)-CF_1(H)CF_2(H) & 若CF_1(H)\geq 0,\ CF_2(H)\geq 0 \\ CF_1(H)+CF_2(H)+CF_1(H)CF_2(H) & 若CF_1(H)<0,\ CF_2(H)<0 \\ \dfrac{CF_1(H)+CF_2(H)}{1-\min\{|CF_1(H)|,|CF_2(H)|\}} & 若CF_1(H)与CF_2(H)异号 \end{cases}$$

▲13、DS 证据理论

DS 证据理论目的：

（1）表达由“不知道”带来的不确定性（信息很少）；

（2）处理信息模糊/冲突情况；

DS 证据理论用途：根据各项已知概率给出每种假设的综合概率，对不同数据源数据融合；

基本概念：

（1）识别框架（样本空间、论域）：对问题所能认识到的可能结果组成的集合 X；

X 的幂集（记作 2^X）：X 中所有子集组成的集族；

（2）基本概率分配：给 2^X 每一个元素（假设）分配一个概率（测度），称为 Mass 函数，表示相信的程度（空集的 Mass 函数值为 0，全集合 Mass 函数值累加值为 1）；

焦元：对于 X 的子集 A，使得 m(A)>0 的 A；

（3）信任函数（记作 Bel()）：A 的所有子集的概率之和，表达概率的下限，即对命题 A 为真的总的信任程度；

$$Bel(A)=\sum_{B\subseteq A} m(B),\quad \forall A\subseteq X$$

（4）似真（然）函数（记作 Pl()）：所有与 A 存在交集的集合的概率之和，表达概率的上限，即对命题 A 非假的信任程度；

$$Pl(A)=\sum_{B\cap A\neq\varnothing} m(B)\ =1-Bel(\neg A)\qquad \forall A\subseteq X$$

（5）信任区间：表示对某个命题的确认程度，表示为[Bel(A),Pl(A)]；

Dempster 合成规则（证据合成公式）：

（1）计算归一化常数 K（表示证据间冲突程度）

$$K=\sum_{A_1\cap\cdots\cap A_n\neq\varnothing} m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n)\ =1-\sum_{A_1\cap\cdots\cap A_n=\varnothing} m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n)$$

（2）分别计算各项假设的综合概率

$$(m_1\oplus m_2\oplus\cdots\oplus m_n)(A)=\frac{1}{K}\sum_{A_1\cap A_2\cap\cdots\cap A_n=A} m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n)$$

基于证据理论的推理过程：

（1）建立问题的样本空间 X；

（2）计算 Mass 函数；

（3）将不同来源的 Mass 函数根据 Dempster 合成规则进行组合；

（4）计算所关心子集的信任函数值 Bel(A)或似然函数值 Pl(A)；

（5）由信任函数值或似然函数值得出结论；

证据理论优点：

（1）先验数据比概率论数据更易获得；

（2）可融合多种数据和知识；

（3）能处理由“不知道”带来的不确定性；

证据理论缺点：

（1）证据必须独立（样本空间元素必须互斥）；

（2）证据合成规则缺乏坚固的理论支持；

（3）计算存在“指数爆炸”；

（4）某些情况下得到的结果违背常理（Zadeh 悖论，证据互相矛盾时无法推理）；

14、模糊集合和隶属函数

模糊集合是经典集合的扩充，模糊逻辑中引入隶属度的概念，描述介于真/假中间的过程；

$$A = \{(x, \mu_A(x)), x \in X\}$$

其中 A 为模糊集合，x 为元素，X 为元素 x 的论域，$\mu_A(x)$为元素属于模糊集 A 的隶属度；

▲模糊集合的表示法：

- 论域离散且元素数有限：Zadeh表示法

$$A = \{\mu_A(x_1)/x_1, \mu_A(x_2)/x_2, \cdots, \mu_A(x_n)/x_n\}$$

- 论域连续或元素数无限

$$A = \int_{x \in U} \mu_A(x)/x$$

- 序偶表示法

$$A = \{(\mu_A(x_1), x_1), (\mu_A(x_2), x_2), \cdots, (\mu_A(x_n), x_n)\}$$

- 向量表示法 $A = \{\mu_A(x_1), \mu_A(x_2), \cdots, \mu_A(x_n)\}$

模糊关系：描述两个模糊集合中的元素之间的关联程度，用叉乘表示；

模糊关系的合成：S（Q 与 R 的合成）等于模糊矩阵 Q 与 R 的叉乘

$$Q \in X \times Y, R \in Y \times Z \qquad S \in X \times Z$$

▲模糊关系合成常用方法：

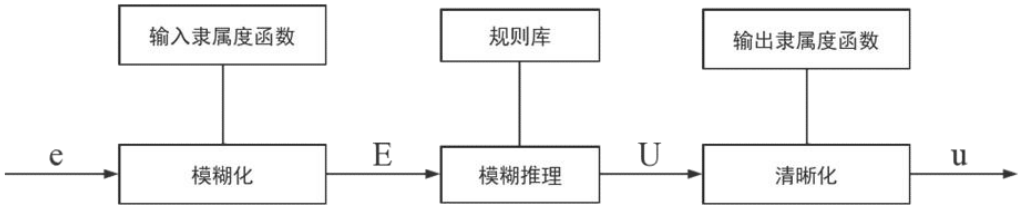
（1）最大-最小合成法：乘积运算用取小运算代替，求和用最大运算代替；

（2）最大-代数积合成法：求和运算用取大运算代替，乘积运算不变；

▲模糊推理法：

模糊知识表示：（<对象>，<属性>，（<属性值>，<隶属度>））；

许多模糊规则可以表示为从条件论域到结论论域的模糊关系矩阵 R。通过条件模糊向量与模糊关系 R 的合成进行模糊推理，得到结论的模糊向量，然后采用“清晰化”方法将模糊结论转换为精确量。



▲对 IF A THEN B 类型的模糊规则的推理：

- **若已知输入为A，则输出为B；若现在已知输入为A'，则输出B'**

用合成规则求取为： $B' = A' \circ R$

其中A 到B模糊的关系R: $\mu_R(x,y) = \min[\mu_A(x), \mu_B(y)]$

模糊决策：由模糊推理得到的结论或者操作是一个模糊向量，需要转化为确定值；

▲模糊决策方法：

（1）最大隶属度法：取隶属度最大的量作为推理结果；

（2）加权平均判决法：将各隶属度作为权值进行加权平均；

（3）中位数法：论域上把隶属函数曲线与横坐标转成的面积平分为两部分的元素称为模糊集的中位数；

15、语义网络与知识图谱

传统知识工程（方法）缺点：自上而下严重依赖专家和人的干预，知识获取和应用困难；

知识图谱地位：

（1）作为一种技术体系，是大数据时代知识工程的代表性进展；

（2）作为一门学科，知识图谱属于人工智能范畴；

（3）知识表示是发展知识工程最关键的问题之一，知识图谱是知识表示的一个重要方式；

语义网络：以图形化 (Graphic)的形式，由点和边组成（类似数据库的 ER 图）；

知识图谱本质上是一种大规模语义网络，富含实体、概念（实体集）及其之间的各种语义

关系，是大数据时代知识表示的重要方式之一；

知识图谱组成：实体、概念、值、关系、属性；

知识图谱优势：尺度大、语义丰富、质量高、结构易实现；

知识图谱挑战：高质量模式缺失、封闭世界假设不成立、大规模自动化知识获取成为前提；

知识的类别：事实知识、概念知识、词汇知识、常识知识、其他知识；

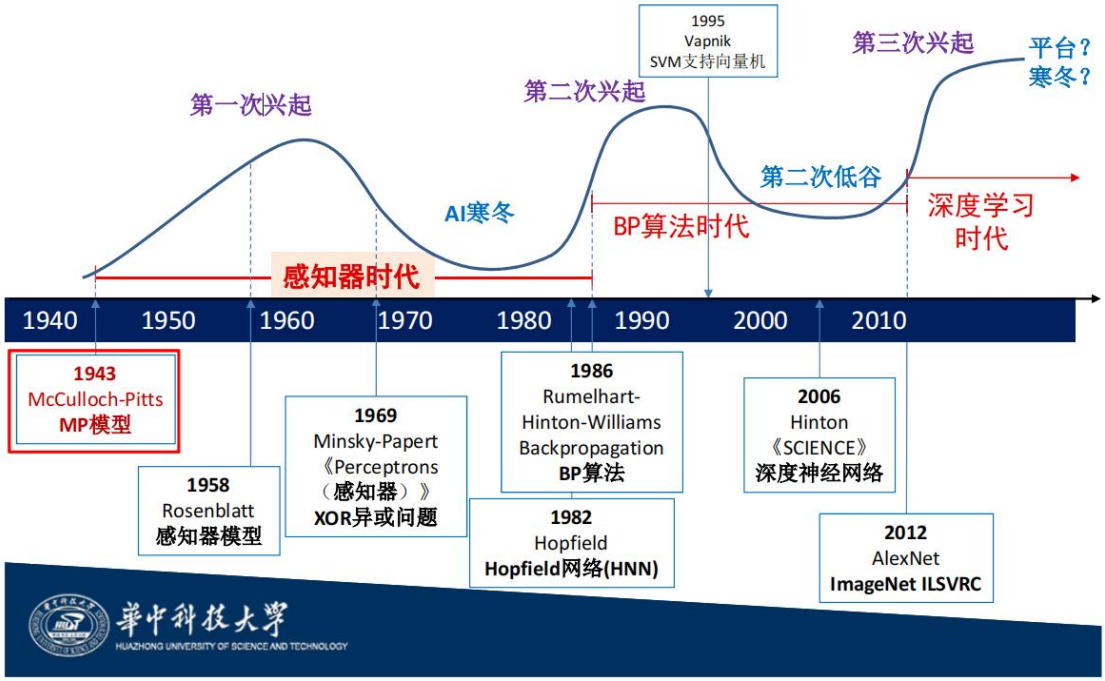
领域知识图谱构建流程：（1）模式设计；（2）明确数据来源；（3）词汇挖掘；

（4）实体发现；（5）关系发现；（6）词汇挖掘；（7）质量控制；（8）人工干预；

知识图谱推理的主要任务和作用：问句扩展、图谱补全、错误检测、关联关系推理。

五、连接学派-历史基础结构

▲1、人工神经网络发展简史



（1）MP 模型（1943）

建模人工神经元，为验证型模型；

MP 模型输入和输出均为布尔型，采用阶跃响应函数，模型没有可学习的权重；

▲（2）感知器模型（1958）

感知器将输入空间通过一个（超）平面划分为两个半空间，可以完成分类任务；

感知器模型允许输入和输出为实值，采用阶跃响应函数，模型有可学习的权重；

限制：为线性模型，无法解决线性不可分问题，少量不可分样本都会导致学习的不收敛；

（3）ADALINE 模型（1960）

是多层网络中 BP 算法的先驱，广泛应用于现在的信号处理过程；

激活函数：由阶跃函数变为连续函数；

量化函数：增加了 Quantizer 用于类别预测；

定义了代价函数的概念（均方误差），使用梯度下降优化权重；

▲（4）XOR 问题

异或问题不是线性可分，无法用单一感知器找到 XOR 问题的分类面（需要三层感知器）；

XOR 问题造成了 AI 寒冬，后者在 1973 年左右开始；

（5）Hopfield 神经网络（HNN）（1982）

是一种递归和反馈神经网络，输出到输入均有反馈连接；

Hopfield 网络能够收敛到一个或者几个稳定的状态（吸引子）；

Hopfield 网络具有内容可寻址存储或者联想存储的能力，常用于模式识别和组合优化问题；

（6）BP 神经网络（1986）

为训练多层感知器提供方法，让神经网络的发展迎来了第二春；

“万能近似定理”证明了神经网络的表达能力：多层前馈网络可以近似任意函数；

BP 网络存在的问题：维度灾难（大规模问题维度大）、泛化问题（不一定找到最优解）；

（7）支持向量机（SVM）（1963）

处理非线性可分问题时，利用“核函数”来完成转换；

相较于神经网络的优势：无需调参，速度快，全局最优解；

标志着神经网络第二次进入低谷期；

（8）深度学习时代（2006）

神经网络的再次翻身，利益于在一些经典困难问题上取得了显著成效：

2006 手写字符识别 MNIST（深度信念网络 DBN）；

2010 语音识别；

2012 图像分类（AlexNet，8 层深度网络）；

2016 围棋人机大战击败李世石（AlphaGo，基于深度神经网络+强化学习）；

算法哲学：模块化+层次化，拓扑叠加+算法升级，对复杂问题“分而治之”；

工程成本：大量深度学习工具的出现，大大降低了神经网络的入门门槛；

存在的问题：

暴力美学：拼数据，拼资源，成本高昂；

炼丹：可解释性和定向优化能力差；

与符号主义的交融：先验知识如何表达、如何融入网络；

▲2、前馈神经网络（BP 神经网络）（近似函数）

▲目标：逼近某个函数 f*，通过定义一个映射并调整参数，尝试获得一个最好的 f*的逼近；

作用：通常用于监督式机器学习或模式识别任务；

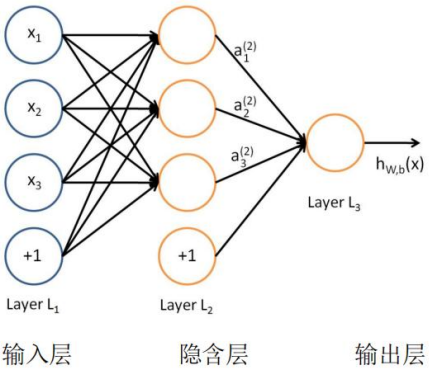
▲特点：相比于感知器模型增加了非线性的激活单元，使得网络拥有了非线性建模能力；

▲前馈神经网络主要由三种类型的网络层构成：输入层、隐含层、输出层；

隐含层的个数可以是任意的，神经元的个数也可以是任意的，在实践中通常作为超参数；

同层不连接，相邻层之间的神经元两两连接，是一个全连接的结构，故也称为全连接层；

输入层和隐含层通常会额外增加一个偏置单元；



标准前馈神经网络使用“S”型的非线性激活函数：Logistic 函数和 Tanh 函数；

非线性激活函数的存在是使网络拥有非线性建模能力的关键；

前向传播：由输入层向输出层传播；

后向传播：用于网络参数的更新，核心为链式法则；

BP 网络的学习由损失函数驱动，目的为调整前馈神经网络的连接权重，使网络的输入与输出与给定的样本相同，需要从输出层往回求损失函数对网络中每个权重的偏导数，因此叫做后向（反向）传播；

计算方法：

对输出层，d = 激活函数求导×实际输出和样本值之差；

对隐层，d = 激活函数求导×与更深一层相连的每个神经元的 d’*w 之和；

$\Delta w_{ij}^{k-1} = -\varepsilon d_i^k y_j^{k-1}$ 因此求它即可得到权值的修正量

▲前馈神经网络的特点：

多层前向网络（输入层、隐层、输出层），可为任意的网络模型（卷积、全连接）；

连接权值：通过学习算法进行修正；

神经元传输函数：非线性激活函数；

学习算法：正向传播、反向传播；

层与层的连接是单向的，信息的传播是双向的；

优点：强大逼近特性、较强的通用能力（实现任意函数的拟合）、具有较好的容错性；

缺点：收敛速度慢、可能陷入局部极值、没有选择隐层数和隐层结点数的通用准则；

▲3、Hopfield 网络（HNN）（解决优化问题）

是一种单层、全连接、固定参数的递归和反馈神经网络，输出到输入均有反馈连接；

开拓了神经网络用于联想记忆和神经优化的新途径；

每个神经元既是输入也是输出，输入包含自身输入；

引入能量函数的概念，判断网络运行的稳定性；

▲有离散型（适用于联想记忆）和连续性（适用于优化问题）两种：

（1）离散 Hopfield 神经网络（DHNN）

二值神经网络，单层网络，各节点无自反馈，存在异步（串行）和同步（并行）工作方式；

稳定判据：某一时刻开始，其中所有神经元的状态不再改变；

W 是对角元为 0 的对称矩阵，网络具有串行稳定性，但可能受到串扰问题影响（误判）；

▲联想记忆（应用）：记忆训练样本输入→自联想记忆→对测试样本去噪；

（2）连续 Hopfield 神经网络（CHNN）

比 DHNN 更接近生物神经元的特性，神经元状态可以取连续值，激活函数为“S”型连续函数，各神经元同步工作；

稳定判据：神经元传递函数连续且有界，且权值系数矩阵对称；

▲Hopfield 神经网络与优化：

起始于 1985 年 Hopfield 和 Tank 将 HNN 网络用于求解经典的旅行商问题（TSP）；

CHNN 求解优化问题的动机：如果一个优化问题的代价函数能被写为 Hopfield 能量函数的形式，那么 Hopfield 网络平衡态处于的点可以代表优化问题的解；

玻尔兹曼机（BM）：

可以通过让每个单元按照一定的概率分布发生状态变化，来避免陷入局部最优解；

BM 可由可见单元和隐藏单元共同构成，存在部分神经元不与外部相连（隐单元）；

神经元的状态为 0 或 1 的概率取决于相应的输入；

受限玻尔兹曼机（RBM）：

含有隐藏变量的波尔兹曼机训练非常困难，故提出 RBM；

学习目标：最大化似然；

深度玻尔兹曼机（DBM）：

把隐藏层的层数增加，多个受限玻尔兹曼机堆栈构成 DBM；

深度信念网络（DBN）：

在靠近可视层的部分使用贝叶斯信念网络，在最远离可视层的部分使用 RBM，可得 DBN；

最底层为可观测变量，其他均为隐变量；

最顶部连接是无向的，其他层之间连接是有向的；

作用：识别特征、分类数据、生成数据；

▲4、循环神经网络（RNN）（近似动力学系统）

序列化数据：存在顺序依赖的数据；

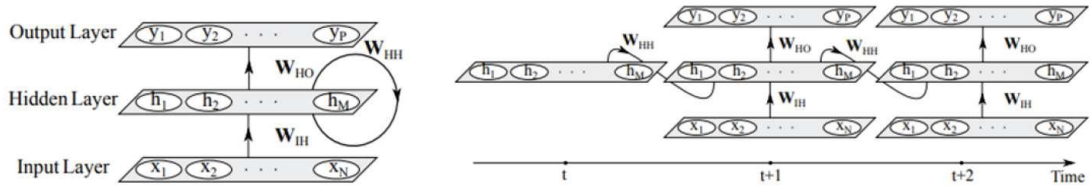
解决序列问题→序列建模→需要解决的问题：

处理变长序列、保留序列顺序、能建模上下文依赖、全序列共享模型参数→提出 RNN；

▲RNN 基本结构：

是一种为适应序列化数据的序列特性而设计的神经网络，具有短期记忆能力并能够在序列化数据上进行端到端的学习和计算；

RNN 的两种计算图表示方法：折叠表示、展开表示；



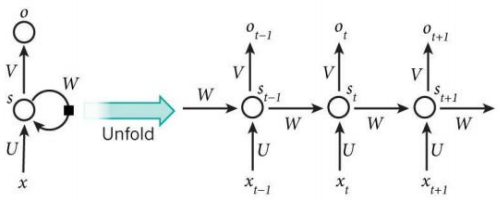
(a) Folded RNN. (b) Unfolded RNN through time.

展开的 RNN 结构：由于序列的序列特性，特征 s_t 不仅仅取决于当前输入 x_t，还取决于 s_{t-1}；

即RNN可表示为：

$$\mathbf{o}_t = g(\mathbf{V}\mathbf{s}_t),$$

$$\mathbf{s}_t = f(\mathbf{U}\mathbf{x}_t + \mathbf{W}\mathbf{s}_{t-1})$$



RNN 的通用近似定理：一个完全连接的循环神经网络可近似任何非线性动力系统；

▲RNN 典型应用：

（1）自然语言处理：情感分类（序列到类别）、中文分词（同步序列到序列）、信息抽取（同步序列到序列）、机器翻译（异步序列到序列）；

（2）计算机视觉：图像描述/看图说话、手写体识别；

（3）多媒体：计算机合成音乐；

RNN 优点：可处理任意长度序列、参数共享（权重系数）、通用计算能力（支持任意精度）；

RNN 缺点：建模的单向性、长序列的记忆丢失（梯度消失）；

▲长序列梯度爆炸与消失的原因：

（1）计算损失函数对权重的梯度时，很大影响梯度结果是激活函数求导值连乘的这项；

（2）循环网络要在很长时间序列的各个时刻重复对激活函数求导值连乘；

（3）连乘项若在量级上大于 1 则会爆炸，小于 1 时则会消失（梯度消失，大部分情况）；

▲改善梯度消失的途径：改进 RNN 的结构（LSTM、GRU 等）、使用合适的激活函数（tanh）；

RNN 模型的问题：长序列记忆丢失（梯度消失）、关系建模单向性的局限→提出 LSTM；

长短期记忆网络（LSTM）：

引入门控机制，特定设计节点的各个状态与各状态更新方式，解决 RNN 记忆丢失的问题；

引入自循环，产生梯度长时间持续流动的路径（解决梯度消失的根本原因）；

LSTM 使用两个状态来建模节点的状态：

（1）细胞状态（cell state）C 长记忆；

（2）隐藏状态（hidden state）h 短记忆；

LTSM 构建了三个门（gate）来更新状态：遗忘门、输入门、输出门；

一个 LSTM 单元可以被表示为一个多输入多输出函数，输入为上一个时间节点的细胞状态 c_{t-1}、上一个时间节点的隐藏状态 h_{t-1} 和当前的输入 x_t，输出为当前的细胞状态 c_t、当前的隐藏状态 h_t 和输出 y_t；

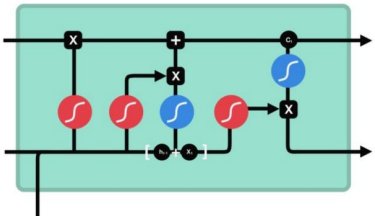
遗忘门：生成用来控制自循环的权重，权值视上下文动态调整，主要对上一个节点传进来的输入进行选择性忘记；

输入门：将这个阶段的输入有选择性地进行记忆；

细胞状态更新：有选择地忘记+有选择地记忆；

输出门：输出可以由输出门关闭（LSTM 中：长记忆 C、短记忆 h）；

$$
\begin{aligned}
\mathbf{f}_t &= \sigma(\mathbf{W}_f[\mathbf{h}_{t-1}, \mathbf{x}_t] + \mathbf{b}_f) \\
\mathbf{i}_t &= \sigma(\mathbf{W}_i[\mathbf{h}_{t-1}, \mathbf{x}_t] + \mathbf{b}_i) \\
\mathbf{o}_t &= \sigma(\mathbf{W}_o[\mathbf{h}_{t-1}, \mathbf{x}_t] + \mathbf{b}_o) \\
\tilde{\mathbf{C}}_t &= tanh(\mathbf{W}_C[\mathbf{h}_{t-1}, \mathbf{x}_t] + \mathbf{b}_C) \\
\mathbf{C}_t &= \mathbf{f}_t \otimes \mathbf{C}_{t-1} + \mathbf{i}_t \otimes \tilde{\mathbf{C}}_t \\
\mathbf{y}_t &= \mathbf{h}_t = \mathbf{o}_t \otimes tanh(\mathbf{C}_t)
\end{aligned}
$$



LSTM 与 RNN 的联系：

（1）同样采取了循环链式结构；

（2）都假设了元素之间的依赖关系是单向的；

LSTM 与 RNN 的区别：

（1）LSTM 引入了大量的非线性单元，为不同状态引入丰富的非线性性；

（2）LSTM 增加了细胞状态 C_t 和门控单元用于有选择性地建模长期记忆；

双向 RNN：

时刻 t 的输出不仅取决于之前时刻的信息，还取决于未来的时刻；

每个隐藏层有两个节点，分别进行正向计算和反向计算，输出层由这两个值决定；

正向计算和反向计算的权重不共享；

六、连接学派-深度学习 CNN

1、浅层学习：机器学习的第一次浪潮（以反向传播算法的发明为标志）

浅层机器学习模型：支撑向量机（SVM）、Boosting、最大熵方法（LR）；

机器视觉感知的流程：

经典视觉感知流程中的若干关键步骤均依赖人手工设计；

传统视觉描述子：尺度不变特征变换、梯度方向直方图、纹理描述

视觉中经典描述子的特征编码过程过于抽象，表达能力有限；

不同视觉任务下，描述子表现不一，通用性不足；

对于新的任务，需要通过试错的方式选择描述子，甚至需要重新发明新的描述子；

深度学习流行之前，主流图像分类均基于词袋模型（对底层描述子的再次抽象）；

2、深度学习（特征学习、表示学习）：机器学习的第二次浪潮

▲生物学启发（动机）：发现了视觉系统的信息处理机制；

生物学证据：

（1）神经元具有一个很小的局部感受野；

（2）方向选择性细胞；

（3）视觉系统的信息处理是分级的，由低级模式组合成的高级模式做出反应；

▲深度学习的思想：

层级思想：通过堆叠神经网络的层来模拟人类视觉；

模块化思想：分层，模块化处理；

深度学习的挑战：算力限制、算法限制（梯度消失）；

Hinton 在《Science》发表的论文提出了一种在前馈神经网络中进行有效训练的算法，做出重大贡献，展现了神经网络具有特征学习能力，降低了深度神经网络的训练难度；

▲深度学习强调模型结构的深度，明确突出特征学习的重要性；

▲深度学习在 ImageNet 上的巨大成功得益于成熟的算法（卷积神经网络）、强大算力的使用（GPUs）、以及之前被忽略的——大规模的数据集（大数据）；

▲核心思想：

（1）从数据中学习数据间的统计特性以及相关性；

（2）学习的表达可以作为特征用于不同的任务中；

（3）研究目标是通过发现有效的学习算法，学习层次化的特征分布与表达，通常更高层应表达更加抽象的特征；

3、深度卷积神经网络

科学与生理学启发：

（1）整体结构：简单细胞（卷积）+复杂细胞（池化）；

（2）局部感受野（局部性）；

（3）在视场中的自适应感受野（权值共享）；

（4）视觉皮层中的下采样率（2 到 3）；

▲基本构成：卷积层、池化层、非线性激活单元、归一化层、全连接层与分类器；

▲（1）卷积：按卷积核对图像局部像素进行加权求和的过程；

给定输入 x 以及一个滤波器 W，卷积输出特征 y = x * W；

卷积核的超参数：卷积核大小、步长、填充；

卷积的作用：局部算子、平移同变性、特征增强、降噪；

▲（2）池化（下采样、降采样）：用于降低特征图的空间分辨率；

常用方法：最大池化（选择区域最大值保留）、平均池化（取区域平均值保留）等；

经过池化运算通道数不变，池化层一般不训练学习参数；

池化的作用：局部变化的不变性（增加特征的鲁棒性）、增大感受野、降维（降低卷积层输出的特征维度）、防止过拟合；

卷积网络的优势：局部连接、权值共享→参数减少；

▲4、CNN 典型架构

（1）LeNet（训练 MNIST 手写体识别数据集）

平均池化，Sigmoid or tanh 非线性激活单元，全连接层用于分类；

（2）AlexNet

GPU 实现，7 个隐含层（共 8 层），650,000 神经元，60,000,000 参数，百万原始数据推广，采用 ReLU 激活函数，更好的正则化（DropOut）、LRN 局部响应归一技术；

（3）VGGNet

朴素的实现，更深的模型（16 层或 19 层），由连续 3x3 卷积取得的更大的感受野（所需参数更少）；

（4）GoogLeNet

Inception 模块（1x1, 3x3, 5x5 的不同感受野分支用于捕获），在昂贵的卷积计算前使用 1x1 卷积降低特征通道维数；

（5）ResNet

主要解决深度网络变深后难以优化的问题，引入跳层残差连接，避免梯度消失问题，后续引入引入稠密跳层连接、通道维度自注意机制全局池化；

5、深度卷积网络存在的问题

（1）对几何变换的鲁棒性一般；

（2）对抗性一般；

（3）没有关于整体与局部的显式表达，因而难以理解它们的关系；

（4）模型大：参数量/复杂度呈现指数爆发；

（5）代价高：训练时间所需时间指数增长。

七、连接学派-GAN ATT GNN

1、生成与对抗

背景：Ian Goodfellow 在 Generative Adversarial Networks 中首次提出了生成对抗网络（GAN），初始想法为两个神经网络一个生成图片，另一个判断生成质量，进行相互对抗；

GAN 用途：图像生成、动漫头像生成、图像风格迁移、文字转图像、图像编辑、图像复原；

▲GAN 组成：生成器、判别器；

▲GAN 原理：生成器接收一个随机的噪声，并生成“假数据”；判别网络接收“真数据”和生成的“假数据”，并预测不同数据的真实性概率；先固定生成器参数不变，提升判别器

效果；再固定判别器参数不变，提升生成器效果；不断循环训练，使生成器和判别器不断提升，直至收敛；

▲GAN 学习目标：假设 G 为生成器，D 为判别器，真实数据为 x，噪声为 z，D(·)为计算数据的真实性概率（1 为真，0 为假），生成器的目标是生成尽可能真实的“假数据”，即 D(G(z))→1，判别器的目标是尽可能判断出数据的真假，即 D(x) →1，D(G(z))→0；

$$\min_G \max_D V(D,G) = \mathbb{E}_{\boldsymbol{x}\sim p_{data}(\boldsymbol{x})}[\log D(\boldsymbol{x})] + \mathbb{E}_{\boldsymbol{z}\sim p_{\boldsymbol{Z}}(\boldsymbol{z})}[\log(1-D(G(\boldsymbol{z})))]$$

GAN 优点：并未局限生成结构的具体形式，且降低了损失函数设计的困难；

▲GAN 缺点：可解释性差，训练困难（要求生成器与判别器之间需要很好的同步）；

发展历程：

▲（1）DCGAN

具体改进：

在生成器中使用转置卷积进行上采样，判别器中使用步长卷积代替池化层；

在生成器和判别器中都添加了批量归一化操作（batch normalization）；

去掉了全连接层，使用全局池化层替代，使网络变为全卷积网络；

生成器中使用 ReLU 作为激活函数，最后输出层使用 Tanh 激活函数；

判别器中使用 LeakyReLU 激活函数；

局限性：生成器和判别器的损失函数无法指导训练进程，生成样本缺乏多样性，容易出现模式崩塌；

▲（2）WGAN：解释了 GAN 训练不稳定的原因，并给出了理论证明和解决方法

具体改进：

判别器最后一层去掉 sigmoid；

生成器和判别器的损失函数不取 log；

每次更新判别器的参数后，把参数截断在某个范围内；

不使用基于动量的优化算法如 momentum 和 Adam，推荐使用 RMSProp，SGD 也行；

▲（3）CGAN

在生成器和判别器中同时加入条件约束来引导数据的生成过程，实现控制图像的生成类别；

在 MNIST 数据集上训练好的 CGAN 能够自由控制生成数字的类别；

▲（4）Pix2Pix

将 CGAN 应用于有监督的图像到图像翻译任务，有监督表示 Pix2Pix 使用成对的数据进行训

练，可以使得输出图像和输入对应、有关联；

▲（5）CycleGAN

在 Pix2Pix 的基础上，使用不成对的数据即可训练网络，大大降低了数据收集的难度；

（6）PGGAN：一种渐进训练方式

PGGAN 递增分辨率过程：增加新的网络层时利用 α 进行平滑过渡；

（7）StyleGAN

在 PGGAN 的基础上，受风格迁移中 AdaIN 操作启发，对传统生成器网络结构进行了修改；

（8）StyleGAN V2

通过观察 StyleGAN 生成中的伪影瑕疵，改进 AdaIN 操作与网络结构，进一步提升生成质量；

2、注意力网络

▲注意力定义：在神经网络中，注意力机制表示一类模拟人类认知注意力的技术，主要通过引入乘法交互使输入的重要部分得到加强，同时弱化剩余输入——网络应将算力关注到某些虽小但重要的区域；

▲注意力本质：用来分配有限信息处理能力的选择机制，抑制某区域 input/output 阻止干扰信息进入，加强某区域 signal 促进该信息的处理；

▲注意力机制的总分类：

（1）点积注意力

强注意力（关注点）：0/1 二值分类问题，0 表示区域不被关注，1 表示区域受到关注；

软注意力（关注区域/特征通道）：[0, 1]连续分布问题，参数值表示每个区域被关注的程度高低，可以通过神经网络计算出梯度并且通过前向传播和后向反馈学习得到注意力的权重；

（2）自注意力（关注全局信息）：特征间的自主学习

自注意力是强/软注意力的改进，减少了对外部信息的依赖，更擅长捕捉数据或特征的内部相关性，自注意力机制可通过捕捉全局信息获得更大的感受野和上下文信息，每一个点都要捕捉全局上下文信息，计算量较大；

▲点积注意力根据作用对象分类：

（1）空间注意力：通过注意力机制让网络自主地关注关键空间位置；

（2）通道注意力：应用对象通常是张量，通道注意力可以对不同通道的重要性加权，实现通道域的注意力机制（SENet，将通道注意力分为挤压、激励、缩放）；

（3）混合注意力：将空间注意力（where）和通道注意力（what）结合；

（4）时间注意力：对于时间域的注意力机制，应用最早于 NLP 领域；

自注意力机制：

▲三元组：（key, query, value）

▲key 和 query 通过点乘的方式获得相应的注意力权重，最后把得到的权重和 value 做点乘得到最终的输出；

$$Attention(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}) = softmax(\frac{\boldsymbol{Q}\boldsymbol{K}^T}{\sqrt{d_k}})\boldsymbol{V}$$

• $\boldsymbol{Q}$表示query，$\boldsymbol{K}$表示key，$\boldsymbol{V}$表示value，d_k表示k的维度。

▲作用：提供了一种有效的捕捉全局上下文信息的建模方式；

图像中的（全局）自注意力机制：基于图片滤波领域的非局部均值滤波操作思想；

典型应用：文本翻译、图像分类、目标检测、语义分割、点云分类和分割、行为识别；

3、图深度学习的基本概念

网格化数据：常见图像、语音、以及自然语言均为规则的网格化数据；

图结构数据：现实世界中的许多数据并非建立在规则网格之上；

非结构化（图）数据的难点：

（1）图的大小任意，拓扑结构复杂，没有像图像一样的空间规律性；

（2）图没有固定的节点顺序，或者说没有参考节点；

（3）图通常是动态的，可能包含多模态的特征；

图：一种数据结构，包含顶点和边，分为有向图、无向图；

属性图：节点和边都可以具有属性（特征），每一个节点由它自身的特征以及与其相连的节点特征来定义该节点；

针对图的研究：经典图算法、概率图模型、图神经网络；

▲图相关任务：

（1）图级别任务：图分类、图嵌入、群体检测（图聚类）、图生成；

（2）节点级别任务：节点分类；

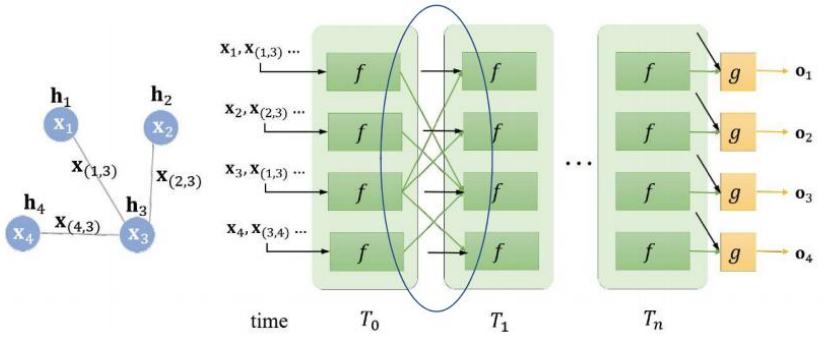
（3）边级别任务：连边预测；

4、图神经网络（GNN）（2005）

2019 年被称为图神经网络元年；

图神经网络是将图数据和神经网络进行结合，在图数据上进行端到端的学习和计算；

▲GNN 的结构：给定一张图 G，每个节点 v 的特征用 x_v 表示，连接节点 v 和节点 u 的边的特征用 $x_{(u,v)}$表示；



GNN 的学习目标：获得每个节点 v 的隐藏状态 h_v（用于捕捉动态和复杂关系）；

▲GNN 工作模式：

（1）对于每个节点，它的隐藏状态由自身节点的特征、相邻节点的特征、隐藏状态以及与自身节点相连的边的特征共同决定；

（2）不断地利用当前时刻邻居结点的隐藏状态作为部分输入来生成下一时刻中心结点的隐藏状态，直到每个结点的隐藏状态变化幅度很小，整个图的信息流动趋于平稳；

（3）隐藏状态参数 f 逐步更新稳定，函数 g 描述根据每个结点的隐藏状态向量产生对应的输出；

GNN 与 RNN 区别：

（1）GNN 在不同时刻的输入相同，RNN 在不同时刻的输入不同；

（2）GNN 在收敛后才输出，RNN 每个时间步上都可以输出；

（3）沿时间展开的长度不同，展开的结构不同，优化算法不同；

5、图卷积网络（GCN）

卷积神经网络 CNN 无法处理 Non Euclidean Structure 的数据，是 GCN 起源的主要动机之一；CNN 有能力去抽取多尺度局部空间信息，并将其融合起来构建特征表示，但只能应用于常规的欧几里得数据上；

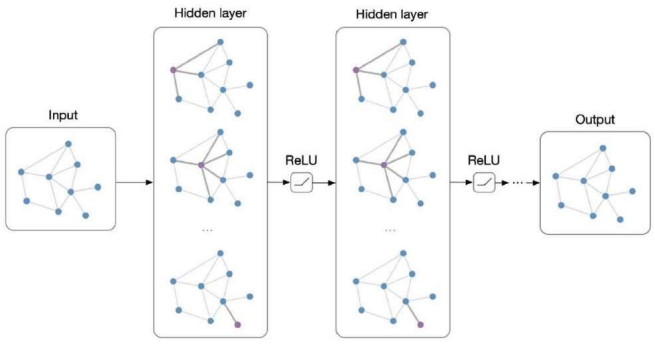
GCN 和 CNN 的共同点：局部连接、权值共享、多层网络；

GNN 与 GCN 的联系：都属于图表示学习的范畴（图嵌入），通常有两个层次的含义：将图中的节点/整个图表示成低维、实值、稠密的向量形式；

GNN 与 GCN 的区别：初代 GNN 通过循环迭代更新节点的特征，而 GCN 通过堆叠层更新节点特征；

GCN 特点：局部特性、一阶特性、参数共享；

▲GCN 基本结构：



▲GCN 工作模式：

输入：整张图；

每个结点进行卷积操作，用卷积结果更新该结点，多层计算，通过堆叠层更新节点特征；

输出：

（1）节点级别输出：N×F 大小的特征矩阵，F 是输出特征维数；

（2）图级别输出：可通过引入某种形式的池化算子；

▲常规卷积与图卷积差异：

（1）常规卷积定义在欧式空间，图卷积定义在非欧空间；

（2）常规卷积节点的邻域数量固定，图卷积节点的邻域不固定；

（3）常规卷积卷积核大小固定，图卷积卷积核大小不固定；

GCN 难点：邻居结点数量不固定；

GCN 本质：想找到适用于图的可学习卷积核；

GCN 思路：

（1）把非欧空间的图转换成欧式空间：按照每个团中的结点顺序可将所有团转换成固定长度的序列，再将它们按照中心结点排序从前到后依次拼接；

（2）可处理变长邻居结点的卷积核：核心在于聚合邻居结点的信息，最简单无参卷积可以是将所有直连邻居结点的隐藏状态加和，来更新当前结点的隐藏状态，但实际上图卷积在建模时需要的都是带参数、可学习的卷积核；

▲6、图神经网络的典型应用

（1）计算机视觉：图像生成场景图、场景图生成图像、点云分类、姿态估计、图像匹配；

（2）自然语言处理：文本分类；

（3）网络应用：推荐系统；

（4）智能交通：车联网；

（5）生物：分子分类。

八、行为学派-智能优化

1、行为主义（进化主义、控制论学派）

原理：控制论及感知-动作型控制系统；

行为主义认为人工智能源于控制论，研究重点是模拟人在控制过程中的智能行为和作用；

控制论：研究一切系统在信息的调控下如何保持动态平衡和稳定的科学；

控制理论：关注机器本身的控制；

自动化：一类以机器为研究和应用对象的技术；

行为主义认为智能取决于感知和行动，认为人工智能的研究方法应采用行为模拟方法；

2、最优化方法

智能优化：包括进化计算和群智能，是典型的元启发式随机优化方法；

实际问题中对最优化方法的要求：

（1）对问题的描述要宽松（目标和约束函数）；

（2）可以用一段程序来描述（程序中带判断、循环），函数可以非连续、非凸、非可微、非显式；

（3）并不苛求最优解——通常满意解、理想解就可以了；

（4）计算快速、高效，可随时终止（根据时间定解的质量）；

（5）能够处理数据、信息的不确定性（如数据的模糊性，事件的随机性）；

3、遗传算法（GA）

进化的生物学思想：适者生存；自然界的生物体在遗传、选择和变异等一系列作用下，优胜劣汰，不断地由低级向高级进化和发展；

▲生物进化与遗传算法：遗传算法的大量术语来自生物学：

染色体→字符串；基因→字符；基因座→字符位置；等位基因→字符所有可能取值；

▲GA 的基本思想（算法流程）：

（1）根据目标函数构造适应度函数；

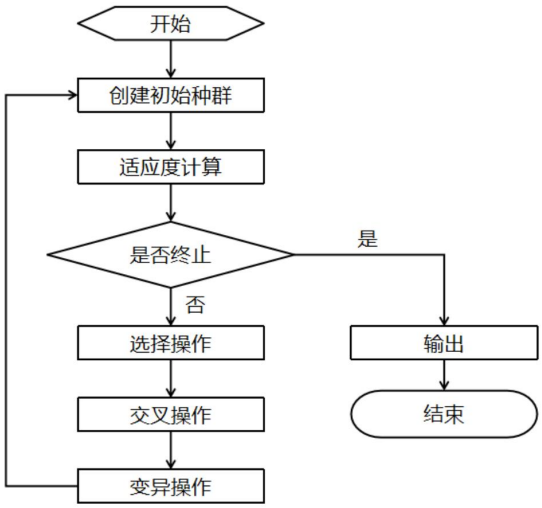
（2）产生初始种群；

（3）适应度计算与评估，根据适应度好坏不断选择繁殖；

（4）进化操作，使用变异、交叉、选择等操作更新解以求得最优解；

GA 要素：种群、编码方法、遗传算子（交叉、变异）、选择策略、停止准则；

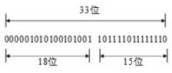
▲GA 算法框架：



▲（1）基因表达（编码）：将问题空间的参数编码为一维排列的染色体；

- 假设x_1和x_2需要的精度都是小数点后4位，两个变量需要的总串长按下面计算：
  - $(12.1-(-3.0))\times 10^4 = 151000,\ 2^{17} < 151000 \le 2^{18}$，所以$m_1$=18。
  - $(5.8-4.1)\times 10^4 = 17000, 2^{14} < 17000 \le 2^{15}$，所以$m_2$=15。
- 染色体的总长为18+15=33位，可表示如下：

$$-3.0 \leqslant x_1 \leqslant 12.1$$
$$4.1 \leqslant x_2 \leqslant 5.8$$



变量x1和x2的值为　　对应的十进制值为

	二进制码	十进制码
x_1	000001010100101001	5417
x_2	101111011111110	24318

x1=-3.0+5417x(12.1-(-3.0))/(2^{18}-1)=-2.687969

x2=4.1+24318x(5.8-4.1)/(2^{15}-1)=5.361653

（2）种群初始化：随机产生初始种群；

（3）适应度计算：

将染色体的基因型转换为表现型，即将二进制串转换为十进制值；

计算目标函数值 $f(x^k)$；

将目标函数值转换为适应度值，对于最大化问题，可简单地取目标值为适应度值；

▲（4）选择：轮盘赌法（正比选择策略）

对各个染色体 v_k 计算适应度值 $eval(v_k) = f(x)$；

计算种群中所有染色体的适应度之和 F；

对各染色体 v_k，计算选择概率 $p_k = eval(v_k) / F$；

对各染色体 v_k，计算累积概率 q_k（为各项 p_k 下标由 1 到 k 的值累加）；

产生[0,1]的随机数，观察随机数落在 q_k 的某区间，向上选取对应序号的染色体组新种群；

▲（5）交叉（单点交叉）

设定交叉率，选取随机数中小于交叉率的染色体（选择后）；

任意选定断点，两染色体断点右侧互换；

▲（6）变异

根据变异率随机选定染色体和基因位，进行取非操作；

4、群智能算法（1989）

生物群体的体现：由单个个体组成的群体，似乎在某种内在规律的作用下，表现出异常复杂而有序的群体行为；

群：某种交互作用的组织或 agent 的结构集合（相互作用的相邻个体的集合）；

▲群体智能：群集系统能够在没有外部指导和中心协调控制的情况下，完成动态变化环境中的复杂任务；

基本原则：

（1）个体仅有简单行为；

（2）解决单一个体无法解决的复杂问题；

（3）具有群体鲁棒性，单一个体失败对全局影响不大；

（4）个体仅有局部信息，极小的存储能力，没有全局信息；

▲群智能和进化计算的差异：

（1）群智能试图模拟简单智能体的集体和协同行为（模拟群体决策），速度快；

（2）进化计算受到生物进化的启发（模拟生物进化），收敛速度偏慢；

群智能算法共性：

（1）有多个粒子，代表每种智能体；

（2）每个个体通过一定的机制进行位置的变化或者移动，来对解的空间进行搜索；

（3）个体之间具有一定的独立性，利用局部信息和全局信息进行交互；

（4）群体在演变过程中都引入了随机数，以便进行充分探索；

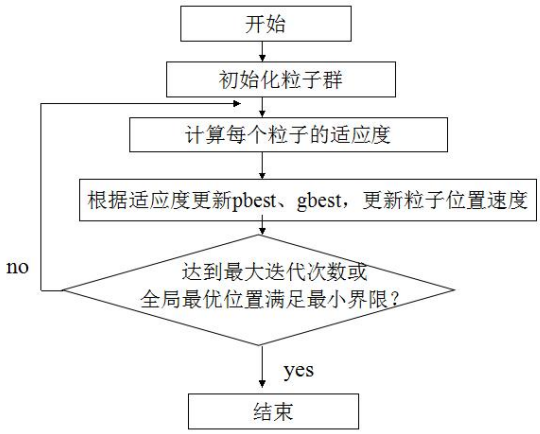
典型群体智能算法：

粒子群算法（模拟鸟类觅食的社会行为）、蚁群算法（模拟蚁群觅食的寻路机制）；

5、粒子群优化算法

基本思想：源于对鸟群觅食过程中的迁徙和群居的模拟，利用群体中的个体对信息的共享使整个群体的运动在问题求解空间中产生从无序到有序的演化过程，从而获得问题的可行解；系统初始化为一组随机解，通过迭代搜寻最优值，粒子（潜在的解）在解空间追随最优的粒子进行搜索；

算法流程：



pbest 为个体历史最优位置，gbest 为群体最优位置；

▲位置速度更新（三部分相加）：

$$v_i = \omega \times v_i + c_1 \times rand() \times (pbest_i - x_i) + c_2 \times rand() \times (gbest_i - x_i)$$

第一部分考虑惯性，使得粒子按惯性飞往边界；

第二部分考虑认知，可防止陷入局部最优解；

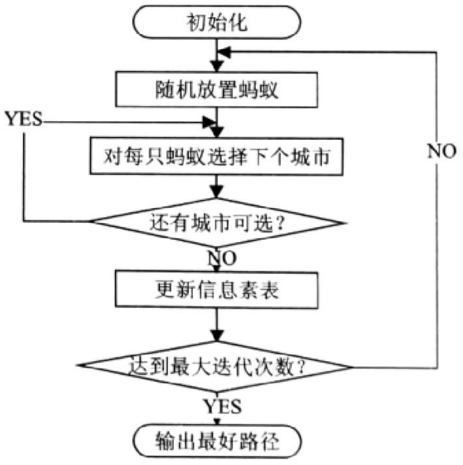
第三部分考虑社会，实现全局信息交互；

6、蚁群算法

▲蚁群寻路：随机移动，释放信息素（用于通信），信息素随时间挥发，故较短路径信息素浓度大（正反馈），后续蚂蚁大概率选择信息素浓度大的路径，经过迭代全部选择较短路径；

旅行商问题（TSP）：某旅行者寻求一条由起点出发，通过所有给定的需求点之后，最后再回到起点的最短路径；

▲算法流程：



（1）路径构建

随机概率规则选择下一个城市，随机概率受信息素强度和能见度（路径长度倒数）影响；

不允许选择已走路径（禁忌表）；

（2）信息素更新方式

信息素挥发：所有路径信息素按比率减少，模拟随时间挥发特性；

信息素增强：给已选择的边增加信息素，模拟有蚂蚁走过补充信息素；

7、对智能优化方法的批评

（1）全局最优的概率收敛性；

（2）有时无法在当前状态下在搜索空间的探索和利用之间取得适当的平衡；

（3）参数选择较困难，且算法结果高度依赖于参数选择；

九、行为学派-强化学习

1、强化学习（RL）基本概念

输入：状态-动作空间；

目的：通过选择动作来最大化预期未来奖励；

主体：智能体（Agent）；

▲强化学习与其他机器学习范式的区别：

（1）没有监督，只有奖励信号；

（2）延迟反馈，而非瞬时结果；

（3）时序的重要作用（使用序列训练数据，而非独立同分布数据）；

（4）智能体与环境的互动（动态特性）：机器动作影响它接下来获取的数据；

2、强化学习机制由来

效果法则：动物由一定条件触发产生的行为造成了满足感，则在再次出现相同条件时，触发该行为的可能性提高（行为主义心理学的主要原理）；

实验心理学启发：（操作）条件反射（行为主义心理学的主要原理）；

计算神经科学启发：

（1）赫布学习：通过共同激活神经元，来强化它们之间的突触权重，从而发展模型的形式（神经元间联系）；

（2）多巴胺和基底核模型：与运动控制和决策有直接联系，选择带来最大奖励的动作；

最优控制：以优化方法的形式框架，求取连续时间控制问题中的最优控制策略；

最优控制问题经典方法：动态规划；

3、强化学习模型

▲强化学习：通过与未知和不确定（如随机）环境的直接交互（试错）学习行为策略，使长期奖励总和（延迟奖励）最大化，是通过智能体与环境交互作用的一种试错学习范式；

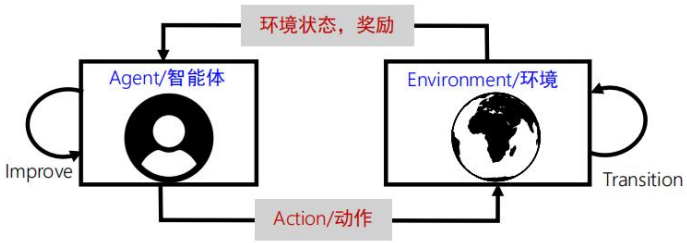
▲算法流程与基本模型：

（1）智能体观察环境；

（2）智能体利用观测到的状态和奖励改进自己的 policy/策略；

（3）智能体选择并执行相应动作；

（4）环境对智能体动作做出响应，根据自身上一时刻的状态和智能体动作（可能）转移到下一个状态，回到（1）；



▲强化学习要素：智能体、环境、状态 s、动作 a、奖励 r；

（1）智能体：决策者，可以与环境交互、评估动作好坏、学习并改进动作选择策略；

（2）环境：除决策体外的一切，通常选择会影响决策的变量组合（状态）

状态空间：状态所有可能的取值空间；

观测：智能体可以看到的状态变量；

观测空间：智能体可观测到的变量的取值空间；

（3）动作：智能体根据环境做出选择得到；

动作空间：所有可能动作组成的空间；

环境接收动作后，通过其状态转移函数改变自身状态，状态转移后环境会通过其奖励函数释放出一个瞬时奖励信号；

环境模型：状态转移函数、奖励函数；

在 t 时刻，智能体：执行动作 A_t，收到观察 O_t，收到标量奖励 R_t；环境：收到动作 A_t，释放观察 O_{t+1}，释放标量奖励 R_{t+1}；环境决定了时刻 t 如何变化；

（4）状态：决定下一步做什么所需要的信息；

状态是历史的函数（从历史中提取必要信息）：$S_t = f(H_t)$；

历史：观察、动作、奖励的序列，包括了截止到 t 时刻所有能观察到的变量；

环境状态：环境的自我刻画，决定下一步（观察/奖励）所需的全部信息，对智能体并不全部可见，即使可见也可能包含无关信息；

智能体状态：智能体的内部表达，决定下一步（动作）所需的全部信息；

马尔可夫性质：某状态包含了历史中的全部有用信息→马尔科夫状态，则下一时刻状态仅由当前状态决定（无记忆性/无后效性）；

完全可观：智能体可直接看到所有环境状态（智能体状态=环境状态），可用动态规划；

部分可观：智能体不能直接观察环境，要通过学习，用强化学习解决部分可观环境，可用部分可观马尔科夫决策过程，智能体必须自行建立其状态表达；

（5）奖励：是一种标量的反馈信号，反映在 t 时刻智能体 Action 的好坏；

智能体的任务：最大化累积奖励；

4、序贯决策

目标：选择合适的动作来最大化未来总奖励；

动作可能造成长期后果，延迟奖励，可能需要牺牲短期的奖励来获得长期回报；

例子：

（1）金融投资（需要数月甚至一年才能得到结果）；

（2）直升机加油（预防数小时后的坠机）；

（3）围棋的一着（可能帮助了许多步后棋局的胜利）；

每个时刻都进行强化学习循环，RL 用来解决序贯决策问题，笼统地讲，RL 包括给定状态预测奖励的预测算法和通过试错来学习好的动作的控制算法；

▲5、强化学习的预测与控制

预测：评估未来，给定策略计算策略下各状态的值函数，预测未来结果；

控制：优化未来，对于所有可能策略计算并找出最优值函数，寻找最优策略；

6、智能体学习

RL 智能体的核心构成：

（1）策略：决定智能体行为的函数，表示从状态到动作的映射，包含确定性策略、随机型策略（处于状态 s 时采取动作 a 的概率）等；

▲（2）值函数：评估状态/动作好坏的函数，是对未来奖励的预测；

状态值函数：评估给定策略的好坏，需联合 MDP 模型才能找到最佳策略，解决预测问题；

动作值函数：用来改进给定策略，不需要 MDP 就可以给出最佳策略，解决控制问题；

状态值函数：$V_\pi(s) = E_\pi[G_t|S_t = s]$

动作值函数：$Q_\pi(s,a) = E_\pi[G_t|S_t = s, A_t = a]$

RL目标：$V^*(s) = \max_\pi V_\pi(s)$或$Q^*(s,a) = \max_\pi Q_\pi(s,a)$

回报的递归形式：

$$G_t = R_{t+1} + \gamma G_{t+1}$$

值函数的递归形式：

$$V_\pi(s) = E_\pi\left[R_{t+1} + \gamma G_{t+1} | S_t = s\right]$$

$$= E_\pi\left[R_{t+1} + \gamma V_\pi(S_{t+1}) | S_t = s\right]$$

贝尔曼方程
（动态规划方程）

$$Q_\pi(s,a) = E_\pi\left[R_{t+1} + \gamma Q_\pi(S_{t+1}, A_{t+1}) | S_t = s, A_t = a\right]$$

（3）模型：智能体对环境的表达（主观认识），预测环境的接下来如何变化；

转移模型：根据先前的状态以及动作，预测环境所处下一个状态的概率；

$$\mathcal{P}^a_{ss'} = \mathbb{P}[S_{t+1} = s' \mid S_t = s, A_t = a]$$

奖励模型：根据先前的状态以及动作，预测下一个瞬时奖励的概率；

$$\mathcal{R}^a_s = \mathbb{E}\left[R_{t+1} \mid S_t = s, A_t = a\right]$$

7、Q 学习

无模型、基于动作值函数 Q(s,a)，通过与环境交互直接训练 Q(s,a)，找到 Q*(s,a)和 π *(s)；

Q 表（可先假设状态数量已知、可添加行和列）：

（1）行：状态；

（2）列：动作；

（3）单元格：状态动作对的 Q 值；

▲Q 学习的流程（思路）：

初始化 Q 表、选择一个动作 a、执行该动作、得到奖励 R、更新 Q 值

Q(s1,a2)估计： Q(s1,a2)

Q(s1,a2)现实： R + γmaxQ(s2)

差距=现实-估计

新Q(s1,a2)=老Q(s1,a2)+α差距

$$Q(S_t, A_t) \leftarrow Q(S_t, A_t) + \alpha\left[R_t + \gamma \max_{A_{t+1}} Q(S_{t+1}, A_{t+1}) - Q(S_t, A_t)\right]$$

更新后的Q值　当前Q值　学习率　执行动作A_t产生的回报值　当前Q值

时序差分目标　时序差分（Temporal Difference）

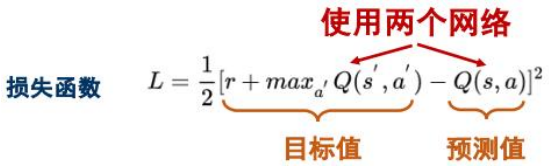
▲深度 Q 网络（DQN）：Q 学习演变而来，可看作深度学习与 Q 学习的结合体，用深度神经网络（DNN）取代 Q 表，转化为监督学习，目标为找到 Q 函数；

▲DQN 的关键技术：

（1）经验回放：收集（后 N 个）样本存入回放缓存，均匀采样小批量样本用于 Q 学习更新；

优势：提高数据使用效率、减少参数震荡或发散；

（2）目标网络：使用动作网络和目标网络，固定目标 Q 值；



优势：减少目标 Q 值与 Q 网络参数间依赖关系，解决算法训练的不稳定问题。