人工智能导论

张翼英 张茜 张传雷 主编

课后题参考答案

第一章 人工智能 （课后题及参考答案）

1. 什么是人工智能？

人工智能是是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。

2. 什么是符号智能与计算智能？请举例说明。

符号智能是模拟智能的人工智能，是以符号形式的知识和信息为基础，主要通过逻辑推理，运用知识进行问题求解。如搜索技术、专家系统、定理证明等；计算智能是模拟群智能的人工智能，以数值数据为基础，主要通过数值计算，运用算法进行问题求解。

3. 人工智能主要有哪几种研究途径和技术方法？请简单说明。

（1）符号智能：主要以符号知识为基础，通过符号推理进行问题求解而实现的智能，主要包括知识工程和符号处理技术；

（2）计算智能：是以数据计算为基础，通过数值计算进行问题求解而实现的智能，包括人工神经网络，进化计算，模糊技术等。

4. 人工智能的主要研究和应用领域有哪些（至少列出 7 个）？其中，哪些是新的研究热点（至少列出 3 个）？

应用领域：零售、交通运输和自动化、农业、制造业、智能医疗、智能金融、智能安防、智能家具、智能电网。

研究热点：智能医疗、智能金融、智能安防、智能家具、智能电网。

5. 在人工智能的发展过程中，有哪些思想和思潮起了重要作用？

20 世纪 30 年代和 40 年代：数理逻辑和关于计算的新思想；

20 世纪 80 年代后期以来，不同人工智能学派间的争论推动了人工智能研究和应用的进一步发展，特别值得一提的是神经网络的复兴和智能真体的突起；

6. 人工智能的发展对人类有哪些方面的影响？试结合自己了解的情况和理解，从经济、 社会和文化等方面加以说明。

（1）人工智能对经济的影响。人工智能系统的开发和应用，已为人类包造出可观的经济效益，专家系统就是一个例子。随着计算机系统价格的继续下降，人工智能技术必将得到更大的推广，产生更大的经济效益。

（2）人工智能对社会的影响。劳务就业问题；社会结构变化；思维方式与观念的变化；心理上的威胁；技术失控的危险。

（3）人工智能对文化的影响。改善人类知识:改善人类语言;改善文化生活。

第二章 表示与理解（课后题及参考答案）

1. 什么是知识？它有哪些特性？有哪几种分类方法？

在长期的社会生活实践和科学研究当中，我们人类积累了对客观世界认知的经验。将获取的经验信息关联在一起就形成了知识。

特性：（1）相对正确性 （2）不确定性 （3）可表示性与可利用性

分类方法：产生式表示法、框架表示法、状态空间表示法

2. 用产生式表示：如果一个人发烧、呕吐、出现黄疸，那么得肝炎的可能性有 7 成。

IF 病人发烧、呕吐、出现黄疸 *THEN* 病人患肝炎（0.7）

3. 试述产生式系统求解问题的一般步骤。

(1)对规则库中的知识进行合理的组织和管理。

(2)当规则库中的一条产生式的前提 P，可以和事实库中的一些已知事实匹配时，则该产生式被激活，并将该式子推出的结论放入事实库，以作后面推理的已知事实。

(3)推理机由一组程序组成，控制了整个产生式系统的运行，并实现对问题的求解，一般推理机要做以下几项工作：推理、冲突消解、执行规则、检查推理终止条件。

4. 构造一个描述你的一个教室的框架。

框架名：〈教室-1〉

教室号：310

校区：西院

楼号：8

所属院系：人工智能学院

5. 用状态空间法表示问题时，什么是问题的解？求解过程的本质是什么？什么是最优解？最优解唯一吗？

$$S_0 \xrightarrow{O_1} S_1 \xrightarrow{O_2} S_2 \xrightarrow{O_3} \cdots \xrightarrow{O_i} G$$

求解路径上的一个操作算子序列被称为状态空间的一个解。

对状态空间图的搜索，即在状态空间图上寻找一条初始状态到目标状态的路径。

在不考虑搜索的代价时，即假设状态空间中各节点之间的有向边的代价相同时，最优解就是解路径中长度最短的那条路径，在考虑搜索代价时，最优解则是解路径中代价最小的那条路径。因为在状态空间图中，可能会存在几条长度相等的最短解路径，所以，最优解可能会不唯一。

6. 在确定性推理中，应该解决哪几个问题？

求解问题的策略和方法

7. 在不确定性推理中，应该解决哪几个问题？

不确定性的表示与度量，不确定性的匹配，不确定性的传播和更新，不确定性的合成。

8. 解释双向推理的基本思想？

一方面根据已知事实进行正向推理，但并不推到最终目标;另一方面从某假设目标出发进行逆向推理，但并不推至原始事实，而是让它们在中途相遇，即由正向推理所得到的中间结论恰好是逆向推理此时所要求的证据，这时推理就可结束，逆向推理时所做的假设就是推理的最终结论。

9. 什么是盲目搜索？

在搜索过程中没有利用任何与问题有关的知识或信息，则称之为盲目搜索。

1. 用深度优先方法求解下面的二阶梵塔问题，画出搜索过程的状态变化示意图。对每个状态规定的操作顺序为：先搬 1 柱的盘，放的顺序是先 2 柱后 3 柱； 再搬 2 柱的盘，放的顺序是先 3 柱后 1 柱；最后搬 3 柱的盘，放的顺序是 先 1 柱后 2 柱。

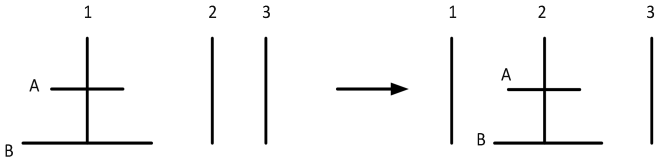
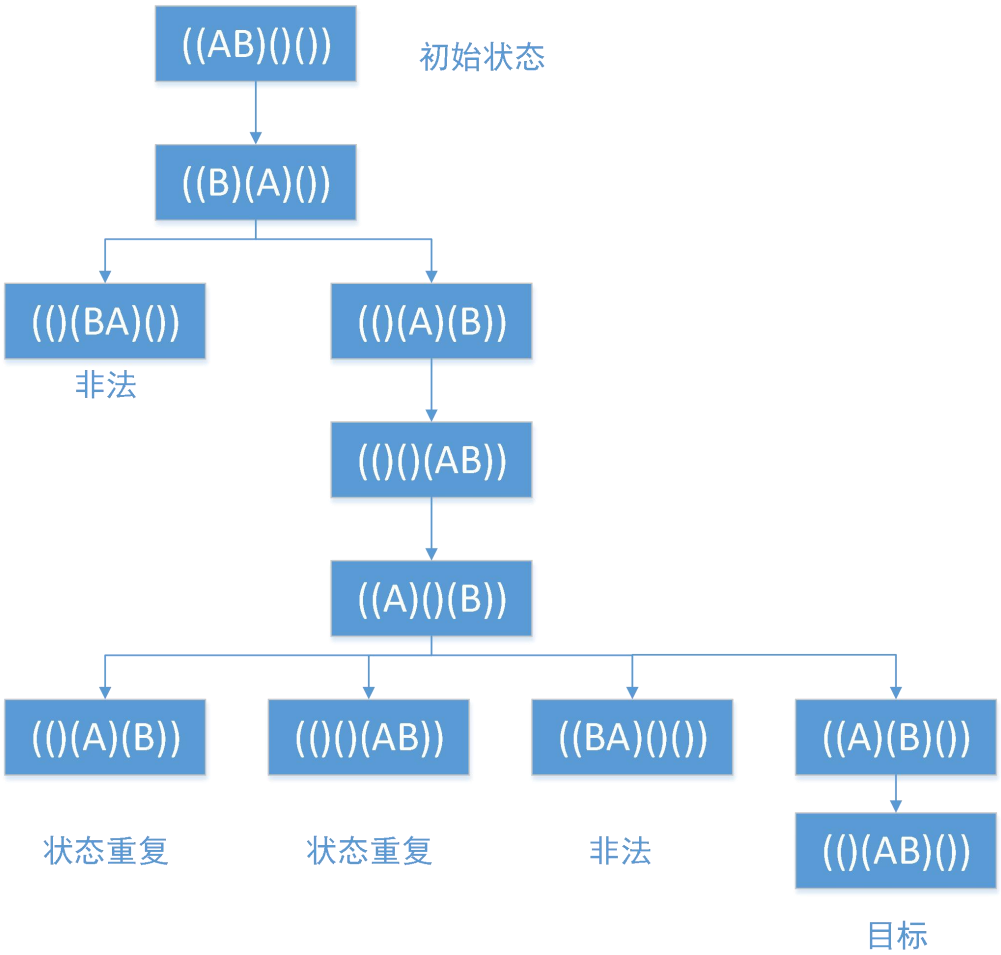


图 2.22 梵塔问题



10. 解释什么是宽度优先搜索策略。

宽度优先搜索策略的基本思想是优先搜索深度浅的节点，即每次扩展节点时选择深度最浅的节点，若有深度相同的节点，则根据规则从深度最浅的几个节点中选择一个。

11. 请用 A*算法求解下述八数码问题：

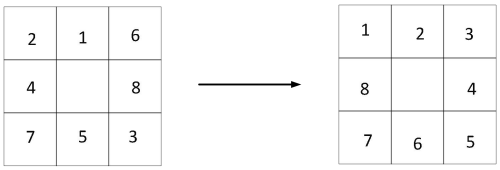


图 2.23 八数码问题

Source:	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
2 1 6	2 1 6	2 1 0	2 0 1	2 8 1	2 8 1	2 8 1
4 0 8	4 8 0	4 8 6	4 8 6	4 0 6	4 6 0	4 6 3
7 5 3	7 5 3	7 5 3	7 5 3	7 5 3	7 5 3	7 5 0

Step 7	Step 8	Step 9	Step 10	Step 11	Step 12
2 8 1	2 8 1	2 8 1	0 8 1	8 0 1	8 1 0
4 6 3	4 0 3	0 4 3	2 4 3	2 4 3	2 4 3
7 0 5	7 6 5	7 6 5	7 6 5	7 6 5	7 6 5

Step 13	Step 14	Step 15	Step 16	Step 17	Step 18
8 1 3	8 1 3	8 1 3	0 1 3	1 0 3	1 2 3
2 4 0	2 0 4	0 2 4	8 2 4	8 2 4	8 0 4
7 6 5	7 6 5	7 6 5	7 6 5	7 6 5	7 6 5

12. 在八数码问题中，如果移动一个将牌的耗散值为将牌的数值，请定义一个启发函数并说明该启发函数是否满足 A*条件。

略

第三章感知与连接（课后题及参考答案）

1. 什么是感知技术？生活中哪些地方运用了感知技术？

感知技术就是利用传感器等技术来感知外部世界的自然信息。在人脸识别、声纹识别、指纹识别、温湿度感知和有害气体感知等方面都运用到了感知技术。

2. 简述感知技术与传感器技术的区别与联系。

区别：传感器感知技术是一种检测手段,感知技术是利用各种检测手段实现对日标的准确识别。

联系:“传”为信息传递的方式,“感”为感受信息或是获取信息的手段,“知”即得到信息。因此，传感是感知的过程，而感知是传感的结果。

3. 简述感知技术与人工智能的联系。

感知是人工智能与现实世界交互的基础和关键,为人工智能提供数据基础和信息基础， 是人工智能服务于工业社会的重要桥梁。人工智能通过对感知的信号与信息进行识别、判 断、预测和决策，对不确定信息进行整理挖掘，实现高效的信息感知，让物理系统更加智 能。人工智能与信息感知是被高度关注的热门领域，将两者进行有机结合具有重要的理论 与应用价值。没有感知技术，人工智能就成为“无米之炊”。

4. 数据传输技术都有哪些？

有线传输技术、无线传输技术、移动通信技术和卫星通信技术。

5. 简述人工智能与数据传输的关系。

人工智能与传输技术融合发展已经成为主流趋势。在传输技术逐渐发展的背景下，人工智能能够对海量数据进行更加细致的分析，并进一步提高整体智能化水平。人 工智能的应用本身就有助于优化通信网络及提高网络传输效率，并且人工智能作为一种模 拟人类思维的技术，可以依靠机器的学习能力实现对数据的筛选过滤、分类整理以及深入分析，同时通过从中不断学习知识和积累经验来提升自身，从而可以在短时间内完成大量 的数据传输、整合及运算 ；传输技术可以使人工智能实现远距离控制，例如超远距离无线 遥控人工智能机器人。

6. 简述 5G 传输的原理。

1）发送方获取数据拆分传输规则。其中，数据拆分传输规则根据待传输数据的安全 保密等级确定得到,包括数据拆分规则和拆分后各数据段的传输切片标识。2）接入传输切片标识对应的若干网络切片，并获取切片信息，得到发送方切片信息。 其中，发送方切片信息包括接入切片 IP 与端口信息。 3）将发送方切片信息传输至接收方,并对接收到的接收方切片信息进行记录。 4）接收数据段，

并根据发送方切片信息以及数据拆分传输规则对数据段进行数据 还原，得到传输数据。

7. 简述卫星通信技术的原理。

卫星通信简单地说就是地球上（包括地面、水面和低层大气中）的无线电通信站之间 利用人造卫星作为中继站转发或反射无线电波，以此来实现两个或多个地球站之间通信的 一种通信方式。它是一种无线通信方式，可以承载多种通信业务，是当今社会重要的通信手段之一。

8. 碎片化数据有什么特点？

碎片化数据具有多源分布、社会性、无序性、不完整性、冗余性和隐匿等特点。

9. 简述海量计算与大数据挖掘的关系。

各种计算技术的发展与大数据的出现密不可分，也 正是大数据技术与各种计算技术的出现促进了人工智能的发展。只有将大量数据输入计算 机，计算机同时以超快的速率进行相应的计算才能保证人工智能算法的顺利运行。

10. 简述分布式计算的实现技术。

分布式计算主要研究分布式操作系统和分布式计算环境。典型分布式计算技术包括：中间件技术、移动 Agent 技术、P2P 技术、网格技术、云计算技术。

第四章 判断与控制（课后题及参考答案）

1 机器学习、人工智能和深度学习之间有什么区别和联房

机器学习是实现人工智能的方法，深度学习是机器学习的一种技术；可以说，深度学习是机器学习的子集，而机器学习又是人工智能的子集。

2. 如果将机器学习进行分类， 可以分成哪几类?试着举例说明。

基于学习方式可以将机器学习分为监督式学习、非监督式学习、半监督式学习、强化学习等。

3. 有监督学习和无监督学习之间的区别是什么了它们分别时以，下什么向阳么区别?

对有监督学习而言，输入数据需要有标签，或者是一个已知的结果，这就需要人力对数据进行标注；而无监督学习则不需要数据标签。有监督学习适用于有标注数据集，无监督学习适用于无标注数据集。

4. 有监督学习、无监督学习、弱监督学习和半监督学习分别是什于什它们之间有什

有监督学习：通过给定有标签数据得出一个函数，这个函数可以对新的数据给出预测结果。无监督学习：对没有标签的数据根据数据相似性进行分类。弱监督学习：在数据标签有限或者标签准确性存在问题的前提下解决问题。半监督学习：训练数据中同时包含有标签数据和无标签数据，通过使用有标签数据和无标签数据提升学习的性能。这四种学习的区别主要在于对于标签数据利用情况的区别。

5. 弱监督学习有哪几种类型?它可以分成哪几种方法?

弱监督学习的类型有不完全监督学习、不确切监督学习和不准确监督学习。

6. 集成学习可以分为哪几种?试说明一下它们之间的区别。

集成学习主要有 Bagging 和 Boosting 两种分类方法，Bagging 是通过多个不同模型通过投票或平均决定输出结果；而 Boosting 则是将多个不同模型组合得到一个强学习器输出结果。

7. 试着实现集成学习中的 Bagging 和 Boosting 两种算法。它们的实现方式有着怎样的不同?

Bagging 的训练集是发生变化的，而 Boosting 的训练集每轮都没有变化；在预测时，Bagging 的每个预测函数权重都是相同的，而 Boosting 会根据预测误差的大小调整分类器的权重大小；在计算时 Bagging 的各个预测函数可以并行生成，而 Boosting 只能顺序生成，因为分类器的权重需要根据上一轮的预测结果动态调整。

8. 迁移学习的目的是什么?简要的概括一 下迁移学习。

基于特征的迁移学习是指通过特征变换迁移，或是将源域和目标域的数据特

征变换到统一的特征空间中再使用传统机器学习方法进行分类。

9. 什么是基于特征的迁移学习?

基于特征的迁移学习是指通过特征变换迁移，或是将源域和目标域的数据特征变换到统一的特征空间中再使用传统机器学习方法进行分类。

10. 什么是强化学习?什么是马尔可夫决策过程?它们之间有什么关系?

强化学习是智能体与环境交互过程中通过调整学习策略实现利益最大化。马尔可夫决策过程是指在智能体与环境的交互过程中，完全依靠智能体的当前状态做出决策。马尔可夫决策过程是强化学习的一种模型。

11. 强化学习的目标是什么?

强化学习的目标是从环境状态到行为的映射，使智能体选择的行为能够得到环境的最大奖赏，并使外部系统对学习系统的评价最佳。

12. 基于概率的主动强化和基于价值的主动强化有什么区别?

基于价值的主动强化学习一般适合处理离散数据，而基于概率的主动强化学习一般适合处理连续数据；基于概率的主动强化学习需要计算所有行为的值，而基于价值的主动强化学习一般只给出较高价值的行为。

13. 什么是群体智能?群体智能算法有哪些?

群体智能是指集体层面去中心、分布式的自组织行为。群体智能的算法有蚁群算法、粒子群优化算法等。

14. 质量控制、成本控制、延迟控制在任务中有什么作用?

使用众包完成的任务存在个体差异，也就是任务的完成质量可能会存在差异，为了获得平均高质量的任务结果需要进行质量控制；众包能够降低成本但是对大规模数据而言成本依旧昂贵，为了进一步降低成本需要进行成本控制；为了更快的完成任务或者更快的获取任务结果需要进行延迟控制。质量控制、成本控制、延迟控制都是为了更好、成本更低的完成任务。

第五章 人工智能安全（课后题及参考答案）

1. 人工智能安全体系架构分为哪几部分，分别包括什么，各部分之间有什么联系？

可将人工智能安全分为 3 个子方向：人工智能助力安全（AI for Security）、人工智能内生安全（AI Security）和人工智能衍生安全（AI Safety）。其中，人工智能助力安全体现的是人工智能技术的赋能效应；人工智能内生安全和衍生安全体现的是人工智能技术的伴生效应。人工智能系统并不是单纯依托技术而构建的，还需要与外部多重约束条件共同作用，以形成完备合规的系统。

2. 人工智能助力安全主要表现在哪两个方面，并分别阐述其内涵。

人工智能助力安全主要表现为助力防御和助力攻击两个方面。

在助力防御方面，防御者正在利用人工智能技术提升和扩展其原有的防御方法。防御者可利用计算机视觉技术助推物理智能安防监控产业快速发展，从而提升防盗报警、防爆安检等物理安全保障能力；利用机器学习算法，构建可在运行时不断自我提升的智能入侵检测系统；利用深度学习和机器学习技术检测未知特征的恶意代码，提升网络威胁发现能力；引入网络攻防知识图谱，使得“人机结合”的威胁猎杀更加高效，从而发现关键信息资产中潜伏的隐蔽威胁；基于海量用户与实体行为的正常历史数据，构建异常检测系统，从而发现偏离正常轨迹的可疑行为。由此可见，融入了人工智能因素的网络空间防御系统可弥补传统方法的不足，为网络空间安全防御提供新方法。

在助力攻击方面，攻击者可能利用人工智能技术突破其原有能力边界。攻击者借助人工智能技术，可以实现自动化漏洞挖掘、构建智能恶意代码、为神经网络模型植入后门、自动化构造鱼叉式钓鱼邮件、精准锁定目标、深度隐藏攻击意图、生成高逼真度假视频等攻击方法，从而提升漏洞挖掘效率和降低成本、提升恶意代码免杀和隐蔽通信能力、污染神经网络模型供应链、实现无人介入的鱼叉式钓鱼邮件大面积投放、提升网络攻击的精准打击和意图隐藏能力、实现伪造欺骗等新形态攻击能力。因此，融入了人工智能技术的网络攻击已经涵盖了攻击准备、生存对抗、武器投递、目标识别、意图隐藏、网络欺骗这个较为完整的攻击链，且使得攻击链上各节点的能力都有明显提升，这必将给防御工作带来新的挑战。

3. 人工智能内生安全是指什么？人工智能内生安全涉及哪方面的安全？

人工智能内生安全指的是人工智能系统自身存在脆弱性。脆弱性的成因包含诸多因素，人工智能框架/组件、数据、算法、模型等任一环节都可能给系统带来脆弱性。

4. 阐述数据集如何质量影响人工智能内生安全？

数据集的质量会直接影响到人工智能算法的执行效果，但是在设计算法的时候通常并不会针对具体的数据集设计算法，而是根据任务的输入和输出设计算法。数据集的质量取决于数据集的规模、均衡性、准确性等。

首先，数据集的规模如果较小，有可能导致算法执行产生不安全的结果。不同任务的难度不同，需要的数据量也不同。对于不同的任务，如果数据集规模达不到要求，训练后得到的人工智能模型运行的准确率就低，很有可能会在识别任务中产生错误的识别结果、在机器翻译任务中产生错误甚至含义相反的语句，从而造成训练好的人工智能模型在执行过程中出现不安全的结果。

数据集的均衡性也是影响人工智能算法效果的一个重要因素，即不均衡的数据集会造成人工智能算法失效。一般而言，数据集的均衡性是指数据集中包含的各种类别的样本在数量上的均衡程度。数据集越均衡，数据样本分布偏差越小，人工智能算法的运行效果往往越好。然而很多实际应用的数据集存在着不均衡的问题，如在欺诈交易识别任务中，如果根据历史交易数据构造用于该任务训练的数据集，而实际交易过程中大部分交易是正常的，属于欺诈的交易数量极少，若将该问题抽象为一个二分类问题，那么很有可能在收集到的 100 个数据样本中仅有 1 个是欺诈数据，利用这样的数据集训练的人工智能算法必定很难准确识别欺诈交易。最后，数据集的准确性也是影响人工智能算法内生安全的一个重要因素。数据集中的数据通常都是经过标注的数据，数据标注是构建数据集很重要的一步。以车辆目标检测任务为例，人们首先可以通过摄像头拍摄道路上的各种车辆，然后对拍摄到的图片进行标注，即在这些图片上人工标出哪些是车辆，圈出卡住每辆车的外接矩形。在这个过程中，如果数据不完整，将导致算法不能正确识别。

5. 人工智能的核心是算法模型的生成，算法模型的生成主要涉及哪两点？从算法的可解释性层面阐述人工智能可能存在的内生安全问题。

可以把算法理解为解决某问题的方法，比如解决手写数字识别问题的多层神经网络、解决文本翻译问题的循环神经网络（RNN），而这些算法仅仅提供了解决问题的办法，大多数人工智能算法都需要根据样本数据进行训练，从而生成神经网络中的各种参数，这里将采用的算法和针对该算法进行数据训练后生成的各种参数组合在一起称作模型。当一个神经网络通过样本数据学到各种参数以后，这些参数将会以特殊的形式进行保存，在执行任务（如手写数字中根据输入的数字图片进行分类或文本翻译时根据输入的文本翻译为其他语种）时直接调用模型中的算法和参数，便可快速完成任务。一般而言，训练模型得到参数的过程比较耗时，而调用模型执行任务时十分快捷，因此模型便成为很重要的成果，可以看作是通过样本数据学习得到的“精华”，即使这些精华还无法有效解释。既然模型是人工智能算法中很重要的环节，那么模型自身存在的安全问题将会在很大程度上造成人工智能的内生安全问题。

6. 人工智能衍生安全问题是指什么？举例说明人工智能衍生安全问题。预防人工智能技术失控的举措有哪些。

人工智能衍生安全问题指的是人工智能系统因自身脆弱性导致危及其他领域安全。人工智能系统的故障引发安全事故是常见的事情，这与将人工智能系统用于安全攻击不同。前者是失效后的副产品，其结果往往是不可控制的，不是在设计者的预期之内的；而后者则是有意为之的，攻击原本就是运用人工智能的目的所在。在这种情况下，我们说前者是一种衍生安全，是需要防范的；而后一种则属于赋能攻击，一旦这种赋能被滥用，甚至这种赋能未能被加以有效约束，那势必会直接导致人类被笼罩在人工智能赋能攻击的阴影之下。

比如自动驾驶汽车失效、智能机器人失效、智能音箱失效、人工智能系统“失控”等。

预防人工智能技术失控的举措有：人机协作国际规范、阿西洛马人工智能原则、自我终结机制防范系统性失控风险等。

第六章 智能视觉（课后题及参考答案）

1. 理解基础上简述视觉感知和视觉认知。

视觉感知是一种直观而内在的观察和理解过程，外部的视觉通过眼睛传递给大脑后，视觉神经几乎同时会对线条、质地、颜色、形状的空间关系、距离和其他大脑里已有的视觉进行加工。认知指在认识活动的过程中，个体对感觉信号接收、检测、转换、简约、合成、编码、储存、提取、重建、概念形成、判断和问题解决的信息加工处理过程。视觉自身具有无需努力的特性，人们几乎把它的认知过程当作理所当然的。

2. 简述计算机视觉中的多层次视觉理论。

在 20 世纪 70 年代，David Marr 提出了一个多层次的视觉理论，分析了不同抽象层次的视觉过程，标志着计算机视觉成为一门独立的学科。为了专注于理解视觉中的特定问题，理论确定了三个层次的分析：计算，算法和硬件实现水平。Marr 将视觉描述为从二维（2D）视觉阵列（在视网膜上）到作为输出的世界的三维（3D）描述。

3. 简述计算机视觉的定义。

计算机视觉（Computer Vision，CV）是利用摄像机和电脑代替人眼使得计算机拥有类似于人类的那种对目标进行分割、分类、识别、跟踪、判别决策的功能。作为一个新兴学科，计算机视觉是通过对相关的理论和技术进行研究，从而试图建立从图像或多维数据中获取“信息”的人工智能系统。

4. 理解计算机视觉和人工智能的关系。

计算机视觉与人工智能有密切联系，但也有本质的不同。人工智能的目的是让计算机去看、去听和去读。图像、语音和文字的理解，这三大部分基本构成了现代意义上人工智能。而在人工智能的这些领域中，视觉是核心。人工智能更强调推理和决策，但至少计算机视觉目前还主要停留在图像信息表达和物体识别阶段。“物体识别和场景理解”也涉及从图像特征的推理与决策，但与人工智能的推理和决策有本质区别。

计算机视觉和人工智能的关系：

第一，它是一个人工智能需要解决的很重要的问题。

第二，它是目前人工智能的很强的驱动力。

第三，计算机视觉拥有大量的量子人工智能的应用基础。

5. 简述相机的成像过程，理解其相关的四个坐标系：世界坐标系、相机坐标系、图像坐标系、像素坐标系。

相机将三维世界中的坐标点映射到二维图像平面的过程能够用几何模型进行描述，其中最简单的是针孔模型，也被称为理想的透视模型，它描述了一束光线通过针孔之后，在针孔背面投影成像的关系。

物体的空间坐标和图像坐标之间是线性的关系，相机的成像过程涉及到四个

坐标系：世界坐标系、相机坐标系、图像坐标系、像素坐标系以及这四个坐标系的转换。

（1）世界坐标系：是客观三维世界的绝对坐标系，也称客观坐标系。

（2）相机坐标系：以相机的光心为坐标原点，X 轴和 Y 轴分别平行于图像坐标系的 X 轴和 Y 轴，相机的光轴为 Z 轴。

（3）图像坐标系：以图像传感器的图像平面中心为坐标原点，X 轴和 Y 轴分别平行于图像平面的两条垂直边，用(x,y)表示其坐标值。图像坐标系是用物理单位（例如毫米）表示像素在图像中的位置。

（4）像素坐标系：以图像传感器图像平面的左上角顶点为原点，X 轴和 Y 轴分别平行于图像坐标系的 X 轴和 Y 轴，用(u,v)表示其坐标值。

6. 简述立体视觉的概念。

立体视觉是基于视差原理并利用成像设备从不同的位置获取被测物体的多幅图像，通过计算图像对应点间的位置偏差，来获取物体在位置空间的三维坐标信息的方法。立体视觉是计算机视觉领域的一个重要课题，它的目的在于重构场景的三维几何信息。

7. 理解数字直方图的概念。

图像直方图（Image Histogram）是用以表示数字图像中亮度分布的直方图，标绘了图像中每个亮度值的像素数。在直方图中，横坐标的左侧为纯黑、较暗的区域，而右侧为较亮、纯白的区域。直方图是对图像亮度或者色彩值的统计方法，它统计了每一个强度值所具有的像素个数，是图像中像素强度分布的图形表达方式。

8. 简述图像卷积的概念，解释图像卷积的过程。

卷积（Convolution）是两个变量在某范围内相乘后求和的结果，和均值滤波一样，它也是一种线性运算。数字图像是一个二维的离散信号，对数字图像做卷积操作其实就是利用卷积核（模板）在图像上滑动，将图像点上的像素灰度值与对应的卷积核上的数值逐点相乘，然后将所有相乘后的值相加作为卷积核中间像素对应的图像上像素的灰度值，并最终滑动完所有图像的过程。

使用卷积核的计算，一定要考虑卷积后图像的尺度问题，滑动步长（即卷积核在图像每次平移滑动的像素数）为 s，原图像大小为$N_1 \times N_1$，卷积核大小$N_2 \times N_2$，则卷积后的图像大小为$(N_1 - N_2)/s + 1 \times (N_1 - N_2)/s + 1$。

9. 理解并描述一个典型的卷积神经网络结构。

一个典型的卷积神经网络结构是由一系列的过程组成的。最初的几个阶段是由卷积层和池化层组成，卷积层的作用是探测上一层特征的局部连接，然而池化层的作用是在语义上把相似的特征合并起来。实际训练中，池化层一般有两种方式：Max Pooling 和 Average Pooling。

卷积层的单元被组织在特征图中，在特征图中，每一个单元通过一组叫做滤波器的权值被连接到上一层的特征图的一个局部块，然后这个局部加权和被传给一个非线性函数。全连接层在整个卷积神经网络中起到“分类器”的作用。通过这一层之后可接自定义的一层结构用来做分类或者回归问题。

10. 简述三维视觉重建的基本步骤。

利用深度相机实现三维重建，对于单个景物，一般经过数据流采集、深度图像增强、点云计算与配准、数据融合、模型表面生成等步骤。对拍摄输入的每一帧深度图像均进行上述前六步操作，直到处理完若干帧，最后完成纹理映射。

第七章 智能语音（课后题及参考答案）

1. 智能语音预处理技术有哪些技术？分别是怎么处理的?

智能语音的预处理技术包含分帧、加窗、预加重；

分帧：将语音信号分为一帧一帧来处理，采用可移动的有限长度窗口进行加权的方法来实现。帧长一般设置为 10～30ms，帧移与帧长的比值一般取 0～1/2。

加窗：将语音信号与一个窗函数相乘，窗函数：一般具有低通特性，分成以下几种类型矩形窗：主瓣宽度最小，旁瓣高度最高，会导致泄漏现象。矩形窗函数如下：

$$W(n,\alpha) = 1, 0 \le n \le N-1$$

汉明窗：主瓣最宽，旁瓣高度最低，可以有效克服泄漏现象，具有更平滑的低通特性。汉明窗函数如下：

$$W(n,\alpha) = (1-\alpha) - \alpha \cdot \cos(2\pi m/(N-1)), \quad 0 \le n \le N-1$$

预加重：将语音信号通过一个高通滤波器，目的是为了对语音的高频部分进行加重，去除口唇辐射的影响，增加语音的高频分辨率。一般通过传递函数为:$H(z) = 1- az^{-1}$ 的一阶 FIR 高通数字滤波器来实现预加重，其中 a 为预加重系数，$0.9<a<1.0$。设 n 时刻的语音采样值为 x(n)，经过预加重处理后的结果为 y(n) = x(n)-ax(n-1)。

2. 语音信号的端点检测是如何实现的？

语音信号的端点检测是指从包含语音的一段信号中确定出语音的起始点和结束点的位置。在没有噪声的情况下，用短时平均能量就可以检测出语音的端点。在有噪声情况下，语音信号的端点检测可分为三类：基于阈值的端点检测、作为分类器的端点检测、模型端点检测。

1).基于阈值的端点检测：通过提取时域（短时能量、短期过零率等）或频域（MFCC、谱熵等）特征，通过合理的设置门限，达到区分语音和非语音的目的。

2).作为分类器的端点检测：可以将语音检测视作语音/非语音的两分类问题，进而用机器学习的方法训练分类器，达到检测语音的目的。

3).模型端点检测：可以利用一个完整的声学模型（建模单元的粒度可以很粗），在解码的基础，通过全局信息，判别语音段和非语音段。

3. 语音识别的主要模块有哪些？

语音识别系统的基本任务就是将输入的语音信号，识别成文字符号输出，基本上分成两个部分：前端处理(Front End Processing，FE)、搜索和解码(Search and Decoding)。其中，搜索和解码需要利用训练好的声学模型(Acoustic Model，AM)、语言模型(Language Model，LM)，以及联系这两个模型的发音词典(Lexicon)。

前端处理完成的基本任务就是特征提取和归一化，在广播语音或者电话语音等大段语音处理中，还需要做相应的前端预处理工作，切分成语音片断输入；搜索和解码引擎是整个识别器的主要算法所在，主要采用 Viterbi 搜索算法等动态规划方法，搜索在给定模型情况下的最优结果；语言和声学模型则是通过统计方法训练得到的，发音词典是将这两个模型联系起来的桥梁。

第八章 智能机器人（课后题及参考答案）

1．什么是智能机器人？

智能机器人是一种具备一些与人或其他生物相似的智能能力 ，如感知能力、规划能力、
动作能力和协同能力，具有高度灵活性的自动化机器。智能机器人相较于一般机器人而言，
具有感知周围环境的能力，并且能对周围的环境进行分析，调整自己行为来达到操作者的
要求，甚至能够在信息不充分及环境迅速变化的情况下完成动作。

2．根据不同的应用环境，机器人主要分为哪几类？

机器人主要分为工业机器人、服务器人和特种机器人。

3．智能机器人主要关键技术有哪些？

智能机器人主要关键技术包括智能感知技术、机器视觉技术、智能导航与规划技术、智能控制技术和智能交互技术，这些关键技术用于实现智能机器人感知、决策和行为。

4．请简述智能搬运机器人整理玩具的流程，并说明采用卷积神经网络识别物体的步骤。

智能搬运机器人整理玩具的流程主要包括（1）玩具物体识别；（2）物体抓取；（3）导航与路径规划；（4）人际交互等流程。

利用卷积神经网络实现物体识别主要包括两个步骤 ：①是构建卷积神经网络模型，卷积神经网络模型具体步骤包括准备训练图像集、图像的标注，然后通过基于 Keras/Tensorflow 训练网络得到模型。②是构建玩具 /非玩具探测器，利用网络模型进行判断图片是玩具还是非玩具。

第九章 自然语言处理（课后题及参考答案）

1. 自然语言处理的发展工程化、实用化应用，展经过萌芽期、发展期和复繁荣期三个阶段，其中（ ）注重工程化、实用化应用，并重新认识经验主义方法。

A. 20 世纪 20-60 年代　　B. 20 世纪 60-80 年代

C. 20 世纪 80 年代后期　　D. 20 世纪 80-90 年代

C

解析：20 世纪 80 年代后期，工程化、实用化的解决问题方法成为关注焦点，经验主义方法被重新认识并得到迅速发展。在自然语言处理研究中，重要的标志是基于语料库的统计方法被引入到自然语言处理中，并发挥出重要作用。使得研究和关注基于大规模语料的统计机器学习方法及其在自然语言处理中的应用，客观地比较和评价各种方法的性能成为目标。在这一时期，基于语料库的机器翻译方法得到了充分发展，尤其是 IBM 的研究人员提出的基于噪声信道模型的统计机器翻译模型，这一时期也成为机器翻译领域的里程碑。

2. 自然语言处理的常见任务包括（ ）(多选)。

A. 信息抽取　　B. 信息过滤　　C. 问答系统

D. 语音识别　　E. 图像分割　　F. 文档分类

解析：自然语言处理研究的内容十分广泛，根据其应用目的不同，我们可以大致归纳如图 9-2 所示研究方向，包括信息抽取、信息过滤、问答系统、文档分类。

3. 文本表示是将非结构化或者是半结构化的信息转换为一种以结构化形式语言描述且计算可理解识别的信息。文本表示可以用图的形式表示，也可以用向量表示。这种说法是（ ）的。

A. 正确　　B. 错误

A

解析：在做完语料预处理之后，需要考虑如何把分词之后的字和词语表示成计算机能够计算的类型。有两种常用的表示模型分别是词袋模型和词向量。因此正确。

4. 文本分类是在预定 义的分类体系下，根据文本的特征，将给定文本与多个类别相关联的过程。因此，文本分类研究涉及文本内容理解和模式分类等若 F 自然语言理解和模式识别问题，其处理流程一般包括输入文档、____、 文 本表示、____、类别输出。

预处理、分类模型

5. 最大熵模型属于哪一种学习方法?请简述其在解决消歧问题时的应用原理。

在词性标注环节，，基于统计的方法较为常用，如基于最大熵的词性标注、基于统计最大概率输出词性和基于 HMM 的词性标注。

第十章 无人驾驶（课后题及参考答案）

1. 限制无人驾驶发展的主要因素？

人在驾驶中的本能包含了人类在行为判断上的智能控制，也包含了驾驶经验积累带来的预判。应对突发事件的前提是对周围环境的有效感知，人类有复杂的视觉系统能够看到周围的环境，并对看到的信息进行理解和处理。而对无人驾驶车辆而言，需要给无人驾驶车辆配置高清的视觉系统，有序高清图像的识别和计算需要计算机有强大的数据处理能力，同时也需要有优秀的算法对图像进行分析，理解，然后转化成机器能够执行的指令。在过去受限于机器对图像的处理能力，无人驾驶并没有获得有效的发展。

2. 简述无人驾驶的传感系统？

传感器有四种：GPS/IMU、激光雷达、摄像头和毫米声波雷达和声纳，全球定位系统（Global Positioning System，GPS）最初是用于军用，现在发展成低成本的消耗品，是一个相对精确的定位传感器，但是它的更新频率很慢，因此无法提供实时更新。惯性测量单元（Inertial Measurement Unit，IMU）是一系列复杂设备的集合，包括里程计、加速计、陀螺仪、指南针等，能够弥补 GPS 不准确计算，通过融合 GPS 和 IMU 可以提供准确和实时的位置更新。激光雷达通过发射激光束，接收表面反射，测量反射时间，确定距离来制作高精地图、定位和探测障碍物，可用于建图、定位和避障。摄像头主要用于目标识别和跟踪，比如：车道、交通灯、人脸检测。无人驾驶汽车通常需要安装 8 个摄像头来探测车辆前方、后方、两侧的物体。毫米波雷达和声纳组成避障的最后一道防线，能够感受到车辆前方障碍物的距离和速度，一旦有可能发生碰撞，无人驾驶汽车就应该制动或者转向进行避障。

3. 简述无人驾驶的感知系统？

无人驾驶的感知系统主要是通过各种传感器，实时获取车辆周围的动态数据。完备的数据集是识别问题和改进解决方案的重要组成。无人驾驶要面对复杂多变的道路环境，为了对无人驾驶感知算法进行公正全面的评估，需要有大量细致的道路信息数据集。

4. 简述最短路径算法？

第十一章 智能电子商务（课后题及参考答案）

1. 简述电子商务的特点。

电子商务目前可以总结为这样几个特点：

1）快捷化：快捷是电子商务的重要特点，在互联网技术支持下，电子商务交易可以瞬间完成；

2）虚拟化：交易双方无需当面进行，交易虚拟化；

3）低成本化：通过互联网进行的电商交易时间成本和交易成本都大大降低；

4）透明化：在电商平台支持下，电商交易的各个环节都在平台上直接公示出来，较传统交易方式更为透明；

5）标准化：电商平台要求交易按统一要求进行，更加标准化。

2. 为什么说电子商务天然具备人工智能的基础。

主要原因为：

1）电商拥有非常庞大的数据，是训练人工智能模型的必要条件；

2）电商拥有巨大的规模优势，可以摊薄人工智能研发的成本；

3）电商的商品销售，比传统交易存在更大的不确定性，使用人工智能识别这种不确定性成为天然的需求。

3. 传统电子商务包含的技术有哪些？

一般而言，传统的电子商务技术一般主要包括：

1）网络技术

2）Web 浏览技术

3）数据库技术

4）安全技术

5）电子支付技术

4. 简述电子商务购物节技术支持的高并发秒杀等应用场景，需要注意的两个原则。

电子商务购物节技术支持高并发秒杀等应用场景，主要需要注意两个原则：首先尽量将请求拦截在前端，如果不做拦截的话网络请求会瞬间压倒了后端，响应速度极慢，几乎所有请求都超时。在设计支持秒杀的架构时，要保证到后端的网络请求不超过设计的最大容量，让整个系统能撑住，即使部分用户前端出现响应慢也要保证系统整体是可用的。其次要注意多使用缓存，秒杀是典型的读多写少的场景，非常适合使用缓存。

5. 举例说明人工智能在电子商务中的作用？

电商是人工智能应用较为容易获得收益的领域，一方面，人工智能的应用可以直接在电商网站应用，很容易获得反馈。另外，人工智能的模型训练可以直接以 GMV（Gross Merchandise Volume，即网站的成交金额）等收益型指标最大化作为训练的目标，从而直接在应用人工智能模型后获得利润上的增长。

6. NLP 技术在电子商务领域可以用来做什么应用？请简述。

NLP 技术在电子商务领域广泛地应用于搜索、前端导购、智能问答、创新业务。能够帮助品牌商透视全局数据，帮助平台治理运营发现问题商品，帮助行业基于确定的信息选品，做人货场匹配提高消费者购物体验等等。NLP 技术还可以为新零售提供可靠的智能引擎。

第十二章 智能医疗（课后题及参考答案）

1. 人工智能技术在医疗领域的主要应用有哪些，简述目前智能医疗在我国的主要应用场景？

从目前我国智能医疗领域产品的分布来看，“AI+医疗”主要集中在八大应用场景，包括疾病风险预测、医学影像、辅助诊疗、药物挖掘、健康管理、医院管理、辅助医学研究平台、虚拟助理等。因计算机视觉与基因测序技术的发展，疾病风险预测和医学影像场景下的应用数量最多，相关产品相对成熟，产品主要以尚未成熟的软件形态存在，算法模型尚处于训练优化阶段，未完成大规模应用，主要面向医院、体检中心、药店、制药企业、研究机构、保险公司、互联网医疗等，业务模式主要以科研合作方式展开，引入技术、训练模型、获取数据与服务。

2. 人工智能在智能医疗领域的探索始于哪一年代？我国智能医疗的发展始于哪一年代？

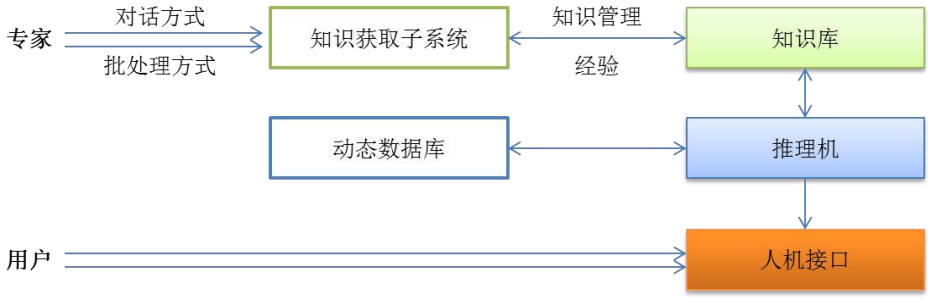
最早在医疗领域进行 AI 的探索出现在上世纪 70 年代。1972 年，由利兹大学研发的 AAPHelp 是医疗领域最早出现的 AI 系统，这个系统主要是用于对腹部剧痛的辅助诊断和手术。

我国智能医疗的发展始于 20 世纪 80 年代初，1978 年北京中医医院关幼波教授与计算机科学领域的专家合作开发了“关幼波肝病诊疗程序”，第一次将医学专家系统应用到我国传统中医领域。

3. 医疗人工智能应用可以分为哪三个阶段？请详细说明。

从数据有效性和商业模式的发展来看，医疗 AI 应用可以分为三个阶段：第一阶段为数据整合阶段。深度学习等先进算法已经出现，但由于医疗数据标准化低，共享机制弱，导致 AI 在医疗行业的应用领域和效果受限。第二阶段是“数据共享+感知智能”阶段。当医疗数据融合到一定程度后，将会在辅助诊疗、图像识别等各领域出现辅助技术。在这个阶段，数据和算法相辅相成，有效数据将促进算法的实施得到进一步优化。第三阶段是“健康大数据+认知智能”阶段。在此阶段，AI 整体上从感知智能向认知智能发展，健康大数据的获取成本也将降低，人类将步入个性化医疗时代，该阶段将出现替代人类医生的 AI 应用。

4. 请画出智能诊断系统的结构框架图。



5. 我国智能医疗在哪些方面存在不足？

开放性问题，鼓励同学拓展思考。参考答案如下：

医学是一个前沿学科，会随时遇到新问题和新的疑难杂症，而相关数据的积累需要时间，因而算法模型难以迅速得到优化，同时 AI 医疗产品的数据算法也需要不断更新和迭代，算法技术难度也会加大。医学领域的高门槛和技术力量的欠缺相对限制了 AI 医疗的快速发展。虽然我国智能医疗发展较快，但各应用场景产品及服务多处于试用阶段。目前我国智能医疗仍面临医疗数据孤岛及结构化数据不足（超过 80%以上的医疗数据都是非结构化的）、医疗 AI 技术仍相对不成熟、医疗器械许可证监管政策相对偏紧等三大突出问题，限制了 AI 医疗落地的速度和规模。医疗健康领域是一个强监管行业，国内医疗数据和信息隐私保护也给医疗 AI 企业进入医院设置了一定的门槛，2018 年 8 月 1 日起，新版《医疗器械分类目录》施行，若诊断软件通过算法，提供诊断建议，仅有辅助诊断功能，不直接给出结论，则申报第二类医疗器械；若对病变部位进行自动识别，并提供明确诊断提示，则按照第三类医疗器械管理。CFDA 认证是产品合法上市的必经阶段，CFDA 部门对于医疗器械三类证书审核非常严格，目前提出申报的 AI 医疗企业极少数可以获批。此外，在 AI 人才短缺的背景下，既懂医学又懂 AI 的复合型人才的巨大缺口也限制了 AI 医疗的发展速度。作为一个特殊的传统行业，医疗对于新技术的接受是偏保守的，目前 AI 医疗难以取得爆发式的增长。在当前弱 AI 医疗的背景下，虽然应用场景很广泛，医疗行业 AI 服务供应商覆盖了全价值链用户场景，如虚拟助理、药物研发、健康管理、医疗影像辅助诊断等，但产品真正落地在医院并大规模使用的还比较少。目前主要是解决效率问题，对医生起到辅助诊疗的作用，AI 医疗不能代替医生。