**绪论部分**

**思考与练习答案**

1. 人工智能（Artificial Intelligence）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. 假设:任何一个系统，如果它能够表现出智能，那么它就必定能够执行上述6种功能:输入符号;输出符号;存储符号;复制符号;建立符号结构;条件性迁移:反之，任何系统如果具有这6种功能，那么它就能够表现出智能，这种智能指的是人类所具有的那种智能。把这个假设称为物理符号系统的假设。物理符号系统的假设伴随3个推论，

推论1:既然人具有智能，那么他(她)就一定是个物理符号系统。

推论2:既然计算机是-一个物理符号系统，它就一定能够表现出智能。

推论3:既然人是一个物理符号系统，计算机也是一个物理符号系统，那么就能够用计算机来模拟人的活动。

1. 回顾人工智能的发展阶段 ,可大致分为孕育、 形成、 知识应用和综合集成这4个阶段。
2. 人工智能存在许多不同的研究领域 ,如语言处理、 自动定理证明、 计算智能、智能数据检索系统、视觉系统、问题求解、人工智能方法和程序语言以及自动程序设计等。在过去的 40 年中已经建立了一些具有人工智能的计算机系统 ,能够求解微分方程、下棋、设计和分析集成电路、合成人类自然语言、检索情报、诊断疾病以及控制太空飞行器和水下机器人等。
3. 人工智能未来研究的三个热点是:智能接口、数据挖掘、主体及多主体系统。

智能接口技术是研究如何使人们能够方便自然地与计算机交流。为了实现这一目标，要求计算机能够看懂文字、听懂语言、说话表达，甚至能够进行不同语言之间的翻译，而这些功能的实现又依赖于知识表征的研究。因此，智能接口技术的研究既有巨大的应用价值，又有基础的理论意义。目前，智能接口技术已经取得了显著成果，文字识别、语音识别、语音合成、图像识别、机器翻译以及自然语言理解等技术已经开始实用化。

数据挖掘就是从大量的、不完全的、有噪声的、模糊的、随机的实际应用数据中提取隐含在其中的、人们事先不知道的、但又是潜在有用的信息和知识的过程。数据挖掘和知识发现的研究目前已经形成了三根强大的技术支柱:数据库、人工智能和数理统计。其主要研究内容包括基础理论、发现算法、数据仓库、可视化技术、定性定量互换模型、知识表示方法、发现知识的维护和再利用、半结构化和非结构化数据中的知识发现以及网上数据挖掘等。其中的主体技术尤为被人工智能专家看好。

多主体系统试图用主体来模拟人的智能行为，主要应用在对现实世界和社会的模拟、机器人以及智能机械等领域。目前对主体和多主体系统的研究主要集中在主体和多主体理论、主体的体系结构和组织、主体语言、主体之间的协作和协调、通信和交互技术、多主体学习以及多主体系统应用等方面。

**拓展阅读**

人工智能让我们害怕什么？

从法律的角度谈谈人工智能带来的挑战。从人机关系的视角看，主要包括两项巨大的挑战，一是机器替换人类，导致失业浪潮；二是人工智能的军事化，智能武器在利比亚内战中已大量使用。用美国科幻文学的口号来说，未来已经来到。

**挑战之一：个人隐私的逐渐消亡**

人工智能带来的首要挑战是个人隐私的消亡。在传统社会，隐私之所以被称为“私”，是因为它可以“隐”。中文词将其特点诠释得非常完美。

　　当前社会已经普遍使用机器智能，它能够记录每个人的行为与信用表现，其背后涉及的法律问题就是个人的隐私权。在法律层面，隐私权是一项非常重要的权利。美国在经过了多年的宪法诉讼后，隐私权早已被确立为宪法中的一项基本权利，中国编纂起草的统一《民法典》正在审核中，隐私权正是其中一项非常重要的内容。

**AI商业模式：与知识产权相反的数据获取**

今天，人工智能的来临，导致隐私从人类的日常生活中消失。那么，我们是否有必要保护这种正在消失的权利？就像脸书创始人马克·扎克伯格说的：我们为什么需要隐私？我的客户很乐意把隐私交给我们，因为我们的服务能给他们带来不可抗拒的便利。尽管我们可从哲学、伦理学、法学等各个角度切入，寻找多种理论上的应对方案，但人工智能技术实际上在现有的市场经济条件下，必定会按照一定的商业模式涌入社会。推广人工智能最有利的产品就是智能手机。扎克伯格和他的团队惊人地推出人工智能的商业模式。

人工智能的商业模式与知识产权模式完全相反。所谓知识产权，就是在任何无形的东西上设立产权。例如，一束花并不是知识产权，但拍花的照片，它的使用就可以成为知识产权，这朵花的香味也能做成一个具有识别性的标记，称作商标，也就是知识产权。因此，知识产权的主要用途就是禁止他人随意复制或使用，需要付费才能使用。

在目前的商业竞争和经济活动中，知识产权是一个非常有效的竞争手段，因为它可以打击竞争对手，通过诉讼强迫他人付费或承担更多的成本，促使对方不得不屈服。

从本质上说，商业模式的基础是对价交易，法律语言表述为，交易双方需要付出对价，形成契约。当前网络企业大平台采用免费或廉价的付费模式，而我们付出的对价就是个人信息。从我们购买手机的那一刻起，就已经提交了个人信息，并且还需不断地提交，我称之为硬规则，因为消费者必须接受。这些数据被企业获取，用于建立数据库，再转卖给第三方或者用于其他用途，例如开发新产品等等。

**数据财产化后，企业掌握了每个人的隐私**

数据如此重要，以至于现有的法律无法对其进行估算。数据所蕴含的巨大价值令业界非常希望将其财产化。那数据的原始主人是谁？难道不是我们每一个人吗？难道数据不是我们的财产吗？若是这样思考，脸书就无法运营了，因为它需要与几亿人签订合同。因此，数据的财产化是个法律问题，目前无解。虽然利益集团的游说非常激烈，不久的将来或会进行立法，但即使没有立法，数据事实上也已经是财产了，因为它是我们每天进行的无数次交易的标的物。法学理论认为，只要能成为交易的标的物，例如数据，那它就已享有财产的地位，只不过对它的保护缺少明文规定而已。所以，这些企业事实上已经掌握了我们每个人的隐私。

当然，还有一位参与数据收集竞争的主导者，即政府。在拥有发达的互联网产业之后，任何国家的政府必然深度介入数据的抓取。中国在这方面做得最好，大城市道路每50米就安装一个摄像头，促使暴力犯罪大幅降低，即便与发达国家相比，中国也走在最前端。虽然从隐私角度来说，这或许令人不安，但从产业发展以及政府对数据的抓取来说，这可以解决诸多问题。例如，许多传统上难办的案件到了数据时代非常容易破获。

**挑战之二：引领法律走向硬规则体系**

人工智能使我们忽视原本异常繁琐的程序、调查，不得不接受一些硬规则，这对于法制建设的影响非常巨大。什么是硬规则？中国的马路中间通常都设有一排铁栏，用于分隔两个车道，它强迫车辆必须在它自己的那条车道里行驶，不得越界。这也可以说明软规则的失效，政府可以选择其他整治交通的措施，但都不如硬规则方便、廉价。

**警惕人工智能带来的规则制订权之争**

　 硬规则带来了什么好处？它不需要像传统的法制建设那样由政府积极推动普法，也不用通过文艺作品向大众宣传规则的重要性，也无须事先征求民众的意见。一般来说，我们国家的立法应当按照民主原则，通过人民代表大会制度进行，或通过政府有关部门制定规章。但硬规则不同，硬规则主要由商家制定，它通过智能终端添加到我们身上，智能手机就是最佳的例子。手机硬规则通过用户点击“同意”键进入系统，如果用户不同意，也可以点“取消”键。这种合同在过去的人类社会中很少出现，而按照现在的制度和商业模式来看，这就是一种单方面为用户制定规则，使之通过衡量利弊或被迫接受的格式合同。

所以，整个法律制度实际上被人工智能引领着走向了硬规则体系。这令人感到害怕和忧虑，值得引起世人的注意。因为这种情况将导致资本力量过于强大。从国家的立场来看，立法必须回应民众的要求、呼声与利益诉求。但是，如果规则的制定权大量落入企业手中，其结果就大为不同了。

从某种角度来说，政府将比过去的工业化社会更大幅度地介入商业活动，这不利于建设健康的社会主义市场经济。依据市场经济理论，最理想的市场经济是政府只负责一部分的监管、注册和维稳等传统要求，但智能终端、智能经济、智能技术将改变原有格局。

**商家过度承担硬规则的制定，将加剧贫富差距**

事实上，硬规则的制定权越来越多地归于商家，商家乐见其成，因为可增加利润收益。它的危机表现形式就是十多年前美国发生的华尔街金融危机。

我们要防止因网络技术、网络产业发展导致的贫富差距拉大和社会分化。不久前，美国黑石集团共同创始人、全球主席兼首席执行官苏世民向麻省理工大学捐款建立人工智能学院，明确要求该学院必须包括关于人机伦理的研究，而这类研究必须解决贫富分化、财富过度集中的问题。可见，苏世民已经清醒地认识到，人类社会所面临的新挑战，是财富的巨大分化带来的社会难题。作为富豪，他有责任提出这个问题，而学者必须在研究科技的同时关注伦理问题。中国“基因编辑婴儿”事件，是个典型的负面例子。其背后的投资人和合作者都是外国商家，试图进行商业冒险。

这表明，商业资本在市场博弈中具有盲目性，缺乏伦理约束。正如马克思所说：为了100%的利润，资本就敢践踏一切人间法律；有300%以上的利润，资本就敢犯任何罪行，甚至去冒绞首的危险。既然如此，我们该如何注意伦理问题？必须加强政府部门和行业本身的约束。政府部门相当于外部约束、外部监管，行业本身也有自我教育、自我培训等自律的要求。

**挑战之三：深刻改变生活习惯和生命意义**

从科学发展的角度来说，探索是非常必要的。对那些不得不发展的产品而言，我们必须在技术条件与科学原理上继续探索，以便获得对人类有益而非有害的结果。人工智能在这方面的表现特别醒目。

**麦当劳配方秘诀：按基因喜好迎合全人类口味**

开发人工智能的商家非常聪明，智能终端通常根据反复实验研究人的心理和习惯，以及由基因决定的倾向性来设计界面，因此，一个出生不久还不会说话的婴儿会很快发现手机或平板电脑的可爱之处，并与之互动，这是设计的成功之处。

另以麦当劳为例，它是实验室的产物。以工业化养殖的牛、猪、鸡作为原始材料，经过混合、配方以及化学处理，调试出令全球儿童都喜欢的口味，并为此成立了一所麦当劳大学。在美国，即便是含着金钥匙出生于贵族家庭的小布什也爱吃这种食品，因为他无法拒绝这种根据人类基因构成研制出的味觉配方。

终端界面的设计也是如此，比如手机制造商研制的可折叠手机最初也受到批评，但很快就寻找到了感觉与方向，因为这些企业拥有全球最顶尖的设计团队。设计者并不仅仅是为了让用户使用方便，而是要让用户无法摆脱。

**改变审美趣味，机器设置的产品影响生命意义**

微软小冰作诗是个很有意思的现象，如果将机器人与杜甫、李白相比，那就理解有误了。在我看来，微软研发小冰的意图并非让它成为杜甫，华为研发5G产品也并非想让其成为爱因斯坦或牛顿，他们的根本目的是占领市场。AlphaGo团队将其研发的机器人投入市场，是为了实现取代人类智慧的最终目标。因此，我所关心的是小冰下一步商业化之后如何改变我们与下一代人类对诗歌、文学以及艺术的感受。这一团队以及它的竞争者或许已在基因层面探索人类对文字和音乐的感受，以便研发出的产品能够改变人机关系，我将其称作较为终极的挑战，因为它改变了生命的意义。

可以想象那个时代，杜甫将是极少数学院派研究的对象，因为机器已经研发出完全不同的风格，让我们从小就会喜欢。音乐、美术、戏剧表演都是如此。

在立法领域，一旦机器大规模介入，人类将无法厘清规则，因为每部机器都会将规则无限复杂化，其复杂程度远超人类所能理解的范围，只有利用机器才能与之对抗。

**未来走向：我们是否需要机器？这是终极挑战**

那时，我们是否需要机器？这是一个终极挑战，它不仅颠覆了生命的意义，也颠覆了日常生活，它提供的便利和规则正在温水煮青蛙式地将人类逼至无法反抗的境地。

为此，提出了两个方向，一是企业主导的知识产权垄断，主宰了我们的生活和社会；一是数据国有化，政府深度介入规则制定，从这个意义上讲，未来我们完全有可能进入共产主义社会。列宁曾说，人类将按照科学的进步程度来接受共产主义，共产主义在科学技术不发达的情况下是无法实现的。1960年代，一位苏联数学家提出综合数学模型，解说计划经济成功与失败的可能性，并获得了诺贝尔经济学奖。受此启发，我认为计划经济并非过去式，只不过不适合科技不发达的时代，将来人类有可能计划得非常完善，考虑到每一个人的需求。在无人驾驶领域，已有专家提出，机器驾驶的安全性远远高于人类。

**机器学习部分**

7.4 引言

监督学习需要有明确的目标，很清楚自己想要什么结果。比如：按照“既定规则”来分类、预测某个具体的值…

监督并不是指人站在机器旁边看机器做的对不对，而是下面的流程：

1. 选择一个适合目标任务的数学模型
2. 先把一部分已知的“问题和答案”（训练集）给机器去学习
3. 机器总结出了自己的“方法论”
4. 人类把”新的问题”（测试集）给机器，让他去解答

上面提到的问题和答案只是一个比喻，假如我们想要完成文章分类的任务，则是下面的方式：

1. 选择一个合适的数学模型
2. 把一堆已经分好类的文章和他们的分类给机器
3. 机器学会了分类的“方法论”
4. 机器学会后，再丢给他一些新的文章（不带分类），让机器预测这些文章的分类

7.5 引言

输入数据没有被标记，也没有确定的结果。样本数据类别未知，需要根据样本间的相似性对样本集进行分类（聚类，clustering）试图使类内差距最小化，类间差距最大化。通俗点将就是实际应用中，不少情况下无法预先知道样本的标签，也就是说没有训练样本对应的类别，因而只能从原先没有样本标签的样本集开始学习分类器设计。

无监督学习目标不是告诉计算机怎么做，而是让它（计算机）自己去学习怎样做事情。无监督学习有两种思路。第一种思路是在指导Agent时不为其指定明确分类，而是在成功时，采用某种形式的激励制度。需要注意的是，这类训练通常会置于决策问题的框架里，因为它的目标不是为了产生一个分类系统，而是做出最大回报的决定，这种思路很好的概括了现实世界，agent可以对正确的行为做出激励，而对错误行为做出惩罚。

7.6 引言

顾名思义，半监督学习介于受监督学习和无监督学习之间。受监督学习采用带有正确答案（目标值）的标记过的训练数据。在学习过程之后，将得到一个经过调优的权重集的模型，这可以用于预测尚未标记的类似数据的答案。半监督学习同时使用标记和未标记的数据来拟合模型。在某些情况下，比如Alexa的添加未标记的数据的确提高了模型的准确性。在其他情况下，未标记的数据可能会使模型更差。正如我将在下面所讨论的，在不同的数据特性条件下，不同的算法会有不同的缺点。一般来说，标记数据需要花费金钱和时间。这并不总是问题，因为有些数据集已经有了标记。但是如果您有很多数据，其中只有一些是标记过的，那么半监督学习这种技术很值得一试。

**思考与练习答案**

1. 机器学习的研究内容有三个方向，一个方向是以模拟人类的学习过程出发，试图建立学习的认识生理学模型，这个方向与认知科学的发展密切相关。第二个方向是基础研究，发展各种适合机器特点的学习理论，探讨所有可能的学习方法，比较人类学习与机器学习的异同与联系。第三个方向是应用研究，建立各种实用的学习系统或知识获取辅助工具，在人工智能科学的应用领域，机器人系统，专家系统等建立自动获取知识系统，积累经验，完善知识库与控制知识，进而能使机器的智能水平像人类一样。
2. 决策树学习是一种利用决策树逼近离散函数的方法。
3. 神经网络学习方法提供了一个鲁棒的方法来逼近重值、离散值和向量值函数。
4. 贝叶斯推理提供了一种概率推理方法。
5. 强化学习解决了任务如何学会选择最佳的行动来达到它的目标。
6. 归纳逻辑编程源于从例子中学习概念，是一种相对简单的归纳形式。
7. 基于案例的推理(Case-Based Reasoning, CBR)是一种惰性学习算法，它通过分析相似的实例来分类新的查询实例，同时忽略与查询有很大差异的实例。
8. 支持向量机(SVM)是近年来非常流行的分类和优化方法。
9. 遗传算法提供了一种学习方法，其动机类似于生物进化，寻找一个合适的假设。当前种群的成员通过选择、交叉和突变等操作产生下一代种群。
10. 从1950年代发展到现在，经历了推理期、知识期、学习期。

（1）推理期。在推理期，只要给予机器逻辑推理能力，机器学习就具备智能。同时期产生了A.Newell和H.Simon的Logic Theorist程序和General Problem Solving 程序。但是这时的逻辑推理机器，不能满足人工智能研究的需求。

（2）知识期。在1970年代人工智能的发展进入了知识期，知识期即由人把知识总结出来再教给计算机。这一时期发展了大量专家系统，人工智能在众多应用领域取得了大量成果。随着知识系统的发展，专家系统越来越复杂，人们发现这种人工总结知识教给计算机做法 非常困难的，专家系统迎来了知识工程瓶颈。于是，人工智能迎来了学习期，即机器自己学习知识，也就是机器学习。

（3）学习期。追溯机器学习的第一次出现，是在1950年图灵关于图灵测试的文章中。其后在1950年代中后期基于神经网络的连接主义（Connectionism）学习开始出现， 产生了F.Rosenbatt的感知机（Perceptron）， B.Widrow 的Adaline等。此时，基于decision theory（决策理论）为基础的学习技术和强化学习技术发展迅速。随后在1980年代，机器学习成为一个独立学科，各种机器学习技术百花齐绽。1980年第一届机器学习研讨会IWML在美国卡耐基梅陇大学 （Carnegie Mellon University）举行。同期各种机器学习专业期刊，有关机器学习的专辑文章雨后春笋般的出现。

（1）监督学习

是有特征（feature）和标签（label）的，即便是没有标签的，机器也是可以通过特征和标签之间的关系，判断出标签。举例子理解：高考试题是在考试前就有标准答案的，在学习和做题的过程中，可以对照答案，分析问题找出方法。在高考题没有给出答案的时候，也是可以给出正确的解决。这就是监督学习。

（2）无监督学习

只有特征，没有标签。举例子理解：高考前的一些模拟试卷，是没有标准答案的，也就是没有参照是对还是错，但是我们还是可以根据这些问题之间的联系将语文、数学、英语分开，这个过程就叫做聚类。在只有特征，没有标签的训练数据集中，通过数据之间的内在联系和相似性将他们分成若干类。

（3）半监督学习

使用的数据，一部分是标记过的，而大部分是没有标记的。和监督学习相比较，半监督学习的成本较低，但是又能达到较高的准确度。综合利用有类标的和没有类标的数据，来生成合适的分类函数。半监督学习出现的背景：实际问题中，通常只有少量的有标记的数据，因为对数据进行标记的代价有时很高，比如在生物学中，对某种蛋白质的结构分析或者功能鉴定，可能会花上生物学家很多年的工作，而大量的未标记的数据却很容易得到。

监督学习：

优点：决策过程接近人的思维习惯，模型容易理解。

缺点：决策树学习方法的准确率不如其他模型，不支持在线学习，有新样本来的时候需要重建决策树，容易产生过拟合现象。

半监督学习：

优点：自我训练使用模型自己对未标记数据的预测结果，将其添加到已标记的数据集中。实际上，这为预测的置信水平设置了一些阈值，通常为0.5甚至更高，高于该阈值时，相信预测结果并将其添加到已标记的数据集中。不断地重新训练这个模型，直到没有更多可信的预测结果为止。这就回避了用于训练的实际模型的问题。和大多数机器学习一样，你可能会尝试每一个合理的候选模型，以期找到一个能很好工作的模型。  
缺点：自我训练在一定程度上是成功的，可谓是好坏参半。最大的缺点是模型无法纠正自己的错误：例如，对异常值高度自信（但错误）的预测可能会破坏整个模型。

**拓展阅读**

**从AlphaGo看机器学习现状**

围棋是最复杂的棋类游戏,人类高手下围棋主要靠宏观的直觉,加上局部的计算。AlphaGo凭借两招出奇制胜:深度卷积网络,模仿高手,寻找好的落点;深度

强化学习,形成左右互搏,自我进化。

AlphaGo的第一招:模仿高手，学习高手的棋形。要模仿高手棋形，AlphaGo需要一个分类器来判断棋形是否与高手的棋形相像。围棋盘可以看成是19x19的图像,虽然这个图像很小，但约有250150种变化。将这些变化分成高手棋形、非高手棋形，是一个挺难的机器学习问题，主要难在高手棋形的特征不好定义、不易提取。在人脸识别、车牌识别中，可以定义颜色、边缘、关键点等特征，显然围棋棋形的特征不能使用同样的方法。

AlphaGo使用了最新图像分类器——深度卷积神经网络(deep convolutional neural network, DCNN),可以自动学习图像中好的特征。不同于传统的人工神经网络,该网络的层数特别多,学习和分类的能力非常强。神经网络早在1943年就已提出,在1950年代末和1980年代曾兴起过两波研究热潮。以前的人工神经网络层数很浅,只能解决一些简单识别问题。2000年前后,欣顿(G. Hinton)等提出一套预训练后向传播的方法,解决了深度学习问题川。DCNN是专门针对图像识别的深度学习方法,对局部图像进行卷积计算,效率很高。

深度学习能够发挥巨大威力的前提是,必须要有大量的数据才能训练深度结构。深度学习会涉及，上百万、甚至上亿的参数,如果数据不够,很容易过拟合、

性能降低。此外,进行这样大规模的训练,需要超强的计算能力。据说，AlphaGo 存有15万职业棋手、百万业余高手的棋谱,训练的时候会用到1202个中央处理.单元( central processing unit，CPU )和176个图形处理单元( graphics processing unit, GPU )。

AlphaGo的第二招:自我学习,自我进化。模仿高手还不足以超越高手。为超越顶尖高手，AlphaGo用了一个自我学习的机制，就像金庸小说《射雕英雄传》中的老顽童周伯通,左右互搏。人类高手通过自我复盘、摆棋谱来提高棋艺,但是人类高手复盘慢,一次复盘往往需要数小时甚至数天，其间棋手还需要吃饭、休息。而AlphaGo只要有电就可以一直左右“互搏”下去,其复盘速度极快，每分钟就可以研究上万盘棋,这样的特性使得AlphaGo有可能在学习速度上超越人类高手。

为了达到左右互搏的效果，AlphaGo采用了一个名为深度强化学习的技术。强化学习很符合智能体(agent)的学习规律,类似孩子在不断跌倒中自我强化学会走路,猴子在胡萝卜加大棒下自我强化学会表演。强化学习有两个特点,一是智能体通过环境交互学习，二是训练标注稀少,且通常有一定的延时。强化学习主要通过感知、行动、奖赏三个环节构成一个状态转移空间,学习过程可以用马尔科夫决策过程来表示。

之前,强化学习的算法训练只能解决很小规模的状态转移空间。围棋是超大转移空间的问题,同时也是个带有超长延时训练标注的问题。一开始的棋难以量化好坏,双方要下多步后才能够数出各自大概的目数，从而判定输赢。AlphaGo 将围棋这一-特征视为深度强化学习问题,这个问题恰恰可以用深度的递归神经网络( diagonal recurrent neural network, DRNN)解决。DRNN的训练和DCNN没有太大区别。在左右互搏中，AlphaGo局部会采用--种名为蒙特卡洛搜索树的随机策略进行搜索,令整个系统能够自我进化。AlphaGo是最新深度学习方法、棋谱大数据以及最新超算体系的总和，并按现代科学技术的指数式发展继续进化，没有任何情绪波动。尽管在此次人机大战中,人类个体告负,但AlphaGo却是人类挑战自我的里程碑!