普通高中教科书

# 信息技术

选择性必修 4

## 人工智能初步

人民教育出版社 中国地图出版社

微信公众号：电子课本大全

普 通 高 中 教 科 书

# 信息技术

选择性必修 4

## 人工智能初步

人民教育出版社课程教材研究所信息技术课程教材研究开发中心
中国地图出版社教材出版分社 编著

总主编 祝智庭 樊 磊

人民教育出版社 中国地图出版社
·北京·

微信公众号：电子课本大全

总 主 编：祝智庭　樊　磊
副总主编：高淑印　郭　芳　李　锋
本册主编：方海光　马　涛

编写人员：袁中果　高永梅　王　岚　谭向华　吴劲松

责任编辑：沈万君　梅栾芳
美术编辑：李　媛　徐海燕

微信公众号：电子课本大全



# 前言

同学们，欢迎探索信息技术这个神奇而充满魅力的世界。

在以往的学习、生活中，你们已经积累了许多信息技术方面的知识与技能，例如：在网上查阅资料，用手机与亲朋好友保持联系，使用移动终端、自动柜员机等设备……你们知道这些应用中都包含哪些关键技术，涉及哪些领域吗？怎样有效地利用这些技术帮助我们培养信息意识，提升计算思维，进而通过数字化学习与创新，承担起信息社会责任呢？即将开始的这门课程，会帮助你们对信息技术有更多的认识和思考，获得更丰富的体验和感受。

为了很好地掌握信息技术，希望同学们按以下三个要求去努力。

1. 认真阅读教科书，理解基本概念和原理。信息技术发展非常迅猛，各类信息系统不断涌现，但信息系统的基础和运行体系相对稳定，离不开算法的设计及对数据的利用。只有夯实基础，才能学好本领，跟上时代发展的步伐。

2. 敢于动手，勤于实践。信息技术是一门实践性较强的课程。实践能帮助同学们熟练操作技能，进一步掌握知识。因此，要认真阅读理解每章的主题学习项目，并逐步完成“实践活动”“思考活动”“技术支持”“阅读拓展”等栏目的学习内容，在实践中获取知识和经验。

3. 要有积极探究、锲而不舍的精神。掌握信息技术的知识与技能需要一个过程，不可能一蹴而就。信息技术学科内容非常丰富，各知识点之间联系密切，但名词术语多，有可能令人感到繁杂，甚至产生畏难情绪。学习新知识，首先要知其然，接着通过不断学习，积极动手操作，大胆请教，加深对知识的理解，然后才能知其所以然，在不断的探索过程中取得进步。

本书中涉及的配套资源，可在教科书配套教学资源平台的信息技术栏目中获得。让我们开始一段信息技术新旅程，成长为信息社会中合格的中国公民！

微信公众号：电子课本大全

# 目录




第1章　人工智能概述　1

主题学习项目：人工智能在身边　2

1.1　人工智能基础　3

1.1.1　初识人工智能　4

1.1.2　人工智能的基本特征　5

1.2　人工智能发展历程和现状　9

1.2.1　人工智能的发展历程　10

1.2.2　人工智能的发展现状　12

1.3　人工智能研究内容与应用　16

1.3.1　人工智能的主要研究内容　17

1.3.2　人工智能的应用　18

总结评价　22

第2章　人工智能技术基本原理　23

主题学习项目：智能技术初体验　24

2.1　知识表示与专家系统　25

2.1.1　知识表示　26

2.1.2　启发式搜索　28

2.1.3　贝叶斯推理　31

2.1.4　专家系统　33

2.2　回归算法　37

2.2.1　回归在学习中的应用　38

2.2.2　回归算法的一般流程　39




微信公众号：电子课本大全

2.3 使用决策树进行分类 42
2.3.1 认识决策树 43
2.3.2 构造决策树的一般流程 45
2.4 使用K-均值算法进行聚类 52
2.4.1 认识基于距离的聚类 53
2.4.2 K-均值聚类算法的一般流程 56
2.5 神经网络与深度学习 60
2.5.1 人工神经网络 61
2.5.2 卷积神经网络与循环神经网络 70
2.5.3 深度学习及软硬件平台 76
总结评价 82

第3章 人工智能领域应用 83

主题学习项目：智能陪伴巧实践 84
3.1 计算机视觉 85
3.1.1 计算机视觉简介 86
3.1.2 计算机视觉的应用 89
3.2 自然语言处理 98
3.2.1 自然语言处理简介 99
3.2.2 自然语言处理的应用 102
3.3 机器理解与推理 111
3.3.1 机器理解与推理的发展和现状 112
3.3.2 人工智能与脑科学 114
3.3.3 认知推理的实践应用与展望 117



微信公众号：电子课本大全

3.4 博弈决策 121
3.4.1 博弈决策的发展历程 122
3.4.2 强化学习及其应用 123
3.5 智能机器人 129
3.5.1 智能机器人简介 130
3.5.2 智能机器人应用实践 134
总结评价 140

第4章 人工智能发展 141

主题学习项目：优势局限之我见 142
4.1 价值和未来发展 143
4.1.1 人工智能的应用价值 144
4.1.2 人工智能的未来发展 145
4.2 伦理及安全挑战 148
4.2.1 人工智能的隐私挑战 149
4.2.2 人工智能的安全挑战 150
4.2.3 人工智能的伦理挑战 152
4.3 法规与应用规范 155
4.3.1 法规与责任 156
4.3.2 规范与安全 157
总结评价 159

项目评价 160



微信公众号：电子课本大全

# 第 1 章
# 人工智能概述

在一次北京国际消费电子博览会上，首次亮相的“小蚂哥”吸引了众多观众，大家纷纷上前与其互动。

“小蚂哥”是一款用于无人配送的智能物流机器人，到达目的地后会自动通过语音电话通知客户取货，在一定区域范围内实现自动化配送。

“小蚂哥”具有卫星定位、自主行驶、主动避障和规划路线等多种功能，应用了机器人自主定位、计算机视觉、嵌入式控制和机械设计等多种技术。

除此之外，还有许多人工智能技术已经应用于人们的生产和生活当中。人工智能（Artificial Intelligence，AI）对社会的影响，远比人们今天所认识的还要广泛。

本章将以“人工智能在身边”为主题开展项目活动，引领同学们了解人工智能的典型应用，感受人工智能给我们生活带来的巨大变化，体验人工智能新应用，关注人工智能的发展趋势，激发同学们学习人工智能课程的兴趣。



微信公众号：电子课本大全

# 1 主题学习项目：人工智能在身边

## 项目目标

随着大数据和深度学习等技术的不断进步，人工智能开始走出科幻电影，走出科学实验室，来到我们的现实生活中。人工智能正在改变我们的工作、生活和学习方式。本章以“人工智能在身边”为主题开展项目活动。各小组成员分工合作，以多媒体形式呈现研究成果，并与全班同学进行交流。

1. 能够发现身边的人工智能，描述其应用场景。

2. 能够识别人工智能中用到的技术，积极尝试人工智能新应用，感受人工智能给我们生活带来的巨大变化。

3. 关注人工智能的发展趋势，激发对人工智能的学习兴趣。

## 项目准备

为完成项目，需做如下准备。

- 全班同学分成若干小组，组内明确分工，包括资料搜集、体验反馈、报告制作和汇报展示等。
- 在人工智能开放平台上完成注册，熟悉并学习使用项目过程中所涉及的软硬件。

## 项目过程

在学习本章内容的同时开展项目活动。为了保证本项目的顺利完成，要在以下各阶段检查项目的进度。

**初步体验** ①

搜索并体验不同的人工智能应用，描述人工智能应用的主要功能和特点。完成活动记录表中的相关内容。 P8

**深入了解** ②

结合教科书和其他相关资料，了解人工智能的发展历程和现状，完成思维导图的绘制和小论文的撰写。 P15

**完成项目** ③

列举人工智能的应用场景，说出其涉及的研究内容，完成项目报告填写，提交项目学习成果，并与全班同学进行分享、交流。 P21

## 项目总结

完成本章项目后，各小组提交项目学习成果，进行作品交流与评价，体验小组合作、项目学习和知识分享的过程，发现身边的人工智能，了解人工智能的特征、现状及其未来的发展趋势。



微信公众号：电子课本大全

# 1.1
# 人工智能基础

## 学习目标 ▶▶▶

- 理解人工智能的概念，知道人工智能的基本特征。
- 通过体验和探索，激发对人工智能技术的学习兴趣。

## 体验探索

### 人脸识别

某学校宿舍门口安装了门禁系统，人员进门时需要直视屏幕，完成“刷脸”操作，脸部识别成功，确认身份后，机器会发出“欢迎回家”的声音，同时打开门锁。本案例中应用的人脸识别技术属于人工智能的范畴，它还应用于考勤签到和安防监控等领域。

同学们可以按照以下步骤，体验人脸识别技术。

1. 登录人工智能开放平台。

2. 建立一个包含多张人脸照片的图片比对库。

3. 上传一张需要识别的人脸照片。

4. 通过人脸识别技术找出与你上传的那张照片最相似的一张或多张人脸图片（图 1.1.1）。




图 1.1.1　人脸识别结果的界面

思考：

1.“人脸识别”为什么被认为是人工智能技术？它与生活中使用的其他技术有什么不同？

2. 生活中你还体验过哪些人工智能应用？试着与同学分享应用体验。



微信公众号：电子课本大全

### 1.1.1 初识人工智能

人工智能是极具挑战性的领域。目前，信息技术、互联网等领域的发展和突破的关键环节几乎都与人工智能有关，如搜索引擎、智能硬件、机器人和无人机等。

**思考活动**

**图灵测试**

“图灵测试”一词来源于计算机科学的先驱艾伦·图灵（Alan Turing）写于1950年的一篇论文——《计算机器与智能》。图灵测试对检验“机器是否具有人类智能”给出了一个可操作的方法：在测试者与被测试者相互隔离的情况下，测试者通过一些装置（如键盘）向被测试者随意提问，如图1.1.2所示，经过5分钟问答后，如果测试者不会有多于70%的机会作出正确的区分，那么这台机器就通过了图灵测试，即被认为具有人类智能。



图1.1.2 图灵测试

2014年6月，英国雷丁大学宣布，由俄罗斯团队开发的人工智能软件尤金·古斯特曼（Eugene Goostman，一款聊天机器人软件）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。尤金模拟的是一个13岁的乌克兰男孩，“他”成功地被33%的评委判定为人类，成为首款通过图灵测试的计算机软件。

思考：

你认为“尤金·古斯特曼”是否具备了人类智能？通过了图灵测试的机器，是不是就和人一样具有思维和意识了？试阐述你的观点。

“人工智能”一词最初是在1956年达特茅斯会议上被提出的。半个多世纪以来，人们从不同的层面对人工智能提出了不同的定义。《辞海》对人工智能的界定为“用机器（主要指计算机）模拟类似于人类的某些智能活动和功能”。《不列颠百科全书》（又称《大英百科全书》）则定义人工智能为“数字计算机或者数字计算机控制的机器人在执行智能生物体才有的一些任务上的能力”。

我国在《人工智能标准化白皮书（2018版）》中提出“人工智能是利用数字计算机或



微信公众号：电子课本大全

者数字计算机控制的机器模拟、延伸和扩展人的智能，感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统”。

### 实践活动

#### 识别网络图片中的文字

当我们打开一些社交、电商网站时，会发现屏幕上充斥着各种各样的图片，其中不乏一些广告或敏感信息。通过文字识别技术可以准确识别图片中的文字（图1.1.3），从而筛选并屏蔽此类信息。

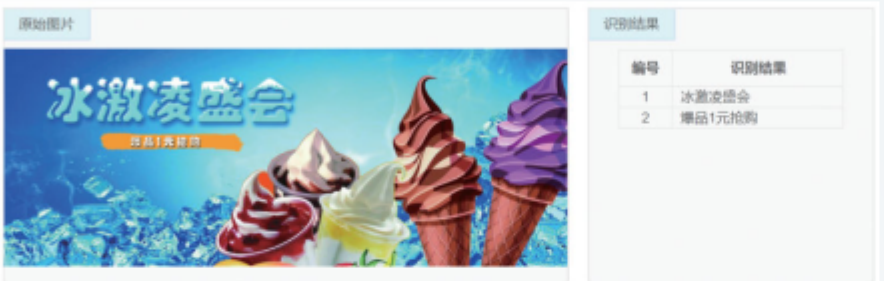



图1.1.3　识别网络图片中的文字

1. 任意选取一张带有文字的图片，上传到人工智能开放平台上进行识别。

2. 任意选取一组带有文字的图片，利用识别技术筛选出包含广告内容的图片。

## 1.1.2　人工智能的基本特征

人工智能的基本特征是能够使机器完成一些通常需要人类智能才能完成的复杂工作。

### 思考活动

#### 智能陪护机器人

智能陪护机器人（图1.1.4）主要应用于养老院或社区服务站等场所，它具有生理信号检测、语音交互、远程医疗、智能聊天和自主避障等功能。

智能陪护机器人在养老院中能够实现自主导航避障，通过语音和屏幕与人进行交互。配合相关检测设备，机器人可以检测和监控血压、心跳和血氧等生理信号，并将数据通过无线网络传输到社区医疗中心；在紧急情况下还可及时报警或通知亲人。机器人还具有智能聊天功能，可以辅助老人进行心理康复。



微信公众号：电子课本大全



图 1.1.4　智能陪护机器人

思考：

智能陪护机器人可主动帮助人们完成哪些工作？是如何实现交互的？

根据《人工智能标准化白皮书（2018 版）》，可将人工智能的特征描述如下。

■ 由人类设计，为人类服务，本质为计算，基础为数据

人工智能系统是人类设计出的机器，它按照设定的程序逻辑或软件算法通过芯片等硬件载体来运行或工作，通过对数据的采集、加工、处理、分析和挖掘，形成有价值的信息流和知识模型，为人类提供延伸人类能力的服务，实现对人类期望的一些“智能行为”的模拟。

■ 能感知环境，能产生反应，能与人交互，能与人互补

人工智能系统能借助传感器等器件对外界环境（包括人类）进行感知，可以像人一样通过听觉、视觉、嗅觉和触觉等接收来自外界环境的各种信息，对外界刺激产生文字、语音、表情和动作（控制执行机构）等形式的反应，借助于按钮、键盘、鼠标、屏幕、手势、体态、表情、力反馈、虚拟现实和增强现实等方式，人与机器间可以产生交互，机器设备越来越“理解”人类乃至与人类共同协作、优势互补。这样，人工智能系统能够帮助人类做人类不擅长、不喜欢但机器能够完成的工作，而人类则可以去从事更需要创造性、洞察力、想象力、灵活性、多变性的一些工作。

■ 有适应特性，有学习能力，有演化迭代，有连接扩展

在理想情况下，人工智能系统能够随环境、数据或任务变化调节自适应参数或优化自身模型，且能够在此基础上通过与云、端、人、物越来越广泛深入的数字化连接扩展，实现机器客体乃至人类主体的演化迭代，以增强系统的适应性、鲁棒性、灵活性和扩展性，来应对不断变化的现实环境，从而在各行各业得到广泛的应用。



微信公众号：电子课本大全

## 实践活动

### 体验美颜应用

人脸识别是美颜应用的核心技术，人脸识别的准确性决定美颜的效果。它可以对人体面部和五官进行精准定位，以此呈现出自然的妆容。这项技术能实现人脸图像采集检测、人脸图像预处理、人脸图像特征提取以及匹配识别等。系统对图片进行整体扫描，自动精确定位人脸五官的关键点（图1.1.5），获取关键点以后，将明显的特征作为脸部美化工作的基础，后期再作进一步处理，例如，增加美妆和萌宠贴图等。

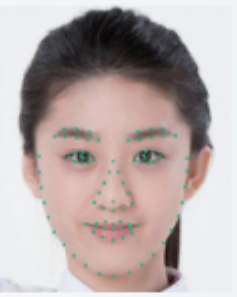


图1.1.5　人像关键点精确定位

任选一款美颜应用进行操作，体验美颜应用的功能，并结合人工智能的特征进行分析。

## 阅读拓展

### 人工智能的划分

弱人工智能和强人工智能是美国哲学家约翰·塞尔（John Searle）提出的术语，用来描述关于人工智能的两种对立的观点。

■ 弱人工智能

弱人工智能的观点是：尽管计算机程序在检验关于思维和心灵的假设方面是有价值的，但无论怎样编程，计算机都不可能产生真正的思维或心灵。也就是说，弱人工智能机器即使在某些方面具有非凡的智能水平，但其无法将这些方面的能力迁移到其他方面，更不会具有自主意识。

■ 强人工智能

强人工智能的观点是：经适当编程的计算机可以产生真正的思维或心灵。强人工智能机器在各方面都能与人类比肩，这样的机器能够真正推理和解决问题，是具有知觉和自主意识的人类级别的人工智能。强人工智能也用来泛指人工智能技术最终将变得超越人类。

强弱人工智能的划分不体现在其外部功能上，而是强调人工智能的内省能力。目前，在人工智能专业研究领域，还有一种从可应用性角度将人工智能划分为专用人工智能和通用人工智能的观点。这种划分强调人工智能适用的范围。

■ 专用人工智能

专用人工智能往往面向特定的任务，需求明确、应用边界清晰、专业领域知识丰富、建模相对简单，在局部智能水平的单项测试中可以超越人类智能。



微信公众号：电子课本大全

■ 通用人工智能

通用人工智能可处理视觉、听觉、判断、推理、学习、思考、规划和设计等各类问题，并能举一反三、融会贯通，是一个更趋近于人类的智能系统。

人工智能的近期进展主要集中在专用人工智能领域。专用人工智能在信息感知、机器学习等方面进步显著，但是在概念抽象和推理决策等方面的能力还很薄弱。实现从专用人工智能向通用人工智能的跨越式发展，既是下一代人工智能发展的必然趋势，也是研究与应用领域面临的重大挑战。

## 项目实施

### 体验人工智能

一、项目活动

1. 查找人工智能相关资料，搜索人工智能应用。

2. 体验不同的人工智能应用，根据体验描述各应用的主要功能和特点。

二、项目检查

1. 完成人工智能开放平台账号的注册，下载安装相应的手机应用程序。

2. 结合本节所学内容，完成人工智能体验，填写项目活动记录，如表1.1.1所示。

表1.1.1　项目活动记录表

| 体验人工智能 | | |
|---|---|---|
| 人工智能应用 | 主要实现功能 | 特点描述 |
| | | |
| | | |
| | | |

3. 留存过程性资料，如操作步骤、体验过程微视频和体验感受记录等。

## 练习提升

1. 梳理本节所学内容，查阅资料，总结人工智能的概念与基本特征。

2. 任意选取一种自己体验过的人工智能应用，试对其不足提出改进意见或方案。



微信公众号：电子课本大全

# 1.2
# 人工智能发展历程和现状

## 学习目标 ▶▶▶

- 了解人工智能的发展历程，分析人工智能发展过程中出现高潮和低谷的原因。
- 知道人工智能的发展现状，了解我国在人工智能领域的成就。

## 体验探索

### 智能推荐引擎

智能推荐引擎常应用于电子商务、视频推荐和媒体咨询等领域。随着电子商务规模的不断扩大，电商平台的商品种类快速增长，消费者要花大量的时间才能找到自己需要的商品。用户在浏览大量商品及无关信息的过程中，可能会因信息过载而流失。为了解决这些问题，个性化推荐引擎（图1.2.1）应运而生。它能根据网站最热卖商品、用户所处城市、用户过去的购买行为和购买记录，自动完成个性化商品的筛选，并将其推荐给用户，以满足用户的个性化需求。



图1.2.1　个性化推荐引擎

在电脑或手机上任意打开一个购物网站，先观察网站推荐的商品目录，然后搜索并浏览某一个（类）商品，刷新页面后再观察推荐商品目录与之前相比有何变化，最后根据你的体验评价智能推荐引擎。

思考：

网站第二次推荐的内容是否与刚刚搜索的内容完全一致？网站推荐的内容与你的实际需求是否有偏差？如有，试分析产生偏差的原因。



微信公众号：电子课本大全

### 1.2.1 人工智能的发展历程

1956年达特茅斯会议上，约翰·麦卡锡（John McCarthy）提出了“人工智能”一词，人工智能也被正式确立为一门学科。这次会议为人工智能奠基人相互交流提供了机会，并对人工智能的发展起了重要的铺垫作用（图1.2.2为2006年达特茅斯会议50周年时5位重要参与者合影）。此后60多年的发展历程中，人工智能经历了多次高潮和低谷，大致可以分为三个阶段。



图1.2.2 摩尔、麦卡锡、明斯基、塞尔弗里奇和所罗门诺夫（从左到右）

■ 第一阶段：从早期尝试到符号推理

从达特茅斯会议到20世纪70年代中期，人工智能从萌芽迅速走向繁荣。这个阶段的标志性成果及事件列举如下。

◇因编写计算机弈棋程序的需要，提出了多种“智能”搜索算法，比如“深度优先”和“广度优先”等，其中很多算法在今天看来都堪称经典。

◇艾伦·纽厄尔和赫伯特·西蒙开发了“逻辑理论家”及“通用问题求解机”，为早期专家系统和符号推理系统奠定了基础。

◇弗兰克·罗森布拉特最先提出了一类神经网络模型——感知机模型。

◇乔舒亚·莱德伯格和布鲁斯·布坎南等人设计了第一个具有实用价值、基于知识的专家系统——DENDRAL。

◇约翰·麦卡锡和阿兰·科莫劳尔分别设计专门面向人工智能的计算机编程语言LISP和PROLOG，其引入的语言范式和特点（如面向对象、逻辑编程语言）至今仍为同类语言的典范。

◇爱德华·费根鲍姆和乔尔·摩西首先成功开发了基于知识的数学推理程序——MACSYMA。

◇我国著名数学家吴文俊提出了几何定理机械化证明的“吴氏方法”。

基于数理逻辑的符号知识表示与推理是这一阶段的主要特色。人工智能在自然语言处理、专家系统、定理自动证明与自动推理等方面取得了一系列重要成果。同时，神经网络（感知机）及贝叶斯方法研究也开始萌芽并逐渐发展。不过，繁荣中也隐藏着危机。



微信公众号：电子课本大全

◇ 1969年，马文·明斯基（Marvin Minsky）和西摩·佩珀特（Seymour Papert）出版的《感知机：计算几何导论》一书，证明感知机有重大缺陷，这直接导致神经网络的研究陷入低谷，也为后来人工智能领域的全面衰落埋下了伏笔。

◇ 1971—1972年，斯蒂芬·库克和理查德·卡普等人建立了计算复杂性理论，揭示出很多计算问题原则上不存在“能行解”，暗示基于纯符号推理的人工智能之路不可行。

◇ 1973年，英国数学家詹姆斯·莱特希尔（James Lighthill）提交报告，对英国政府资助的人工智能研究作出了全盘否定。随后，英国及其他国家陆续终止或大幅削减对人工智能研究的资助，人工智能的发展第一次经历了“寒冬”。

■ 第二阶段：从专家系统到知识工程

20世纪80年代初开始，“知识”逐渐成为人工智能领域的核心观念，研究者们在人工智能系统中导入人类的“专家知识”。这一发展为符号推理的理论框架添加了领域“知识”，使机器能够解决更实用、更专业和更复杂的问题。

这一阶段出现了大量的新型“专家系统”，如基于非经典逻辑的专家系统、概率专家系统、模糊专家系统、演化专家系统和神经专家系统等。最具有代表性的专家系统有：由爱德华·费根鲍姆主持设计的用于检查血液传染病的MYCIN系统，及其后续的通用型专家系统EMYCIN；由斯坦福研究院基于贝叶斯推理开发的用于矿物勘探的概率型专家系统PROSPECTOR，这是首批将贝叶斯推理付诸实践的人工智能系统。

在此期间，人工智能在基础研究方面，包括神经网络、统计学习与并行信息处理等领域都取得了长足的进步，这为日后机器学习领域的全面爆发奠定了基础。1982年，日本政府启动“第五代计算机系统计划”，同期英国政府也全面恢复了对人工智能研究的资助。这些都标志着人工智能领域步入第二次快速发展时期。

但是，由于专家系统核心的知识表示和推理机制内在局限性的影响，以及数据采集、存储和计算能力等计算基础架构和设施的严重制约，人工智能的大规模应用遭遇瓶颈，第二次发展浪潮也逐渐停息。

■ 第三阶段：从大数据到深度学习

20世纪90年代中后期开始，人工智能领域迎来了第三次发展浪潮。受益于浏览器和搜索引擎技术的突破，互联网开始迅速普及并呈现出井喷式发展态势，以采集、存储及处理海量数据为目标的新一代计算基础架构（大规模并行处理、高性能计算、大数据、云计算及物联网技术等）和“智能”信息处理技术（语义网及本体技术、数据可视化技术、统计数据分析、数据挖掘、知识发现和机器学习等）趋向成熟，并迅速显示出巨大价值，人工智能复兴提速，并最终在2012年全面爆发。

这一阶段，人工智能发展的标志性事件是一系列以深度学习为代表的突破性算法和应用的不断涌现。深度学习是过去几十年间机器学习乃至整个人工智能领域中所取得的重大进展，几乎开启了人工智能在所有领域和行业中应用的大门。



微信公众号：电子课本大全

◇2012年，以全球范围的图像识别算法竞赛ILSVRC作为标志性事件，深度学习先后在自动翻译、自然语言处理、图像识别和人机博弈等人工智能传统领域取得明显进步，同时也为机器人与智能制造、自然人机交互、自动驾驶、机器应答系统、垃圾邮件过滤、网络安全取证和推荐系统等全新应用领域提供了发展基础和动力。

◇2015年，谷歌、亚马逊和微软等国际信息技术公司开始相继发布自己的人工智能开放平台。国内的百度、阿里巴巴、腾讯和科大讯飞等公司承担了国家级人工智能行业应用开放平台的建设，一批新兴人工智能开发公司也推出了各具特色的人工智能应用开放平台，这些平台为开展人工智能在各个行业的创新应用，特别是教育应用，提供了更多的可能。

◇2017年，谷歌人工智能程序阿尔法围棋（AlphaGo、AlphaGo Zero）以绝对优势战胜人类围棋的顶尖高手，将以深度学习为代表的新一代人工智能的应用水准提升到了历史性的新高度。

**阅读拓展**

**深度学习与大数据**

以深度学习为标志的新一代人工智能的兴起依赖于三个紧密相关的方面：基于深度学习的机器学习架构和算法的突破、各行业数十年信息化及互联网发展所积累的大量数据、廉价通用的图形处理器（Graphics Processing Unit，GPU）被广泛应用于训练学习模型。

如果将深度学习比作人工智能应用的“引擎”，那么大数据就是“燃料”。某种特定的数据集提供了与应用相关的各种记录，是深度学习算法用于训练和优化模型所必需的。对大数据处理分析的需求已经完全超出了人工编程所能达到的处理极限，必须发展能自动、智能、高效处理大数据的技术，而这些技术的研发正是人工智能算法的用武之地。

### 1.2.2 人工智能的发展现状

随着人工智能技术的发展，一些人工智能机器已经可以承担某种比较复杂的脑力劳动，也可以协助人们完成记忆和逻辑运算。经过性能改善，一些智能机器有可能超越人类的某种能力，代替人类完成难度较大的工作。这些智能机器虽然可以代替部分人类劳动，却还不能达到人类多方协调和自我学习提升的智能水平。想要制造出像人类一样拥有智慧的机器，还需深入研究。当前，人工智能的发展现状主要体现在以下几个方面。

#### 智能接口技术研究

智能接口的研究是为了建立高效和谐的人机交互环境，让人与机器之间的交互能够像人与人之间的交流一样便捷、自然。人工智能技术在自然语言理解、脑-机接口（意识控制计算）、步态识别和情感识别等方面都取得了重要进展，有效地推动了智能接口



微信公众号：电子课本大全

技术的发展。

### 大规模并行计算

近年来，基于图形处理器的大规模并行计算异军突起。云计算的出现、GPU的大规模应用使得分布式的数据计算处理能力迅速增强。这种超大规模的并行计算大大提升了人工智能的信息处理能力。

### 大数据技术

随着移动互联网的爆发式发展，每天都会产生大量的数据，数据量的大幅度增长为人工智能的发展提供了基础。大数据的应用已经渗透到农业、工业、商业、服务业和医疗业等领域，成为影响人工智能发展的一个重要因素。

### 深度学习

深度学习是人工智能现阶段的重要研究领域。深度学习通过建立、模拟人脑的分层结构来实现对输入数据从低级到高级、从局部到整体、从具体到抽象的特征提取和建模。通过深度学习，机器可以识别数据中隐藏的复杂模式，揭示数据的分布规律和局部特性，并将结果用于预测和建模新的数据，提出深刻的见解。



## 阅读拓展

### 我国在人工智能领域的应用案例

在国际信息技术公司相继发布人工智能开放平台的同时，国内的百度、阿里巴巴、腾讯和科大讯飞分别承担了自动驾驶、城市大脑、智慧医疗和语音技术国家级人工智能行业应用开放平台的建设。

百度与金龙汽车合作研发了一款无人驾驶小巴车，并于2018年7月实现量产。小巴车基于高精度地图和智能感知技术，能实时感知环境信息并根据地图数据规划路线。该车还能对车辆、行人的行为进行预测，从而作出行车决策，以应对路面交通情况的变化。

阿里云ET城市大脑是目前全球规模最大的人工智能公共系统之一，可以对整个城市进行全局实时分析。截至2017年10月，杭州城市大脑接管了杭州128个信号灯路口，试点区域通行时间减少了15.3%，高架道路通过时间节省了4.6 min。在主城区，城市大脑事件报警日均500次以上，准确率达92%；在萧山区，已经实现了救护车等特种车辆的优先调度，到达现场的时间可缩短一半。

腾讯发布了一款人工智能医学影像产品——腾讯觅影。它是首款人工智能食管癌筛查系统，筛查准确率超过90%；在肺结节方面，它可以检测出3 mm及以上的微小结节，检测准确率超过95%。腾讯觅影还将与医学院和医疗机构合作，助力更多病种检测。



微信公众号：电子课本大全

科大讯飞语音识别的准确率达到95%，其语音合成技术在2017年的国际语音合成比赛中成功摘得桂冠，实现了在该项比赛中的十二连冠。

人工智能并不是一个独立、封闭和自我循环发展的智能科学体系，而是通过与其他科学领域的交叉，融入人类社会发展的各个方面。人工智能的发展有以下三大趋势。

第一，现在人工智能技术是相对独立的，如图像处理、声音处理等，人工智能的发展必然会使其具备接近人类大脑思维能力的功能，可以同步处理多类信息。

第二，人类对机器的干预贯穿于人工智能发展的始终。人类始终是智能机器的制造者，是智能机器的服务对象，是智能机器价值的评判者。人工智能的发展必然会将人的作用或人的认知模型引入人工智能系统，形成“混合增强人工智能”技术。

第三，自主性和智能性是智能无人自主系统最重要的两个特征。依靠图像识别、人机交互、智能决策、自动推理和深度学习等人工智能技术的发展，人类可以创造出具有更高自主性和智能性的无人自主系统。



微信公众号：电子课本大全

## 项目实施

### 了解人工智能

一、项目活动

1. 查阅资料，从不同角度了解人工智能的发展历程，并绘制思维导图。

2. 了解现阶段我国人工智能开放平台的发展状况及特点，任选一个平台，分析其给人们生活方式带来的影响，完成小论文。

二、项目检查

1. 完成思维导图的绘制（图 1.2.3）。




图 1.2.3 “人工智能的发展历程”思维导图

2. 自拟题目，完成一篇 300 字左右的小论文，文中要有个人的观点。

3. 留存过程性资料，如研究文档、体验过程微视频和体验感受记录等。

## 练习提升

1. 在史蒂文·斯皮尔伯格执导的科幻电影《人工智能》中，一个具有感情的小机器人在被其人类养母抛弃后，为了缩短与人类的差距，不断奋斗、找寻自我、探索人性。你认为人工智能可能发展出意识吗？人工智能会超越人类智能吗？试组织以此类话题为主题的辩论会。

2. 随着技术的进步与发展，未来的人工智能会是什么样的？它将给我们的生活带来怎样的影响？



微信公众号：电子课本大全

# 1.3
# 人工智能研究内容与应用

## 学习目标 ▶▶▶

- 了解人工智能的主要研究内容和重点应用领域。
- 了解人工智能的应用现状，知道人工智能的典型应用。
- 能够发现身边的人工智能，感受人工智能对我们生活的影响。

## 体验探索

### 智能手机中的人工智能

智能手机是目前普及率和使用率非常高的电子产品。随着人脸识别、语音翻译、智能遥控、娱乐休闲、电子商务和个人理财等众多手机应用程序的开发和应用，人们的生活变得更加便捷。

例如，语音翻译技术不仅可以做到实时翻译，还可以用标准的发音朗读文字。语音翻译技术作为跨语言沟通的桥梁，极大地方便了不同语种国家和地区的人们之间的交流。语音翻译技术主要应用于会议记录、语音笔记和实时字幕等场景以及社交聊天等应用程序，如图1.3.1所示。




图1.3.1　语音实时翻译界面

思考：

生活中你是否体验过语音翻译技术的应用？如果体验过，试分析该应用的功能是如何实现的。



微信公众号：电子课本大全

### 1.3.1 人工智能的主要研究内容

人工智能是一门综合性学科，涉及哲学、心理学、认知科学、计算机科学、数学和工程学等学科，这些学科为人工智能的研究和发展提供了丰富的知识基础和研究方法。

#### 思考活动

**智能菜单翻译**

我们在异国旅游的时候，自然要品尝当地美食。使用手机拍摄菜单照片，“智能菜单翻译”应用程序就可将照片中的菜品文字内容翻译出来，让点菜不再困难，如图1.3.2所示。



图1.3.2 智能菜单翻译

“智能菜单翻译”应用程序依托海量的菜品语言数据资源，基于深度学习技术，通过高效的训练平台，在大规模通用模型基础上，实现了精准的翻译。

思考：

拍照翻译与语音实时翻译的区别是什么？这两种智能翻译功能应用了人工智能的哪些技术？

人工智能的主要研究内容如表1.3.1所示。

表1.3.1 人工智能的主要研究内容

| 研究内容 | 描述 |
| --- | --- |
| 知识表示 | 知识表示是对知识的一种描述，或者说是一组约定，是一种计算机可以接受的用于描述知识的数据结构。对知识进行表示的过程就是把知识编码成某种数据结构的过程 |
| 专家系统 | 专家系统是一种具有特定领域内大量知识与经验的智能计算机程序系统，即模拟人类专家的计算机程序系统 |
| 人工神经网络 | 人工神经网络是一种应用类似于大脑神经元连接的结构进行信息处理的数学模型。通过调整内部大量节点之间相互连接的关系，达到处理信息的目的 |
| 计算机视觉 | 计算机视觉就是用各种成像系统代替视觉器官作为输入手段，由计算机来代替大脑完成处理和解释。计算机视觉的最终研究目标就是使计算机能像人一样，通过视觉观察了解世界，具有自主适应环境的能力 |
| 自动推理 | 从一个或几个已知的判断逻辑推论出一个新的判断逻辑的思维过程称为推理。自动推理是知识的使用过程，人解决问题就是利用以往的知识，通过推理得出结论 |
| 模式识别 | 模式识别是通过计算机用数学计算的方法对表征事物或现象的各种形式的信息进行处理和分析，是对事物或现象进行描述、辨认、分类和解释的过程 |
| 自然语言处理 | 自然语言处理是实现人与计算机之间用自然语言进行有效通信的各种理论和方法 |



微信公众号：电子课本大全

## 阅读拓展

### 人工智能杀毒引擎

人工智能杀毒引擎是我国完全自主研发的第三代杀毒引擎（具有我国的自主知识产权）。它采用了人工智能算法模型——支持向量机，不仅查杀速度快、病毒检出率高，而且还具备“自学习、自进化”的能力，无须频繁升级特征库，就能免疫90%以上的加壳和变种病毒，有效解决了前两代杀毒引擎“不升级病毒库就无法查杀新病毒”的技术难题，在全球范围内属于首例。

从技术角度来说，对付病毒木马的关键点就是要把已潜入或打算潜入到用户电脑中的危险程序找出来，而这个“查找”的过程类似于互联网上的搜索引擎。在海量的信息数据中，杀毒软件通过搜索引擎智能地找出已知或未知的病毒，这种“智能”的“查找识别”是新一代杀毒软件的核心所在。

研发一个具备学习能力的病毒智能识别引擎，就是让电脑具备人类的学习能力，让电脑自己来发现和学习病毒的变化规律。这样，就能独立地将新老病毒的查杀率提升到前所未有的高度。

人工智能杀毒引擎向世界展示了我国自主创新的领先科技成果。

## 1.3.2 人工智能的应用

人工智能在众多领域中的应用都取得了举世瞩目的成就，特别是计算机视觉、专家系统、自然语言处理、模式识别和机器人等技术的应用，极大地改变了我们的生活。

### 智能家居

智能家居通过物联网技术，实现家庭中硬件设备的互联互通，使用户可以远程遥控设备。设备具有自我学习等功能，可以收集、分析用户行为数据，为用户提供个性化生活服务，使家居生活更加便捷、舒适。例如，远程遥控各类家用电器的运转，通过人脸识别和指纹识别技术实现开锁等，如图1.3.3所示。



图1.3.3 智能家居



微信公众号：电子课本大全

### 智能交通

智能交通集成了通信、信息采集、信息分析和控制技术。通过网络技术将交通设备进行联通，对交通信息进行采集、分析，并形成决策，达到相互协调、资源优化、高效运转的目的。例如，根据上下班高峰路段车辆信息实时调整道路红绿灯时长，应用电子不停车收费系统（Electronic Toll Collection，ETC），等等，如图1.3.4所示。




图1.3.4　智能交通

### 智能安防

智能安防是通过人脸识别、视频图像分析等技术对图像进行智能判断，实现实时的安全防范和处理。人工智能技术的应用使安防不再是被动防御，而是主动发现、精准判断、及时预警。例如，区域入侵检测、人脸检测等，如图1.3.5所示。




图1.3.5　智能安防

### 智能穿戴

智能可穿戴设备正在改变我们的生活方式。它通过便捷的穿戴形式、实时的数据采集、精准的数据分析，为用户提供建议，协助用户解决问题。例如，可穿戴设备会主动提醒作息时间，实时检测身体状况并给出改善建议等。

### 智能物流

智能物流利用智能搜索技术，通过分析历史库存数据，建立预测模型，实现对库



微信公众号：电子课本大全

存商品的动态调整。物流仓库的分拣机器人接到订单后，可以迅速定位商品在仓库内的位置，规划最优拣货路径，完成拣货后自动规划路线，把货物送到打包台，如图1.3.6所示。这不仅节约了劳动力，还提升了物流速度，提高了工作效率。



图1.3.6　分拣机器人

随着人工智能理论和技术的日益发展，人工智能的应用领域也在不断扩大。可以设想，未来的人工智能产品，将会是人类智慧的“容器”。从智能可穿戴设备到智能家居、智能机器人、智能驾驶、智能教育、智能医疗、智能金融、智能工业和智能农业等，人工智能正在不知不觉中改变着人们的生活，人工智能的发展将给人们带来更加美好的未来。

## 阅读拓展

### 智能公交

2017年12月2日，全球首批智能公交车（图1.3.7）从深圳福田保税区开出，引起广泛关注。智能公交车满载25人，其中有17个座席和8个站席。车辆运行时速25 km，最高时速为30 km，单次续航里程可达150 km，40 min即可充满电。



图1.3.7　智能公交

智能公交试运营线路为全长1.2 km的环线，设有海梁、深巴、福田三站。目前这条线路只是处于“数据采集试运行阶段”，即“有人驾驶、试验线路、只针对特定人群开放”。

该公交车装有智能驾驶公交系统，能实现减速避让、紧急停车、绕行障碍物和自动靠站等功能，基本实现了无人驾驶。



微信公众号：电子课本大全

## 项目实施

### 关注人工智能

一、项目活动

1. 结合生活中人工智能的应用场景，尝试说出这些人工智能应用主要涉及的研究内容，感受人工智能给我们生活带来的变化。

2. 结合本节所学内容，在你了解的人工智能应用中，推荐一个你认为发展前景最好的应用，完成项目报告，并以多媒体的形式呈现研究成果，与全班同学分享、交流。

二、项目检查

1. 结合本节所学内容，能够说出人工智能的主要研究内容和典型应用。

2. 填写项目报告，如表1.3.2所示，并与全班同学分享、交流。

表1.3.2　项目报告

| | |
|---|---|
| 项目名称 | |
| 项目成员 | |
| 成员分工 | |
| 人工智能的应用 | |
| 功能及应用场景 | |
| 研究内容及相关技术 | |
| 应用价值 | |
| 未来的应用前景 | |

3. 留存过程性资料，如研究文档、体验过程微视频和体验感受记录等。

## 练习提升

1. 在手机上下载不同的翻译应用程序，对比几款应用程序的翻译功能，了解它们各自的特点，推荐你最喜欢的一款。

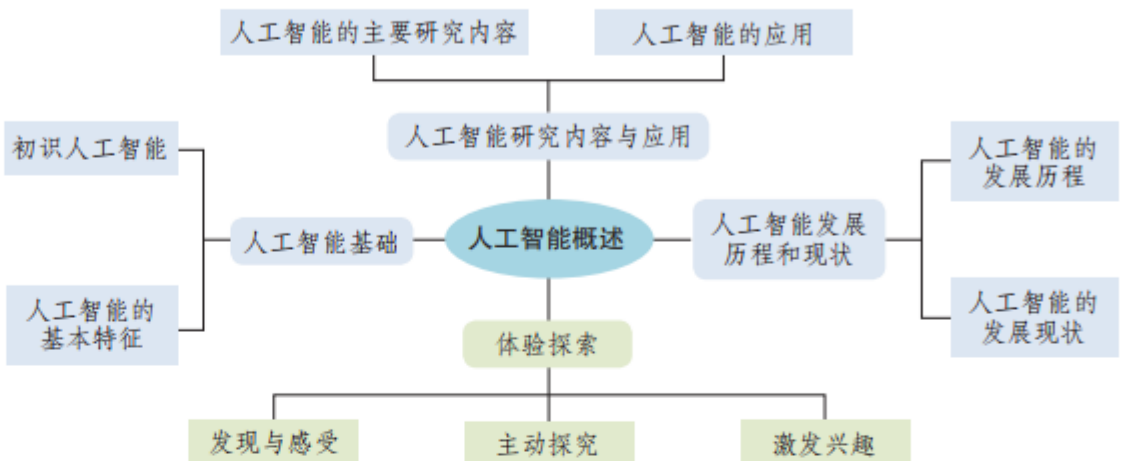
2. 利用人工智能开放平台，熟悉定制化图像识别工具，完成模块测试。



微信公众号：电子课本大全

## 总结 评价

1. 下图展示了本章的核心概念与关键能力，请同学们对照图中的内容进行总结。




2. 根据自己的掌握情况填写下表。

| 学习内容 | 掌握程度 |
| --- | --- |
| 人工智能的概念 | □不了解 □了解 □理解 |
| 人工智能的基本特征 | □不了解 □了解 □理解 |
| 人工智能的发展历程 | □不了解 □了解 □理解 |
| 人工智能的发展现状 | □不了解 □了解 □理解 |
| 人工智能的主要研究内容 | □不了解 □了解 □理解 |
| 人工智能的应用 | □不了解 □了解 □理解 |



微信公众号：电子课本大全

# 第 2 章
# 人工智能技术基本原理

智能手机已成为人们生活的一部分，它到底隐藏着多少人工智能的神奇“魔术”？智能助理和智能聊天等手机应用，正颠覆着我们与手机的交互方式；新闻资讯、在线购物等热门应用总在推送着适合我们的内容；图像识别智能应用能够识别图像或现实中的人、风景、地点，可帮助我们快速组织和检索图像；图像处理软件能对图像进行美化，打造个性化图像；当人们开车出行时，可以使用导航软件规划最佳路线……

手机中的智能应用涉及许多人工智能技术，各类应用的智能表现离不开“机器学习”。机器学习与人类学习不同，它需要收集大量数据或积累大量经验。本章的核心是机器学习，涉及回归、分类和聚类等算法，以及神经网络、深度学习和强化学习等概念和理论。

在本章的学习中，我们将以“智能技术初体验”为主题，开展项目活动，探索手机应用中的人工智能技术，领略技术背后人工智能算法的魅力，进而学习人工智能技术的基本原理。



微信公众号：电子课本大全

# 2 主题学习项目：智能技术初体验

## 项目目标

本章以“智能技术初体验”为主题开展项目学习，通过剖析生活中的真实案例，了解人工智能技术的基本原理，体验人工智能算法的处理过程，为未来的学习和生活打下坚实的基础。

1. 体验手机中常见的各类应用服务，感受人工智能技术的神奇魅力。

2. 剖析手机中典型应用服务的实现技术，了解人工智能技术的基本原理和核心算法。

3. 基于手机应用服务背景，小组合作设计出一个基于人工智能技术的个性化手机应用，并描述所采用的人工智能算法及其处理过程。

## 项目准备

为完成项目，需做如下准备。

- 全班同学分为若干小组，建议每组3~5人，明确组员分工。
- 分享手机中常用的应用服务及其功能，并按照功能对手机中的应用服务进行分类，探讨其可能使用的人工智能技术。
- 小组讨论，确定项目主题，并描述项目的功能。

## 项目过程

在学习本章内容的同时开展项目活动。为了保证本项目的顺利完成，要在以下各阶段检查项目的进度。

| 搜索与推理算法 ① | 回归算法 ② | 分类算法 ③ | 聚类算法 ④ | 深度学习 ⑤ |
| --- | --- | --- | --- | --- |
| 尝试通过搜索与推理算法，完成具有特别功能的应用程序设计。P36 | 尝试通过回归算法，完成基于回归的应用程序功能设计。P41 | 尝试通过分类算法，构造一棵能实现手机消息分类的决策树。P51 | 尝试通过聚类算法，寻找合适的特征，实现对手机照片的聚类。P59 | 了解神经网络与深度学习算法，完成利用卷积神经网络实现手势识别。P81 |

## 项目总结

完成本章项目后，各小组提交项目学习成果，开展作品设计展示及交流评价，体验小组合作、项目学习和知识分享的过程，了解人工智能技术的基本原理和核心算法。



微信公众号：电子课本大全

# 2.1
# 知识表示与专家系统

## 学习目标 ▶▶▶

- 了解知识表示的方法以及知识表示对人工智能的重要性。
- 了解常用的搜索算法，理解启发式搜索算法的过程，通过案例剖析掌握A*算法的使用方法。
- 了解不确定性推理的概念，理解贝叶斯定理，掌握使用贝叶斯定理进行推理的方法。
- 了解专家系统及构建专家系统的步骤。

## 体验探索

### 认识人工智能的应用——搜索和推理

阿尔法围棋战胜人类围棋高手后，人工智能又一次进入大众的视野。其实，在阿尔法围棋出现之前，我们可能就在手机上玩过人机博弈的游戏，如中国象棋、五子棋等。人类是凭借棋路和经验完成落子的。人工智能决策落子的思路与人类不同，是从所有可能的状态中搜索并推理出赢棋概率最高的下一步，然后落子，如图2.1.1所示。对人工智能而言，搜索是它进行推理的基础。



图2.1.1　机器通过搜索决策下一步落子位置

通过搜索与推理，智能程序能够从大量的数据中快速找到人们想要的结果，诸多智能程序通过搜索与推理提供决策性的服务。

思考：

1. 购物类手机应用程序是如何为使用者推荐他可能想要的商品的？新闻类手机应用程序又是如何为他推送自己可能感兴趣的新闻的？

2. 自己曾经用过哪些智能类应用程序辅助学习？在使用这些程序一段时间之后，这些应用程序是否会为自己推荐其他学习内容？



微信公众号：电子课本大全

### 2.1.1 知识表示

人工智能在发展初期主要研究问题求解，主要的方法为搜索和推理。搜索一般指从给定的数据中寻找指定数据，问题求解中的搜索则指从众多中间状态中寻找到包含问题的解或最接近解的状态。推理则是根据多种已知的状态推测下一步的可能性。因此，当借助人工智能程序来完成搜索或者推理时，最重要的是让机器读懂状态，并根据当前状态作出下一步搜索动作的决策。要做到这一点，需要记录人的思考与判断过程，并用符号表示成机器能够读懂的“规则”。人工智能领域把这种转化过程称为“知识表示”，如图2.1.2所示。

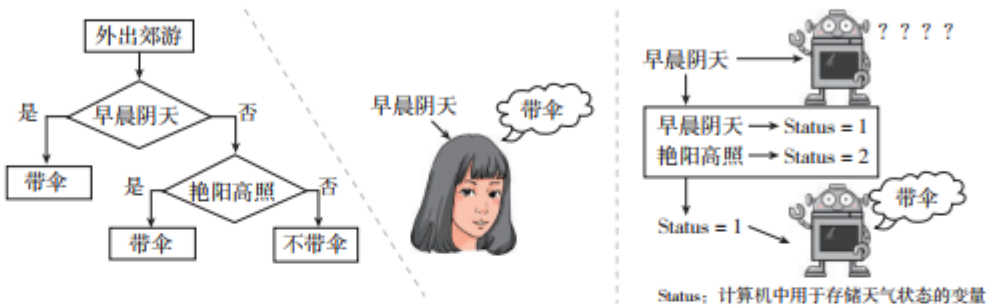



图2.1.2 人与机器识别“知识”的区别

知识表示是人工智能领域最基础的一个概念，在人工智能中，知识通常属于特定领域。为了能让智能系统理解、处理特定领域的知识，并完成基于知识的任务，需要首先对知识构建模型，这就是知识的表示。基于知识的不同任务、不同类型，知识表示方法也不同。常用的知识表示方法包括状态空间法、谓词逻辑与规则、语义网络和本体技术等。

早期人工智能在问题求解时常常采用穷举法或简单试探式的搜索方法，即根据某个规则遍历所有可能的状态，并从中寻找一个状态，这种求解方法称为状态空间法。

**阅读拓展**

**状态空间法的核心概念**

■ 状态

为了描述问题在不同时刻的差别，引入一组列表$Q$。$Q=[q_0, q_1, \cdots, q_n]$，元素$q_i(i=0, 1, \cdots, n)$称为状态变量，当$Q$中的每个状态变量为具体值时，就得到了一个具体的状态。

■ 算符

将待求解的问题从一个状态转化到另一个状态的方式就是算符。算符可以是过程、数学算子、移动走步或运算符号等。

■ 问题的状态空间

状态空间用来表示当前待求解问题全部可能存在的状态及各个状态之间的关系，可以使用三个集合来表示：所有可能存在的问题的初始状态集合、算符集合、所有可能存在的问题的目标状态集合。



微信公众号：电子课本大全

## 实践活动

### 使用“状态空间法”表示八数码问题

在一个大小为3×3的九宫格中摆放8个棋子，并在棋子上分别标上1~8这8个数字。九宫格中有一个格子是空的，空格周围的棋子可以移动到空格中。八数码问题就是给定一个初始状态和一个目标状态，求解如何移动棋子（即找到合适的移动序列），使各棋子的摆放从初始状态变为目标状态。

假设棋子的初始状态和目标状态分别如图2.1.3和图2.1.4所示。

| | | |
|---|---|---|
| 2 | | 3 |
| 1 | 8 | 4 |
| 7 | 6 | 5 |

图2.1.3　棋子的初始状态

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 8 | | 4 |
| 7 | 6 | 5 |

图2.1.4　棋子的目标状态

如何找到一个合适的移动序列，将初始状态变为目标状态呢？这个序列可能是：“右移棋子2，上移棋子1……”解决这个问题的一般方法就是尝试各种可能的移动方法，直到某一步偶然得到目标状态。即从初始状态开始，按照可能的移动方式得到下一状态，然后再次通过尝试得到下一状态，这样依次向下进行，直到目标状态出现。从初始状态通过移动棋子可能出现的所有状态组成一个空间，将这个空间转化为一个由各种状态对应的节点组成的图，该图就称为状态空间图。图2.1.5所示的是八数码问题的状态空间图，图中的每个节点表示一个状态。

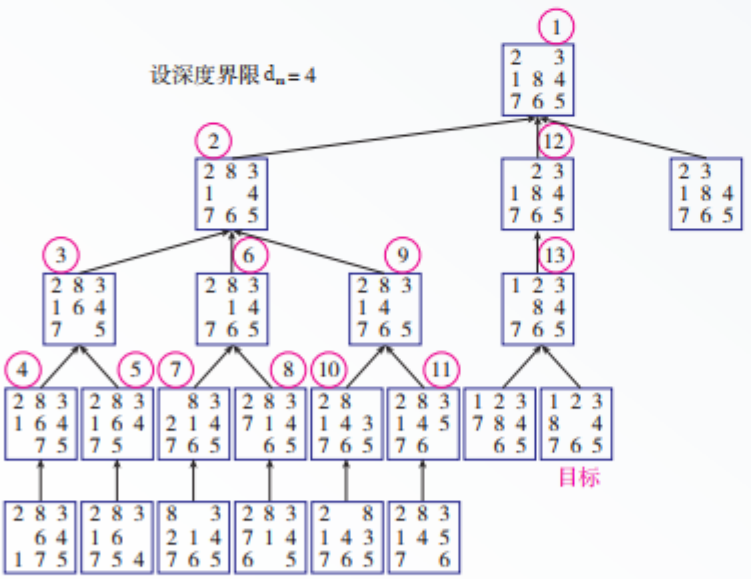



图2.1.5　深度界限为4的八数码问题的状态空间图

通常使用有向图来表示状态空间（也可能是一个树结构）。有向图中的各个节点表示求解问题中可能出现的各个状态。各个状态之间存在关系，也



微信公众号：电子课本大全

就是状态空间中的算符可以用有向图的有向边来表示。一个当前状态只可能存在有限个可以通过问题中运算符操作达到的状态，转化为图的概念就是一个节点一般只有有限个后继节点。

两人一组，每人写出一个八数码问题的初始状态和目标状态交给自己的同伴，让同伴画出深度界限为4的状态空间图。小组讨论如何能够快速找到一个到达目标状态的路径。

### 2.1.2 启发式搜索

传统人工智能问题的求解算法基本都包含两个方面的内容，即问题表示和答案搜索。一个待求解的问题经过知识表示后，就转变为机器能够理解的知识，下一步就可以对这个问题进行求解了。求解过程的实质就是在不同问题状态中搜索解状态的过程，这个过程需要选用适当的搜索算法。常用的搜索算法包括盲目搜索算法和启发式搜索算法。

盲目搜索又叫非启发式搜索，是一种无信息搜索算法，一般只适用于求解比较简单的问题。盲目搜索通常是按预定的搜索策略进行搜索，不会考虑问题本身的特性。常用的盲目搜索算法有宽度优先搜索算法和深度优先搜索算法。

启发式搜索又称为有信息搜索，使用这种算法进行搜索时一般需要求解问题所属领域的特殊信息，这些信息称为启发信息。利用启发信息来引导搜索，可以缩小搜索范围、降低问题的复杂度，故能高效地对状态空间进行搜索，从而快速得到问题的解。利用启发信息搜索状态空间的算法就是启发式搜索算法。



**阅读拓展**

**图搜索算法与启发式搜索算法的关系**

用状态空间法表示知识时，常用图结构来描述问题的所有可能的状态，其问题求解的过程就成为在状态空间图中寻找一条从初始节点到目标节点的路径。图搜索算法简单来说就是在图中寻找某个节点（代表初始状态的节点）到某个节点（代表目标状态的节点）之间的可达路径。图搜索算法的一般过程如下。

1. 建立搜索图$G$，初始时只含有起始节点$S$，搜索图$G$中每个子节点有一个指向其父节点的指针（指针即某个变量的地址，利用指针指向的地址可以读取存储器中这个位置存储的值）。建立一个OPEN表用于存放未扩展的节点，建立一个CLOSED表用于存放已扩展的节点，初始时CLOSED表为空。

2. 将起始节点$S$接入到OPEN表中，如果此节点是目标节点，则得到解。

3. 如果OPEN表为空，则输出无解，并退出（失败）；否则继续执行第4步。

4. 选择OPEN表中的第一个节点（记为节点$n$），把它从OPEN表中移出，同时存入CLOSED表中。



微信公众号：电子课本大全

5. 如果$n$是目标节点，则输出解，并退出（成功）。此时的解是搜索图$G$中沿着节点$n$指向父节点的指针方向，从$n$回溯到$S$得到的一条路径。

6. 扩展节点$n$的所有节点，同时生成$n$的后继节点的集合$M$（$M$中不包含$n$的前驱节点），将集合$M$中的节点作为$n$的后继节点添加到搜索图$G$中。

7. 对于那些在搜索图$G$中没有出现过，但是属于集合$M$的节点，设置一个通向$n$的指针，把集合$M$中的节点（以下简称$M$节点）放入OPEN表中；对于已经在OPEN表或者CLOSED表中的$M$节点，确定是否需要更改该节点到$n$的指针；对于已经在CLOSED表中的每个$M$节点，确认是否需要更改搜索图$G$中通向它的每个后继节点的指针。

8. 按某个算法规则对OPEN表进行重排，转向第3步。

图搜索算法的第8步（对OPEN表进行重排），目的是在下一次搜索时，能够选出一个最大可能为解的最优节点，为第4步节点扩展所使用。如果此时的排序是任意的或者没有进行过排序，那么这个算法就属于盲目搜索算法。此时也可以依据一个启发函数来排序，即使用启发式搜索算法，改善盲目搜索算法效率低的问题（搜索过程耗费较多的时间与空间）。

如果能够找到一种对OPEN表进行重排的方法，那么就能够尽量保障每次扩展的节点是相对最优的。

启发式搜索算法中有一个函数，称为估价函数，将这个函数作为标准对OPEN表进行重排。重新排列OPEN表的过程，需要估算每一个节点的可能性，衡量可能性的标准就是估价函数。通常使用符号$f$表示这个估价函数，节点$n$的估价函数值就记作$f(n)$。$f$就是起始节点通过节点$n$到达目标节点的最小代价路径上的一个估算代价。重排后，可以认为搜索是沿着某个最有希望的方向进行节点扩展的。

A*算法是一种特殊的启发式搜索算法。将节点$S$到节点$n$的最小代价路径的代价定义为$g(n)$，从节点$n$到某个目标节点的追加代价路径的代价定义为$h(n)$。定义$f(n)=g(n)+h(n)$，$f(n)$是节点$S$到节点$n$之间的一条最佳路径的实际代价加上节点$n$到某目标节点的一条最佳路径代价之和，所以$f(n)$是从节点$S$开始通过节点$n$的一条最佳路径的代价。采用估值函数$f(n)=g(n)+h(n)$的启发式搜索算法称为A*算法，A*算法的一般过程如下。

1. 将起始节点$S$放到OPEN表中，记$f=h$，令CLOSED表为空。

2. 重复下列步骤，直到找到目标节点。若OPEN表为空，输出无解，退出。

3. 从OPEN表中选取一个未设置过的且$f$值最小的节点$i$作为最佳节点，加入CLOSED表中。

4. 若$i$为目标节点，则成功得解；若$i$不是目标节点，则扩展$i$，得到$i$的后继节点。

5. 对于每一个$i$的后继节点$j$，计算$g(j)=g(i)+g(i,j)$，若$j$既不在OPEN表中也不



微信公众号：电子课本大全

在CLOSED表中，则加入到OPEN表中；如果$j$在OPEN表中，则用刚刚计算的$g$值与之前该节点的$g$值比较，如果新的$g$值较小，则用新值代替旧值，指针从$j$指向$i$；如果$j$在CLOSED表中，则将$j$移回OPEN表。

6. 计算$f$值，并回到第2步。

## 实践活动

### 利用启发式搜索A*算法求解八数码问题

对于八数码问题，设估价函数$f(n)=g(n)+h(n)$，其中，$g(n)$为从初始节点$S_0$到节点$n$移动的棋子数目，也就是搜索树中节点$n$的深度；$h(n)$为节点$n$所处状态中各数码到达目标状态的距离之和，即与目标状态相比，不在目标位置的棋子个数。

利用启发式搜索A*算法求解八数码问题的过程如图2.1.6所示。

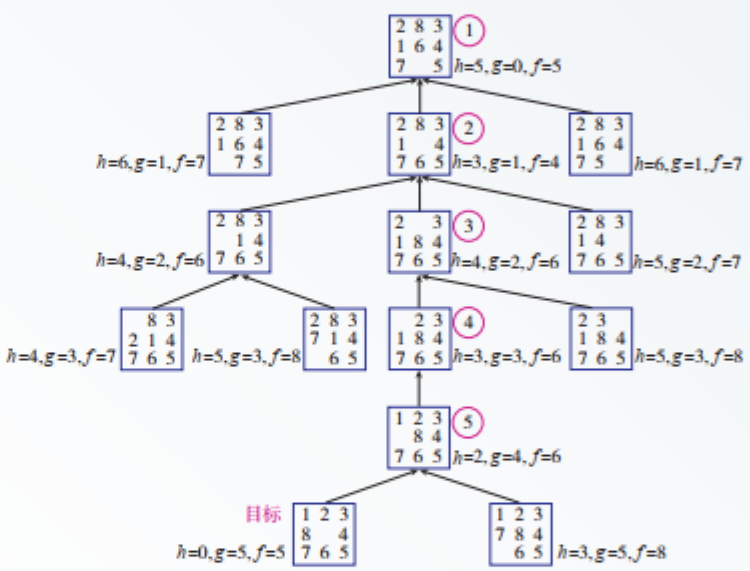



图2.1.6　利用启发式搜索A*算法求解八数码问题的过程图解

启发式搜索A*算法的一般过程如下。

1. 将$S_0$加入OPEN表中，计算估价函数$f(S_0)$。

2. 如果OPEN表为空，则无解，退出，否则继续执行第3步。

3. 选取OPEN表中$f$值最小的节点$i$放入CLOSED表中。

4. 判定节点$i$是否为目标节点，如果是，则求得解，否则继续。

5. 扩展节点$i$，得到后继节点$j$，计算$f(j)$，提供$j$返回到$i$的指针，利用$f(j)$对OPEN表进行重新排序，调整节点的父子关系及关联指针，转向第2步。



微信公众号：电子课本大全

### 2.1.3 贝叶斯推理

搜索算法进行搜索的过程属于确定性过程，它建立在经典逻辑的基础上，运用确定性的知识进行精确搜索或推理。而现实中的情境往往比较复杂，比如，人们普遍认为夜里下雨，第二天早晨草地一定会是湿的，而实际到了早上草地可能就干了，也许因为风的因素，草上的雨水很快就被吹干了。对于这样的不确定性问题，很难使用经典的精确推理方法来反映此类情境。解决这类问题往往需要根据人类已有的经验来计算某种状态出现的概率，这种推理方式叫做贝叶斯推理。贝叶斯推理根据贝叶斯定理进行概率计算及推理，属于不确定性推理方法。

贝叶斯定理表述如下：符号$P(A|B)$表示事件$B$发生的条件下事件$A$发生的概率，$P(A|B)$等于事件$A$发生的条件下事件$B$发生的概率乘以事件$A$发生的概率，再除以事件$B$发生的概率。

用公式表示为：

$$P(A|B)=\frac{P(B|A)P(A)}{P(B)}$$



**阅读拓展**

**基于贝叶斯定理的逆向概率**

问题：当你在电影院售票大厅等待入场看电影时，忽然看到前面有个人的电影票掉了。此时你想提醒那个人，但是根据背影你无法判断其性别，仅知道这个人是长发，那你会说“女士打扰一下”还是“先生打扰一下”？

假设当前大厅中男女各占一半。女士中一半为长发，一半为短发；男士中96%为短发，4%为长发。那么，你先要判断这位长发、掉电影票的人是女士的概率有多少。

对于这个问题，可以使用贝叶斯定理来解决。事件$A$代表背对你的人是女士，事件$B$代表背对你的人是长发。那么问题就简化为：事件$B$出现的前提下，判断事件$A$出现的概率是多少。

用$P(A)$代表此人是女士的概率，根据问题描述，我们知道$P(A)=50\%$；用$P(A')$代表此人是男士的概率，则$P(A')=1-P(A)=50\%$；$P(B|A)$代表女士头发为长发的概率（在使用贝叶斯定理进行推论时，这个值一般是便于估计的值），$P(B|A)=50\%$；同理，$P(B|A')$代表男士头发为长发的概率，$P(B|A')=4\%$；$P(B)$表示此人是长发的概率，$P(B)=P(B|A)P(A)+P(B|A')P(A')=27\%$。

根据贝叶斯定理公式，通过计算得到$P(A|B)=P(B|A)P(A)/P(B)\approx 93\%$，即背对你的人是长发时，此人是女士的概率约为93%。

根据贝叶斯定理，我们可以利用便于统计的事件发生的概率去推理难以统计的事件发生的概率。如同本例中，根据男女比例和男女中长短发的比例去推断只能看到长发背影的前提下，这个人是女士的概率。



微信公众号：电子课本大全

## 思考活动

### 利用贝叶斯定理推断是否下雨

周日一早天空多云，小王与同学小李相约去户外露营。

小王对小李说："60%下雨天的早上是多云的，我们真的要决定外出露营么？"

小李不甘心就此取消露营活动，作出如下分析：

1. 多云不见得会下雨，咱们城市约有30%的早上是多云的；

2. 咱们城市平均一个月才下3天雨，所以今天下雨的概率只有10%。

小王现在不知道该不该出行，于是询问自己的人工智能助手。

人工智能助手根据小王提供的信息，利用贝叶斯定理开始推测：

某天早上有云，当天会下雨的概率即$P(雨 \mid 云)$，由公式可知$P(雨 \mid 云)=P(雨)P(云 \mid 雨)/P(云)$；

$P(雨)$就是某天下雨的概率，也就是小王与小李所在城市下雨的概率，为10%；

$P(云 \mid 雨)$是在下雨天，且早上有云的概率，$P(云 \mid 雨)=60\%$；

$P(云)$是早上多云的概率，为30%。

小王的人工智能助手很快就得出了结论。

思考：

1. 你觉得小王的人工智能助手推算的$P(雨|云)$是多少呢？据此帮助小王决定是否去露营。

2. 根据该场景，解释求解$P(A|B)$时，为什么要使用$P(B|A)$？

日常生活中也常使用贝叶斯定理进行决策。比如在河边钓鱼时看不清楚河里有没有鱼，似乎只能盲目选择，但实际上可以根据贝叶斯定理，利用以往积累的经验找一处回水湾区开始垂钓。这就是根据先验知识进行主观判断，在一处钓过鱼之后，对这个地方有了更多了解，然后再进行选择。所以，在对事物认识不全面的情况下，贝叶斯定理不失为一种理性且科学的推理方法。

## 阅读拓展

### 搜寻失踪的"天蝎号"

1968年5月，美国海军"天蝎号"核潜艇在亚速海海域失踪。军方通过各种技术手段调查无果，最后不得不求助数学家约翰·克雷文(John Craven)。约翰·克雷文提出的方案使用了贝叶斯定理。他召集了数学、潜艇和海事搜救等各个领域的专家，通过贝叶斯定理一一排除小概率发生意外事故的搜索区域，具体计算情况如图2.1.7所示，图中不同的颜色代表某一时刻不同区域能搜救到潜艇的不同概率。

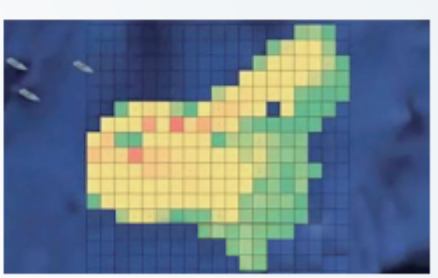


图2.1.7 "天蝎号"可能位置的概率图



微信公众号：电子课本大全

贝叶斯定理已应用于诸多领域，从物理学到癌症研究，从生态学到心理学，从博弈论到教育学等。特别是在人工智能领域，很多模仿人脑思考和决策的过程，被设计成一个个贝叶斯推理的程序，让我们能够轻松感受到贝叶斯定理的魅力。

### 2.1.4 专家系统

专家系统是一个智能计算机程序系统，其内部包含有某个领域专家水平的大量知识和经验，能够利用人类专家的知识和解决问题的方法来处理该领域的问题。专家系统模拟人类专家的决策过程，以解决那些需要人类专家处理的复杂问题。

在与用户进行交互时，专家系统进行决策的过程为：如果情况是A，那么请☆☆☆，否则请△△△。其中专家系统作出决策时，依据某个领域的专业知识和经验，根据该领域专家水平的知识和经验来构建规则。专家系统根据规则来判断用户的需求属于哪一种情况，并按照规则进行判断和预测，场景如图2.1.8所示。

#### 专家系统的组成

专家系统一般包括知识获取、知识库、综合数据库、推理机、解释器和人机交互界面（接口），如图2.1.9所示。




图2.1.8 用户与专家系统交互场景

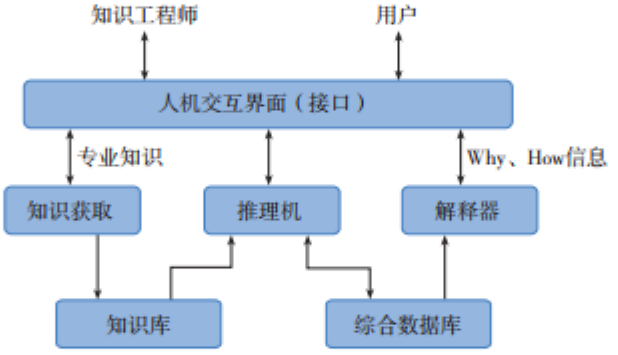



图2.1.9 专家系统的构成示意图

知识获取是知识工程师把获取的专业知识进行加工整理并加入到知识库中的过程。

知识库用于存储某领域专家系统的专业知识，包括事实、可行性操作与规则等。为了建立知识库，要解决知识获取和知识表示等问题。

综合数据库也叫全局数据库，用于存储某领域或问题的初始数据和推理过程中得到的中间数据。

推理机用于存储推理所采用的规则和控制策略的程序，使整个专家系统能够以合乎逻辑的方式协调地工作。推理机能够根据知识进行推理，得出结论，而不是简单地搜索现成答案。

解释器能够向用户解释专家系统的行为，包括解释推理结论的正确性以及系统输出其他候选解的原因。



微信公众号：电子课本大全

人机交互界面是系统与用户、知识工程师的交互接口。通过该界面，用户可以输入基本信息，回答系统提出的相关问题，系统则输出推理结果及相关解释。

### 构建专家系统的一般流程

构建专家系统的一般流程如图2.1.10所示。

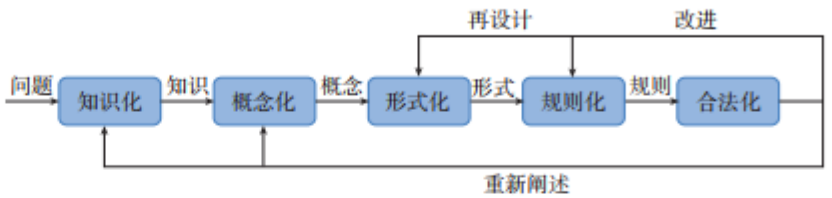



图2.1.10　构建专家系统的一般流程示意图

■ 设计初始知识库。问题知识化，辨别所研究问题的实质，梳理清楚要解决的任务是什么，是否还可以拆分成子任务或者子问题，包含哪些典型数据；知识概念化，概括知识表示所需要的关键概念和关系，比如数据类型、控制策略等；概念形式化，确定用来组织知识的数据结构形式，应用人工智能知识表示方法来表达关键概念、子问题及信息流特性；形式规则化，即编制规则，把形式化的知识转化为用编程语言表示的计算机可执行程序；规则合法化，检验知识的合理性、规则的有效性。

■ 原型机的开发与试验。建立整个系统所需要的实验子集，包括整个模型的典型知识，而且只涉及与试验相关的足够简单的任务和推理过程。

■ 知识库的改进与归纳。反复对知识库和规则进行试验，归纳出更完善的结果。



### 阅读拓展

#### 中医诊断专家系统

1979年，我国第一个中医诊断专家系统——诊疗肝病计算机程序问世。到了20世纪80年代，国内相继出现了中医肾系统疾病计算机诊疗、教学、护理和咨询系统，妇科专家诊疗系统，医学智能通用编辑系统和乙型肝炎专家诊疗系统等。目前，中医专家系统的代表是数字名医服务系统和中医全科专家系统。

某中医诊断专家系统根据症状自动生成的诊断数据如表2.1.1所示，该系统的工作流程如图2.1.11所示。医师通过对患者体征的观察，结合病人症状，将获取的相关数据输入专家系统，专家系统根据系统数据库中存储的中医诊断知识，反馈几种可能的证名，再由医师根据专家系统提供的结果完成诊断。



微信公众号：电子课本大全

表2.1.1　中医诊断专家系统诊断数据

| 诊断数据 | |
|---|---|
| 中医症状 | 无汗，恶寒发热，脉紧，舌苔薄白，脉浮，咽喉痒，酸痛，四肢或肢体痛，头痛，痰多质稀，痰色白，鼻塞流清涕，咳嗽，气喘/急，声音重浊 |
| 结果1 | 证名：风寒袭肺证<br>匹配度：66.67%<br>中医病名：咳嗽<br>病机：风寒外束，内袭于肺，肺卫失宣，肺气闭郁，不得宣通<br>治法：疏风散寒，宣肺止咳<br>处方：三拗汤合止嗽散加减<br>方药：炙麻黄9g，杏仁9g，甘草6g，荆芥9g，桔梗9g，紫菀9g，百部9g，白前9g，陈皮6g |
| 结果2 | 证名：风寒证<br>匹配度：33.33%<br>中医病名：头痛<br>病机：风寒外袭，上犯巅顶，凝滞经脉<br>治法：祛风散寒<br>处方：川芎茶调散加减<br>方药：川芎9g，防风10g，荆芥10g，羌活15g，白芷15g，细辛3g，薄荷10g |
| 结果3 | 证名：风盛挛急证<br>匹配度：33.33%<br>中医病名：咳嗽<br>病机：风邪犯肺，邪客肺络，气道挛急，肺气失宣<br>治法：疏风宣肺，解痉止咳<br>处方：苏黄止咳汤加减<br>方药：炙麻黄6g，蝉蜕6g，紫苏叶9g，前胡9g，牛蒡子9g，枇杷叶9g，地龙9g |
| 医师意见 | 证名：风寒袭肺证<br>中医病名：咳嗽<br>病机：风寒外束，内袭于肺，肺卫失宣，肺气闭郁，不得宣通<br>治法：疏风散寒，宣肺止咳<br>处方：三拗汤合止嗽散加减<br>方药：炙麻黄9g，杏仁9g，甘草6g，荆芥9g，桔梗9g，紫菀9g，百部9g，白前9g，陈皮6g |

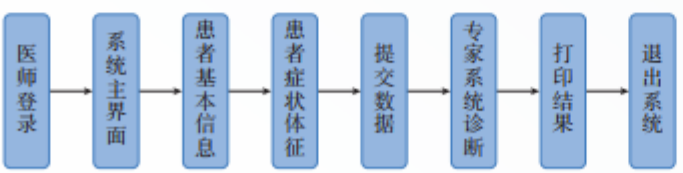



图2.1.11　中医诊断专家系统的工作流程示意图



微信公众号：电子课本大全

## 项目实施

### 分析手机中的智能应用，体会搜索与推理的魅力

一、项目活动

大家平时可使用智能手机应用程序辅助学习，比如记忆单词应用程序等。根据自己的学习生活，结合本节学习的关于搜索与推理的知识，从手机应用程序类型、所使用人工智能的技术原理、对应实现原理的算法等方面展开小组讨论，设计一个适合自己的、利用人工智能搜索与推理算法的智能学习类手机应用程序的方案，并用思维导图呈现。

二、项目检查

1. 各小组绘制手机应用程序设计方案的思维导图，并在班级内进行交流、分享。

2. 根据思维导图，讨论是否存在只使用搜索与推理算法的人工智能，思考如何能够让设计的智能手机应用程序效率更高。

## 练习提升

1. 什么是不确定性推理？为什么需要不确定性推理？上网搜索最近一年足球赛事的对战数据，收集某两支球队的历史胜率，并计算其中一支球队获胜的概率。利用这些概率，根据贝叶斯定理建立一个预测球队胜负的专家系统核心功能的思维导图。

2. 智能手机里的应用程序会根据人们的浏览偏好进行内容推送，思考智能应用程序是如何推测出人们的喜好，并在大量的知识数据中找到人们感兴趣的内容的。



微信公众号：电子课本大全

# 2.2
# 回归算法

**学习目标** ▶▶▶

- 通过剖析案例，了解回归算法的基本原理，能举例说明回归算法的应用场景。
- 掌握线性回归问题的两种求解方法，能应用求解方法解决实际问题。

## 体验探索

### 智能手机里的预测功能

生活中，人们往往需要依据以往的经验或数据，预测一些事情的发展趋势，智能手机也提供了一些有预测功能的应用程序。例如，天气类应用程序会依据近期天气数据来预测降水量等天气情况，指导人们出行，有些预测在时间上甚至能精确到小时；地图类应用程序除了能帮助我们规划出行线路外，还能根据实时路况预测行程需要花费的大概时间，如图2.2.1所示；旅行类应用程序会预测部分景区节假日的热门指数，根据这些数据，游客能制订更加合理的出行计划，景区也能制订更合理的节假日预案，为游客提供更好的旅行体验。




图2.2.1　天气及地图类应用程序的预测功能

思考：

查阅相关资料，看看还有哪些手机应用程序能够借助预测功能来提高我们的生活品质。



微信公众号：电子课本大全

### 2.2.1 回归在学习中的应用

“回归”这个词看起来陌生，其实在物理实验中，同学们经常借助回归思想，来寻求事物运动的特点和规律。其中一个经典的实验就是借助打点计时器和纸带，来探究小车速度随时间变化的规律，如图 2.2.2 所示。在实验过程中，同学们可以基于实验获取的数据来推断数据之间蕴含的关系。简单地说，“回归”就是一种由果索因的过程，即由大量事实所呈现的状态，设法去推断其形成的原因。

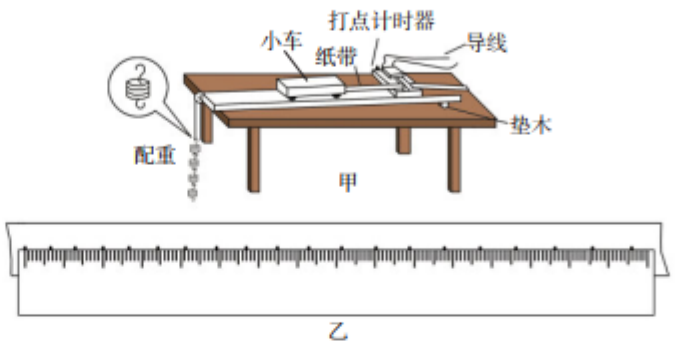



图2.2.2 小车运动速度随时间变化规律的探究实验

**实践活动**

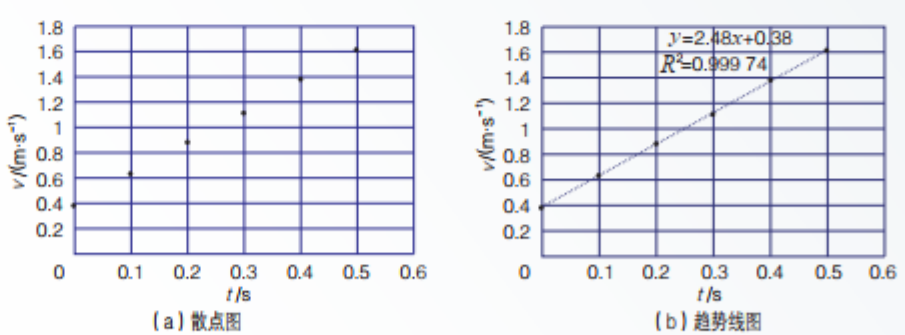
**借助电子表格软件绘制实验图像**

在“探究小车的运动速度随时间变化的规律”的实验中，获得的一组实验数据如表2.2.1所示。

表2.2.1 小车的运动速度随时间变化的实验数据

| $t$/s | 0 | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 |
|---|---|---|---|---|---|---|
| $v$/(m·s$^{-1}$) | 0.38 | 0.63 | 0.88 | 1.11 | 1.38 | 1.62 |

打开电子表格软件（Excel或WPS），在相邻的两行中分别填入时间$t$和速度$v$的值，用鼠标选中所有数据后，单击“插入”菜单，选择绘制一幅散点图，得到如图2.2.3(a)所示的散点图。




(a) 散点图　　(b) 趋势线图

图2.2.3 使用电子表格软件绘制的散点图和趋势线图



微信公众号：电子课本大全

得到散点图后，可以添加一条趋势线来观察这些点的分布特点。由于实验所得数据几乎分布在一条直线上，所以可以选择“线性”类型的趋势线，同时勾选在图表上“显示公式”和“显示$R$平方值”选项，可得如图2.2.3(b)所示的趋势线，其中速度和时间的关系表达式为$y=2.48x+0.38$。$R^2$值表示线性趋势线对数据拟合的程度，$R^2$越接近1，代表拟合的图像越趋近于真实情况，预测效果越好。

这个实验其实是在探究速度和时间两个变量间的定量关系，确定速度$y$和时间$x$的关系式（$y=2.48x+0.38$）后，可以根据需要推测出时间为某一个数值时的速度大小。

回归算法一般用于确定两种或两种以上变量间的定量关系。按照自变量的数量多少，可以分为一元回归和多元回归；按照自变量和因变量之间的关系类型，可以分为线性回归（图 2.2.4）和非线性回归（图 2.2.5）。因变量和自变量之间的关系如果类似于一次函数，则属于线性回归问题；如果类似于指数函数或对数函数等，则属于非线性回归问题。

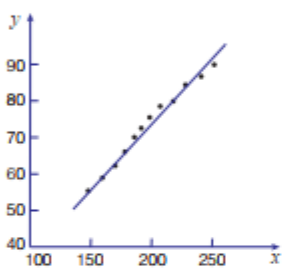



图2.2.4　线性回归问题趋势线图

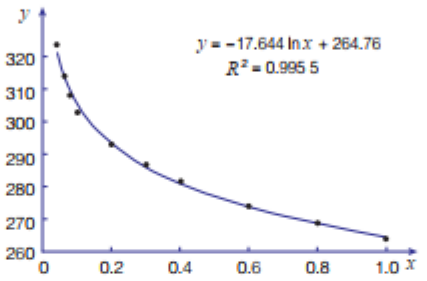



图2.2.5　非线性回归问题趋势线图

回归分析一般适用于求解因变量是连续值的情况，而不适用于求解因变量是离散值的情况。如明天的气温、超市每天的销售额、近期的房屋价格和股票走势等适合用回归分析法求解，而明天是否下雨、图片中的动物是小猫还是小狗等则属于分类问题。

## 2.2.2　回归算法的一般流程

回归算法在学习中已得到广泛应用，在生活中的应用也有很多，如可以用来预测近期的房屋价格、电影票房走势及人口增长趋势等。回归算法的一般流程如图2.2.6所示，下面将通过一个简单的一元线性回归问题来进行说明。

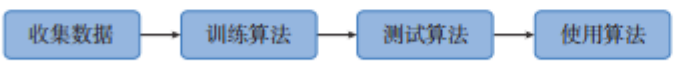



图2.2.6　回归算法的一般流程示意图

### 收集数据

在放学的路上，小明收到了一份传单，传单中有一家新开业蛋糕店的蛋糕售价。表2.2.2所示为某种口味的蛋糕不同尺寸的售价。通过这组数据可以探索店铺定价的奥秘。



微信公众号：电子课本大全

表2.2.2　某种口味蛋糕尺寸与售价的关系

| 蛋糕尺寸/英寸 | 6 | 8 | 9 | 10 | 12 |
|---|---|---|---|---|---|
| 价格/元 | 40 | 56 | 69 | 77 | 96 |

（注：1英寸=2.54 cm）

### 训练算法

根据收集的数据，编程求得蛋糕尺寸和价格两个变量之间的定量关系。

## 实践活动

### 借助Python探索蛋糕价格的奥秘

借助Python编程语言中的sklearn模块来探索蛋糕尺寸和价格之间的关系，并以蛋糕尺寸为$x$轴，价格为$y$轴，通过matplotlib模块绘制出拟合的图像。

```
from sklearn import linear_model
import matplotlib.pyplot as plt
# 解决中文显示问题
plt.rcParams['font.sans-serif']=['SimHei']
plt.rcParams['axes.unicode_minus']=False
# 样本数据(Xi, Yi)，Xi是蛋糕尺寸，Yi是蛋糕价格
Xi=[[6],[8],[9],[10],[12]]
Yi=[[40],[56],[69],[77],[96]]
# 设置模型
model=linear_model.LinearRegression()                    # 普通最小二乘线性回归
# 训练数据，并用训练得出的模型预测数据
y_plot=model.predict(Xi)                                 # 使用线性模型预测
# 打印价格y和尺寸x的关系式
print("y=",model.coef_[0],"x+",model.intercept_)
print(model.score(Xi, Yi))                               # score()返回预测的R平方值
# 绘制散点图，并设置标记的大小和颜色
plt.scatter(Xi,Yi,color="red",label="sample data",linewidth=2)
# 绘制散点的连线
plt.plot(Xi,y_plot,color="green",label="regression data",linewidth=2)
plt.ylabel("价格/元")
plt.xlabel("蛋糕尺寸/英寸")
plt.legend(loc="lower right")                            # 在轴上放置图例
plt.show()                                               # 显示绘制的图形
```

得到蛋糕尺寸和价格之间的关系式及$R^2$的值如下：

$$y=[\,9.45\,]x+[\,-17.45\,]$$

$$R^2=0.996\,012\,714\,7$$

绘制出的图像如图2.2.7所示，其中红色圆点为获得的样本数据的散点分布，绿色的直线为拟合出的趋势线。

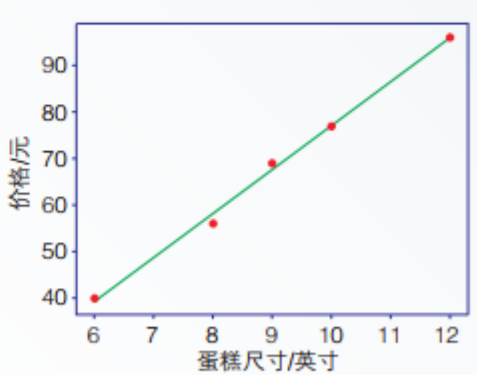


图2.2.7　蛋糕尺寸与售价关系

查阅相关资料，学习sklearn模块的用法，将上述训练数据的代码补充完整。



微信公众号：电子课本大全

## 技术支持

### sklearn模块与matplotlib模块

当前有许多基于Python编程语言的人工智能应用框架和平台，这些框架和平台积累了丰富的模块和类库，用户可根据不同需求自行调用。在这些模块中，sklearn模块是一个简单、有效的数据分析工具，提供了解决回归、分类和聚类等问题的方法，功能十分强大。matplotlib模块是常用的绘图工具之一，可以非常方便地创建2D图表和一些简单的3D图表。

### 测试算法

算法训练完成后，得到$R^2$的值约为0.996，非常接近1，说明得到的关系式效果较好。

### 使用算法

求得蛋糕尺寸和价格之间的关系后，如果给定一个新的蛋糕尺寸，就可以将尺寸的数值代入关系式中，计算出这一尺寸的蛋糕价格，从而实现预测蛋糕价格的功能。

## 项目实施

### 回归算法助力学习类移动应用程序

一、项目活动

基于上一节设计的智能学习类移动应用程序，结合本节所学内容，进行小组讨论，完成一个基于回归算法的应用程序设计方案。

思考应用程序每天会记录用户的哪些数据，在此基础上可以作出什么样的预测。例如，通过记录用户每天记过的单词量，预测用户未来可能完成的任务量，并依据预测结果推荐合适数量的单词供用户记忆。

二、项目检查

进一步完善上一节绘制的思维导图，添加基于回归算法的功能，并在班级内进行交流。

## 练习提升

1. 生活中还有哪些问题能够使用回归算法进行分析？查阅相关资料，借助电子表格软件得出因变量与自变量之间的关系。

2. 借助Python编程语言求解上面的问题，对比两种求解方式的优劣。



微信公众号：电子课本大全

# 2.3
# 使用决策树进行分类

## 学习目标 ▶▶▶

- 通过剖析案例，了解决策树的基本概念，能举例说明算法的应用场景。
- 了解生成决策树的经典算法之一——ID3，能解释算法的关键环节。
- 了解分类问题的基本概念和应用场景。

## 体验探索

### 如何在网络上快速买到心仪的商品

网上商城不同于传统商场，几乎没有空间和时间的限制，可以全天候出售琳琅满目的商品。有些商品型号众多，如何快速找到自己心仪的那一款呢？

以购买手机为例，当前一些购物类应用程序提供了手机选购指南，如图2.3.1所示。用户可以先选择自己喜欢的类型，如音乐手机、商务手机和长辈用机等，然后再针对选定的类型根据具体的参数进行选择，如机身内存、中央处理器核数和电池续航时间等，随后这类应用会推荐一个满足用户需求的手机列表供用户挑选，从一定程度上提升了用户的购物效率。



图2.3.1　手机选购智能指南

思考：

1. 如果自己去挑选手机，会优先考虑手机的哪些特征呢？根据自己的需求将“容量、续航、外观、摄像头像素、系统和价格”等特征进行排序。

2. 根据自己的需求，到网上商城中选购手机，看看挑选结果是否令自己满意。



微信公众号：电子课本大全

### 2.3.1 认识决策树

决策是人们日常生活中普遍存在的作出判断或选择的行为。比如，购物时要判断是否为最佳购买时机，旅行时要选择游玩地点，用餐时要挑选菜品，假期要选择是待在家里还是和同伴一起出游。在我们作出决策前，需要考虑很多相关因素并加以权衡，但是从多种因素中找到一个平衡点却没那么容易。实际上人们在决策时并不会把所有因素都考虑进去，而总是优先考虑自己认为最重要的那个因素。

分类是人工智能领域的一个重要问题，一般用于判断事物的类型。例如，识别图片中的动物是猫还是狗，判断明天的天气是晴还是阴，分析用户的心情是愉快还是伤心等。在人工智能领域，可以通过分类实现决策。本节将讨论一种经典的分类算法——决策树。

#### 思考活动

**小明会推荐妈妈购买哪款手机**

小明的妈妈想购买一款智能手机，要求手机的闪存容量达到64 GB，屏幕尺寸为5.5英寸或以上，价格不超过1 300元。

思考：

图2.3.2为依据小明妈妈的要求构建的手机选择决策树。结合此图判断小明会推荐妈妈购买表2.3.1中的哪款手机。

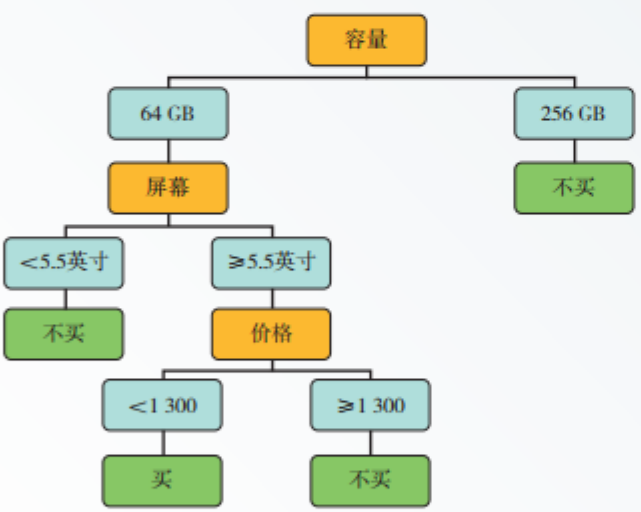



图2.3.2　手机选择决策树

表2.3.1　不同型号手机的参数

| 手机型号 | RAM容量/GB | 闪存容量/GB | 屏幕尺寸/英寸 | 操作系统 | 最大像素值 | 价格/元 | 是否购买 |
|---|---|---|---|---|---|---|---|
| A | 3 | 64 | 6.09 | Android | 1 300万 | 999 | |
| B | 4 | 64 | 6.21 | Android | 2 400万 | 1 299 | |



微信公众号：电子课本大全

续表

| 手机型号 | RAM容量/GB | ROM容量/GB | 屏幕尺寸/英寸 | 操作系统 | 最大像素值 | 价格/元 | 是否购买 |
|---|---|---|---|---|---|---|---|
| C | 4 | 64 | 5.45 | Android | 1 200万 | 799 | |
| D | 6 | 64 | 6.21 | Android | 2 400万 | 1 699 | |
| E | 8 | 256 | 6.39 | Android | 2 400万 | 3 098 | |
| F | 2 | 64 | 4.70 | iOS | 1 200万 | 3 899 | |

由于这类问题的决策流程类似一棵倒立的树（图2.3.2），因此这种决策方法一般称为“决策树”，其中影响决策结果的因素叫做“特征”，如表2.3.1中的容量、屏幕尺寸和价格等。一棵典型的决策树通常由以下三部分组成。

■ 决策节点，用于表述决策的特征，图2.3.2中的橙黄色节点即为决策节点。

■ 分支（通路），代表特征的某个可能的属性值，图2.3.2中的黑色连接线及蓝色节点即为分支（通路）。

■ 终节点，给出决策的结论，因为这种节点下面不会再有子节点，故又称叶子节点，图2.3.2中的绿色节点即为终节点。

在图2.3.2中，每一个特征都有两个取值，故这是一棵二分支的决策树。如果一个特征有多个取值，则能构造一棵多分支的决策树。图2.3.3所示的决策树是通过判断天气情况，得出是否出游的决策。决策流程是：先判断天气情况，对于“天气”这个特征，有三种取值，分别为雨、晴和阴；如果是阴天则出游，否则需要再判断风的大小或阳光的强弱，从而进行最终的决策。

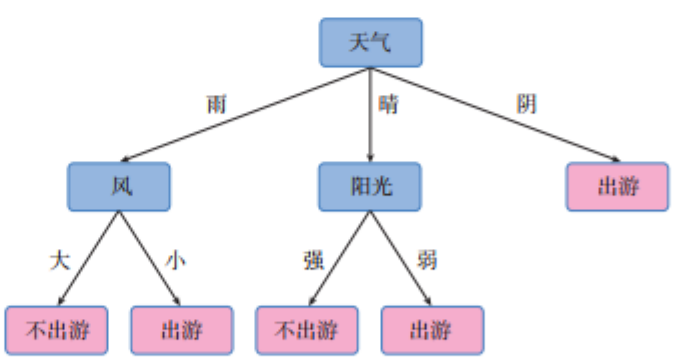



图2.3.3　是否出游的多分支决策树

决策树是一种将实际问题“分而治之”的学习策略。机器可以通过逐一判断多个特征的取值，顺着决策树找到对应的分支，直至作出最终的决策。这种方法通常用于处理分类问题。例如，判断邮箱中的邮件是否为垃圾邮件、图片中的生物是动物还是植物等。



微信公众号：电子课本大全

值得注意的是，决策树与回归分析有着显著的不同：决策树一般用于处理离散型数据的问题，如判断是否出游、是否买下商品等；而回归分析一般用于处理连续型数据的问题，如预测最终购买商品的价格、明天下雨的概率等。

### 2.3.2 构造决策树的一般流程

构造一棵决策树的过程其实与“思考活动”中“小明会推荐妈妈购买哪款手机”的过程完全相反，首先需要收集类似表2.3.1中的一批样本数据；其次对这些数据进行处理，方便机器按照一定的算法来学习这些样本数据；最后“训练”出一棵决策树，并能通过一些指标来评估这棵决策树的好坏，从而决定是否将这棵决策树投入使用。

构造决策树的一般流程可以概括为图2.3.4所示的5个环节，其中最重要的环节是训练算法。




图2.3.4 构造决策树的一般流程

下面将运用决策树的一种经典算法——迭代二叉树3代算法（Iterative Dichotomiser 3，ID3），结合一个实际问题来介绍决策树的具体构造过程。

生活中，眼科医生是如何判断患者应该选择佩戴哪种隐形眼镜镜片的？下面我们根据决策树的原理和构造环节，借助决策树算法来判断适合患者的镜片类型。

#### 收集数据

为解决这个问题，可选择从美国加州大学欧文分校（University of California Irvine，UCI）数据集获取数据，该数据集是该校提供的用于机器学习的数据库，是一个常用的机器学习标准测试数据集。在这个隐形眼镜数据集里，共提供了24条训练数据，表2.3.2节选了其中的6条数据。

表2.3.2 UCI隐形眼镜数据集信息（节选）

| 年龄 | 症状 | 是否散光 | 眼泪数量 | 适合的隐形眼镜类型 |
|---|---|---|---|---|
| 青年人 | 近视 | 否 | 不足 | 不适合佩戴 |
| 青年人 | 远视 | 否 | 正常 | 软材质 |
| 青年人 | 近视 | 是 | 不足 | 不适合佩戴 |
| 青年人 | 远视 | 是 | 正常 | 硬材质 |
| 中年人 | 近视 | 否 | 不足 | 不适合佩戴 |
| 老年人 | 远视 | 否 | 正常 | 软材质 |



微信公众号：电子课本大全

从表2.3.3可以看出，最终的决策分类共有三种，分别为硬材质、软材质和不适合佩戴。影响最终决策的特征共有四个，分别为年龄（青年人、中年人、老年人）、症状（近视、远视）、是否散光及眼泪数量（不足、正常）。

### 准备数据

我们将借助Python编程语言来构造一棵决策树。为了方便程序计算，需要将收集到的原始数据进行处理，将输入的特征全部进行数值化，比如“年龄”这个特征，有青年人、中年人和老年人三种值，可以将其转化为：青年人=1，中年人=2，老年人=3。类似地，可以将表2.3.2中的数据转化为表2.3.3所示数据。

表2.3.3　转化后的UCI隐形眼镜数据集信息（节选）

| 年龄 | 症状 | 是否散光 | 眼泪数量 | 适合的隐形眼镜类型 |
|---|---|---|---|---|
| 1-青年人 | 1-近视 | 1-否 | 1-不足 | 不适合佩戴 |
| 1-青年人 | 2-远视 | 1-否 | 2-正常 | 软材质 |
| 1-青年人 | 1-近视 | 2-是 | 1-不足 | 不适合佩戴 |
| 1-青年人 | 2-远视 | 2-是 | 2-正常 | 硬材质 |
| 2-中年人 | 1-近视 | 1-否 | 1-不足 | 不适合佩戴 |
| 3-老年人 | 2-远视 | 1-否 | 2-正常 | 软材质 |

### 训练算法

数据准备完成后，接下来的关键问题是排列出影响决策结果的所有特征的优先级。需要从当前的四类特征中找出对决策影响最大的特征。为了找到这个决定性的特征，需要借助数学计算来评估每个特征的重要性。具体来看，决策树的ID3算法中采用了较为符合统计学和信息论原理的指标——信息熵与信息增益，来评估特征的重要程度。



**阅读拓展**

#### 信息熵与信息增益

信息是很抽象的概念。人们常说信息量很大或很小，但却很难说清楚信息量到底有多少。比如，一本50万字的中文书籍到底包含多少信息量？直到1948年，克劳德·香农（Claude Shannon）提出了“信息熵”的概念，才解决了对信息的量化度量问题。信息熵这个词是香农从热力学中借用的。热力学中的热熵是表示分子状态混乱程度的物理量，香农则用信息熵的概念来描述信息量的不确定度。



微信公众号：电子课本大全

信息熵是度量样本集合纯度的一种指标。假设当前样本集合$D$中第$k$类样本所占的比例为$p_k(k=1, 2, \cdots, |y|)$，则$D$的信息熵定义为：

$$\mathrm{Ent}(D)=-\sum_{k=1}^{|y|}p_k\log_2 p_k$$

计算得到的值越小，$D$的纯度越高。

假定离散特征$a$有$V$个可能的取值$\{a^1, a^2, \cdots, a^V\}$，若使用$a$来对样本集进行划分，则会产生$V$个分支节点，其中第$v$个分支节点包含了$D$中所有在属性$a$上取值为$a^v$的样本，记为$D^v$。可根据上面的公式计算出$D^v$的信息熵。考虑到不同的分支节点所包含的样本数不同，需要给分支节点赋予权重，即样本数越多的分支节点影响越大，于是可计算出用属性$a$对样本集$D$进行划分所获得的信息增益$\mathrm{Gain}(D, a)$：

$$\mathrm{Gain}(D, a)=\mathrm{Ent}(D)-\sum_{v=1}^{V}\frac{|D^v|}{D}\mathrm{Ent}(D^v)$$

一般而言，信息增益越大，意味着使用特征$a$来进行划分所获得的“纯度提升”越大。因此，可以用信息增益来选择决策树的划分属性。著名的ID3决策树学习算法就是以信息增益为准则来选择决策树的划分属性的。

可以使用隐形眼镜数据集的24个样本数据来计算出4个特征（年龄、症状、是否散光及眼泪数量）的信息熵和信息增益。第一轮能够计算出4个特征的信息增益，并得出Gain(*D*, 眼泪数量)数值最大，即特征眼泪数量的信息增益最大，于是它被选为划分属性，因此它成为决策树的根节点。接下来基于眼泪数量对根节点进行划分，其结果大致可以生成一棵如图2.3.5所示的决策树。其中眼泪数量“不足”的样本数据，分类结果均为“不适合佩戴”，属于同一类别，因此无须再进行划分；而眼泪数量“正常”的样本数据，对应了12条数据，还需进一步划分。




图2.3.5　隐形眼镜决策树的第一层

下面对眼泪数量“正常”的12条数据计算剩余3个特征（年龄、症状、是否散光）的信息熵和信息增益。第二轮能够计算出这3个特征的信息增益，并得出Gain(*D*, 是否散光)数值最大，即特征“是否散光”的信息增益数值最大，从而将决策树进一步构造，如图2.3.6所示。



微信公众号：电子课本大全

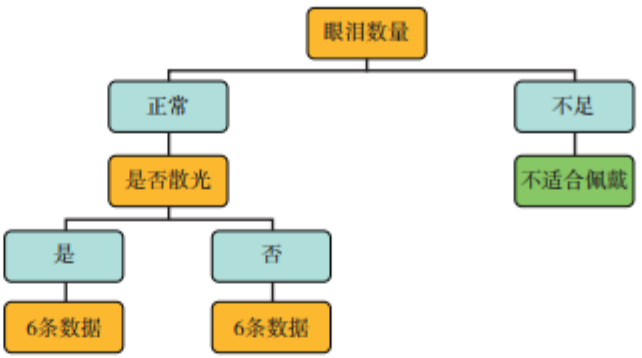



图2.3.6　隐形眼镜决策树的第一层和第二层

接下来第三轮需要再对特征“是否散光”分别为“是”和“否”的各6条数据计算其信息熵和信息增益，从而继续构造这棵决策树。

通过观察上述构造过程，可以发现，决策树的构造是一个递归的过程，其中递归结束的条件有三种，分别为：

1. 当前决策节点包含的样本数据全部属于同一个类别，不需要继续划分；
2. 当前决策节点不存在任何样本数据，不能继续划分；
3. 已经遍历完所有划分数据集的特征。

## 实践活动

### 使用Python编程语言绘制决策树

访问教学资源平台，查看提供的程序，本程序分为两个文件，其中calTree.py文件用于生成决策树的结构，treePlotter.py用于绘制决策树的结构，下面节选程序的部分关键代码：

```
# calTree.py
def createDataSet():  # 此函数用于返回全部样本数据的特征值及特征名
    dataSet=[[1,1,1,1,"no lenses"],
             [1,1,1,2,"soft"],
             [1,1,2,1,"no lenses"],
             [1,1,2,2,"hard"],
             [1,2,1,1,"no lenses"],
             [1,2,1,2,"soft"],
             [1,2,2,1,"no lenses"],
             [1,2,2,2,"hard"],
             [2,1,1,1,"no lenses"],
             [2,1,1,2,"soft"],
             [2,1,2,1,"no lenses"],
             [2,1,2,2,"hard"],
             [2,2,1,1,"no lenses"],
             [2,2,1,2,"soft"],
             [2,2,2,1,"no lenses"],
             [2,2,2,2,"no lenses"],
             [3,1,1,1,"no lenses"],
             [3,1,1,2,"no lenses"],
             [3,1,2,1,"no lenses"],
```



微信公众号：电子课本大全

```
                [3,1,2,2,"hard"],
                [3,2,1,1,"no lenses"],
                [3,2,1,2,"soft"],
                [3,2,2,1,"no lenses"],
                [3,2,2,2,"no lenses"]]
        labels=["age","prescript","astigmatic","tearRate"]
        # age代表"年龄"，有3个值：1（青年人）、2（中年人）、3（老年人）
        # prescript代表"症状"，有2个值：1（近视）、2（远视）
        # astigmatic代表"是否散光"，有2个值：1（否）、2（是）
        # tearRate代表"眼泪数量"，有2个值：1（不足）、2（正常）
        return dataSet, labels

    def calcShannonEnt(dataSet):
        numEntries=len(dataSet)
        labelCounts={}
        for featVec in dataSet:
            currentLabel=featVec[-1]
            if currentLabel not in labelCounts.keys():
                labelCounts[currentLabel]=0
                labelCounts[currentLabel]+=1
        shannonEnt=0.0
        # 计算给定数据集的信息熵
        for key in labelCounts:
            prob=float(labelCounts[key])/numEntries
            shannonEnt-=prob*log(prob,2)
        return shannonEnt
```

程序绘制出的决策树如图2.3.7所示，图中的数字含义在程序的注释中进行了说明。

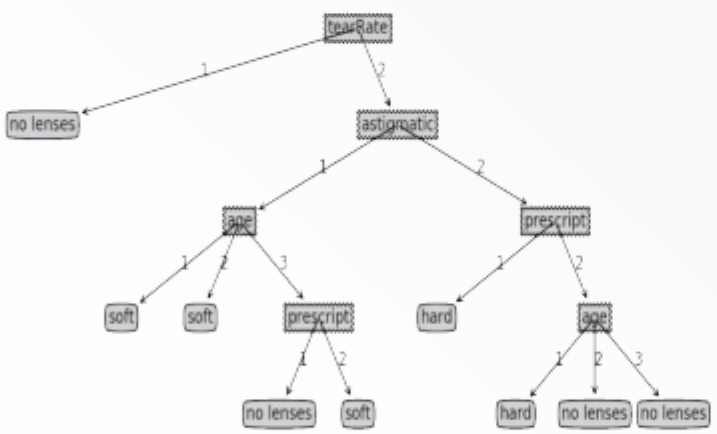



图 2.3.7　借助 Python 编程语言绘制的决策树

### 测试算法

构造出一棵决策树后，如何来验证这棵决策树的优劣呢？一般我们会多提供一些样本数据，但不用在训练算法阶段，而是用在测试算法阶段，只提供数据的特征值，然后使用训练好的决策树来求解最终的分类结果，并与这些样本数据的真实分类结果相比较，得出



微信公众号：电子课本大全

错误率，进而评估算法的优劣。

例如，在隐形眼镜问题中，一共只有24个样本数据，可以采用留出法，即使用部分数据来训练算法，比如只使用16个数据来训练，剩余的8个样本数据用于测试算法，根据其特征值求解最终的分类结果，计算得出错误率。



**阅读拓展**

### 决策树的剪枝

可以使用的训练数据终归是有限的，通过训练数据生成的决策树也未必与实际情况完全一致，这就影响到应对其他数据时决策的准确性，即泛化能力。所谓泛化能力就是应对一般性数据时，能给出正确结论的能力。因为决策树算法在学习的过程中为了尽可能正确地分类训练样本，不停地对节点进行划分，可能会导致整棵树的分支过多。这个问题可通过以下两种剪枝策略来解决。

■ 预剪枝：在构造决策树的过程中，先对每个节点在划分前进行评估，若当前节点的划分不能提升决策树的泛化性能，则不对当前节点进行划分，并将其标记为叶子节点。例如，可以指定树的高度或者深度，或指定每个节点所包含的最小样本数目，小于该数目则标记为叶子节点。

■ 后剪枝：先把整棵决策树构造完毕，然后自下而上对非叶子节点进行分析，若将该节点对应的子树换为叶子节点能够带来泛化能力的提升，则把该子树替换为叶子节点。

### 使用算法

生成的决策树可用于执行实际任务，当患者向医生咨询什么样的隐形眼镜适合自己时，医生可以就前述特征信息（年龄、症状、是否散光及眼泪数量）询问患者，然后将患者的回答输入决策树中，得到一个分类结果（不适合佩戴、软材质、硬材质），从而为患者推荐适合的隐形眼镜。



**阅读拓展**

### 监督学习

决策树又被称为分类树，是一种十分常用的分类方法，属于监督学习的方法。所谓监督学习就是给定一些样本，每个样本都有一组属性和一个类别，这些类别是事先确定的，那么机器通过学习就可以得到一个分类器，分类器能够为新出现的对象进行正确的分类。



微信公众号：电子课本大全

## 项目实施

### 手机消息分类

一、项目活动

每天我们的手机都会收到很多不同类型的消息，将这些消息进行合理分类，就可以帮助我们改善使用手机收发消息的体验。

1. 分析手机中已经收到的消息，并按照学习类、生活类、垃圾类等进行分类，寻找能够区分各类消息的特征。

2. 基于找到的特征，设计一棵决策树，当手机收到一条信息时，使用这棵决策树，就可以将该信息分类。

二、项目检查

在学习决策树算法后，尝试分析手机中的消息，找到用于分类的特征并构造一棵决策树，用该决策树完成对手机新消息的分类。



## 练习提升

1. 决策树给出的结论是最优答案吗，为什么？

2. 生活中，我们需要决策或分类的场景有哪些？尝试收集一些数据，通过ID3算法构造决策树。



微信公众号：电子课本大全

# 2.4
# 使用 K-均值算法进行聚类

**学习目标** ▶▶▶

- 通过剖析案例，了解聚类的基本概念，能举例说明算法的应用场景。
- 了解一种基于距离的聚类经典算法——K-均值算法，能解释算法的关键环节。

## 体验探索

### 手机上的推送消息，你感兴趣吗

每天我们的手机都能收到很多推送消息，如图2.4.1所示。为了吸引用户打开手机应用，继续阅读这些推送消息，互联网公司“悄悄”地做了很多工作。

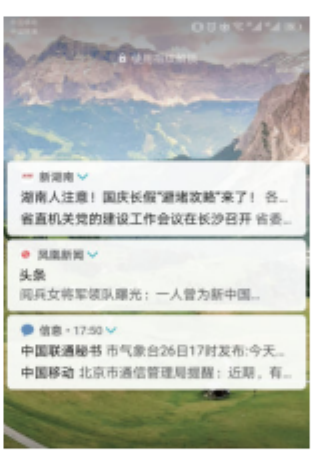



图2.4.1　手机推送消息界面

比如，用户在使用手机应用时，系统会记录他们的消费习惯、阅读偏好、评论风格及地理位置等信息，然后按照“物以类聚，人以群分”的思想，将这款手机应用的用户聚合为不同的类型，比如酷炫科技范等，然后对不同类型的用户“投其所好”，向他们推送该类人群可能感兴趣的消息，从而获得更多的阅读量和潜在的收益。

思考：

除了上面的案例，智能应用中还有哪些功能体现了“物以类聚，人以群分”的思想？



微信公众号：电子课本大全

### 2.4.1 认识基于距离的聚类

2.3节中，我们借助决策树解决了患者应佩戴何种隐形眼镜的问题，分类算法中样本数据的种类是已知的，即不适合佩戴、适合佩戴软材质或硬材质的隐形眼镜。聚类算法不同于分类算法，它在操作时并不知道样本数据有多少种类，而是通过数据分析，发现数据之间的内在联系和相关性，将看似没有关联的事物聚合在一起，并将数据划分成若干集合，方便为数据打上标签，从而进行后续的分析和处理。其中，被划分的数据集合称作“簇”。

**实践活动**

**办事处选址**

一家大型外企拟在我国设立4个办事处，每个办事处承接周边几个省份的业务。为降低管理成本，该企业希望对接的省会城市和直辖市离这4个办事处的距离之和尽可能小一些。

图2.4.2按照经纬度坐标展示了该企业对接的我国部分省会城市和直辖市的位置，其中每一个点代表一座城市。

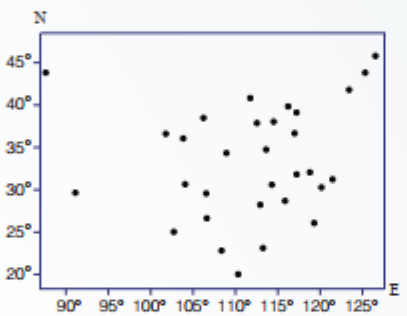



图2.4.2 我国部分省会城市和直辖市的地理位置

尝试将这些城市划分为4类，按选址要求指出4个办事处的位置，并说明理由。

在机器学习中，有很多种划分数据集的方法，其中最常用的一种是基于数据间距离的K-均值聚类算法，又称作K-均值算法。所谓基于距离，指的是如果把数据呈现在坐标系中，数据集中的每个样本都是空间中的一个点坐标，通过简单的计算就可以知道各个点之间的距离，距离越近，即相似程度越高。

K-均值算法是一个迭代算法，需要经过多次重复计算才能得到最终的结果。值得注意的是，由于样本数据不同，特征值的波动范围和计量单位很可能不一致。为了消除不同量纲的特征值对计算结果产生的影响，可以在使用K-均值算法之前，对样本数据作归一化处理。例如，选出样本数据中每种特征值的最大值和最小值，将最大值与最小值的差作为分母，每个特征值与最小值的差作为分子，使得所有数据通过归一化处理后，都分布在区间[0, 1]中，然后再代入算法进行计算。



微信公众号：电子课本大全

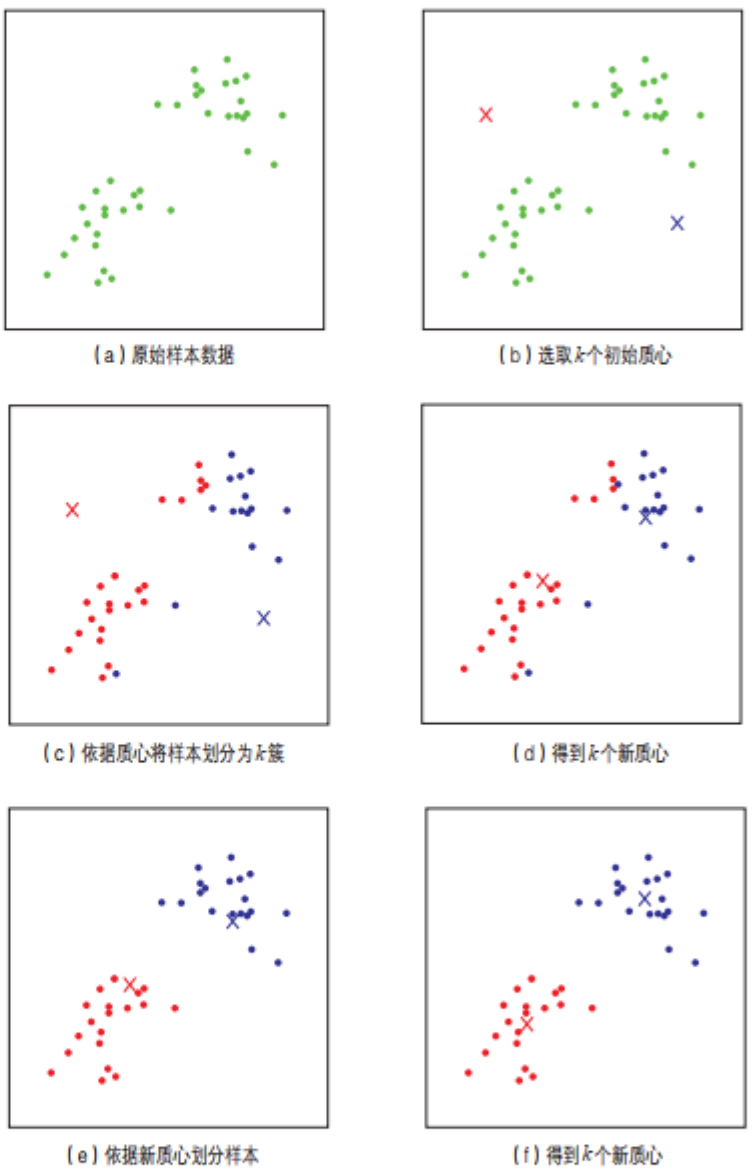
K-均值算法的具体步骤如下：

1. 在空间中找出$k$个点，将这$k$个点称为质心，通过计算其他样本点到这$k$个质心的距离（即每两个点在坐标系中的直线距离），对样本点进行划分，从而把距离近的点划分在一起，组成$k$个簇；

2. 分别计算$k$个簇中所有样本点的几何中心，得到$k$个新的质心；

3. 重复上述过程，直到$k$个新质心与上一轮的质心位置完全相同。

图2.4.3展示了利用K−均值算法对$n$个样本点进行聚类的分步演示过程，这里$k$值取2。



(a) 原始样本数据　(b) 选取$k$个初始质心

(c) 依据质心将样本划分为$k$簇　(d) 得到$k$个新质心

(e) 依据新质心划分样本　(f) 得到$k$个新质心

图2.4.3　聚类算法的分步演示

以“办事处选址”实践活动为例，在使用K-均值算法之前，需要对样本数据进行归一化处理，得到如图2.4.4所示的结果。



微信公众号：电子课本大全

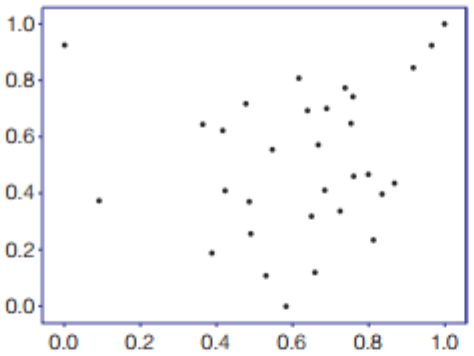



图2.4.4　归一化处理后的城市位置散点图

需要注意的是，$k$值的大小会给分组结果带来显著的区别，如果事先并不知道将数据划分为几簇最合适，那么$k$值的选定是比较困难的，这也是K-均值算法的一个不足之处。

“办事处选址”活动中，当$k$的取值依次为2、3、4、5时，得到的聚类结果如图2.4.5所示，其中相同颜色的点代表归属于同一个办事处管辖，大头钉标志代表推荐的办事处选址地。实际确定办事处所在的城市时，可选择最靠近推荐地的城市，即在相同颜色的点中，寻找最接近大头钉标志的那个点的位置，作为最终的选址地。

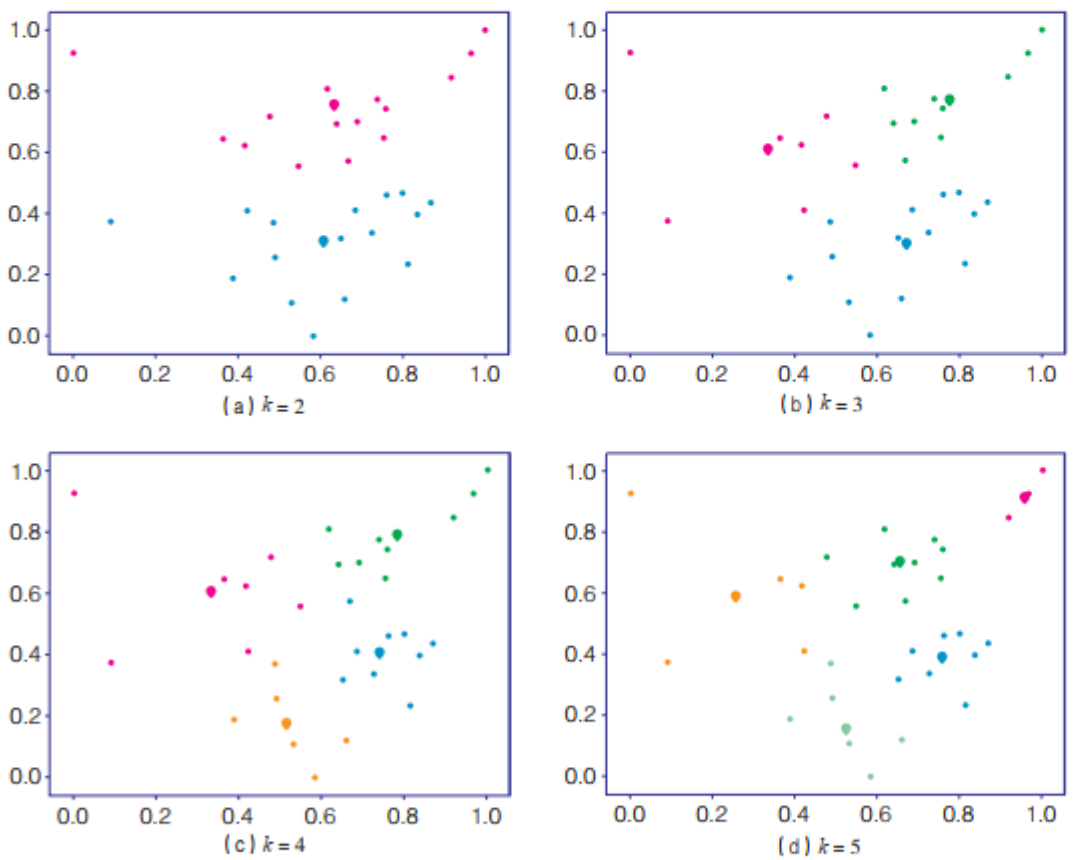



图2.4.5　$k$的取值依次为2、3、4、5时得到的聚类图

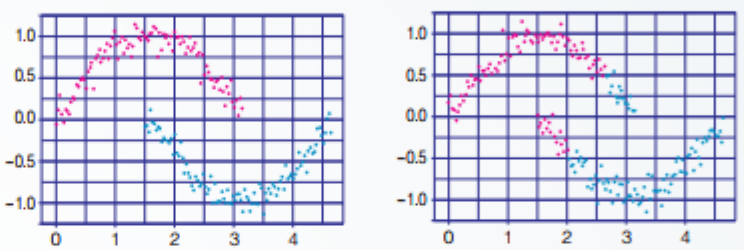


微信公众号：电子课本大全

## 阅读拓展

### 基于密度的聚类和基于层次的聚类

除了基于距离的聚类，常见的聚类方法还有两种。一种是基于密度的聚类，这种方法通过分析样本分布的紧密程度来确定聚类结果。通常，密度聚类算法从样本密度的角度来考察样本之间的可连接性，并基于可连接样本不断扩展聚类簇以获得最终结果。具有噪声的基于密度的聚类方法（Density-Based Spatial Clustering of Applications with Noise，DBSCAN）是一种典型的密度聚类算法。通过图2.4.6能够明显看出两种聚类算法结果的差异。




（a）基于密度的聚类　　（b）基于距离的聚类

图2.4.6　基于密度和距离的聚类结果对比

另一种是基于层次的聚类，这种算法在不同层次对数据集进行划分。以凝聚的层次聚类算法（Agglomerative Nesting，AGNES）为例，它先将数据集中的每个样本看作一个初始聚类簇，然后再逐步将它们两两合并，直到获得最终的聚类结果，如图2.4.7所示。

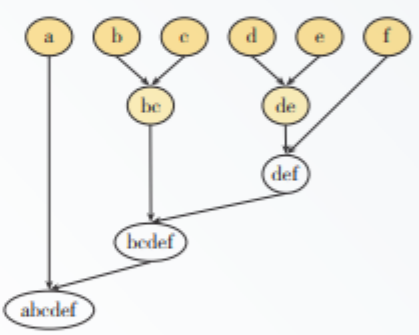



图2.4.7　基于层次的聚类

## 2.4.2　K-均值聚类算法的一般流程

类似决策树的构造过程，K-均值聚类算法的一般流程也可以概括为如图2.4.8所示的4个环节。

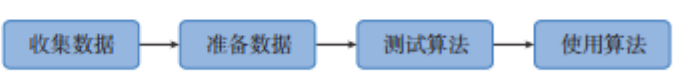



图2.4.8　K-均值聚类算法的一般流程示意图

K-均值聚类算法除了可以用于研究城市之间的距离关系，还可用于分析城市人口与国内生产总值（Gross Domestic Product，GDP）之间的关系，从而将我国部分省会和直辖市聚合成几类。下面通过一个实例来详细介绍这个流程。



微信公众号：电子课本大全

### 收集数据

我们可以通过国家统计局等网站获取相关城市2016年的城市人口和GDP数据。

### 准备数据

由于样本数据计量单位不一致，可以先对样本数据作归一化处理，使所有样本数据集中分布在区间[0, 1]中。归一化后借助Python编程语言绘制散点图，图中的横轴为归一化后的城市人口，纵轴为归一化后的GDP数据，如图2.4.9所示。下面将这些城市的人口和GDP数据进行聚类。

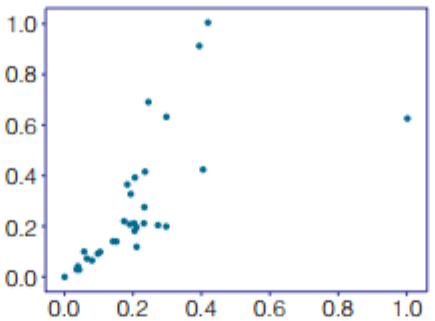



图2.4.9　城市人口和GDP散点图

### 测试算法

不同于决策树的分类算法，由于获得的样本数据本身并没有类型，无须进行训练，所以可直接进入测试环节。

## 实践活动

### 借助Python编程语言完成对城市的聚类

以城市人口和GDP两个特征为例，借助Python编程语言实现对这些城市的聚类分析，当前尝试的簇数（即聚类的数量）为3。具体代码如下：

```
import matplotlib.pyplot as plt
import numpy as np
from sklearn.cluster import KMeans
# X为31个城市的人口，Y为对应城市的GDP归一化后处理的数据
X=[0.41823906,0.392136188,0.244646275,0.296741185,1,0.402932005,
     0.233670728,0.204359665,0.182429538,0.192377626,0.231636776,
     0.173454991,0.202511435,0.230998733,0.18969964,0.272073162,
     0.294824059,0.209580838,0.203880383,0.140492402,0.151575788,
     0.209077593,0.056072947,0.104114932,0.094798896,0.064130868,
     0.081013561,0.03901951, 0.033924148,0.04478287,0]
Y=[1,0.909578903,0.689006871,0.629121162,0.62390384,0.423196907,
     0.413914541,0.392335797,0.363125277,0.325376797,0.273850333,
     0.220192983,0.210762169,0.210142431,0.207997132,0.204537053,
     0.198271942,0.197919196,0.181419414,0.141604183,0.139625708,
     0.118126232,0.099036885,0.098464349,0.091182437,0.073288607,
     0.066271524,0.042976612,0.030003927,0.029661631,0]
# 转化成数组
x1=np.array(X)
x2=np.array(Y)
XX=np.array(list(zip(x1,x2))).reshape(len(x1),2)
# 用K-均值聚类方法来做聚类，首先选择k=3，代码如下：
cluster=3    # 聚类簇数
# KMeans([n_clusters,init,n_init,…]): 属于sklearn模块，构造K-Means聚类器
k=KMeans(n_clusters=cluster)
y_pred=k.fit_predict(XX)     # 聚类
# 绘制聚类后的散点图
plt.scatter(x1,x2,c=y_pred)
plt.show()
```



微信公众号：电子课本大全

聚类得到的图像如图2.4.10所示，横轴为归一化后的城市人口，纵轴为归一化后的GDP。可以看出，如果将城市聚合为3类，得到的绿色点从上到下分别代表上海、北京、广州、天津和重庆，聚类结果基本符合人们对一线城市的认同。

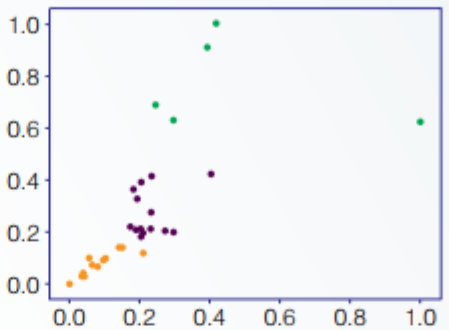



图2.4.10　借助Python编程语言绘制的聚类结果

试调整代码，将$k$值修改为4，然后观察聚类结果的变化。思考聚类时如何能够寻找到一个合适的$k$值。

应用K-均值算法得到结果后，如何评价结果的优劣呢？误差平方和（Sum of Squared Error，SSE）是一种能够评价聚类结果的指标，即求解所有点与其对应质心距离的平方之和。SSE的值越小，聚类的结果越好。

### 使用算法

当获得一个新的数据时，可以计算该数据与所有质心的距离，找出最近的质心，建议将这个新的数据聚合到最近质心所在的类。

K-均值算法是一种常用的聚类算法，它运算快，且较为简单，但是$k$值最初难以选定，且最初的质心选择会影响到最终的聚类结果。



微信公众号：电子课本大全

## 项目实施

### 手机照片的聚类

一、项目活动

手机的拍照功能可以捕捉生活中的美好瞬间，但随着手机中的照片越来越多，想快速从手机中找到一张需要的照片就越来越难。如果手机中的照片能自动聚类，就能大幅提升查找效率。

1. 浏览手机中的照片，选取一些照片中的特征，如照片中人物的数量、是否有动物或照片中面积最大的颜色等，整理出一张特征数据表。

2. 依据整理好的特征数据表，尝试进行照片的自动聚类，将聚类后的照片存储在一个文件夹中，方便查找。

二、项目检查

1. 在学习聚类算法后，能够分析手机中的照片，找到用于聚类的特征，实现聚类分析。

2. 基于所选照片的特征，填写表2.4.1。

表2.4.1　照片的特征统计

| 照片 | 人物的数量 | 是否出现动物<br>（1代表有动物，2代表没有） | … |
|---|---|---|---|
| 照片1 | | | |
| 照片2 | | | |
| ⋮ | | | |

3. 从众多特征中选取两个特征，实现对照片的聚类分析，并在班级里展示聚类结果。

## 练习提升

1. 生活中，有哪些需要聚类的场景？尝试收集一些数据并进行聚类分析。

2. 针对上题收集到的数据，观察$k$取不同数值时的差异，尝试找出最适合的$k$值。



微信公众号：电子课本大全

# 2.5
# 神经网络与深度学习

**学习目标** ▶▶▶

- 通过案例剖析，了解人工神经网络的基本原理。
- 了解卷积神经网络和循环神经网络的基本原理及应用场景。
- 初步认识深度学习（深度神经网络），了解常见的人工智能开源软硬件平台。

## 体验探索

### 图像识别技术

长期以来，图像识别技术一直是人工智能研究领域的难题。近年来，随着算力的提升、物联网与大数据的出现、机器学习算法的快速发展，科学家们终于找到了有效的方法来实现图像识别，这就是基于人工神经网络的深度学习。很多以人工智能技术应用为主要发展目标的公司，如百度、阿里巴巴、腾讯和微软等，都推出了基于深度学习算法的图像搜索引擎，为人们的生产和生活提供了便利。例如，遇到不知名的植物时，只需用手机对其拍照，上传到智能搜索引擎，就可以获得不错的参考信息，如图2.5.1所示。




图2.5.1　智能搜索引擎中的图像识别

思考：

1. 图像识别技术在生活中的应用越来越广泛。试了解还有哪些相关产品使用了这项技术，分享给组内的同学。

2. 小组同学设想并讨论，科研人员是如何“教会”计算机读懂并识别图像内容的？又是如何“教会”计算机对图像进行分类归纳的？



微信公众号：电子课本大全

### 2.5.1 人工神经网络

当前，新一代人工智能领域中最重要研究内容之一就是基于人工神经网络的深度学习。人工神经网络（Artificial Neural Network，ANN）是相对生物神经网络（Biological Neural Network，BNN）而言的，受生物神经网络的启发而生。生物神经网络最基本的结构和功能单位是神经元。神经元的树突较短且分支多，其作用是接收其他细胞传递过来的电信号；轴突则较长且分支少，用于将电信号传递给其他细胞，如图2.5.2所示。成千上万个神经元相互连接，共同组成复杂的生物神经网络。人类大脑皮层中约有140多亿个神经元，在接收外部信号过程中，脑细胞会不断地调整神经元的兴奋阈值，宏观上表现为学习、思考和判断等高级思维活动。

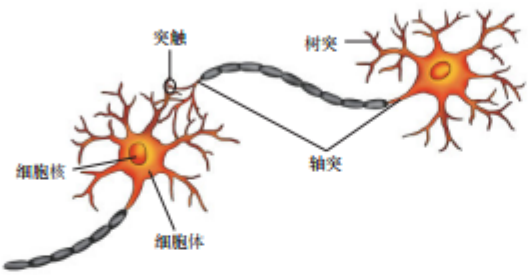



图 2.5.2　生物神经元的组成和结构

#### 人工神经网络的基本原理

1943年，心理学家沃伦·麦卡洛克（Warren McCulloch）和数学家沃尔特·皮茨（Walter Pitts）合作提出M-P神经元模型。M-P神经元模型是按照生物神经元的结构和工作原理构造出来的一个抽象和简化了的计算模型，如图2.5.3所示。

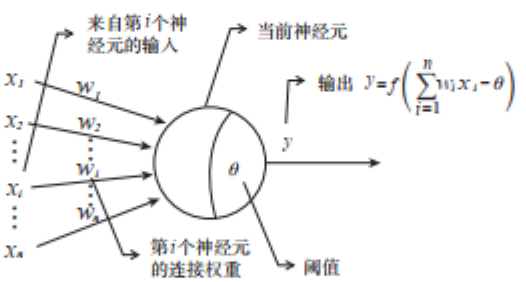



图 2.5.3　M-P神经元模型

在图2.5.3所示的模型中，神经元接收来自$n$个其他神经元传递过来的输入信号$(x_1, x_2, \cdots, x_n)$，这些输入数据通过加权计算之后，神经元将会判断其是否超过神经元阈值$\theta$。如果超过阈值，神经元将被激活，并通过“激活函数$f$”产生神经元的输出。

例如，针对“与运算”问题，建立一个最简单的人工神经网络模型，包含一个输入层和一个输出层。假设这个模型有两个输入端，每个输入端的权重为1，即$w_1=w_2=1$；神经元阈值$\theta=2$。此情况的激活函数$f$可以定义为一个阶跃函数：

$$f(x)=\begin{cases}1, & x\geqslant 0\\ 0, & x<0\end{cases}$$

该函数图像如图2.5.4所示。由此，得到一个模型$y=f(1\times x_1+1\times x_2-2)$，$x_1$、$x_2$属于集合$\{0, 1\}$。只有当$x_1=x_2=1$时，$y$=1。因此，这个模型可以看作一个与门（图2.5.5），即



微信公众号：电子课本大全

当输入端的两个条件都为“真”时，结果输出才为“真”，否则结果为“假”。

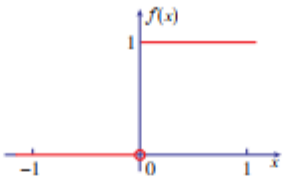


图2.5.4　函数$f(x)$的图像

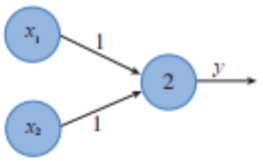


图2.5.5　与门的人工神经网络模型示意图

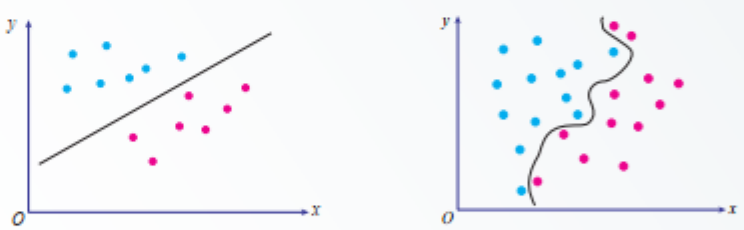
图2.5.3所示的模型也称为感知机，是只有一层的人工神经元模型。输入层被称为第零层，因为它只是缓冲输入。存在的唯一一层神经元形成输出层。输出层的每个神经元都有自己的权重和阈值。感知机只需通过适当地调整参数便可执行类似与、或、非的逻辑操作，但感知机有明显的局限性，比如无法解决非线性问题。

## 阅读拓展

### 线性与非线性

在平面坐标中，如果两个变量之间的关系可以用一次函数来描述，则这两个变量为线性关系，否则就为非线性关系。比如$y=kx$中，$y$与$x$为线性关系，而在$y=x^2$中，$y$与$x$则为非线性关系。

在分类问题中，如果可以用线性函数来划分类别，则该问题为线性问题，否则该问题为非线性问题。图2.5.6(a)是一个线性问题，可以用一条直线将红色和蓝色的点划分为两类，而图2.5.6(b)是一个非线性分类问题，必须用一条曲线才可以对不同颜色的点进行划分。



(a)线性分类问题示例　　(b)非线性分类问题示例

图2.5.6　线性与非线性分类问题示例

将问题扩展到三维空间，线性问题可以用一个平面进行表达和处理，而非线性问题则必须涉及曲面。

### 人工神经网络的相关概念

多层感知机（即多层人工神经网络）在感知机的基础上，增加了若干隐藏层，通过前向传播算法将输入信息进行前向传播，在学习过程中利用反向传播学习算法将误差进行前向传播，以调整每一层的连接参数。图2.5.7所示的是具有一层隐藏层的多层感知机，感知机每层中所有的神经元都与上层所有神经元相连。这种连接方式也称为全连接人工神经网络。


微信公众号：电子课本大全

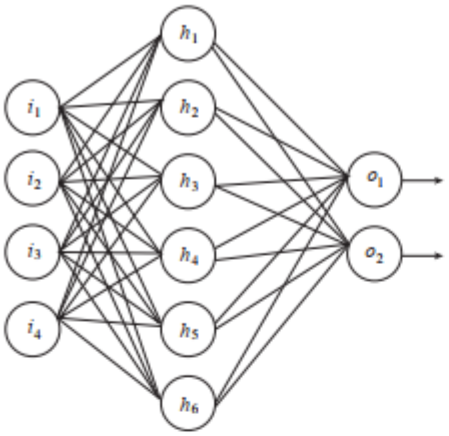



图2.5.7　具有一层隐藏层的多层感知机示意图

欲理解人工神经网络（以下简称神经网络或神经网络模型）具体的训练和工作过程，需要先了解前向传播、激活函数、损失函数、误差反向传播以及优化器与梯度下降等概念。

■ 前向传播

前向传播是指信息从神经网络第一层逐渐向高层进行传递的过程，图2.5.7中$h_1$神经元的输入来自于$i_1$、$i_2$、$i_3$、$i_4$的输出，其本身的输出又可继续传递给$o_1$和$o_2$。在具体的传递过程中，$h_1$神经元的输出满足如下关系：

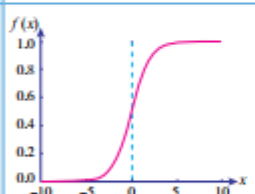
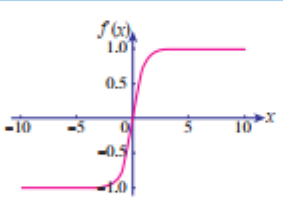
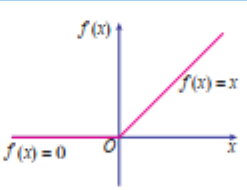
$$h_{1_out}=f(i_1\times w_1+i_2\times w_2+i_3\times w_3+i_4\times w_4+b)$$

式中：$i_1$, $i_2$,…, $i_4$表示来自上层的输入值；$w_1$, $w_2$,…, $w_4$表示对应不同输入值的权重；$b$为偏置项；函数$f$称为激活函数。

■ 激活函数

激活函数为神经元引入非线性因素，可以提升神经网络的表达能力，使得神经网络可以拟合任意非线性函数，解决非线性问题。常用的激活函数有Sigmoid、Tanh和ReLU等，表2.5.1描述了不同的激活函数及其函数图像。

表2.5.1　常用激活函数及其函数图像

| 函数名称 | Sigmoid | Tanh | ReLU |
|---|---|---|---|
| 函数表达式 | $f(x)=\frac{1}{1+e^{-x}}$ | $f(x)=\frac{e^{x}-e^{-x}}{e^{x}+e^{-x}}$ | $f(x)=\max(0,x)$ |
| 函数图像 |  |  |  |



■ 损失函数

损失函数（Loss Function）又称代价函数（Cost Function），用来评估神经网络模型的预测值与真实值的不一致程度。常用的损失函数包括均方误差（Mean Squared Error）、平均绝对误差（Mean Absolute Error）和交叉熵（Cross Entropy）等。不同的损失函数适合处理不同类型的问题，比如均方误差善于处理数值预测问题，交叉熵常用于解决分类问题。神经网络训练的目标是使损失函数的值最小化，得到最优模型。

■ 误差反向传播

神经网络作为一种计算模型在最初生成时，每个神经元中每个输入的权重、偏置都是随机的，这些权重和偏置都成为模型的参数。所谓模型训练的过程，就是对模型参数不



微信公众号：电子课本大全

断进行调整的过程。但是参数的组合情况非常复杂，误差反向传播正是将输出层的误差逐层传播回输入层，使得每一层都更新参数，以实现损失函数值进一步减小的算法。这种有效的算法也称为BP算法（Back Propagation Algorithm），是训练神经网络最常用、最基础的算法之一。

■ 优化器与梯度下降

优化器（Optimizer）的作用是在误差反向传播过程中控制每一层如何朝正确的方向寻找最优的参数组合。常见的优化方法有批量梯度下降法（Batch Gradient Descent，BGD）、随机梯度下降法（Stochastic Gradient Descent，SGD）、动量优化法（Momentum）和Adam优化法等。在所有的优化方法中，梯度下降（Gradient Descend）是核心。在单变量函数中，梯度表示函数在某个点的切线的斜率；在多变量函数中，梯度是一个向量，不仅具有大小，还具有方向。结合前文关于损失函数的概念，优化器的作用可以理解为根据当前的输入值，计算不同方向上损失函数的下降梯度，寻找一条最快到达损失函数最小值位置的路径。如图2.5.8所示，在红点处向右移动会更接近最小值位置。

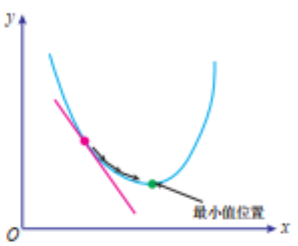


图2.5.8　损失函数的下降梯度示意图

## 阅读拓展

### 学习速率

学习速率（Learn Rate）是在模型梯度下降的过程中用于控制参数变化程度的一个重要参数。较高的学习速率可以让模型的损失函数更快地趋向最小值，但容易在最小值点附近震荡，很难进一步拟合；较小的学习速率可以解决在最小值点附近的震荡问题，但模型训练速度缓慢。图2.5.9为不同学习速率的梯度下降过程比较。

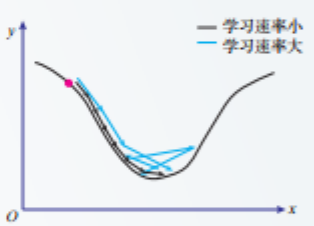


图2.5.9　不同学习速率的梯度下降过程

### 人工神经网络的实现过程

神经网络模型的计算和优化过程需要应用线性代数、微积分和统计学等交叉学科知识，若要从底层开始神经网络模型程序的开发难度很大，通常会基于某个开源的神经网络模型框架来开展。

Keras是一个基于Python编程语言编写的开源神经网络库，可以快速实现包括神经网络模型的搭建、编译、训练、评估和测试等工作。下面通过具体的Keras应用案例来初步体验神经网络的训练、评估和测试等过程。

■ 数据采集与预处理

某企业为了提高产品销售额，计划在各种媒体做广告，常见的媒体主要有电视、广播以及报纸等。在投入资金之前，决策者需要确定在不同媒体的最佳广告投入，以期获得


微信公众号：电子课本大全

最高的产品收益。为了寻求各媒体广告投入与收益之间的关系，该企业收集了200个不同产品在各个媒体中的广告投入资金与最终的销售业绩数据，这些数据被制成表格保存在Advertising.csv文件中，如图2.5.10所示。

| S/N | TV | radio | newspaper | sales |
|---|---|---|---|---|
| 1 | 230.1 | 37.8 | 69.2 | 22.1 |
| 2 | 44.5 | 39.3 | 45.1 | 10.4 |
| 3 | 17.2 | 45.9 | 69.3 | 9.3 |
| 4 | 151.5 | 41.3 | 58.5 | 18.5 |
| 5 | 180.8 | 10.8 | 58.4 | 12.9 |
| 6 | 8.7 | 48.9 | 75 | 7.2 |
| 7 | 57.5 | 32.8 | 23.5 | 11.8 |
| 8 | 120.2 | 19.6 | 11.6 | 13.2 |
| 9 | 8.6 | 2.1 | 1 | 4.8 |

图2.5.10　不同产品在各个媒体中的广告投入资金与销售额（局部）

为了处理这些数据，需在Python编程语言中引用pandas模块，并将文件中的数据读取出来：

```
from pandas import pd
data=pd.read_csv('Advertising.csv')
```

其中当前变量data是一种pandas定义的DataFrame数据结构，可以通过data.head()函数查看最前面的5行数据：

```
Unnamed:  S/N     TV  radio  newspaper  sales
           1  230.1   37.8       69.2   22.1
           2   44.5   39.3       45.1   10.4
           3   17.2   45.9       69.3    9.3
           4  151.5   41.3       58.5   18.5
           5  180.8   10.8       58.4   12.9
```

data数据总共有5列，第1列表示数据的行号，没有列名；第2列到第4列分别表示在电视、广播、报纸上的广告投入，第5列则是对应的销售额。需要注意的是，以上数据并不一定为同一个量纲。接着，需要提取出输入数据$x$，以及标签数据（真实结果）$y$：

```
x=data.iloc[:,1:-1]
y=data.iloc[:,-1]
```

此时$x$与$y$的形状分别是(200, 3)和(200, 1)，即$x$具有200行、3列，$y$具有200行、1列。可以发现$x$与$y$的行数一定是相同的。

■ 模型搭建与编译

对数据的预处理完成后，开始搭建神经网络模型。首先引入Keras库，为了调用方便，还可以直接导入Keras中的layers子包：

```
import keras
from keras import layers
```

Keras支持建立序惯模型与函数式模型。一般情况下，建立一个序贯模型即可，代码



微信公众号：电子课本大全

如下：

```
model=keras.models.Sequential()
```

接着，对模型添加神经网络层。Keras支持很多类型的神经网络层，这里使用add方法添加2个全连接神经网络层（Dense层）：

```
model.add(layers.Dense(units=32,input_dim=3,activation='relu'))
model.add(layers.Dense(units=1))
```

第一层通过input_dim参数指定接收输入数据的维度为3，units=32表示将这个三维数据全连接到32个神经元（神经元数量可自定义，神经元数量越多，模型的拟合能力越强），并通过ReLU激活函数进行激活；从第二层开始，输入数据维度默认为前一层的输出维度，因此不再需要指定输入数据的维度，只需指定神经元个数即可。在上述代码中，第一层的32个神经元输出再次全连接到第二层的1个神经元中，最后这1个神经元的输出就是模型的预测结果。

模型搭建完后，需要对模型进行编译，同时指定训练模型所需要的优化器以及损失的估算方法：

```
model.compile(optimizer='adam',loss='mse')
```

在Keras库的compile方法中，可以通过optimizer参数方便地指定优化器，经验证明，Adam优化器具有非常良好的表现。loss='mse'表示使用均方误差作为损失的估算方法。

■ 模型训练与测试

模型的搭建与编译完成后，接下来需要对模型进行训练。以下代码是利用现有数据$x$和$y$对模型进行2 000次训练，并将整个训练过程记录到变量history中，其中，batch_size表示每次参与训练的数据行数，epochs表示训练轮次。

```
history=model.fit(x,y,batch_size=200,epochs=2000)
```

程序运行后，控制台会打印出每轮次的训练情况：

```
Epoch 1/2000
200/200 [==============================] - 1s 6ms/step - loss: 2849.5693
Epoch 2/2000
200/200 [==============================] - 0s 31us/step - loss: 2692.2920
Epoch 3/2000
200/200 [==============================] - 0s 30us/step - loss: 2539.6829
Epoch 4/2000
200/200 [==============================] - 0s 18us/step - loss: 2391.9819
Epoch 5/2000
200/200 [==============================] - 0s 42us/step - loss: 2249.1899
                                ⋮
Epoch 1996/2000
200/200 [==============================] - 0s 16us/step - loss: 0.3596
Epoch 1997/2000
200/200 [==============================] - 0s 33us/step - loss: 0.3596
Epoch 1998/2000
200/200 [==============================] - 0s 16us/step - loss: 0.3595
Epoch 1999/2000
200/200 [==============================] - 0s 16us/step - loss: 0.3595
Epoch 2000/2000
200/200 [==============================] - 0s 21us/step - loss: 0.3595
```

可以看出，训练开始时的loss值非常大，随着训练次数的不断增加，loss的值逐渐减小。history中记录的训练过程数据可以通过绘图表现出来：


微信公众号：电子课本大全

```
import matplotlib.pyplot as plt
plt.plot(range(2000),history.history['loss'])
```

绘制的图像如图2.5.11所示，从图中可以发现，训练大约100个轮次后，loss值已经非常小了，在后面的训练过程中，loss值进一步下降幅度很小。这时可称模型已经收敛，说明该模型在经过几百个训练轮次后已经得到了充分的优化，因此可以适当地减少训练轮次，以缩短训练时间。

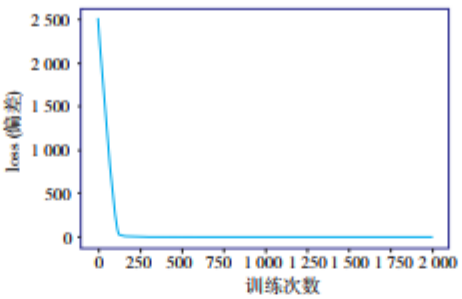



图2.5.11　训练过程中loss值的变化

只通过loss值评价一个模型的训练效果还不够理想。为了让模型更好地用于对未知数据的预测，可以把已有的数据分割成三个数据集，分别是训练集、验证集和测试集。

训练集用于神经网络的训练，训练集中的数据可作为神经网络模型进行参数调整的依据，类似于教师在课堂上讲解的题目。

验证集也参与神经网络的训练过程，但是与训练集不同，验证集的数据不参与神经网络模型的参数调整，类似于学生的课后作业。

测试集不参与训练过程，但可以用于评价整个神经网络模型最后的训练结果是否良好，类似于学生的期末考试。

以上面的200组数据为例，可以先将其先后顺序随机打乱，然后取前160组作为训练集数据，之后的20组为验证集数据，最后的20组为测试集数据：

```
data=data.sample(frac=1).reset_index(drop=True)    #打乱数据的先后顺序
x=data.iloc[:,1:-1]
y=data.iloc[:,-1]
x_train,y_train=x[:160],y[:160]
x_val,y_val=x[160:180],y[160:180]
x_test,y_test=x[180:],y[180:]
```

修改模型的训练参数为：

```
history=model.fit(x_train,y_train,batch_size=160,epochs=500,
                                                validation_data=(x_val,y_val))
```

最后绘制训练过程中的训练集loss值以及验证集loss值的变化图像，如图2.5.12所示。

```
plt.plot(range(500),history.history['loss'])
plt.plot(range(500),history.history['val_loss'])
print("test_loss:",model.evaluate(x_test,y_test))
```

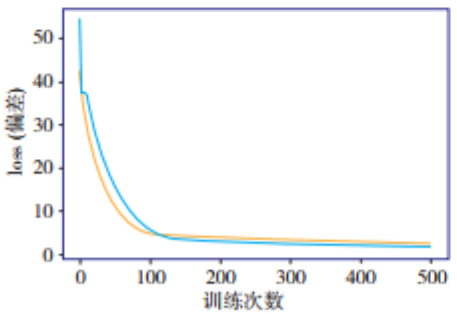



图2.5.12　经过改进后训练过程中loss值的变化



微信公众号：电子课本大全

打印出的测试集loss值为：

test_loss: 2.198000431060791

图2.5.12是经过改进后的训练过程数据图像，其中蓝色曲线表示训练集上loss值的变化，橙色曲线表示验证集上loss值的变化。从图中可以发现：首先，该模型的训练过程中，训练集loss值成功下降到一个较小的值，表示模型收敛较好，没有欠拟合；其次，尽管最后的测试集loss值与训练集loss值有一定差距，不过差距较小，说明该模型也没有过拟合；最后，该模型在验证集上依然表现较好。

当成功训练出一个神经网络模型后，便可以使用该模型进行预测了，假设需要预测如表2.5.2所示三种情况的销售额。

表2.5.2　各个媒体中广告投入资金的三种情况

| TV | radio | newspaper |
|---|---|---|
| 100 | 50 | 0 |
| 50 | 100 | 0 |
| 0 | 0 | 150 |

可以通过pandas库中的DataFrame方法构造x_input，并运用模型的predict方法进行预测：

```
x_input=pd.DataFrame({'TV':[100,50, 0], 'radio': [50,100,0],
                                                    'newspaper':[0,0,150]})
model.predict(x_input)
```

预测结果为：

```
array([[10.005433],[16.689125],[26.042202]],dtype=float32)
```

表示表2.5.2中三种情况的销售额预测值分别为10.005 433、16.689 125、26.042 202。



## 阅读拓展

### 欠拟合与过拟合

欠拟合指由于模型的复杂度不够或者训练样本过少、训练参数不正确等原因，导致模型无法有效地提取训练集中的特征。比如单层感知机由于层数太少、模型简单，导致无法处理“异或”问题。

过拟合指模型经过训练集训练后，过度地记录了训练集中的特征，使得模型对新数据的预测能力不足。可以理解为学生通过“死记硬背”的方式学习，做过的习题可以轻松答对，而没有做过的习题就难以应付。过拟合也称为泛化能力不足。



微信公众号：电子课本大全

## 实践活动

### 利用IRIS数据集搭建鸢尾花分类模型

IRIS数据集又称鸢尾花卉数据集。数据集中包括150条不同鸢尾花的花萼长度、花萼宽度、花瓣长度和花瓣宽度数据，并根据这四个属性将这些鸢尾花分为三类，即山鸢尾（Setosa）、变色鸢尾（Versicolor）和维吉尼亚鸢尾（Virginica），如图2.5.13所示。

| S/N | Sepal.Length | Sepal.Width | Petal.Length | Petal.Width | Species |
|---|---|---|---|---|---|
| 1 | 5.1 | 3.5 | 1.4 | 0.2 | setosa |
| 2 | 4.9 | 3 | 1.4 | 0.2 | setosa |
| 3 | 4.7 | 3.2 | 1.3 | 0.2 | setosa |
| 4 | 4.6 | 3.1 | 1.5 | 0.2 | setosa |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 51 | 7 | 3.2 | 4.7 | 1.4 | versicolor |
| 52 | 6.4 | 3.2 | 4.5 | 1.5 | versicolor |
| 53 | 6.9 | 3.1 | 4.9 | 1.5 | versicolor |
| 54 | 5.5 | 2.3 | 4 | 1.3 | versicolor |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 146 | 6.7 | 3 | 5.2 | 2.3 | virginica |
| 147 | 6.3 | 2.5 | 5 | 1.9 | virginica |
| 148 | 6.5 | 3 | 5.2 | 2 | virginica |
| 149 | 6.2 | 3.4 | 5.4 | 2.3 | virginica |
| 150 | 5.9 | 3 | 5.1 | 1.8 | virginica |

图2.5.13　IRIS数据集中的数据（局部）

鸢尾花分类属于比较典型的多分类问题，因此在对数据进行预处理时，首先需要对分类结果标签“Species”进行独热编码化。所谓独热编码（One-Hot），指用0和1构成的数组来表示一种情况。鸢尾花分类中，顺序编码用0、1、2表示不同的鸢尾花品种，而独热编码用[1, 0, 0]表示setosa、[0, 1, 0]表示versicolor、[0, 0, 1]表示virginica。与顺序编码相比，独热编码避免了神经网络把没有数值大小意义的数据错误地理解为有数值大小意义。如果用顺序编码来表示鸢尾花品种，神经网络会错误地认为2表示的品种与0表示的品种之间的差距比较大，而与1表示的品种差距比较小。

在pandas库中，可以调用get_dummies方法方便地把数据独热编码化：

```
import pandas as pd
data=pd.read_scv('./iris.csv')
data=pd.get_dummies(data,columns=['Species']) #对“Species”进行独热编码
```

随后，进一步整理得到输入数据x_data与标签数据y_data：

```
x_data=data[['Sepal.Length', 'Sepal.Width', 'Petal.Length','Petal.Width']]
y_data=data.iloc[:,-3:]
```

以小组为单位，运用所学的知识，利用IRIS数据集训练一个可以用于鸢尾花分类的神经网络模型。



微信公众号：电子课本大全

## 技术支持

### 二分类问题与多分类问题

二分类问题是指最终输出为“是”或“否”的一类问题。在神经网络中，一般通过输出一个0~1的值来表示“是”的概率。比如判断一封电子邮件是否是垃圾邮件，这是一个二分类问题，神经网络最后的输出值表示模型预测某封邮件是垃圾邮件的概率。在二分类的神经网络模型中，一般在最后一层设置一个神经元，并通过Sigmoid函数进行激活，而损失函数会采用二元交叉熵。在Keras框架下使用Python编程语言对模型进行编译时，可通过loss='binary_crossentropy'指定该损失估算方法。

多分类问题是二分类问题的扩展。当分类数大于2时，就是多分类问题。比如把笔分成铅笔、圆珠笔和钢笔等，就是多分类问题。多分类问题需要将神经网络最后一层的神经元个数设置为与分类数相同，并以数组的形式输出，这个数组的长度就是分类数，数组中每个数值对应在不同类别上的可能性。多分类问题一般通过Softmax函数激活，损失函数使用类别交叉熵。在Keras框架下使用Python编程语言对模型进行编译时，可通过loss='category_crossentropy'指定该损失估算方法。

## 2.5.2 卷积神经网络与循环神经网络

采用全连接神经网络处理复杂、大样本数据时，由于训练参数过多会导致模型收敛缓慢、梯度消失等问题。在处理图像识别和序列数据等问题的过程中，科学家陆续提出了卷积神经网络和循环神经网络来解决相关问题。

### 卷积神经网络

来自生物科学的实验表明，视觉皮层的细胞对视野中的某些局部特征非常敏感，这与数学中的卷积运算非常相似。受此启发，科学家引入了卷积神经网络的方法，用来处理图像识别等问题。

数学运算中的卷积指两个变量在某范围内相乘后求和的结果。在图像处理领域，一般采用二维卷积。假设有数组$A$和数组$K$，经过卷积运算后可得到数组$B$，如图2.5.14所示。

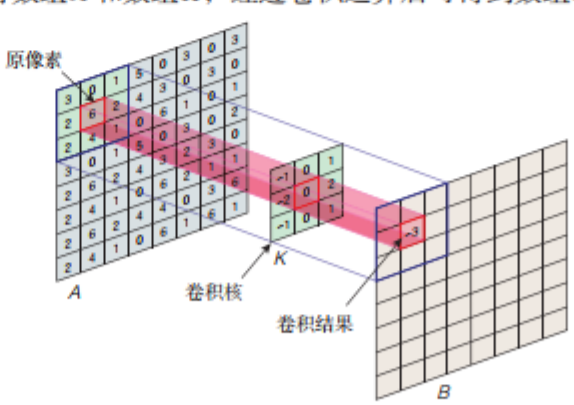



图2.5.14 二维卷积过程



微信公众号：电子课本大全

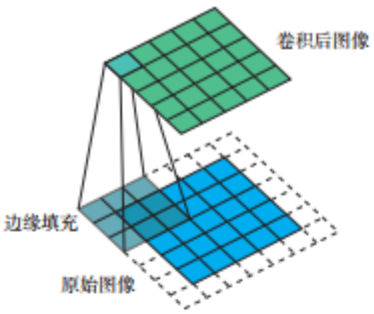



图2.5.15　卷积运算前图像处理

图2.5.14中，由数组$A$最左上方的9个数据与数组$K$对应位置的9个数据相乘，然后求和，得到数组$B$最左上方的数据−3。数组$A$相当于图像的像素数据，数组$K$为卷积核，数组$B$是图像通过卷积核进行卷积运算后得到的。在实际应用中，由于卷积运算后数据个数会减少，为了保持图像的尺寸不变，一般在卷积前会对输入图像的边缘像素用0填充，如图2.5.15所示。

图像的卷积过程就是对图像进行特征筛选的过程。不同的卷积核数值可以检测到图像内不同的轮廓特征，从而得到不同的特征图像。

卷积神经网络（Convolutional Neural Networks，CNN）是一种带有卷积结构的神经网络。由于图像的空间联系往往是局部的，因此每个神经元不需要对全部的图像进行处理，只需对局部特征进行处理，然后在更高层将这些局部神经元连接起来综合处理。在卷积神经网络中，不同神经元之间的参数（卷积核）可以共享。因此，使用卷积神经网络可以有效地减少神经网络模型的训练参数，并且使图像位移、缩放和非线性变形等具有一定的稳定性。

卷积神经网络有一个重要的特征是池化（Pooling），也称为降采样或下采样，池化可以在保留图像显著特征的前提下减少数据处理量。一般池化方法有最大值池化（Max Pooling）和平均值池化（Mean Pooling），最大值池化过程如图2.5.16所示。

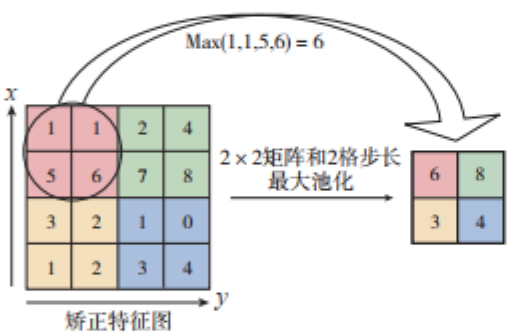



图2.5.16　最大值池化算法过程示意图

卷积神经网络识别图像的过程是将输入的图像进行多次卷积、池化，在多次卷积、池化的过程中图像的尺寸会越来越小，特征越来越明显，最后输入全连接网络完成预测或者分类任务，如图2.5.17所示。

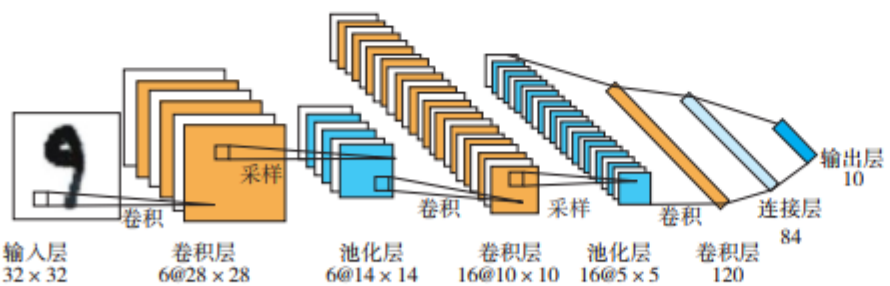



图2.5.17　利用卷积神经网络进行图像识别的过程



微信公众号：电子课本大全

以前，利用计算机处理手写体文字是个难题，因为每个人的书写风格、书写习惯不同，很难通过传统算法对书写内容进行判断。卷积神经网络可以很好地处理这类问题，通过大量手写体样本进行训练，卷积神经网络可以“学会”识别手写文字。MNIST数据集是一个手写体数据集，其中包括了60 000张不同人书写的0~9数字组成的训练图片以及10 000张测试图片，每张图片为28×28像素的灰度图。通过以下代码将训练数据和测试数据准备好。

```
from keras import datasets
import numpy as np
(train_i,train_label),(test_i,test_label)=datasets.mnist.load_data()
train_image=np.expand_dims(train_i,axis=-1)
test_image=np.expand_dims(test_i,axis=-1)
```

使用Python编程语言的绘图模块，查看测试集与训练集的某张图片：

```
import matplotlib.pyplot as plt
plt.imshow(test_i[0])
```

测试集第一张图片是手写体数字7，如图2.5.18所示。




图2.5.18　测试集中手写体样本

在Keras库中可以通过Conv2D和MaxPool方便地添加二维卷积层和最大池化层对图像进行卷积和池化，通过以下代码建立卷积神经网络模型并进行编译和训练：

```
model=keras.models.Sequential()
#第一层要设置输入图片的尺寸，即28*28像素、1个颜色通道
model.add(layers.Conv2D(64,(3,3),activation='relu', input_shape=(28,28,1)))
model.add(layers.Conv2D(64,(3,3),activation='relu'))
model.add(layers.MaxPool2D())
model.add(layers.Conv2D(64,(3,3),activation='relu'))
model.add(layers.Conv2D(64,(3,3),activation='relu'))
model.add(layers.MaxPool2D())
model.add(layers.Flatten())  #在全连接之前，需要将二维图片数据转换成一维数组
model.add(layers.Dense(256,activation='relu'))
#为了防止过拟合，Dropout层会随机丢弃一部分神经网络连接
model.add(layers.Dropout(0.5))
model.add(layers.Dense(10,activation='softmax')) #使用softmax函数处理多分类问题
model.compile(optimizer='adam',loss='sparse_categorical_crossentropy',
                          metrics=['acc'])  #在训练过程中打印出准确率（acc）指标
model.fit(x=train_image,y=train_label,batch_size=1000,epochs=5,
            validation_data=(test_image,test_label))
```

训练过程如下：



微信公众号：电子课本大全

```
Train on 60000 samples, validate on 10000 samples
Epoch 1/5
60000/60000 [==============================] - 217s 4ms/step - loss: 1.4189 - acc:
0.7792 - val-loss: 0.0802 - val-acc: 0.9754
Epoch 2/5
60000/60000 [==============================] - 230s 4ms/step - loss: 0.1045 - acc:
0.9680 - val-loss: 0.0428 - val-acc: 0.9854
Epoch 3/5
60000/60000 [==============================] - 224s 4ms/step - loss: 0.0671 - acc:
0.9795 - val-loss: 0.0328 - val-acc: 0.9895
Epoch 4/5
60000/60000 [==============================] - 229s 4ms/step - loss: 0.0492 - acc:
0.9847 - val-loss: 0.0303 - val-acc: 0.9888
Epoch 5/5
60000/60000 [==============================] - 228s 4ms/step - loss: 0.0390 - acc:
0.9882 - val-loss: 0.0263 - val-acc: 0.9919
```

由于图片的数据量比较庞大，而且卷积神经网络的训练需要大量计算，因此每一轮次的训练需要较长的时间，不过仅训练了5个轮次，神经网络模型就拥有了非常好的表现，最后一次训练完成后，模型在训练集上的准确率达到了98.82%，在测试集上高达99.19%。如果仅使用全连接神经网络，其准确率达到90%左右时就很难再提高了。

train_label和test_label中分别存储训练集与测试集中每张手写体图片中的数字标签，可以通过代码查看测试集前10张图片的数字标签。

```
In [98]: print(test-label[0:10])
[7 2 1 0 4 1 4 9 5 9]
```

再利用模型来识别测试集中前10张图片的内容，可以看到图片中的手写体被成功地识别出来了。

```
In [99]: [l,index(max(l)) for l in model.predict(test_image[0:10]).tolist()]
Out[99]: [7, 2, 1, 0, 4, 1, 4, 9, 5, 9]
```

### 循环神经网络

处理某些问题时，数据的先后顺序往往蕴含着重要的信息。比如阅读时，单词的先后顺序会影响我们对语句内容的理解。在卷积神经网络中，每一层的输出都只取决于该层的输入，而没有考虑前面其他层输入的影响，这使得卷积神经网络在处理有时序问题的数据时，会显得无能为力。

循环神经网络（Recurrent Neural Network，RNN）是一类以序列数据为输入，并在序列的演进方向上进行递归处理的神经网络结构。循环神经网络中层的输出结果不仅与当前输入有关，还和之前的状态有关，具体的表现形式相当于神经网络会对之前的信息进行记忆并应用到当前的输入中，如图2.5.19所示。

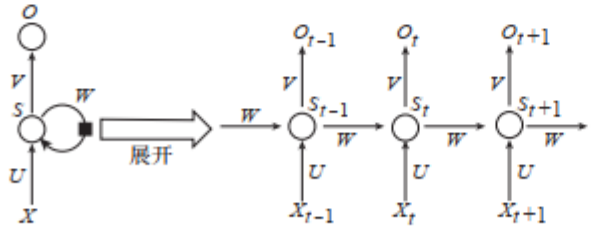



图2.5.19 循环神经网络示意图



微信公众号：电子课本大全

如果序列过长，早期的循环神经网络在训练过程中容易出现梯度消失等问题，于是出现了许多基于循环神经网络的优化方法，比如长短期记忆网络（Long Short-Term Memory，LSTM）等。长短期记忆网络最大的特点是引入了遗忘门的概念。类似于人脑处理问题的特点，长短期记忆网络会对近期输入或者经常出现的信息加深印象，而淡忘早期输入且不常出现的信息。

IMDb是亚马逊旗下互联网电影资料库中有关电影评论和情感分类的数据集，其中包括25 000个训练样本和25 000个测试样本。在处理自然语言评论时，由于自然语言评论是关于时间序列的问题，因此比较适合采用LSTM模型处理。IMDb影评数据集成在了Keras中，如下代码可以加载IMDb数据并查看第一条训练集的内容。

```
import keras
data=keras.datasets.imdb
max_word=10000  #影评中出现的最大单词量
(x_train,y_train),(x_test,y_test)=data.load_data(num_words=max_word)
print(x_train[0],y_train[0])
```

运行结果如下：

```
[1,14,  22, 16, 43, 530,  973, 1622, 1385, 65, 458, 4468, 66, 3941, 4, 173, 36, 256, 5,
25, 100, 43, 838, 112, 50, 670, 2, 9, 35, 480, 284, 5,  150, 4,  172, 112, 167, 2, 336,
385, 39, 4, 172, 4536, 1111, 17, 546, 38, 13, 447, 4, 192, 50, 16, 6, 147, 2025, 19,
14, 22, 4, 1920, 4613, 469, 4, 22, 71, 87, 12, 16, 43, 530, 38, 76, 15, 13, 1247, 4,
22, 17, 515, 17, 12, 16, 626, 18, 2, 5, 62, 386, 12, 8, 316, 8, 106, 5, 4, 2223, 5244,
16, 480, 66, 3785, 33, 4, 130, 12, 16, 38, 619, 5, 25, 124, 51, 36, 135, 48, 25, 1415,
33, 6, 22, 12, 215, 28, 77, 52, 5, 14, 407, 16, 82, 2, 8, 4, 107, 117, 5952, 15, 256,
 4, 2, 7, 3766, 5, 723, 36, 71, 43, 530, 476, 26, 400, 317, 46, 7, 4, 2, 1029, 13, 104,
88, 4, 381, 15, 297, 98, 32, 2071, 56, 26, 141, 6, 194, 7486, 18, 4, 226, 22, 21, 134,
476, 26, 480, 5, 144, 30, 5535, 18, 51, 36, 28, 224, 92, 25, 104, 4, 226, 65, 16, 38,
1334, 88, 12,  16, 283, 5, 16, 4472, 113, 103, 32, 15, 16, 5345, 19, 178, 32 ] 1
```

在IMDb中，用户的影评内容被编码成不同长度的数值列表，其中每个数值表示一个特定的单词，标签内容由0或者1构成，其中0表示负面情绪（差评），1表示正面情绪（好评）。为了更直观地查看样本数据，可以通过以下代码打印训练集上第一条用户实际评论内容。

```
def get_real_words(index):
    word_index=data.get_word_index()
    index_word=dict((value,key) for key,value in word_index.items())
    #找不到的单词用"?"表示
    real_words=[index_word.get(index-3,'?') for index in x_train[0]]
    return real_words
print(get_real_words(0))
```

运行结果如下：

```
['?' ,  'this' ,  'film' ,  'was' , 'just' , 'brilliant' , 'casting' , 'location' , 'scenery' ,
'story' , 'direction' , 'everyone's' , 'really' , 'suited' , 'the' , 'part' , 'they' ,
'played' , 'and' , 'you' , 'could' , 'just' , 'imagine' , 'being' , 'there' , 'robert' , '?' ,
'is' , 'an' , 'amazing' , 'actor' , 'and' , 'now' , 'the' , 'same' , 'being' , 'director' , '?' ,
'father' , 'came' , 'from' , 'the' , 'same' , 'scottish' , 'island' , 'as' , 'myself' , 'so' ,
'i' , 'loved' , 'the' , 'fact' , 'there' , 'was' , 'a' , 'real' , 'connection' , 'with' ,
```


微信公众号：电子课本大全

```
'great', 'it', 'was', 'just', 'brilliant', 'so', 'much', 'that', 'i', 'bought', 'the',
'film', 'as', 'soon', 'as', 'it', 'was', 'released', 'for', '?', 'and', 'would',
'recommend', 'it', 'to', 'everyone', 'to', 'watch', 'and', 'the', 'fly', 'fishing',
'was', 'amazing', 'really', 'cried', 'at', 'the', 'end', 'it', 'was', 'so', 'sad',
'and', 'you', 'know', 'what', 'they', 'say', 'if', 'you', 'cry', 'at', 'a', 'film',
'it', 'must', 'have', 'been', 'good', 'and', 'this', 'definitely', 'was', 'also', '?',
'to', 'the', 'two', 'little', 'boy's', 'that', 'played', 'the', '?', 'of', 'norman',
'and', 'paul', 'they', 'were', 'just', 'brilliant', 'children', 'are', 'often',
'left', 'out', 'of', 'the', '?', 'list', 'i', 'think', 'because', 'the', 'stars',
'that', 'play', 'them', 'all', 'grown', 'up', 'are', 'such', 'a', 'big', 'profile',
'for', 'the', 'whole', 'film', 'but', 'these', 'children', 'are', 'amazing', 'and',
'should', 'be', 'praised', 'for', 'what', 'they', 'have', 'done', 'don't', 'you',
'think', 'the', 'whole', 'story', 'was', 'so', 'lovely', 'because', 'it', 'was',
'true', 'and', 'was', "someone's", 'life', 'after', 'all', 'that', 'was', 'shared',
'with', 'us', 'all']
```

由于用户的每条评论单词长度不同，为了适合输入到神经网络模型中进行处理，需要对所有评论进行等长处理，如下代码实现了将训练集和测试集评论都处理为512个单词长度，如果原评论长度大于512，则舍弃之后的内容，反之则用空字符填充长度。

```
maxlen=512
#词长度填充
x_train=keras.preprocessing.sequence.pad_sequences(x_train,maxlen=maxlen)
x_test=keras.preprocessing.sequence.pad_sequences(x_test,maxlen=maxlen)
```

尽管LSTM模型的内部结构非常复杂，但Keras提供了简单的调用方法。以下代码可以构建一个拥有LSTM层的神经网络模型并进行二分类预测。

```
model=keras.models.Sequential()
model.add(layers.Embedding(input_dim=max_word,output_dim=64,
                           input_length=maxlen))  #词嵌入层，用于对单词文本的向量化
model.add(layers.LSTM(64)) #添加LSTM层
model.add(layers.Dense(32,activation='relu'))
model.add(layers.Dropout(0.5)) #增加Dropout层，抑制过拟合
model.add(layers.Dense(1,activation='sigmoid'))
model.compile(optimizer='adam',loss='binary_crossentropy',metrics=['acc'])
#抽取20%训练集作为验证集
model.fit(x_train,y_train,batch_size=256,epochs=20,validation_split=0.2)
model.evaluate(x_test,y_test)
```

LSTM的训练过程比较缓慢，训练过程如下：

```
Train on 20000 samples, validate on 5000 samples
Epoch 1/20
20000/20000 [==============================] - 359s 18ms/step - loss: 0.6458 - acc:
0.6579 - val-loss: 0.5014-val-acc:0.7814
Epoch 2/20
20000/20000 [==============================] - 347s 17ms/step - loss: 0.3686 - acc:
0.8608 - val-loss: 0.3603-val-acc:0.8386
Epoch 3/20
20000/20000 [==============================] - 375s 19ms/step - loss: 0.2504 - acc:
0.9098 - val-loss: 0.3275-val-acc:0.8658
Epoch 4/20
16128/20000 [==========================>.....] - ETA: 1:07 - loss: 0.1776 - acc: 0.9436
```

通过对比训练集与验证集准确率的差距，可以发现该模型存在一定程度的过拟合，可以通过调整学习率、网络层数等方法进行优化。



微信公众号：电子课本大全

## 阅读拓展

### 词嵌入

文本处理的过程中，对单词进行独热编码不太符合现实情况。例如，一篇1 000个单词的文章，经过独热编码后每个单词就要用一个长度为1 000的数组来表述，这会造成计算和储存空间的浪费。且独热编码无法准确表达不同词之间的相似度，比如“get”和“got”相差一个字母，但意思是相似的，只是时态不一样而已；而“big”和“pig”也相差一个字母，但意义完全不同。

词嵌入（Word Embedding）可以解决上述的类似问题，将每个词表示成若干长度的数组（多维向量），并通过计算两个向量之间的余弦相似度，使这些向量能较好地表达不同词之间的相似和类比关系。

在Keras中，通过添加Embedding层，可以将输入数据转化为词向量。

## 实践活动

### CIFAR-10数据集分类

CIFAR-10数据集中包括10个类别的彩色图片，共有50 000张训练图片和10 000张测试图片。每张图片为32×32像素，3个颜色通道，如图2.5.20所示。

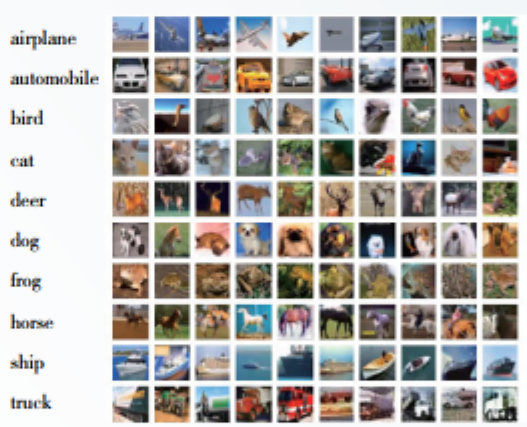



图2.5.20　CIFAR-10数据集中的样本（局部）

通过以下方法可以快速准备好CIFAR-10数据集。

```
import keras
cifar=keras.datasets.cifar10
(train_image,train_label),(test_image,test_label)=cifar.load_data()
```

和同学合作，利用卷积神经网络搭建能够对CIFAR-10数据集进行分类的神经网络模型。

## 2.5.3　深度学习及软硬件平台

深度学习（Deep Learning，DL）广泛应用于人工智能研究领域的方方面面，不仅用于



微信公众号：电子课本大全

分类和回归，还在降维、聚类、语音识别和图像识别等方面有许多应用。深度学习开源框架对计算机算力的要求很高，传统的CPU计算在超大规模的神经网络以及海量的训练数据前会显得力不从心，因此深度学习除了需要优异的软件框架之外，还需要合适的硬件平台。

### 深度学习

深度学习也称深度神经网络（Deep Neural Networks，DNN），指具有多个隐含层的神经网络。广义上，含多隐层的多层感知器、卷积神经网络和循环神经网络等都属于深度学习。深度神经网络包含大量的网络参数，因此具有更强大的拟合能力，使得神经网络更具有实用性。

2012年，深度卷积神经网络结构首度出现，当时的神经网络层数尚且只有个位数。此后，对于深度神经网络的研究不断深入，应用逐渐广泛。2016年，神经网络层达到1 207层。随着卷积神经网络和循环神经网络结构的不断发展，神经网络对图像和序列数据特征具有越来越强的特征感知和拟合能力，深度学习已经成为人工智能研究领域最具活力的研究内容之一。

■ 预训练模型

一味地增加神经网络的深度也会遇到问题。过多的神经网络参数会使训练时间缓慢，一个复杂的神经网络模型训练过程可能耗时几天甚至几周。因此，在具体应用过程中，通过引入预训练模型来进行模型结构及参数的初始化。所谓预训练模型，是指在通用的数据集上训练并优化后的模型，如在ImageNet数据集上训练出的VGG16、VGG19等。如图2.5.21所示的是VGG16网络结构示意图。

| ConvNet Configuration | | | | | |
|---|---|---|---|---|---|
| A | A-LRN | B | C | D | E |
| 11 weight layers | 11 weight layers | 13 weight layers | 16 weight layers | 16 weight layers | 19 weight layers |
| input(224 × 224 RGB image) | | | | | |
| conv3-64 | conv3-64<br>LRN | conv3-64<br>conv3-64 | conv3-64<br>conv3-64 | conv3-64<br>conv3-64 | conv3-64<br>conv3-64 |
| maxpool | | | | | |
| conv3-128 | conv3-128 | conv3-128<br>conv3-128 | conv3-128<br>conv3-128 | conv3-128<br>conv3-128 | conv3-128<br>conv3-128 |
| maxpool | | | | | |
| conv3-256<br>conv3-256 | conv3-256<br>conv3-256 | conv3-256<br>conv3-256 | conv3-256<br>conv3-256<br>conv1-256 | conv3-256<br>conv3-256<br>conv3-256 | conv3-256<br>conv3-256<br>conv3-256<br>conv3-256 |
| maxpool | | | | | |
| conv3-512<br>conv3-512 | conv3-512<br>conv3-512 | conv3-512<br>conv3-512 | conv3-512<br>conv3-512<br>conv1-512 | conv3-512<br>conv3-512<br>conv3-512 | conv3-512<br>conv3-512<br>conv3-512<br>conv3-512 |
| maxpool | | | | | |
| conv3-512<br>conv3-512 | conv3-512<br>conv3-512 | conv3-512<br>conv3-512 | conv3-512<br>conv3-512<br>conv1-512 | conv3-512<br>conv3-512<br>conv3-512 | conv3-512<br>conv3-512<br>conv3-512<br>conv3-512 |
| maxpool | | | | | |
| FC-4096 | | | | | |
| FC-4096 | | | | | |
| FC-1000 | | | | | |
| soft-max | | | | | |

图2.5.21　VGG16网络结构示意图



微信公众号：电子课本大全

使用VGG16进行模型训练时，可以加载卷积层的预训练参数并锁定，只训练神经网络最后用于具体分类的全连接层，从而大大减少模型的训练参数，加快训练速度。

## 阅读拓展

### 查看神经网络结构

在Keras中，通过summary方法可以查看某个模型的神经网络结构，如图2.5.22所示。

```
In [114]: model.summary()
```

| Layer (type) | Output Shape | Param # |
|---|---|---|
| conv2d_9 (Conv2D) | (None, 30, 30, 256) | 7168 |
| max_pooling2d_5 (MaxPooling2D) | (None, 15, 15, 256) | 0 |
| conv2d_10 (Conv2D) | (None, 13, 13, 128) | 295040 |
| max_pooling2d_6 (MaxPooling2D) | (None, 6, 6, 128) | 0 |
| flatten_5 (Flatten) | (None, 4608) | 0 |
| dense_104 (Dense) | (None, 256) | 1179904 |
| dropout_11 (Dropout) | (None, 256) | 0 |
| dense_105 (Dense) | (None, 10) | 2570 |

Total params: 1,484,682
Trainable params: 1,484,682
Non-trainable params: 0

图2.5.22 通过summary方法查看到的某个模型的神经网络结构

在该模型中，输入数据首先经过一个二维卷积层（Conv2D），之后是一个最大池化层（MaxPolling2D），再经过一次卷积和池化后，通过Flatten层将多维数据“拉长”为一维数据，再通过全连接层以及Dropout层防止过拟合，最后全连接到10个神经元完成分类问题。该模型总共有1 484 682个参数参与训练。

■ 残差神经网络

过多的神经网络还容易导致误差反向传播过程中的梯度消失问题，使得神经网络模型很难收敛。残差神经网络能很好地解决这个问题，其神经网络模型如图2.5.23所示。

每一层神经网络相当于一个复杂的函数$F$，其输出$Y$与输入$X$满足：

$$Y = F(X)$$

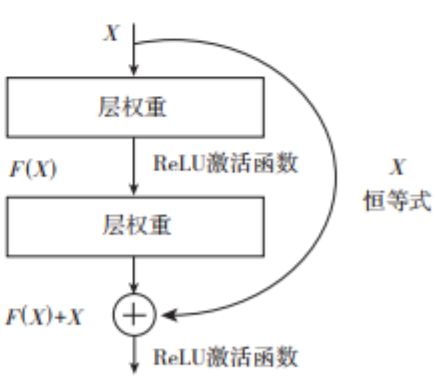



图2.5.23 残差神经网络模型示意图



微信公众号：电子课本大全

而在残差神经网络中，输出$Y$在原来$F(X)$的基础上又合并了原始输入$X$：

$$Y = F(X) + X$$

残差神经网络结构简单，并解决了在极深神经网络下的性能退化问题，因此得到广泛应用。常见的残差神经网络模型有ResNet50、ResNet101等。

深度神经网络的发展离不开数据、算法和算力等三要素。其中海量的数据和高效的算力是深度学习算法实现的基础。

### 软硬件平台

目前，各种开源框架的出现，降低了深度神经网络学习与应用的门槛，可以使更多的人参与到深度学习的研究与优化中。深度学习除了需要优异的软件框架之外，还需要合适的硬件平台。人工智能加速硬件按照承担的任务可分为训练芯片和推理芯片，按照应用场景可分为云端芯片和终端芯片。训练芯片用于神经网络模型的训练与开发，“学习”出具有特定功能的神经网络模型。推理芯片使用已训练好的神经网络模型，对新输入的数据进行计算、“推理”，得到各种有价值的结论。云端芯片部署在公有云、私有云或者混合云上，不但可以用于训练，也可以用于推理。终端芯片一般应用于移动终端或嵌入式开发，具备体积小、集成度高、功耗低和性能相对低等特点，主要用于推理。

常见人工智能芯片主要包括GPU、NPU（Neural network Processing Unit，神经网络处理器）、TPU（Tensor Processing Unit，张量处理器）、FPGA（Field Programmable Gate Array，现场可编程逻辑门阵列）、ASIC（Application Specific Integrated Circuit，专用集成电路）以及类脑芯片。在人工智能新时代，各种智能芯片各自发挥着优势。

■ 本地硬件

本地硬件主要用于神经网络的计算，一般通过GPU或FPGA等的并行计算能力来实现。其中，GPU的特点是单指令、多数据处理、在内部有数量众多的计算单元，当需要处理大量类型统一的数据时，GPU的并行计算特性可以极大提高运算速度。

■ 云计算平台

随着网络技术的发展，云计算平台日益成熟，成本逐渐降低，目前已能为企业和个人提供较好的人工智能解决方案。国内比较著名的云计算平台有腾讯云、阿里云、百度云和网易云等。云计算平台既适用于神经网络模型训练，也适用于利用神经网络模型推理或预测出结果。

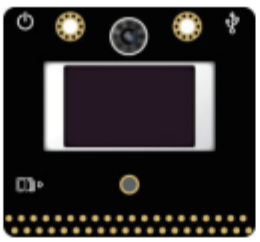
■ 终端专用神经网络芯片

终端专用神经网络芯片是为了实现特定要求而定制的，具有神经网络模型计算加速功能的芯片，在体积、功耗和成本等方面都具有优势，适合应用在嵌入式系统中完成特定的人工智能任务。

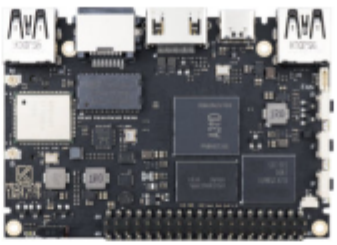
实验和项目式教学用人工智能硬件加速平台一般采用基于GPU、NPU等芯片的嵌入式开发验证系统，常见的有AI掌控板、Khadas VIM3和Jetson Nano等，如图2.5.24所示。



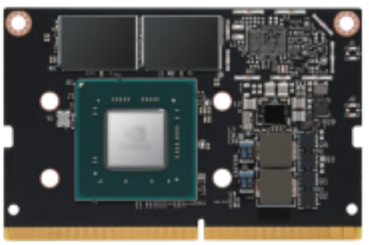
微信公众号：电子课本大全



AI掌控板



Khadas VIM3



Jetson Nano

图2.5.24　常见的嵌入式开发验证硬件

## 技术支持

### 深度学习开源框架

目前，常见的深度学习开源框架有Theano、TensorFlow、Caffe2、CNTK、PyTorch、飞桨和Keras等。

Theano：一个具有较大影响力的Python深度学习框架，目前已经停止开发。

TensorFlow：2015年推出的一个具有影响力的深度学习框架，拥有丰富的社区资源。

Caffe2：一个代码简洁易用，性能优异的深度学习框架，但缺乏灵活性。

CNTK：微软开发的深度学习框架，擅长进行语音处理。

PyTorch：基于Torch的一个简洁的开发框架，目前有赶上TensorFlow的趋势。

飞桨：由百度开发的深度学习框架，目前正处于成长期。

Keras：适合初学者接触深度学习的工具，与其他平台框架不同，Keras更像一个深度学习的编程接口。目前Keras可以构建在Theano、TensorFlow及CNTK之上。在TensorFlow 2.0以后，Keras已经被集成进了TensorFlow中，成为TensorFlow的一部分。



微信公众号：电子课本大全

## 项目实施

### “剪刀、石头、布”游戏中的手势识别

一、项目活动

结合本节所学内容，利用卷积神经网络实现手势识别。

以小组为单位，采集图像样本数据并对数据进行预处理，搭建卷积神经网络模型，对模型进行训练并观察、评估训练结果。

二、项目检查

1. 图像样本数据采集：确定采集方案，并对方案进行简单介绍；完成样本数量统计，填写表2.5.3。

表2.5.3　手势及样本数量

| 手势 | 剪刀 | 石头 | 布 |
| --- | --- | --- | --- |
| 样本数量 | | | |

2. 图像数据预处理：针对图像中不同的手势，对每个图像建立数据标签，并讨论交流快速建立数据标签的方法；对图像尺寸、方向进行统一处理，分享处理方法；完成训练集、数据集、验证集的划分，填入表2.5.4。

表2.5.4　训练集、数据集、验证集的划分

| 手势 | 剪刀 | 石头 | 布 | 合计 |
| --- | --- | --- | --- | --- |
| 训练集 | | | | |
| 验证集 | | | | |
| 测试集 | | | | |
| 标签编码 | | | | |

3. 搭建卷积神经网络模型，描述神经网络模型的结构。

4. 模型训练与结果评价：展示本组神经网络模型的测试集准确率，将使用训练集与验证集进行训练时loss值的变化通过图表描述出来。

## 练习提升

1. 在图像识别中，深度学习需要提取哪些图像特征？

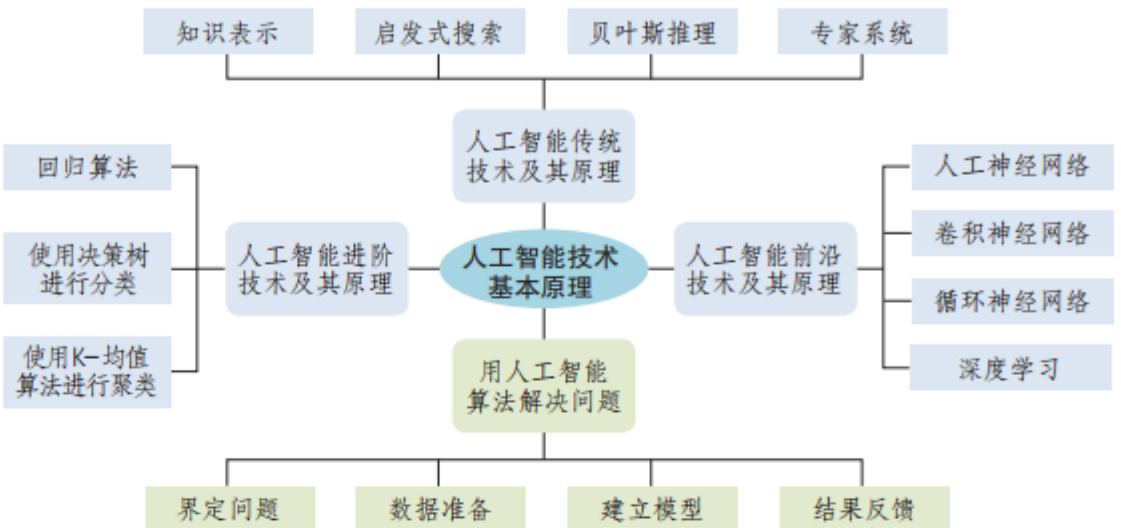
2. 生活中，有哪些方面需要用到深度学习？尝试收集一些数据。



微信公众号：电子课本大全

## 总结 评价

1. 下图展示了本章的核心概念与关键能力，请同学们对照图中的内容进行总结。




2. 根据自己的掌握情况填写下表。

| 学习内容 | 掌握程度 |
| --- | --- |
| 知识表示 | □不了解 □了解 □理解 |
| 启发式搜索 | □不了解 □了解 □理解 |
| 贝叶斯推理 | □不了解 □了解 □理解 |
| 专家系统 | □不了解 □了解 □理解 |
| 回归算法 | □不了解 □了解 □理解 |
| 使用决策树进行分类 | □不了解 □了解 □理解 |
| 使用K-均值算法进行聚类 | □不了解 □了解 □理解 |
| 人工神经网络 | □不了解 □了解 □理解 |
| 卷积神经网络 | □不了解 □了解 □理解 |
| 循环神经网络 | □不了解 □了解 □理解 |
| 深度学习及软硬件平台 | □不了解 □了解 □理解 |

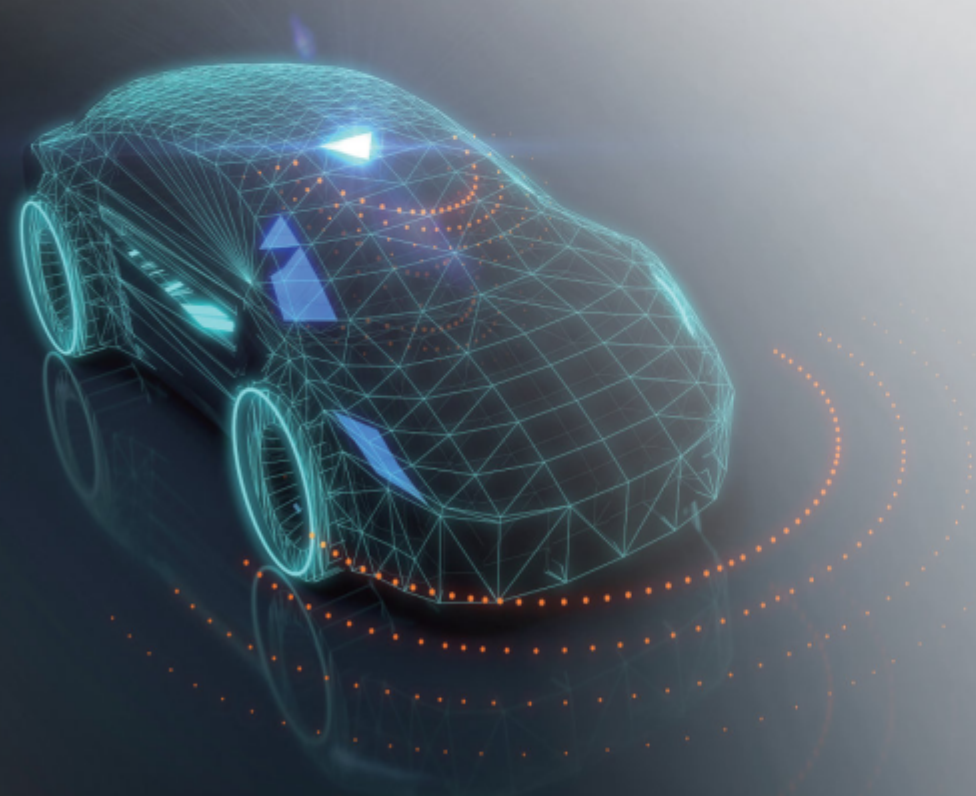

微信公众号：电子课本大全

# 第 3 章
# 人工智能领域应用

人工智能的发展是以各种算法为基础的，而飞速发展的大数据和云计算使人工智能的算法在多个领域发挥了重要的作用，也改变着我们的生活。手机里有语音助理、智能搜索、人脸识别，汽车能自动驾驶……不知不觉中，生活中的常用设备变得越来越智能。

人工智能并不是让机器模拟人的形态和人的行为，而是让机器对人的思维意识和处理信息的过程进行模拟，像人一样处理事情。这一目标是以计算机视觉、自然语言处理、机器理解与推理、博弈决策与智能机器人等基础技术的研究为基础来实现的。

在本章的学习中，我们将借助各领域现有的人工智能开发工具与平台，以“智能陪伴巧实践”为主题，开展项目活动，定制智能陪伴机器人，掌握简单人工智能应用模块的搭建方法，体验人工智能应用的实现过程。



微信公众号：电子课本大全

# 3 主题学习项目：智能陪伴巧实践

## 项目目标

本章建议围绕“计算机视觉、自然语言处理、机器理解与推理、博弈决策以及智能机器人”等方面开展讨论、思考与实践，研究、定制属于自己的智能陪伴机器人，完成搭建、调试，并以多媒体作品的方式进行全班交流。

1. 了解人工智能技术的典型应用，理解人工智能在一些领域中的重要作用。
2. 了解不同领域人工智能应用系统的开发平台和工具，并进行合理的选择。
3. 借助现有的人工智能平台和工具，搭建简单的人工智能应用模块，感受人工智能的广泛应用。

## 项目准备

为完成项目，需做如下准备。

- 全班分成若干小组，建议每组4～6人，明确目标和分工。
- 查阅相关资料，调研并讨论本组搭建的智能陪伴机器人的功能及开发方案。
- 调研并合理选择人工智能平台和工具，安装、搭建人工智能平台，准备所需环境。

## 项目过程

在学习本章内容的同时开展项目活动。为了保证本项目的顺利完成，要在以下各阶段检查项目的进度。

**1 搭建物体识别模块**

利用开源库文件和开放平台编写代码，实现图像中主要物体的检测及识别。 P97

**2 搭建语音对话模块**

利用开源库文件和开放平台搭建语音对话模块，编写代码实现语音对话。 P110

**3 搭建认知推理模块**

利用开源库文件和开放平台编写代码，实现简单的认知推理功能和人机交互功能。 P120

**4 强化学习建模实践**

利用DeepTraffic体验强化学习，构建深度强化学习网络，作为智能陪伴机器人的模拟学习平台。 P128

**5 定制智能机器人**

设计并搭建属于自己的智能陪伴机器人，并与全班同学进行交流。 P139

## 项目总结

完成本章项目后，各小组提交项目学习成果（包括各模块实现代码、智能陪伴机器人代码、多媒体作品和项目学习记录单等），开展作品交流与评价，体验小组合作、项目学习和知识分享的过程，通过搭建智能机器人，了解人工智能在不同领域的重要应用。



微信公众号：电子课本大全

# 3.1
# 计算机视觉

**学习目标** ▶▶▶

- 理解计算机视觉对人工智能的意义。
- 掌握计算机视觉的核心原理及技术。
- 通过典型案例体验计算机视觉在不同领域的应用。

## 体验探索

### “牵挂你”防走失平台

小孩天生活泼好动，在成长的过程中如果有孩子走失，会给家庭和社会带来巨大的伤痛。早些年，无论是走失孩子的家人还是警察，都只能完全依靠人力摸排式的搜寻，需要耗费大量的人力、物力、财力，不少走失孩子在寻找多年后也没有结果。

2017年3月，我国科研人员开发的“牵挂你”防走失平台正式上线（图3.1.1）。该平台利用人脸识别技术，用户在平台上传走失或者疑似走失人员照片，与图库信息进行比对，为帮助寻找走失人员节省了大量的时间。该平台在上线短短两年的时间里，已累计帮助找回走失人员千余人。随着人脸识别技术的深入研究和不断发展，将为我们的生活提供更多的服务和便利。




图3.1.1 “牵挂你”防走失平台人脸识别

思考：

1. 计算机是如何从图像中检测出人脸的？
2. 日常生活中还有哪些人脸识别的应用场景？



微信公众号：电子课本大全

### 3.1.1 计算机视觉简介

人类大脑皮层大约70%的活动是在处理与视觉相关的信息，因而人类可以很容易地感知和理解周围的世界。比如，通过面部表情猜测对方的情感状态，仅通过步态或者背影就能快速识别出这个人是谁。但是，人类视觉系统是如何工作的，这个问题至今也没有得到很好的解答。

人工智能的计算机视觉就像人的“眼睛”一样，它通过电子化的方式来感知和理解周围环境。换句话说，计算机视觉就是利用成像设备对目标进行识别、跟踪和测量，并对图像作进一步处理，使图像更适合人眼观察或仪器检测，建立能够从图像或者多维数据中获取“信息”的人工智能系统。



**思考活动**

**人类视觉与计算机视觉**

如果有人突然朝你扔一个球，你会作何反应？

当然会马上接住或者躲避，这对人来说是很正常的应激反应。人作出这种反应，是受视觉系统和大脑神经系统的支配。首先，球的图像呈现在人的视网膜上，人的视觉系统会辨识出此物体的属性、位置、运行轨迹及速度，然后大脑神经系统会判断接下来要做出的动作——接住或者躲避，并下达对应的行动指令。整个过程几乎在0.1 s内就完成了。

对于计算机而言，仅仅识别出静态图像中的全部物体就已经很困难了，而分析图像中物体之间的关联以及潜在的逻辑关系，又是另一个更高层次的智能问题。

思考：

1. 查阅相关资料，试从神经生物学角度，了解人类视觉系统是如何工作的，人类是如何从零开始，一步一步从认识周围的物体到认识世界的。

2. 人类视觉和计算机视觉有什么异同？人类视觉系统对计算机视觉的工作机理有什么启示？

#### 计算机视觉的发展历程

1966年，麻省理工学院马文·明斯基教授突发奇想，给学生布置了一个课题作业：计算机能否像人类一样读取图像？此问题对计算机视觉的诞生和发展起到了重要的推动作用。随后的几十年，计算机视觉技术不断发展，相继出现的主要理论和技术如表3.1.1所示。



微信公众号：电子课本大全

表3.1.1　计算机视觉主要理论和技术的发展阶段

| 时间阶段 | 计算机视觉的主要理论和技术 |
| --- | --- |
| 20世纪70年代 | 马尔视觉计算理论 |
| 20世纪80年代 | 主动视觉理论和定性视觉理论 |
| 20世纪90年代 | 统计分析方法、局部特征描述算子 |
| 21世纪 | 机器学习、模式识别、现代数据集、深度学习 |

■ 20世纪70年代

1972年，英国人大卫·马尔教授提出了信息处理系统概念的三个层次：计算理论层次、表达和算法层次、硬件实现层次，并提出人类视觉的重构过程是可以通过计算的方式来完成的。他将视觉计算过程分为三个阶段：初始简图、2.5维简图和三维模型，如图3.1.2所示。直到今天，马尔的视觉计算理论依旧是视觉领域表达和解决问题的正确向导。




图3.1.2　马尔视觉计算过程示意图

■ 20世纪80年代

视觉计算理论提出后，计算机视觉进入蓬勃发展期。20世纪80年代提出的主动视觉理论和定性视觉理论认为，视觉的过程是主动的、有目的性和选择性的。

■ 20世纪90年代

这一时期的研究重点关注于定量分析图像和场景的更为复杂的数学方法。机器学习成为计算机视觉中不可或缺的工具，各种检测和识别算法迎来了较大发展。描述图像特征的算子也越来越丰富，其中局部特征描述算子（如尺度不变特征变换算子SIFT）开始流行。

■ 21世纪

随着计算机处理和存储能力的大幅度提升，机器学习已经在视觉领域广泛应用，现代数据集的快速发展也促进了学习算法的发展。深度学习算法特别是卷积神经网络在图像处理、目标识别过程中已能够取得非常好的效果。

### 计算机视觉的主要研究领域

■ 图像理解

与人类通过视觉理解外部世界一样，图像理解是通过计算机系统来感知并理解图像的。根据理解的抽象程度可将图像理解分为三个层次：浅层理解、中层理解和高层理解。

浅层理解：计算机把图像像素点抽象为边缘、角点和纹理等基本元素。



微信公众号：电子课本大全

中层理解：在浅层理解的基础上抽象理解物体边界、轮廓和区域等。

高层理解：主要包括图像分类、目标检测、目标识别和图像文字说明等。

计算机视觉工作的基础是对单张图像的识别和理解。

■ 动态视觉

除理解单张图像外，计算机视觉也关注分析视频或图像序列中的内容，寻找图像元素在时序上的对应关系，提取上下文语义信息。动态视觉研究被广泛应用于目标跟踪、视频分析和人机交互等。

■ 三维视觉

三维视觉即研究如何通过视觉获取三维信息（三维重建）以及三维信息理解的科学。三维信息理解，即使用三维信息辅助图像理解或者直接理解。三维视觉技术可以广泛应用于机器人、无人驾驶、智慧工厂、虚拟现实、增强现实和场景建模等方向的研究。



## 技术支持

### 常用图像数据库

MNIST手写数字图像库：共有约7万张图片，每张大小为28×28像素，包含10类从数字0~9的手写字符图像。

CIFAR-10图像库：包含10类图像，每类有6 000张图片，每张大小为32×32像素。

CIFAR-100图像库：包含100类图像，每类有600张图片。

Tiny图像库：CIFAR-10以及CIFAR-100都是从该库中筛选出来的，该库中有8 000万张图片。

Caltech101和Caltech256：分别有101类和256类图像，多用于图像分类。

FDDB：有2 854张图片，5 171张人脸图片，均拍摄于自然场景。

LFW：无约束自然场景人脸识别数据集，有5 000多人的1.3万多张人脸图片。

JAFFE表情数据库：共有213张图片，涉及10个人，每人有7种表情，每种表情大概有三四张样图。7种表情分别为悲伤、高兴、愤怒、厌恶、惊讶、恐惧和平静。

CK以及CK+表情识别图像库：CK中有97个被测试者的表情，只有静态图片；CK+中包括123个被测试者的593个图像序列，包括静态图片和视频，其中有327个序列做了表情标记。

GENKI-4K笑脸数据库：共有4 000张人脸图片，分为“笑”和“不笑”两种，每张图片中的人脸尺度大小不一、姿态不同、光照不同，并且头部转动角度也有差别。



微信公众号：电子课本大全

### 3.1.2 计算机视觉的应用

我们从表情识别入手，开始实现智能陪伴机器人的人机交互功能。

表情识别基本过程为：首先通过采集的图像检测到图像中的人脸，定位人脸区域；然后提取表情关键特征点；接着利用表情分类器进行表情识别；最后输出识别结果。智能机器人可以根据表情识别结果作出陪伴决策。表情识别的基本流程如图3.1.3所示。




图3.1.3　表情识别的基本流程示意图

#### 人脸检测与定位

按照图3.1.3所示的流程，要实现表情识别，第一个关键任务是检测到图像中的人脸并定位人脸区域。以图3.1.4所示的图像为例，智能陪伴机器人要检测出图像中的人脸，通常要实施以下三个步骤：

1. 选择图像中的某个矩形区域，例如图3.1.5中左上方矩形区域；
2. 在选定区域窗口内，提取特征；
3. 根据特征描述，判断区域窗口内是否恰好是人脸。



图3.1.4　智能陪伴机器人视角中的人脸图像

将待测矩形区域窗口从图像的左上方开始向右下方滑动。如果窗口中检测到人脸，则给出人脸区域的矩形范围，如图3.1.5所示的绿色矩形框，然后继续遍历图像的剩余区域；如果遍历完图像的全部区域后，所有窗口均不含人脸，则判断所给图像不包含人脸。

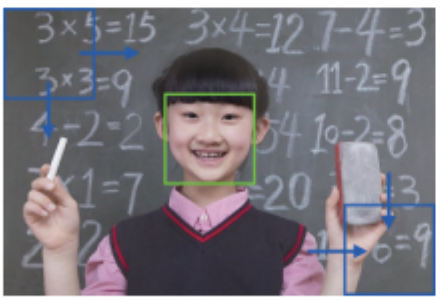


图3.1.5　滑动窗口检测人脸示意图



微信公众号：电子课本大全

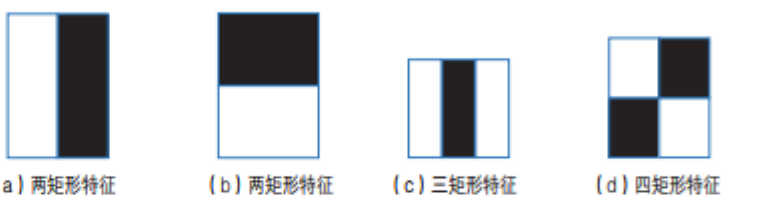
人脸检测与定位流程如图3.1.6所示，其中重要的环节是特征提取和分类器。



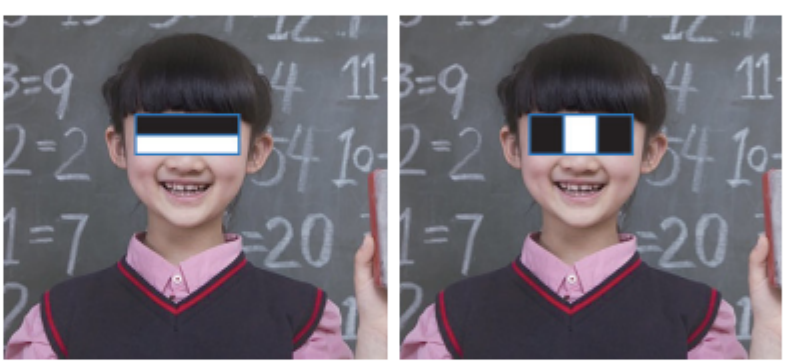

图3.1.6　人脸检测与定位流程示意图

■ 哈尔特征

基于哈尔特征（Haar-Like Features）的算法是人脸检测的经典算法。哈尔特征描述了相邻图像区域的对比模式，有三种基本类型：两矩形特征（包括两类）、三矩形特征和四矩形特征，如图3.1.7所示。图3.1.7（e）和图3.1.7（f）均显示了人脸中的哈尔特征，前者对暗的水平区域首先响应的是人眼部分，后者对相对亮的竖直区域响应的是鼻梁部分。



（a）两矩形特征　（b）两矩形特征　（c）三矩形特征　（d）四矩形特征



（e）人脸中的哈尔特征　（f）人脸中的哈尔特征

图3.1.7　哈尔特征

■ 分类器

使用哈尔特征检测图像，需要遍历所有可行的区域，其中把左上起点和右下终点作为矩形特征的起始点和结束点，来获得图像的矩形特征（图3.1.7）。因此，由一幅图像获得的哈尔特征的数据量是巨大的。可使用分类算法从上述哈尔特征中选取最能够区分人脸区域和非人脸区域的特征，并按照区分准确性进行加权，得到一个人脸区域与非人脸区域的分类器，完成人脸检测。

OpenCV是一个用于图像处理、分析和机器视觉等方面的开源函数库，是完全免费的，因此无论是科学研究还是商业应用，OpenCV都可以作为理想的工具库。该库用C和C++语言编写，支持其他语言接口，可以在Windows、Linux和Mac OS X等操作系统



微信公众号：电子课本大全

中运行。OpenCV 包含了工业产品检测、医学图像处理、安防、用户界面、摄像头标定、三维成像和机器视觉等领域的超过500个接口函数，所有代码都已经过优化，计算效率较高。

OpenCV开源库中有可以直接调用的用于人脸检测的函数包，使用哈尔特征分类器haarcascade_frontalface_alt.xml和多尺度检测人脸算法函数detectMultiScale( )即可检测图像中的人脸。



### 实践活动

#### 利用OpenCV实现人脸检测

使用OpenCV之前，要先安装OpenCV库，在命令行中输入“pip install opencv-python”。

在OpenCV开源库中，haarcascade_frontalface_alt.xml是人脸的哈尔特征迭代分类器模型，detectMultiScale( )是多尺度检测人脸算法的函数。实现过程的代码如下：

```
from PIL import Image
import cv2
import numpy
def detect(frame):
    faceCascade=cv2.CascadeClassifier("haarcascade_frontalface_default.
xml")
    gray=cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    faces=faceCascade.detectMultiScale(gray,scaleFactor=1.15,minNeighbors=5)
    print("Found {0} faces!".format(len(faces)))
    for(x,y,w,h) in faces:
        cv2.rectangle(frame,(x,y),(x+w,y+h),(0,255,0),2)
frame=cv2.imread("01image.jpg")
detect(frame)
cv2.imshow("face found",frame)
cv2.imwrite('img01_detected.jpg',frame)
cv2.waitKey(0)
```

Dlib是一个包含机器学习算法的C++开源工具包，提供了大量的机器学习和图像处理算法，使用非常方便，无须安装和配置，只需要在代码中包含头文件即可。Dlib可以在Windows、Linux和Max OS X等操作系统中使用，已经广泛应用于行业和学术领域，例如嵌入式设备、机器人和高性能计算机等。

Dlib库不仅能够检测人脸区域，还可以提取人脸关键特征点，包括眼睛、眉毛、鼻子、嘴巴和脸部外轮廓等。Dlib库中包含68个人脸关键特征点的模型为shap_predictor_68_face_landmarks.dat，这些关键特征点可用于人脸识别、表情识别等。



微信公众号：电子课本大全

## 实践活动

### 利用Dlib实现人脸关键特征点检测

首先安装Dlib库，在命令行中输入“pip install dlib”。

使用Dlib中人脸检测函数以及人脸关键点模型，提取人脸关键特征点信息，实现过程的代码如下：

```
import dlib
import numpy as np
import cv2

def detect(frame):
    detector=dlib.get_frontal_face_detector()
    predictor=dlib.shape_predictor("shape_predictor_68_face_landmarks.dat")
    # shap_predictor_68_ face_landmarks.dat是Dlib中68个人脸关键特征点的模型
    gray=cv2.cvtColor(frame,cv2.COLOR_BGR2GRAY)
    #人脸数
    rects=detector(gray,0)
    for i in range(len(rects)):
        landmarks=np.matrix([[p.x,p.y] for p in
                                        predictor(frame,rects[i]).parts()])
    for idx, point in enumerate(landmarks):
        # 68点的坐标
        pos=(point[0,0],point[0,1])
        cv2.circle(frame,pos,1,color=(0,255,0))

frame=cv2.imread("01image.jpg")
detect(frame)
cv2.imshow("face found",frame)
cv2.imwrite('01img_landmark_detected.jpg',frame)
cv2.waitKey(0)
```

对图3.1.4进行人脸检测的结果如图3.1.8所示。



（a）人脸检测结果　　（b）人脸关键特征点

图3.1.8　人脸检测结果

百度AI开放平台、阿里云ET大脑、腾讯AI开放平台和讯飞开放平台均有人脸检测在线体验，且提供了在线接口以及离线SDK（软件开发工具包）接口。以百度AI开放平台为



微信公众号：电子课本大全

例，使用POST（客户机和服务器之间进行请求响应的方法）向API（应用程序编程接口）服务地址发送请求，通过调用后台API文档，即可完成人脸检测。图3.1.9为百度AI开放平台中人脸检测在线体验界面，该平台除了可以检测人脸外，还可以预测年龄、性别、种族和表情等。




图3.1.9　百度AI开放平台的人脸检测在线体验界面

## 实践活动

### 多尺度检测

哈尔特征集考虑了图像中目标的旋转问题，具有旋转不变性，但是并没有考虑图像中目标大小的问题，不具备尺度不变性。因此在使用哈尔分类器时，需要考虑被检测对象的比例变化，OpenCV中使用的多尺度检测函数为detectMultiScale()，其函数形式为：

detectMultiScale(const Mat & image, double scaleFactor, int minNeighbors, int flags, Size minSize, Size maxSize)

image为输入的灰度图像。scaleFactor为比例变化因子，变化后的图像构成图像金字塔，如图3.1.10所示。scaleFactor的取值表示检测人脸时的放大比例，一般为1.1～1.4。比例越大，检测速度越快，但越容易漏检；比例越小，检测越细致，但速度较慢。minNeighbors为构成检测目标的相邻矩形的最小个数，默认值为3，如果构成检测目标的小矩形的个数小于minNeighbors的值，则认为该区域无效。flags值为0时，表示使用默认分类器，否则使用Canny边缘检测（另外一种检测算法）来排除边缘过多或者过少的非人脸区域。minSize和maxSize分别为检测对象的最小和最大尺寸，一般只需要设置minSize的值。



微信公众号：电子课本大全

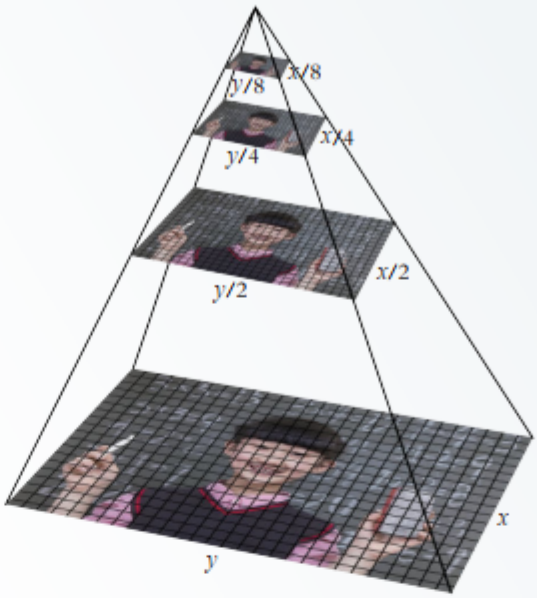



图3.1.10　图像金字塔

理解上述不同参数的含义，设置不同参数进行检测，观察运行结果。

### 表情识别

按照图3.1.3所示的流程，在检测及定位人脸区域后，就可以检测人脸轮廓的关键特征点了，然后利用关键特征点训练分类器来识别表情。表情识别可以定义为多分类问题，将人类表情分为7种模式：悲伤、高兴、愤怒、厌恶、惊讶、恐惧和平静。

图3.1.11展示了除“平静”外其他表情模式的人脸关键特征点，利用关键特征点进行训练，使用训练好的分类器将待测表情进行分类。

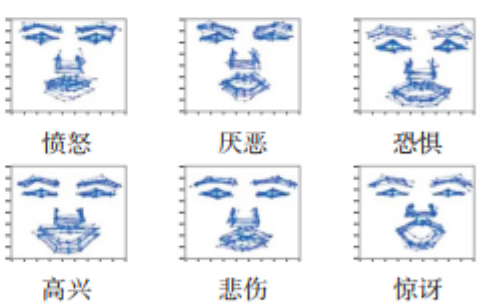



图3.1.11　6种表情模式的人脸关键特征点

Keras是由Python编程语言编写而成的深度学习库，后端基于TensorFlow、Theano以及CNTK（开源深度学习工具包）。Keras提供简单一致的API，可以满足一般应用情况的调用，还提供了清晰的、具有实践意义的纠错反馈。Keras具有高度模块化的特点，高层神经网络中的网络层、损失函数、优化器、初始化策略、激活函数和正则化方法等都是



微信公众号：电子课本大全

独立的模块，用它们可以很方便地构建神经网络模型。Keras具有很好的扩展性，添加新模块非常容易，只需要仿照现有的模块编写新的类或者函数即可。

利用Keras库可以很方便地搭建神经网络，如利用Keras序贯模型（从头到尾的线性结构顺序，不发生分叉）添加卷积层、池化层和全连接层，可构建卷积神经网络模型。利用该网络模型以及标注好的图像库，可以训练表情识别分类器，调用分类器即可完成表情识别。



## 实践活动

### 利用Keras实现表情识别

Keras是一个高层神经网络API，默认以TensorFlow为后端。

首先安装TensorFlow，可在命令行中输入“pip install tensorflow”。还可以用“pip install --upgrade tensorflow”命令更新TensorFlow的版本。

然后安装Keras，可在命令行中输入“pip install keras -U --pre”。

利用Keras搭建卷积神经网络，保存至模型mode.json中（见教学资源平台提供的资源包），使用常用表情图像数据库进行训练，得到分类器模型model.h5，然后使用该模型进行表情识别，代码如下：

```
import cv2
import sys
import json
import time
import numpy as np
from keras.models import model_from_json

expression_labels=["angry","fear","happy","sad","surprise","neutral"]
faceCascade=cv2.CascadeClassifier("haarcascade_frontalface_default.xml")

#载入模型文件和权重
json_file=open("model.json","r")
loaded_model_json=json_file.read()
json_file.close()
model=model_from_json(loaded_model_json)
model.load_weights("model.h5")

#预测表情
def predict_emotion(face_image_gray):
    re_img=cv2.resize(face_image_gray,(48,48),
                                        interpolation=cv2.INTER_AREA)
    image=re_img.reshape(1,1,48,48)
    list_of_list=model.predict(image,batch_size=1,verbose=1)
    angry,fear,happy,sad,surprise,neutral=
                        [prob for lst in list_of_list for prob in lst]
    return[angry,fear,happy,sad,surprise,neutral]

#表情识别
def classify(frame):
```



微信公众号：电子课本大全

```
        #检测人脸
        img_gray=cv2.cvtColor(frame,cv2.COLOR_BGR2GRAY)
        faces=faceCascade.detectMultiScale(img_gray,scaleFactor=1.1,
                                           minNeighbors=5,minSize=(30,30),flags=0)

        #绘制人脸区域，并标注表情
        for (x,y,w,h) in faces:
            face_image_gray=img_gray[y:y+h,x:x+w]
            cv2.rectangle(frame,(x,y),(x+w,y+h),(0,255,0),2)
            angry,fear,happy,sad,surprise,neutral=predict_emotion(face_image_gray)
            l=[angry,fear,happy,sad,surprise,neutral]
            max_index=l.index(max(l))
            frame=cv2.putText(frame,expression_labels[max_index],(x,y),
                    cv2.FONT_HERSHEY_SIMPLEX,1,(0,0,255),3)
            with open("expression_classifier.model","a") as f:
                f.write("{},{},{},{},{},{},{}\n".format(time.time(),angry,
                                                        fear,happy,sad,surprise,neutral))

frame=cv2.imread("01image.jpg")
classify(frame)
cv2.imshow("frame",frame)
cv2.imwrite("01emtion-result.jpg",frame)
cv2.waitKey(0)
```

表情识别的结果如图3.1.12所示，图中显示“happy”，表示识别出的表情为“高兴”。

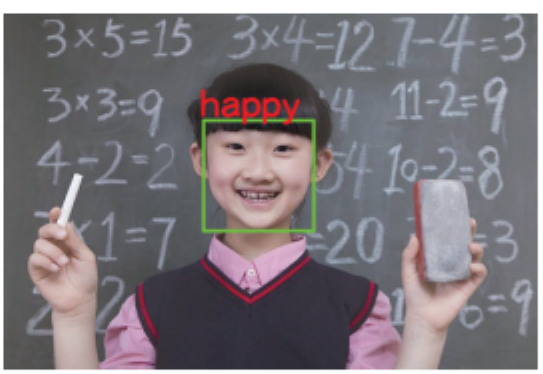



图3.1.12　表情识别结果



微信公众号：电子课本大全

## 项目实施

### 搭建智能陪伴机器人的物体识别模块

一、项目活动

1. 任选一个人工智能开放平台的“图像识别”模块，调用开放平台提供的SDK接口或者利用开源库，搭建图像物体识别模块。

2. 学习并实践计算机视觉的原理和技术，以识别图像中的物体为目标，绘制物体识别的流程图。

3. 按照流程图的要求，分工编写代码，完成至少两类物体的识别。

4. 讨论并理解项目实施过程中的原理、技术和方案等，并用思维导图呈现结果。

二、项目检查

1. 各小组明确分工，绘制智能陪伴机器人的物体识别流程图。

2. 充分调研各开放平台及开源库，完成网络模型搭建。

3. 小组合作完成物体识别模块。

4. 测试智能陪伴机器人的物体识别功能，要求能够识别不少于两类物体，例如动物、植物和车型等，如图3.1.13所示。




图3.1.13　某人工智能开放平台的识别结果示例

## 练习提升

1. 在一幅图像中，往往包含多类目标物体，如猫、人、杯子和玩具等。计算机是如何做到同时区分多类目标物体的？

2. 人脸检测及识别已经广泛应用于实际生活中。在人脸检测的基础上，计算机是如何识别出某人的身份信息的？

3. 围绕计算机视觉，绘制思维导图，梳理知识结构体系。



微信公众号：电子课本大全

# 3.2
# 自然语言处理

## 学习目标 ▶▶▶

- 理解自然语言处理的概念及其对人工智能的意义。
- 知道自然语言处理的发展历史和研究现状。
- 掌握人机对话的简单实现技术。
- 掌握语音识别和语音合成的简单实现技术。

## 体验探索

### 语音交互中的智能生活

向手机助理询问明天的天气情况，告诉智能音箱想听的音乐，用语音输入文字信息，使用语音测评软件纠正发音，使用语音翻译软件与国外友人交流……这都是因为计算机能够听到并理解人的语言，同时还能够模仿人的语气进行表达。

如图3.2.1所示，为了确定人类在讲什么，计算机必须能够分析它所接收的声音信号，并把这些信号复原成词的序列。同样的，为了生成回答，计算机必须把它的回答内容组织成词的序列，并且生成人类能够识别的声音信号。

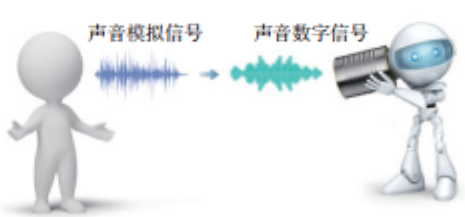



图3.2.1　人机语音交互

思考：

1. 列出5个以上自己接触过的能够接收人类自然语言（语音或文本）的智能工具，尝试分析语音识别功能的实现过程。

2. 讨论人与计算机之间的交流还有哪些应用场景，人工智能的哪些技术可以为这些场景提供应用支持。



微信公众号：电子课本大全

### 3.2.1 自然语言处理简介

从人工智能这门学科诞生之日起，让计算机理解人的语言并自然地与人交流，就是科学家们一直在努力追求的目标。计算机能够听、理解和说人的语言，即具有自然语言处理能力，意味着机器达到了真正的智能水平。

#### 自然语言处理的概念

“自然语言”指人们日常交流使用的语言，如汉语、英语和法语等。整个人类历史中，以语言文字形式记载和流传的知识占到知识总量的80%以上。相对于编程语言和数学符号这类人工语言，自然语言随着人类社会发展在不断演化，因而很难用明确的规则来描述。我们把处理口语和书面语（统称为“语言”）的计算机技术称为语音和语言处理技术，简称自然语言处理。

自然语言处理指利用计算机对自然语言的形、音、义等信息进行处理，即对字、词、句、篇章的输入、输出、识别、分析、理解和生成等进行操作与加工。这个定义包括从词数计算、自动换行等简单技术，到诸如自动问答、实时口语翻译等高级技术，还包括从最简单的通过统计词频来比较不同的写作风格，到最复杂的完全“理解”人类语言含义。

在人工智能领域，普遍认为采用图灵测试可以判断计算机是否理解了某种自然语言，具体评判标准有以下四条：

- 问答，机器能够正确回答输入文本中的有关问题；
- 文摘生成，机器有能力生成输入文本的摘要；
- 释义，机器能用不同的词语和句型来复述接收到的文本；
- 翻译，机器能把一种语言翻译成另一种语言。

#### 自然语言处理的发展

自然语言处理的历史可以追溯到图灵于1950年提出的图灵测试，经过了近70年的发展，其过程基本上可以分为三个阶段，如图3.2.2所示。

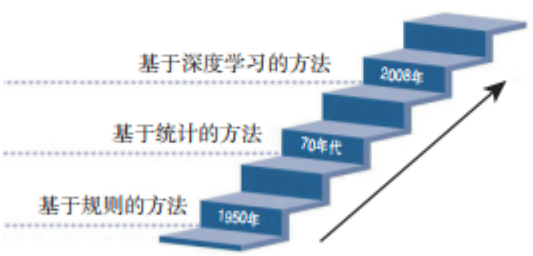



图3.2.2 自然语言处理的发展阶段

- 第一阶段：基于规则的自然语言处理

20世纪50年代到70年代，科学家认为计算机处理自然语言的过程与人类学习一门语言类似，他们试图用计算机算法描述语法、词性和构词法等规则，并导入语言学知识，从



微信公众号：电子课本大全

而建立基于规则的自然语言处理，如图3.2.3所示。基于规则的方法主要依赖人工总结的上下文无关文法的规则，但由于实际句子中的文法和语义十分繁杂，且与上下文甚至常识相关，人们很难写出涵盖所有自然语言现象的规则集合并用计算机来解析。因此，基于规则的自然语言处理给出的解决方案远远不能达到令人满意的效果。

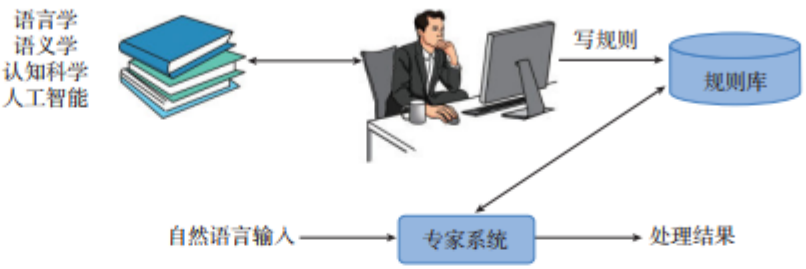



图3.2.3　基于规则的自然语言处理示意图

■ 第二阶段：基于统计的自然语言处理

20世纪70年代，高速发展的互联网提供了丰富的语料库，加上计算机计算能力的提升，科学家开始重新认识自然语言处理问题，提出了基于统计的自然语言处理方法，如图3.2.4所示。统计语言模型最初是为了解决语音识别问题，用文字序列出现的概率来衡量该文字序列是否能构成被人们理解且有意义的句子。基于统计的自然语言处理从数据入手，利用机器学习得到上下文无关文法的概率，通过概率模型预测句法分析结果。基于统计的方法在性能上有明显提升，但还是无法满足实际需求。以语音识别为例，说话者必须放慢语速，力求吐字清晰，机器才能达到令人满意的识别准确率。

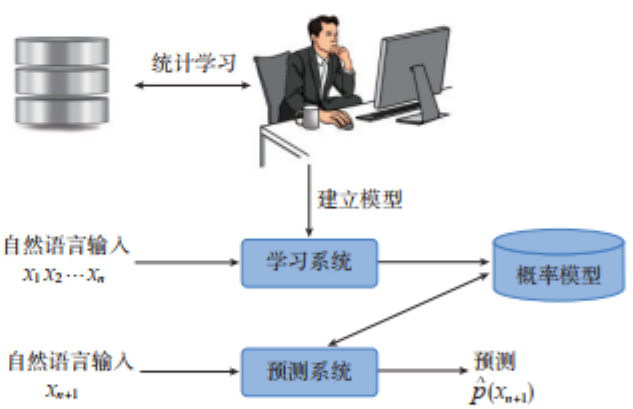



图3.2.4　基于统计的自然语言处理示意图

■ 第三阶段：基于深度学习的自然语言处理

如今，自然语言处理发展到统计模型与深度学习算法相结合的阶段，甚至深度学习算法已经占主导地位。基于深度学习的自然语言处理过程如图3.2.5所示。与依赖人工设计特征的传统机器学习方法不同，深度学习用向量表示单词、短语、逻辑表达式和句子，然后搭建多层神经网络，通过训练数据，自动学习合适的特征及其表征。同时，大规模数据和



微信公众号：电子课本大全

云计算的兴起使深度学习算法在自然语言处理领域进一步得到应用，真正将自然语言处理提升到了实用化的高度。

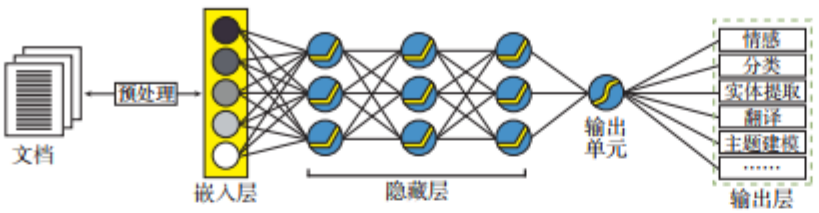



图3.2.5　基于深度学习的自然语言处理示意图

### 自然语言处理的研究及应用领域

自然语言处理的研究领域极为广泛。基础研究方面包括词汇、短语、句子和篇章级别的表示，以及分词、句法分析和语义分析、语言认知模型和知识图谱，此外还涉及词义消歧、指代消解和命名实体识别等。应用技术主要包括机器翻译、信息检索、信息抽取、情感分析、自动问答、自动文摘和社会计算等。

随着研究的不断深入和发展，自然语言处理的应用领域也越来越广泛。

文本方面的应用主要有智能搜索引擎和智能检索、智能机器翻译、智能推荐、自动摘要与文本综合、智能自动作文系统、自动判卷系统、文本分类与文件整理、信息过滤与垃圾邮件处理、语法校对、文本数据挖掘与智能决策以及基于自然语言的计算机程序设计等。

语音方面的应用主要有语音控制、机器同声传译、智能客户服务、机器聊天、智能交通信息服务、智能解说与体育新闻实时解说、语音挖掘与多媒体挖掘、多媒体信息提取与文本转化等。

## 阅读拓展

### 人类语言与机器智能

语言总是与认知能力联系在一起的。大约7万年前，人类就开始用以前所没有的方式进行思考和表达，并逐渐发展出人类特有的且完备的语言系统。借助语言，群居生活的人们得以更准确地表达、交流复杂的信息和情感，甚至产生抽象概念。语言成为最重要的生存工具和智能表现。

艾伦·图灵是第一个认识到计算机的认知能力与语言之间的关系的人，他在著名论文《计算机器与智能》中试图探讨到底什么是人工智能，并提出了著名的“图灵测试”。“图灵测试”的逻辑表明，人类语言足以作为测定机器智能的可操作标准。

1964—1966年间，美国麻省理工学院的约瑟夫·魏岑鲍姆（Joseph Weizenbaum）教授设计了一个名为Eliza的早期自然语言处理对话程序，以



微信公众号：电子课本大全

验证图灵的猜想。这个程序通过简单的模式匹配和对话规则，能与用户通过文本进行一定程度的交流，让人感觉好像是真的在与“人”交谈一样。图3.2.6是Eliza模拟心理医生与人的一段对话。

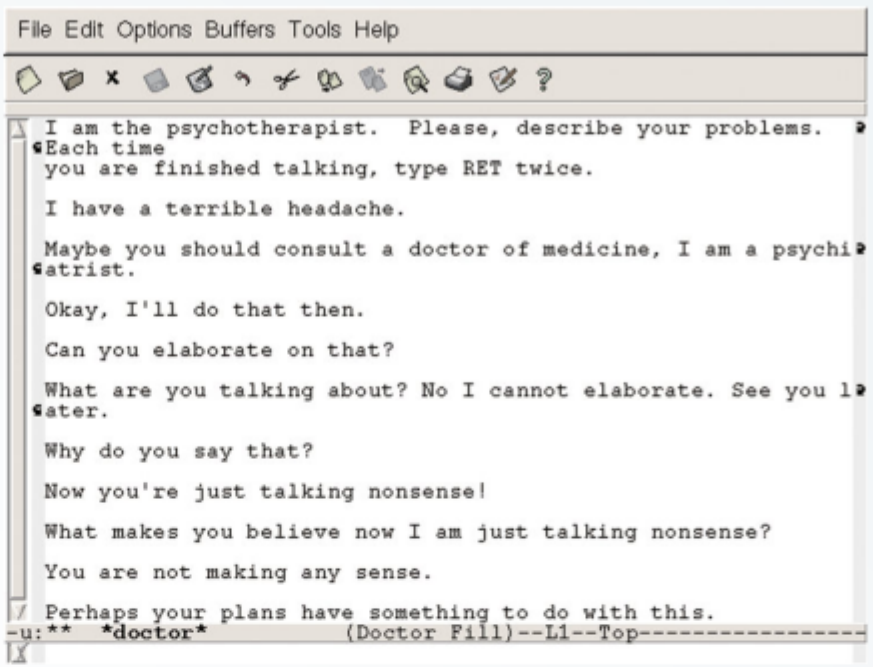



图3.2.6 Eliza模拟心理医生与人的对话

事实上，Eliza并不懂得如何模拟心理医生。它所做的几乎就是根据用户的问话，用关键字映射的方式，在一个相当有限的话题库里找到匹配的答案。比如，当用户说“你好”时，Eliza就说：“我很好，跟我说说你的情况。”此外，Eliza会用“为什么”“请详细解释一下”之类的引导性的句子，来让整个对话不停地持续下去。Eliza还可以借助人称的变化和句式的替换来重复用户的句子。如用户说“我感到孤独和难过”时，Eliza会说“你为什么感到孤独和难过”。就这样，Eliza虽然根本不理解用户到底说了什么，但却用这些小技巧在表面上“装作”可以理解自然语言的样子。

Eliza与图灵思想的深刻联系在于，很多与Eliza交流过的人都相信Eliza的确理解了他们所说的话以及他们提出的问题，甚至在把程序的操作过程向人们作了解释之后，仍然有不少人相信Eliza的能力。Eliza是科学家第一次实现聊天机器人（Chatbot）的尝试，也是现在流行的微软小冰、苹果Siri、谷歌Allo和亚马逊Alexa等智能语音助手的鼻祖。

### 3.2.2 自然语言处理的应用

在智能时代，通过语音进行人机交互显然是最自然、最便捷的方式。如何让智能陪伴机器人能听会说呢？首先要为机器人打造“听觉系统”，把语音信号转化为文本，这项


微信公众号：电子课本大全

技术就是“语音识别”；然后要让机器人识别和理解用文本表示的自然语言，并作出回复或执行命令，这是“对话系统”要解决的主要问题；最后由“语音合成”技术将机器人回复的文本转化为语音作为反馈。下面从“对话系统”开始，逐步实现智能陪伴机器人的语音交互功能。

### 对话系统

“对话”一直是自然语言处理领域的热门话题。对话系统也被称为聊天机器人，是一种以会话的形式与用户进行沟通的程序，是实现人机交互的一种方式。对话系统能部分或全部理解用户所说的内容，并能就问题进行回复。对话系统可以分为基于文字和基于语音两类。

先使用基于Python编程语言的开源自然语言处理工具包NLTK，体验一下与原始的文本对话系统聊天的感觉。NLTK开源库定义了一个使用Python编程语言进行自然语言处理的基础工具，提供了表示自然语言处理相关数据的基本类和实现词性标注、文法分析及文本分类等任务的标准接口，组合利用它们，可以解决复杂的自然语言处理问题。



**实践活动**

**尝试与NLTK的聊天机器人对话**

NLTK的聊天机器人包括心理医生Eliza、二次元少年Iesha、粗鲁的Rude、会说中国谚语的Suntsu，以及充满哲理的Zen。NLTK模拟了第一个聊天机器人Eliza，你能从对话中分辨出Eliza不是一位心理医生么？

```
>>> import nltk
>>> nltk.chat.chatbots( )
Which chatbot would you like to talk to?
1: Eliza (psycho-babble)
2: Iesha (teen anime junky)
3: Rude (abusive bot)
4: Suntsu (Chinese sayings)
5: Zen (gems of wisdom)

Enter a number in the range 1-5:  1
Therapist
---------
Talk to the program by typing in plain English, using normal uppercase
and lowercase letters and punctuation.  Enter "quit" when done.
========================================================================
Hello.  How are you feeling today?
>very sad
How do you feel when you say that?
>sadder
Please tell me more.
>I have too much homework that I cannot finish.
Have you really too much homework that you cannot finish?
>definitely
How do you feel when you say that?
>
```



微信公众号：电子课本大全

尝试与NLTK的聊天机器人对话，体验原始的对话系统。使用之前请先安装NLTK（在命令行执行命令“pip install nltk”）。

那么，像Eliza这样的机器人是如何理解用户输入的文本并产生回复的呢？在下面的实践活动中，将采用基于机器学习的聊天对话开源库ChatterBot，动手搭建一个文本聊天机器人来一探究竟。

ChatterBot是一个构建在Python编程语言上的基于机器学习的聊天对话引擎，可以利用已知的对话库进行学习并产生回应。ChatterBot响应用户输入的过程是：首先从已知句子中匹配出与用户输入最接近的句子，之后找到最有可能的回复。这个回复由所有与ChatterBot交流过的人对这个输入问题（匹配过的）的各个回答的频率决定。因此，一个ChatterBot机器人未经训练前，并不具备与用户对话所需的知识。每当用户输入一句话，机器人就保存这句话，同时也保存回复的句子。机器人接收的句子越多，它能够回答的问题数量就越多，答复准确率就越高。



## 实践活动

### 搭建ChatterBot聊天机器人

使用之前须先安装ChatterBot（在命令行执行命令“pip install chatterbot”）。

首先我们来教机器人“说话”。需要准备一段对话来训练机器人。

```
from chatterbot import ChatBot
# 创建一个新的聊天机器人名叫Chelsea
chatbot=ChatBot("Chelsea",trainer="chatterbot.trainers.ListTrainer")
# 对用户提供的对话列表或指定某语料库进行训练
chatbot.train([
                "你叫什么名字？",
                "我叫Chelsea。",
                "今天天气真好",
                "是啊，这种天气出去玩再好不过了。",
                "那你有没有想去玩的地方？",
                "我想去有山有水的地方。你呢？",
                "还有好多作业没做呢",
                "哈哈，这就比较尴尬了",
            ])
#对用户循环输入的文本进行响应并输出
while True:
    print(chatbot.get_response(input("user:")))
```

运行代码就可以和机器人聊天了。下面是一段测试代码（user代表用户）：

```
user:你好！
你好！
user:想出去玩吗？
我想去有山有水的地方。你呢？
```



微信公众号：电子课本大全

```
user:我想去游乐场。
我梦想我会变得富有。
user: 你最喜欢的歌手叫什么名字?
我叫Chelsea。
user:你多大了?
我可以生气。
```

可见，我们搭建的机器人Chelsea关于闲聊话题回答的正确率并不高。机器人“读”到“想出去玩吗？”后，在已经训练的句子中找到了最相近的一句话“那你有没有想去玩的地方？”并通过这句话找到回答的句子“我想去有山有水的地方。你呢？”然而，这种最相近的方式，并不能总是找到准确的回答。当机器人“读”到“你最喜欢的歌手叫什么名字？”后，找到了最相近的一句话“你叫什么名字？”从而作出“我叫Chelsea。”的回答。

那么，如何才能提高机器人回答的正确率呢？我们可以采用语料库来构建训练的语料。ChatterBot提供了一些简单的聊天语料库，包括汉语、英语和西班牙语等不同语种。下面说明如何加载ChatterBot的语料训练机器人。

```
from chatterbot import ChatBot
chatbot=ChatBot("Chelsea",
                trainer="chatterbot.trainers.ChatterBotCorpusTrainer")
#用ChatterBot自带的语料数据训练机器人
chatbot.train("chatterbot.corpus.chinese")
#对用户循环输入的文本进行响应并输出
while True:
    print(chatbot.get_response(input("user:")))
```

运行程序再测试一次，会发现训练后的聊天机器人还是有点答非所问，这是因为ChatterBot自带的语料仍然比较简单。如果需要聊天机器人有更好的表现，实际搭建时可以通过其他方式补充更多的语料。可以说，语料的质量决定了聊天机器人的“智能”。

除了语料之外，还有什么可以决定机器人的“智能”呢？在ChatterBot中，逻辑适配器定义了机器人从处理输入数据到给出回复的逻辑。在下面的示例中，使用了两个逻辑适配器：MathematicalEvaluation用来回答一些基本的数学计算问题，TimeLogicAdapter用来回答询问当前时间的问句。

```
from chatterbot import ChatBot
chatbot=ChatBot(
              "Math & Time Bot",
              logic_adapters=["chatterbot.logic.MathematicalEvaluation",
                              "chatterbot.logic.TimeLogicAdapter"],
              input_adapter="chatterbot.input.VariableInputTypeAdapter",
              output_adapter="chatterbot.output.OutputAdapter"
               )
# 打印一个获取数学问题响应的例子 (注意数字与加号之间的空格)
response=chatbot.get_response("What is 4 + 9?")
```



微信公众号：电子课本大全

```
print(response)
# 打印一个获取时间问题响应的例子
response=chatbot.get_response("What time is it?")
print(response)
```

1. 查阅相关资料，了解ChatterBot还有哪些处理输入、产生回复的逻辑适配器。

2. 如何进一步提高你所搭建的聊天机器人的“智能”？

## 技术支持

### ChatterBot

ChatterBot将聊天机器人分为输入适配器、逻辑适配器、存储适配器、输出适配器以及训练器几个部分。输入适配器用来获取用户输入的内容，并将其转化为可以进行下一步处理的语句对象。集成语音识别服务商的接口，就可以接受语音输入。逻辑适配器对转化后的输入进行逻辑处理，通过匹配，计算回答，选择出置信度最高的回答。存储适配器将逻辑处理所需的训练集持久化。输出适配器处理输出，与语音合成服务商的接口集成，就可以“开口说话”了。训练器提供训练机器人的方法，自带的训练方法有两种：一种是通过输入列表来训练（比如["你好", "你好啊"]，后者是前者的回答）；另一种是通过导入语料库来训练，用户可以导入已经存在的语料库，也可以自定义语料库。ChatterBot独特的语言设计使它可以通过训练来用多种语言进行对话。处理流程如图3.2.7所示。

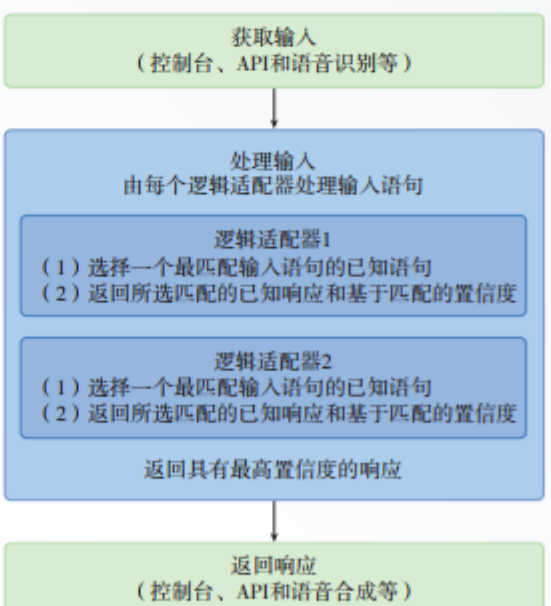



图3.2.7　ChatterBot的处理流程图



微信公众号：电子课本大全

至此，搭建了一个基于文本的聊天机器人。它的回答效果可能差强人意，不过现在诸多流行的商业聊天机器人，还不能进行常识推理或描述知识。自然语言处理研究的一个重要目标就是使用技术完成无限的知识学习和推理，以此来构建智能机器。

### 语音处理

早期基于文本的对话系统如今已发展至口语，并以移动设备作为信息入口和应用载体。生活中常见的人机对话场景大多应用了语音对话系统。例如，个人数码助理（Personal Digital Assistant，PDA）掌握了用户存储在设备上的一些个人基本信息，并记录了用户与系统的交互历史，可以更好地服务用户，如完成拨打电话号码、安排会议、回答问题和搜索音乐等任务。又如，通过语音搜索，用户可以查询餐馆、行驶路线和商品评价等信息，极大地简化了用户搜索请求的输入方式。搜索引擎也已提升到了智能问答、智能助理、智能搜索的新高度。在融合了语音技术的游戏中，玩家可以通过语音发出指令，或通过对话与游戏中的角色互通信息。起居室交互系统和车载信息娱乐系统允许用户使用语音与系统交互，用户通过语音来控制音乐的播放、询问信息等。

如图3.2.8所示，语音对话系统主要包括将语音转化为文本的语音识别系统、提取用户话语信息的自然语言理解系统、生成文本答复的自然语言生成系统、将文本内容转化为语音的语音合成系统，以及完成与实际应用场景沟通的对话管理系统。

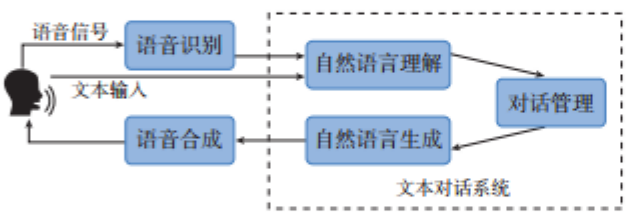



图3.2.8　语音对话系统组成示意图

为了直接与所搭建的机器人进行语音对话，需要进一步了解人机交互中最常见的语音识别和语音合成技术。

■ 语音识别

语音识别技术也被称为自动语音识别。1952年，世界上第一个语音识别系统由贝尔实验室研制实现，能识别出10个英文数字发音。语音识别以语音为研究对象，通过语音信号处理和模式识别让机器自动识别人类的语音。从语音中提取文字、命令、甚至意图，将语音中的词汇内容转换为计算机可接受的输入（例如二进制编码或者字符序列）。

语音识别技术流程如图3.2.9所示，语音信号首先通过麦克风输入，经过信号预处理模块（降噪、回声消除等）过滤不利于识别的内容，由特征提取模块提取出有利于识别文字的部分，如音调、字数等，匹配声学模型（波形）得到“声音”信息，最后匹配语言模型（类似查字典）得到文字。该流程中最重要的环节是声学模型和语言模型的匹配。



微信公众号：电子课本大全

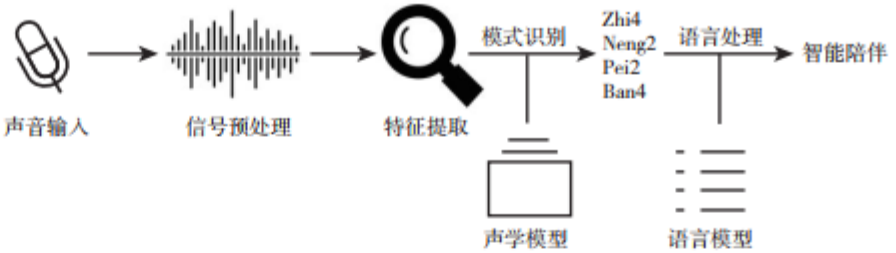



图3.2.9　语音识别技术流程示意图

## 实践活动

### 初探语音识别

1. 访问教学资源平台，下载语音识别示例，其中包含示例代码AipSpeech.py、语音转换工具“tool文件夹”及测试语音文件。

2. 打开命令行，进入示例文件所在目录。

3. 执行“pip install baidu-aip”命令，安装语音识别包python sdk。

4. 执行“python AipSpeech.py test01.wav”命令，运行演示示例。

5. 制作自己的音频文件（WAV格式），并识别出文字信息。

■ 语音合成

语音合成是将计算机产生的或外部输入的文本信息转化为可听的声音信息的一种技术，是人机交互中必不可少的一个环节。汽车导航内嵌的语音系统、智能手机语音助手和听书软件等，都离不开语音合成。让机器拥有高拟人化的声音，而不再是机械、僵硬、毫无感情地“说话”，是语音合成研究者追求的目标。随着技术的发展，合成后的语音的自然度和音质都得到了明显的改善。语音合成技术流程如图3.2.10所示。

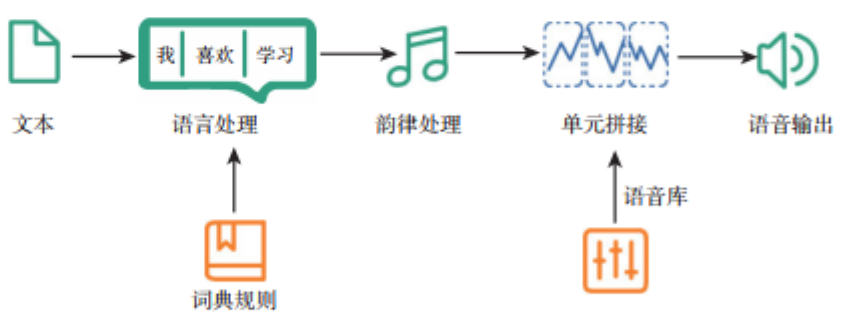



图3.2.10　语音合成流程示意图

要合成语音，首先需要建立语音库，把录音的句子切成独立的基本单元，再根据合成需求，将基本单元排列组合，拼接起来。超大规模语音库的制作涉及语料设计、音库录制、精细切分和韵律标注等十分繁杂的工作。语音合成的研究方向是实现更清晰的音质、更自然的韵律和间隔停顿，以及更小的语音库体积、更低的运算量和系统开销。语音合



微信公众号：电子课本大全

成研究的难点在于为合成后的语音赋予不同的年龄和性别特征，并通过语气、语速表达个人的情感、态度。

### 实践活动

#### 初探语音合成

1. 访问教学资源平台，下载语音合成示例，其中包含示例代码AipSpeech.py及测试文本。

2. 打开命令行，进入示例文件所在目录。

3. 执行“pip install chardet”命令，安装文本编码检测库。

4. 执行“pip install baidu-aip”命令，安装语音识别包python sdk。（如在语音识别示例中已安装，可跳过此步。）

5. 执行“python AipSpeech.py ttest01_anscii.txt”命令，运行演示示例。

6. 制作自己的文本文件（TXT格式），合成新的音频。



微信公众号：电子课本大全

## 项目实施

### 搭建智能陪伴机器人语音对话模块

现在就来试着让我们的智能陪伴机器人和我们聊天吧！想象一下，我们搭建的智能陪伴机器人有什么特别的本领？试设计一个个性化的项目方案，实现某个场景应用，如教低龄儿童学算术、搜索并播放用户想听的歌曲、用纯正口音的英语陪练口语……

一、项目活动

1. 尝试调用 ChatterBot（或其他聊天对话引擎）开发聊天对话模块，实现人机对话功能。

2. 任意选用人工智能开放平台，通过调用开放平台提供的SDK开发语音模块，实现语音识别和语音合成功能。

3. 在聊天对话模块中加入语音模块，集成为语音对话模块，实现语音交互功能。

4. 根据小组设计的个性化项目方案，细化语音对话模块的功能。

二、项目检查

1. 各小组提交项目计划方案，介绍项目要解决的主要问题、拟采用的方案，并绘制流程图，制订分工及时间计划。

2. 各小组提交源代码，并写明注释，体现代码的实现情况。

3. 各小组提交项目总结报告，介绍项目已解决的主要问题、所采用的方案，绘制流程图，并详细介绍对各模块核心技术原理的理解。

## 练习提升

1. 生活中每个人都有自己的语言风格。如何训练聊天机器人，让它具有独特的聊天风格呢？

2. 如何增强聊天机器人的性能，让它无所不知？

3. 如何让聊天机器人实现自我学习后，表现得似乎拥有人的智能？



微信公众号：电子课本大全

# 3.3
# 机器理解与推理

## 学习目标 ▶▶▶

- 了解机器理解与推理的发展历程和现状。
- 体会认知科学与脑科学在人工智能中的重要作用。
- 通过实例了解典型机器理解与推理（机器定理证明）的基本原理。

## 体验探索

### 智力问答

2011年，能够使用自然语言回答问题的认知计算系统——沃森，在美国最受欢迎的智力问答电视节目中亮相，一举打败了人类智力竞赛的冠军（图3.3.1），展示了当时最先进的问答交互。2017年，我国研发的小度机器人在科学类脑力学习节目中获胜（图3.3.2）。除了答题，这类智能机器人还具备理解、推理以及学习的能力，可以处理更多的复杂数据集。




图3.3.1　沃森打败人类智力竞赛的冠军



图3.3.2　小度机器人在脑力比赛中获胜

认知计算的目标就是发现潜藏在非结构化数据中的模式，以便我们能够对重要的事情作出明智的判断。机器的数据分析、统计和推断能力将会是机器认知的真正潜力所在。

思考：

1. 查阅资料，了解沃森能做哪些具体的认知和推理任务？有哪些具体应用？

2. 探索国内外有代表性的智能机器，体验智能机器的认知与推理功能。如百度小度机器人和微软小冰机器人等。



微信公众号：电子课本大全

### 3.3.1 机器理解与推理的发展和现状

机器理解和推理一直被认为是人工智能最集中的体现。一个可以不需要人控制的独立机器人，比如家庭服务机器人，必须像人类一样有认知、有记忆，而且能根据人类的喜好进行活动。

#### 机器理解

人类的认知指通过心理活动（如形成概念、知觉、判断或想象）获取知识。机器的认知即机器理解，代表一种全新的计算模式，包含信息分析、自然语言处理和机器学习领域的大量技术创新，能提高决策者对大量结构化和非结构化数据的洞察能力。

让人工智能像人一样学习和思考，并作出正确的决策，是机器理解的目标之一。人脑与电脑各有所长，机器理解系统可以成为一个很好的辅助性工具，配合人类解决人脑不擅长解决的问题。

目前，人工智能在视觉及语音等应用领域已经取得了长足发展，但是在机器理解方面仍然处于起步阶段。沃森是机器理解系统的杰出代表，它可以回答知识问答竞赛的问题，并战胜人类对手。从算法流程的角度分析，沃森处理问题的步骤如下：

1. 将问题分解为多个关于该问题的特征；
2. 在大量可能包含答案的信息中进行搜索，然后生成一系列潜在答案；
3. 使用特有的算法，为每一个潜在答案打分；
4. 提供评分最高的答案，以及答案的相关证据；
5. 对评分进行权衡，为每个答案的评分指数进行评估。

#### 机器推理

从一个或几个已知的判断（前提）逻辑地推论出一个新的判断（结论）的思维过程称为推理。这是事物的客观联系在意识中的反映。自动推理是知识的使用过程，人类解决问题往往就是利用以往的知识，通过推理得出结论。自动推理的理论和技术是程序推导、程序正确性证明、专家系统和智能机器人等研究领域的重要基础。



**阅读拓展**

**三段论推理**

亚里士多德在他的著作《前分析篇》中提出了三段论的逻辑分析方法。他给出了三段论的定义："只要确定某些论断，某些异于它们的事物便可以必然地从如此确定的论断中推出。"通俗地说，就是只要给定了大前提和小前提，就能推出确切的结论。例如，亚里士多德曾就"苏格拉底之死"发表过著名的三段论：



微信公众号：电子课本大全

“人都会死。”……大前提

“苏格拉底是人。”……小前提

“所以苏格拉底会死。”……结论

三段论是一种常用的推理形式，它由三个性质命题组成，其中两个性质命题是前提，另一个性质命题是结论。

例如：

科学是不断发展的。……大前提

智能科学是科学。……小前提

所以，智能科学是不断发展的。……结论

这就是一个三段论。前两个性质判断包含着一个共同项——“科学”，由这两个具有共同项的判断可推出一个新的性质判断：智能科学是不断发展的。

可能人们很难将亚里士多德的三段论与人工智能联系起来，但正是他所提出的这套推理系统，使逻辑迈上了形式化的轨道。后人在此基础上对其理论不断完善，使逻辑学的发展取得了很大的进步，尤其是布尔代数的发现，使计算可以通过逻辑变换得到。

早期的自动推理工作主要集中在机器定理证明方面。德国数学家莱布尼茨早在17世纪中叶就提出用机器实现定理证明的思想。19世纪，“思想语言”的形式系统，即后来的谓词演算出现，奠定了符号逻辑的基础，为自动推理提供了必要的理论工具。20世纪50年代，电子计算机的出现和应用，加上数理逻辑的发展，使机器证明定理开始变为现实。

证明定理是人类特殊的智能行为，不仅需要根据假设进行逻辑演绎，而且需要某些直觉技巧。机器定理证明就是把人证明定理的过程通过一套符号体系加以形式化，转变成一系列能在计算机上自动实现的符号演算过程，也就是把具有智能特点的推理演绎过程机械化。

机器定理证明是人工智能的重要研究领域，它的成果可应用于问题求解、自然语言理解、程序验证和自动程序设计等方面。尽管数学定理证明过程的每一步都严谨有据，但决定采取什么样的证明步骤，却依赖于经验、直觉、想象力和洞察力，需要人的智能。因此，数学定理的机器证明和其他类型的问题求解，就成为人工智能研究的起点。

在几何定理的机器证明方面，我国著名科学家吴文俊院士提出了平面几何及微分几何的判定法，得到国内外专家的高度评价。张景中院士与合作者创立的计算机生成几何定理可读证明的原理与算法，使这一人工智能领域30多年来进展缓慢的重要问题有了突破性的进展，在国际上取得了公认的领先地位，被誉为计算机处理几何问题的里程碑。



微信公众号：电子课本大全



**阅读拓展**

### 机器定理证明——吴方法

1977年，吴文俊证明初等几何一类主要定理的证明可以机械化（即刻板化、程序化和算法化）。1978年，吴文俊又证明初等微分几何中的一些主要定理的证明也可以机械化。其后，他把机器定理证明的范围推广到非欧几何、仿射几何、圆几何、线几何和球几何等领域。继机器定理证明之后，吴文俊把研究重点转移到数学机械化的核心问题——方程求解上来，得出了作为机械化数学基础的整序原理及零点结构原理，这不仅可用于代数方程组，还可以解代数偏微分方程组，大大扩展了理论及应用的范围。

吴方法不仅应用于机器定理证明、代数系统求解的理论和算法，而且在物理学、化学、计算机科学、数学科学和机器人机构学等方面的应用也都取得了国际领先成果。很多时候，机器给出的证明非常出人意料，更为简洁巧妙。吴方法在机器人路径规划、数控机床、计算机图形学和计算机视觉等方面都有很好的应用。

2017年，机器人作答两套高考数学文科试卷，分别取得了134分、105分的成绩。这一技术背后的核心即综合复杂推理，由自然语言加逻辑引擎组成，覆盖了所有需要综合逻辑推理加数理建模推理的领域。

从几何解题到高考机器人，机器证明在工程领域与教育领域实现着跨步和共生，一步一步突破难点，取得了巨大成就。当前，大数据时代的人工智能发展处于感知智能阶段，机器具有视觉、听觉和触觉等感知能力。随着类脑科技的发展，认知推理必将翻开崭新的一页，推动人工智能向认知智能时代全面迈进。到那时，智能机器有极大可能实现理解、思考的功能。

## 3.3.2 人工智能与脑科学

脑科学（认知科学）与人工智能领域的交叉探索，可以加强我国在智能科学这一交叉领域中的基础性、独创性研究，解决脑科学和信息科学发展中的重大基础理论问题，创新类脑智能前沿领域的研究。研究人脑信息处理的方法和算法，发展类脑计算成为当今人工智能发展的迫切需求。



微信公众号：电子课本大全

## 思考活动

### 人工智能精神病专家系统

“埃莉”是世界上首个人工智能精神病专家系统，由美国国防部高级研究计划局和南加州大学创新技术学院共同设计和研发，用于识别早期心理健康隐患，比如识别士兵的抑郁、焦虑信号，以及创伤后的应激障碍等。

思考：

人工智能技术与应用（如人工智能辅助医疗诊断、人工智能辅助儿童自闭症治疗、人工智能艺术创作及人工智能自动作曲等）有哪些跨学科特点？

### 脑科学

目前，国际上非常重视脑科学的研究。2013年1月，欧盟启动了“人类大脑计划”，此后10年计划投入10亿欧元的研发经费，目标是用超级计算机完全模拟人脑，帮助理解人脑功能。2013年4月，美国宣布计划用10年左右时间进行“运用先进创新型神经技术的大脑研究”，目标是研究数十亿神经元的功能，探索人类感知、行为和意识的奥秘，找出治疗阿尔茨海默病（老年痴呆症）等与大脑有关疾病的方法。

我国也全面启动了脑科学计划。“中国脑计划”形成了开展脑认知原理基础、脑重大疾病、类脑人工智能的研究格局。类脑计算和人工智能研究是“中国脑计划”的重要组成部分，将以类脑人工智能研发及产业化为核心。类脑智能研究将借鉴脑的多尺度结构及认知机制，提出并实现受脑信息处理机制启发的智能框架、算法与系统。

人类的智能主要包括归纳总结和逻辑演绎，分别对应着人工智能中的联结主义（如人工神经网络）和符号主义（如吴方法）。人类对视觉和听觉信号的感知与处理都是下意识的，是基于大脑皮层神经网络的学习；人类对逻辑推导、定理证明是主观意识的，是基于公理系统的符号演算。

■ 联结主义

联结主义的方法虽然具有很高的实用价值，但是依然没有坚实的理论基础。即便通过仿生学和经验积累得到了一些突破，机器依然无法像人类一样做到在认知领域的透彻理解和预测。简单的神经网络学习机制加上超强的机器计算能力，能否真正实现从量变到质变的转变，这需要时间的检验。

■ 符号主义

机器无法抽象出几何直觉，也无法建立审美观念。因此，虽然机器定理证明经常能对已知的定理给出新颖的证明方法，但是迄今为止，机器并没有自行发现深刻的未知数学定理。与人类智慧相比，人工智能的符号主义方法依然处于相对初级的阶段。

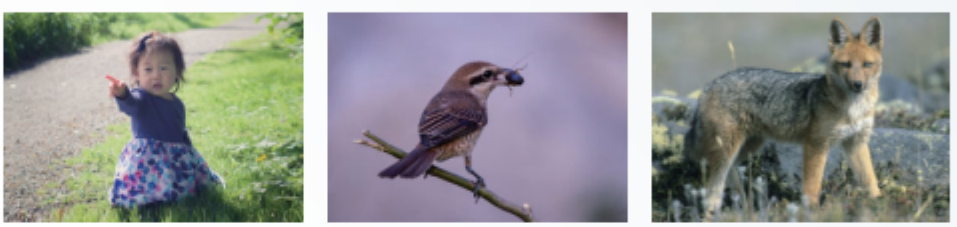


微信公众号：电子课本大全

## 阅读拓展

### 走进内心世界

小孩在一岁左右就能够明白对方的意图。一个关键证据是：小孩会指着东西给大人看，大人看到还是没看到，小孩会知道，如图3.3.3(a)所示。不仅人有侦察与反侦察的能力，动物也有。例如，鸟在藏食物的时候，会查看周围是否有其他鸟类或动物注意到了它，如图3.3.3(b)所示。如果有，它就不藏，并一直等待合适的机会。这就是鸟对周围环境的观察，它知道其他动物的想法。图3.3.3(c)是一只狐狸与水獭对峙的视频截图。水獭抓到鱼之后，发现这只狐狸在岸上盯着它，它知道这只狐狸想抢它嘴里叼着的鱼，就想办法把鱼藏了起来，然后这只狐狸就去寻找。这说明动物之间互相知道对方在想什么。



(a)　　(b)　　(c)

图3.3.3　动物与人对外界的主动应对行为

我们要设计的机器人，就是希望它能知道人类想干什么，这是人工智能的一个核心表现。

### 脑科学和人工智能相互促进

人们对视觉注意力、抉择和学习等认知功能的大脑神经网络机制的研究方兴未艾。发展脑科学基础研究，将促进“深度学习”等类脑智能技术的蓬勃发展。

没有世界一流的脑科学，就不可能有世界一流的类脑智能技术创新。反之亦然，机器学习（包括深度学习）能引进新的方法处理脑科学数据，将带来模拟脑功能的新思路。因此，计算神经科学与信息科学研究应密切合作，联合攻关脑科学与类脑人工智能重大前沿问题。将脑科学与人工智能相结合，可从人工智能的角度来研究如何更好地认识和缓解少年自闭症、中年抑郁症和阿尔茨海默病等疾病。

## 阅读拓展

### 《新一代人工智能发展规划》中对人工智能的跨学科要求

重视复合型人才培养，重点培养贯通人工智能理论、方法、技术、产品与应用等的纵向复合型人才，以及掌握“人工智能+”经济、社会、管理、标准、法律等的横向复合型人才。



微信公众号：电子课本大全

建设人工智能学科。鼓励高校在原有基础上拓宽人工智能专业教育内容，形成“人工智能+X”复合专业培养新模式，重视人工智能与数学、计算机科学、物理学、生物学、心理学、社会学、法学等学科专业教育的交叉融合。加强产学研合作，鼓励高校、科研院所与企业等机构合作开展人工智能学科建设。

开展跨学科探索性研究。推动人工智能与神经科学、认知科学、量子科学、心理学、数学、经济学、社会学等相关基础学科的交叉融合，加强引领人工智能算法、模型发展的数学基础理论研究，重视人工智能法律伦理的基础理论问题研究，支持原创性强、非共识的探索性研究，鼓励科学家自由探索，勇于攻克人工智能前沿科学难题，提出更多原创理论，作出更多原创发现。

### 3.3.3 认知推理的实践应用与展望

除了前面提到的知识问答及自动定理证明等方面的实际应用之外，认知推理在人工智能第三次浪潮发展中也有许多新的进展。例如，沃森的认知计算用于实现专家级别的癌症诊断及治疗方案建议，新一代人工智能助理（苹果的Siri、谷歌的Google Now、三星的Bixby、微软小冰和百度小度）用于日常生活管理等。人工智能越来越能够走进人的内心，也在视觉与语言的认知方面有了长足发展。

下面我们通过微软“小冰读心术”小游戏来解析人工智能“读心术”的技术原理。

游戏的规则很简单，即你在脑海里想好一个人的名字，然后小冰会问你15个问题，每个问题你只能用“是”“不是”“不知道”作答。小冰根据你的回答进行推断、分解，逐步缩小人名范围，最终猜出答案。这与决策树的工作原理非常类似。

假如你想好的人名是鲁迅，下面是15个问题的问答内容：

你：开始
小冰：确认你已经想好了吗？那么，我开始提问了。听好，第一个问题是——他是在中国出生的吗？
你：是
小冰：他是男的吗？
你：是
小冰：他是虚拟人物吗？
你：不是
小冰：他是娱乐圈里的人吗？
你：不是
小冰：第五个问题，他是1960年之前出生的吗？
你：是
小冰：他上过大学吗？
你：不知道
小冰：他是历史中的人物吗？
你：不是
小冰：第八题！他是不是已经去世了？
你：是
小冰：他是革命家吗？
你：是



微信公众号：电子课本大全

小冰：十个问题了！他是曾经的国家领导人吗？
你：不是
小冰：他参加过长征吗？
你：不是
小冰：他有过参军经历吗？
你：不知道
小冰：这下我心里有数了！倒数第三个问题：他是1980年以前去世的吗？
你：是
小冰：还有最后两个问题。他是文学家吗？
你：是
小冰：最后一个问题！他的胡子是不是能给人留下很深印象？
你：是
小冰：完成！我有答案了，哼哼，他就是——鲁迅！怎么样？

可见，小冰成功地猜出了正确人名“鲁迅”。这个过程所构建的决策树如图3.3.4所示。

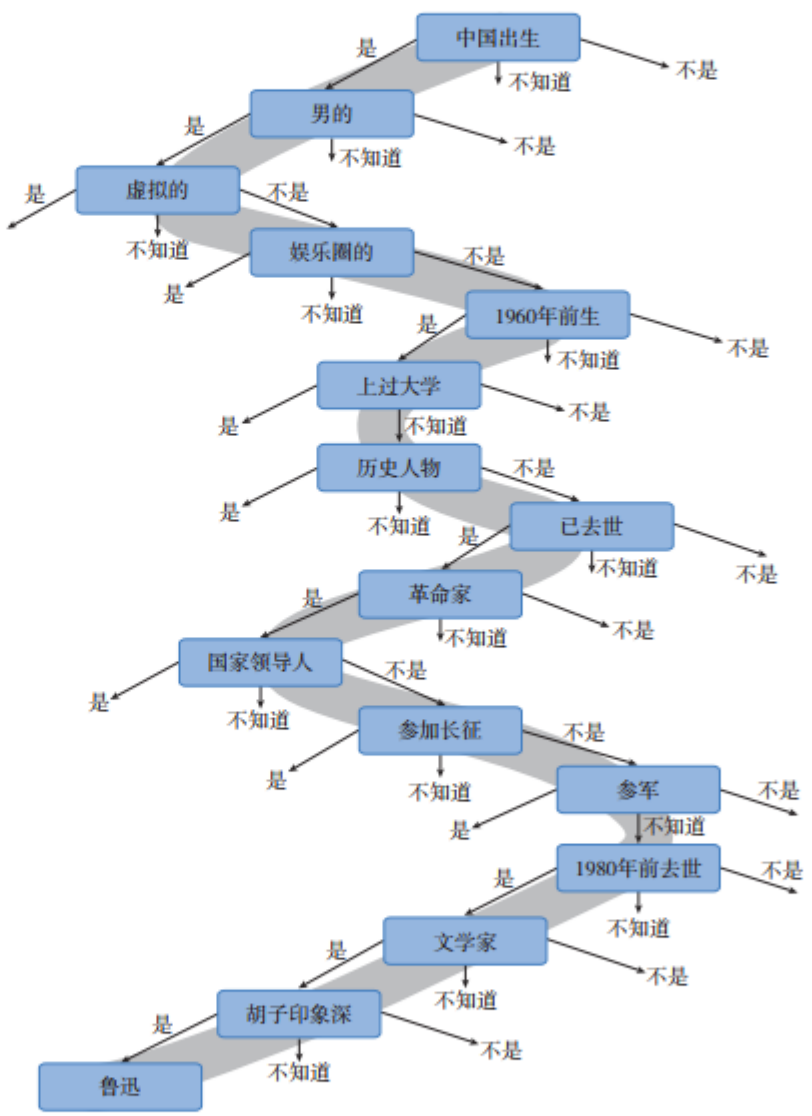



图3.3.4　微软小冰回答问题的过程中构建的决策树


微信公众号：电子课本大全

图像理解和自然语言对话系统都是当前热门的研究领域。基于图像的自然语言对话系统融合了这两个热门领域，以期教会机器使用自然语言与人类讨论视觉内容。通常将这一研究方向简称为“视觉对话”，它利用计算机视觉、自然语言处理和对话系统等前沿技术，达到教会机器使用自然语言与人类交流视觉信息的目的。

通常所说的“对话系统”覆盖的范围很广，下面举两个实例：

1. 为特定目标设计的任务驱动型聊天机器人，如智能客服机器人、机票助手机器人等，它们只能在特定的任务情景下进行简单的对话；

2. 自由对话机器人，如可以与人进行自然交流的、不受任何特定场景限制的聊天机器人，可以随心所欲地和人闲聊。

视觉对话的研究成果介于上述两类机器人具有的功能之间，即它能提供自由的对话，但是对话的内容却仅限于一个具体的图像，如图3.3.5所示。



图3.3.5　视觉对话示例

## 实践活动

### 视觉与语言的联合

“看图说话”本质上是视觉与语言之间的融会贯通，是人类经过漫长的进化与不断的学习所形成的能力。对于机器而言，这意味着视觉处理与语言处理两个领域的联合。

视觉与语言联合的一个典型应用就是聊天机器人微软小冰。小冰不仅可以通过文本、语音跟人聊天，还可以根据图片用视觉方式与人交流。当小冰有了视频聊天的功能之后，它的用户数量在一个月之内增加了60%。有意思的是，很多人不知道小冰只是一个机器人。

视觉与语言的联合也可以应用于搜索领域，即可以用视频搜索语言，也可以用语言搜索视频。此外，视觉与语言的联合还可以基于视频自动生成报告，告诉我们在什么时间发生了什么事情。

1. 搜索网上视觉对话开放平台，选择其一上传图片，试验平台的视觉对话功能，体验机器的认知推理功能。

2. 思考计算机视觉与自然语言处理的联合应用能否提高机器的认知推理能力，提出自己的观点，并举例说明理由。

随着人工智能算法的进步、计算能力的提高、数据的不断积累，以及视觉、语音感知技术的进一步发展，未来人工智能的视觉感知与自然语言理解能力将会得到更大的提升，其对大脑如何产生心智、大脑如何工作的理解会更加深刻。全方位跨领域的创新合作即将到来，这将推动人工智能认知推理的研究迈上新台阶。



微信公众号：电子课本大全

## 项目实施

### 搭建认知推理模块

一、项目活动

1. 访问教学资源平台，下载机器理解与推理部分的Python程序，按照说明进行配置、安装。

2. 运行Python程序，就2～3个与“智能陪伴机器人”相关的问题进行体验和记录，构建对应的决策树，并解析原理。

3. 探究推理知识库，修改某一类物体的相关问题及连接，看程序运行结果如何变化。

4. 编写新的推理规则，为智能陪伴机器人构建简单的认知推理模块。

二、项目检查

1. 各小组基于提供的参考代码进行实践，构建基于具体问题的决策树，并详细介绍“读心术”游戏的原理和技术。

2. 更新知识库和推理规则后，就效果作对比研究，并将结论在全班展示交流。

3. 搭建智能陪伴机器人的简单认知推理模块，使之能够与人交互，进行简单的问答游戏。

## 练习提升

本节“读心术”猜人物名字的例子，如果回答只有“是”“否”两种选择，也就是我们常说的二值化结果，对应的决策树也就是一个典型的二叉树。

1. 如图3.3.6所示，将回答扩展为“是”“否”“或许”“部分地”“罕见地”“接近”六种，以猜测“猫”的过程为例，构建这一过程的决策树。

2. 同学们两人一组，构建回答的规则（多种可能性），采用一问一答形式，进行“读心术”游戏。可以按同一主题，对比人类智能与机器智能在这个游戏中的认知推理能力。

**17. 我猜它是家猫？**
**是，否，接近**

16. 它是爬行动物吗？否。
15. 它可否放置在您的头上？或许。
14. 它是棕色的吗？部分地。
13. 它有犬牙吗？否。
12. 它会否发出咆哮声？罕见地。
11. 它会否抓伤人？是。
10. 它有没有现金价值？是。
9. 它是不是有多种款式？是。
8. 它可以食用吗？罕见地。
7. 您喜欢它吗？是。
6. 它很烦人吗？否。
5. 它能提供保护作用吗？否。
4. 它可否双腿直立？罕见地。
3. 它有危险性吗？或许。
2. 它是野生动物吗？否。
1. 它是动物吗？是。

图3.3.6　人机交互问答



微信公众号：电子课本大全

# 3.4
# 博弈决策

## 学习目标 ▶▶▶

- 了解博弈决策的发展历程、典型应用。
- 通过剖析具体案例，了解强化学习的基本模型与实现原理。
- 利用开源库和人工智能开发平台，搭建简单的博弈决策应用模块。

## 体验探索

### 围棋人工智能：绝艺

绝艺是一款由我国科研团队自主研发的围棋程序（图3.4.1），名称取自唐朝诗人杜牧的诗句“绝艺如君天下少，闲人似我世间无”。



图3.4.1　双人同时与绝艺对弈

绝艺围棋程序采用蒙特卡罗树搜索算法作为基础的搜索框架，使用深度学习和强化学习技术训练策略网络，再通过与机器自我对弈形成价值网络，快速提高棋力。绝艺战胜过柯洁、古力和朴廷桓等100多位职业棋手，在第10届UEC杯世界计算机围棋大会上，以11战全胜的战绩夺得冠军。目前，绝艺成为中国国家围棋队专用训练工具。

思考：

比较中国象棋、五子棋、四子棋、跳棋、井字棋、围棋和国际象棋等棋类游戏的人工智能程序实现难度，并按照难易程度排序。



微信公众号：电子课本大全

### 3.4.1 博弈决策的发展历程

智力游戏被公认为智能的一种具体表现，而人工智能的终极目标就是使机器具有人类的（部分）智能。人工智能诞生元年，即1956年，阿瑟·萨缪尔（Arthur Samuel）编写了一个国际跳棋程序；1959年，这个程序战胜了萨缪尔本人；1962年，它又击败了美国某个州的国际跳棋冠军；1994年，另一款国际跳棋程序Chinook战胜了世界冠军；1997年，国际商业机器公司IBM开发的超级计算机“深蓝”（Deep Blue）击败了国际象棋世界冠军卡斯帕罗夫。

事实证明，机器下国际跳棋和国际象棋比人类厉害，那为什么还要研发其他棋类比赛机器人（如围棋弈棋程序）来挑战人类的智力呢？这是因为围棋更加复杂，大家熟知的所有棋类智力游戏中，围棋的搜索空间最大，所需计算量也最大。因此，研究人机围棋对弈更具有挑战性。

**思考活动**

**围棋的计算空间究竟有多大**

围棋棋盘有361（19×19）个格子，每个格子有3种落子可能性（落黑棋、落白棋、不落子），所以整个棋盘共有$3^{361}$种落子可能性；从棋法角度来看，即使不算提子和劫争，第$n$步有$361-n$种选择，所以至少有361!（超过$10^{200}$）种可能性，比宇宙原子的总量还要多，也远比其他智力游戏（诸如国际象棋和五子棋等）的搜索空间大很多。所以，一般认为，围棋很难用人工智能技术解决。

思考：

按照类似的方法计算国际象棋、五子棋、井字棋和跳棋等棋类的搜索空间，并与围棋进行对比。

1997年超级计算机“深蓝”利用已知的开局棋谱和收官棋谱，采用穷尽所有可能性的简单方法算出最佳走棋法而获胜。“深蓝”的胜利证明了计算机具有强大的计算能力，但这不能证明计算机可以通过学习使自己变聪明。

从四子棋、黑白棋、跳棋、国际象棋，到走棋法更为复杂的围棋，人工智能已经在对弈游戏上做得比人更好。围棋棋局的搜索空间越大，对弈难度也就越大，需要大量的学习和训练。

本节从引爆第三次人工智能浪潮的阿尔法围棋智能程序的核心要素出发，介绍两个重要的算法：蒙特卡罗树搜索与强化学习。阿尔法围棋通过结合蒙特卡罗树搜索算法和两个深度神经网络来完成弈棋。开发者首先用人类对弈的近3 000万种走法来训练阿尔法围棋的神经网络，让它学会预测人类专业棋手的落子；然后让阿尔法围棋跟自己对弈，进一步产生规模庞大的全新棋谱；最后利用蒙特卡罗树搜索算法分析未来一定步数的落子情况，并判断在哪里落子赢的概率更高。



微信公众号：电子课本大全

阿尔法围棋的基本原理如图3.4.2所示，其学习方式分为离线学习（训练阶段）和在线学习（在真正的比赛中学习）。离线学习一方面基于现有的海量历史棋谱，另一方面通过自我对弈不断强化学习，在学习中进步。基于围棋棋盘结构固定以及数据海量等特性，上述两个方面的实现都使用了深度学习方法，即从大量数据中提取特征并解决问题。在线学习主要是在实际对弈中，可能的走法太多，无法直接穷举，因此需要一个高效的求近似解的方法。蒙特卡罗树搜索算法正是通过随机采样达到近似结果的方法来构建搜索树的，因此能够从近乎无数个策略中选出最优策略。

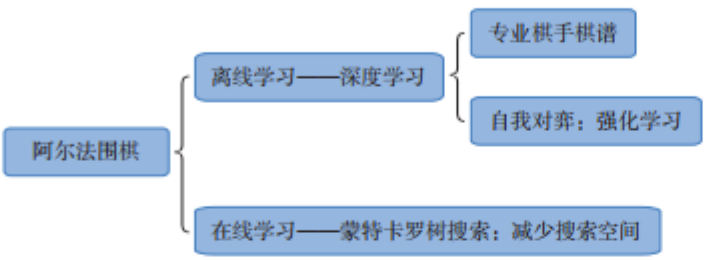



图3.4.2　阿尔法围棋的基本原理示意图

## 3.4.2　强化学习及其应用

阿尔法围棋系列的围棋机器人战胜世界冠军的事件，让人类认识到强化学习的威力。强化学习属于机器学习，它本身是决策科学，也是多学科交叉的产物，因此在许多学科分支中得到了广泛的运用，如计算机科学、神经科学、心理学、经济学、数学和工程学等。

### 强化学习的思想与建模

无论是成年人学习开车，还是婴儿学习走路，整个过程都是通过人与环境的互动来完成的。从互动中学习是所有关于学习和智力理论的一个基本思路。

例如婴儿学习走路，学习的核心是试错，即尝试—出错—改进，这与心理认知有密切关系。婴儿作为一个智能体，试图通过采取动作（行走），来与环境（路面）互动，他（她）试图从一个状态（位置）走到另一个状态（位置）。当他（她）完成一个任务的子模块（比如走两步）时，就会得到奖励（巧克力）；当他（她）出错（不能走路或跌倒）时，就不会得到奖励。这就是对学习走路这一问题的简化描述。智能体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，逐渐产生能获得最大利益的习惯性行为，这个过程便是强化学习。强化学习因具有普适性而应用于很多领域，例如自动驾驶、博弈论、控制论、运筹学、信息论、仿真优化、多主体系统学习、群体智能、统计学以及遗传算法等。

图3.4.3为强化学习用于决策问题的通用模型。其中：强化学习适用于一个具有行动能力的“智能体”，每一个“动作”都影响该“智能体”未来的“状态”，成功是由“奖励”信号来衡量的，目标是选择最大化未来回报的“动作”。“智能体”与“环境”的互动情况是：“智能体”获取“状态”和“奖励”，观察“环境”选择“动作”，“环境”接收到“动作”，更新“状态”和“奖励”。



微信公众号：电子课本大全




图3.4.3　强化学习用于决策问题的通用模型示意图

## 实践活动

### 强化学习在简单游戏中的建模

访问教学资源平台，打开一款名为“Flappy Bird”的休闲游戏，在这款人工智能游戏中，观察机器玩家不断进步和提高的过程。体验该游戏具有的“尝试—出错—改进”的类人学习机制。参照强化学习用于决策问题的通用模型，对这款游戏进行四要素建模，如图3.4.4所示。

智能体：小鸟 ⟷ 环境：游戏

| | |
|---|---|
| 状态<br>（state，用$s$表示） | $d_x$：距离下一对水管的水平距离<br>$d_y$：距离下一对水管的垂直距离<br>生命：存活或结束 |
| 动作<br>（action，用$a$表示） | 飞：点击<br>不飞：什么也不做 |
| 奖励<br>（reward，用$r$表示） | +1 存活<br>−1 000 结束<br>+50 通过一对水管 |

图3.4.4　四要素建模示例

参照上述分析，对其他经典游戏（如超级马里奥、吃豆人和打砖块等），进行强化学习的基本建模。

### Q-学习算法

强化学习是一大类算法，包括环境模型已知的算法和环境模型未知的算法两类。其中Q-学习算法是环境模型未知算法中的一个典型算法。前面“实践活动”的Flappy Bird游戏中，环境是变化的（水管的位置和高度），而且没有针对这个环境的已知模型。Q-学习算法就适用于解决这样的问题。

Q-学习算法的核心是通过Q函数最大值选择具有最大Q值的“动作”，即选择最大化未来回报的“动作”得到解决问题的策略。

### 深度Q网络

强化学习面临的挑战是状态空间太庞大。以“打砖块”游戏的状态空间分析为例：



微信公众号：电子课本大全

$84 \times 84$ 像素的视频分辨率，取连续4帧作为当前状态输入，每个图像像素的颜色值为0～255，那么总的状态空间为 $256^{84\times84\times4} \approx 10^{67\,970}$。这个数量比宇宙中所有原子的总量都要大，根本无法遍历所有“状态—动作”所产生的未来回报，因而无法确定下一步动作。

Q-学习算法的传统求解方法是通过列出Q表格进行表示和求解，但是对于像视频游戏这种输入量巨大的情况，Q-学习算法中Q值的选择空间太大，无法运用传统的方法。而深度学习对于海量结构化数据具有很好的处理能力，能够学习到特征并高效求解。因此，深度Q网络是深度学习加Q-学习算法的创新组合。这种组合利用了深度学习在海量数据支持下的优势，解决了视频游戏输入数据量巨大、Q-学习算法中Q值的选择空间维度过高等难题。

## 技术支持

### 深度Q网络的具体实例

对弈视频游戏中的深度Q网络建模主要有四个要素：一是问题定义，从输入（游戏屏幕对应的像素 $p$）到 $Q(s, a)$ 的端到端学习；二是输入状态，输入状态 $s$ 是从当前状态向前共4帧图像组成的像素堆；三是输出结果，对应游戏手柄或按钮所表示的不同动作的 $Q(s, a)$；四是奖励定义，涉及动作的分数变化。

图3.4.5所示的网络结构适用于各种传统像素级电子游戏。与典型卷积神经网络的一个重要区别是，该网络没有通过降采样（池化层）减小图像矩阵。这是由于在游戏对弈中，位置是至关重要的特征信息。因此在深度学习网络中不能使用降采样。

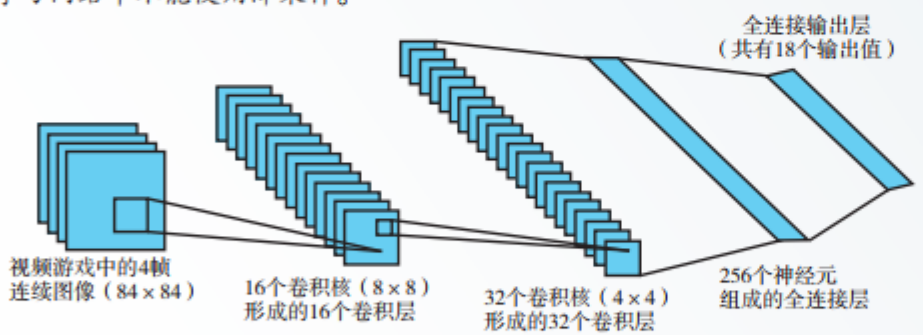



图3.4.5 深度强化学习Q的网络结构示意图

## 实践活动

### 增强学习体验——吃瓜游戏

访问教学资源平台，运行一个名为“吃瓜”的游戏程序。如图3.4.6所示，粉色圆点为西瓜，绿色圆点为毒药，游戏玩家需要吃到尽可能多的瓜，还要避免吃到毒药。



微信公众号：电子课本大全

“吃瓜”游戏中有一个智能体，它有9个不同角度的探测方向，每个方向可以感知3个值：到墙壁的距离、到西瓜的距离和到毒药的距离。显然，这个智能体总共有27个输入状态。整个过程中，智能体有3种“动作”模式：直走、转较小角度后前进较长距离或转较大角度后前进较短距离。

1. 体会该游戏具有的“尝试—出错—改进”的类人学习机制。对照强化学习用于决策问题的通用模型，对游戏进行建模。

2. 按以下要求操作，观察智能体行为的变化：

■西瓜奖励值改为0；

■西瓜奖励值改为0，同时将前进奖励值改为0；

■互换吃西瓜与吃毒药的奖励；

■改变环境中西瓜与毒药的数量。

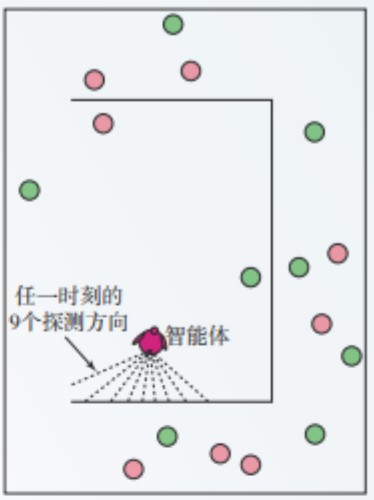



图3.4.6 “吃瓜”游戏示意图（顶视图）

强化学习及其与深度学习的结合，是阿尔法围棋的一个重要算法。接下来介绍阿尔法围棋用来快速评估棋面位置价值的蒙特卡罗树搜索算法，该算法结合了随机模拟的一般性和树搜索的准确性两个特点。

蒙特卡罗树搜索算法非常简单：根据模拟的输出结果，按照节点构造搜索树。其过程可以分为以下步骤，如图3.4.7所示。

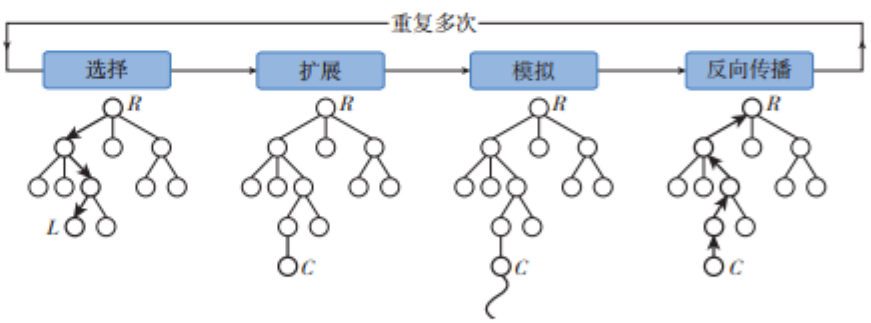



图3.4.7 蒙特卡罗树搜索算法基本过程示意图

1. 选择：从根节点$R$开始，递归选择最优的子节点，直到达到叶子节点$L$。

2. 扩展：如果节点$L$不是一个终止节点（也就是不会导致对弈游戏终止），那么创建一个或者更多的子节点，选择其中一个节点$C$。

3. 模拟：从节点$C$开始运行一个模拟的输出，直到对弈游戏结束。

4. 反向传播：用模拟的结果，更新从$C$到$R$的路径上的节点信息。



微信公众号：电子课本大全

## 阅读拓展

### 蒙特卡罗树搜索算法

假如筐里有100个苹果，每次闭眼拿1个，要求挑出筐里最大的苹果。于是我们首先随机拿1个，再随机拿1个与之对比，并留下大的那一个，接着随机拿1个……每拿一次，留下的苹果都至少比上一次的大。拿的次数越多，挑出的苹果就越大。不过，要想挑出筐里最大的苹果，只能将筐里的100个苹果都拿光。这种挑苹果的办法，就属于蒙特卡罗树搜索算法——尽量找更符合目标要求的，但不保证是最符合目标要求的。也就是说，蒙特卡罗树搜索算法是样本越多，越能找到更佳的解决办法，但不保证是最佳的。

蒙特卡罗算法模拟小程序：计算圆周率。

先使用程序画一个正方形及其内切圆，然后在这个正方形内随机地画点，如图3.4.8所示。设点落在圆内的概率为$P$，则$P$=圆面积÷正方形面积。通过获得圆面积来计算圆周率：$P=\pi R^2/(2R\times 2R)=\pi/4$，即$\pi=4P$。

以下是程序算法步骤：

1. 将圆心设在直角坐标系原点，以$R$为半径作圆，则第一象限的1/4圆面积为$\pi\times R\times R/4$；

2. 作该1/4圆的外切正方形，4个顶点坐标分别为$(0,0)$、$(0,R)$、$(R,0)$、$(R,R)$，则该正方形面积为$R\times R$；

3. 随机取点$(X,Y)$，使得$0\leqslant X\leqslant R$，并且$0\leqslant Y\leqslant R$，即点在正方形内；

4. 计算$X\times X+Y\times Y$的值，判断该值是否小于$R^2$；

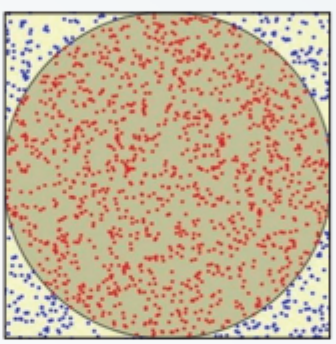


图3.4.8 在正方形内随机地画点

5. 设所有点的个数（也就是实验次数）为$N$，落在1/4圆内的点（满足第4步的点）的个数为$M$，则$P=M/N$，于是$\pi=4\times M/N$。

程序的主要代码如下：

```
#蒙特卡罗算法模拟求π
import random
def M_C(num):
    count=0
    for i in range(1,num+1):
        X=random.uniform(0,1)
        Y=random.uniform(0,1)
        if X**2+Y**2<1:
            count+=1
    return 4.0*count/num
```



微信公众号：电子课本大全

## 项目实施

### DeepTraffic项目实践

DeepTraffic（一款在线的自动驾驶模拟程序）模拟典型的公路环境，可让用户使用深度学习技术来控制自己的汽车。在游戏中，用户通过神经网络控制红色的汽车在拥挤的高速公路上行驶，如图3.4.9所示，目标是使红色汽车尽可能快地通过该路段。



图3.4.9　自动驾驶汽车模拟程序界面

可以在浏览器中使用JavaScript（一种解释执行的编程语言）来控制参数并改变汽车的行驶状态，也可以使用OpenAI Gym（一款用于研发和比较强化学习算法的工具包）访问DeepTraffic，并可通过OpenAI Gym提供的任意Python接口对深度学习网络进行训练。

一、项目活动

1. 从教学资源平台下载本节对应的模拟程序DeepTraffic，并按照说明进行配置、安装，在浏览器中体验自动驾驶汽车模拟程序。

2. 针对该问题建立强化学习的基本模型。

3. 使用JavaScript操纵强化学习的相关参数，观察并分析驾驶行为的变化。（有五种驾驶行为：左变道、右变道、减速、加速、保持不变。）

4. 调整深度学习网络的结构，观察并分析驾驶行为的变化。

二、项目检查

1. 各小组学习DeepTraffic模拟程序的基本使用方法，能够进行简单的训练和测试。

2. 分别调整强化学习相关参数和深度学习网络的结构，观察并分析驾驶行为的变化，进行小组讨论和汇报展示。

3. 构建自己的自动驾驶汽车深度强化学习网络，作为智能陪伴机器人的模拟学习平台，供学习和使用，同时为智能陪伴机器人的自主运动提供一种思路。

## 练习提升

1. 初学者在浏览器中使用JavaScript操纵参数并改变汽车的驾驶行为。希望深入学习的同学可以通过OpenAI Gym进入DeepTraffic，并使用Python来训练深度学习网络。

2. 选用不同游戏案例，小组合作完成强化学习的思维导图，理解关键变量与参数$s$、$a$、$r$和$Q$等的作用。



微信公众号：电子课本大全

# 3.5
# 智能机器人

## 学习目标 ▶▶▶

- 理解智能机器人的概念，了解智能机器人的广泛应用，感受智能机器人对人们生活的影响。
- 合理选择人工智能平台与工具，搭建智能机器人模块，体验智能机器人的实际应用，掌握搭建简单人工智能模块的一般方法。

## 体验探索

### 快递机器人

自动驾驶和智能机器人等人工智能应用正在悄悄地影响着我们的生活。

2018年6月18日，快递机器人在北京海淀区上路了。上午10点，随着平台的指令发出，3台满载着货物的快递机器人依次出发，自动驶向订单所在地。如图3.5.1所示，快递机器人不仅外观简单可爱，而且拥有很多“智能”本领。一路上，它能进行360° 环境监测，自动避让路障和行人，遇到红绿灯时能立刻作出反应，到达目的地后它会自主停靠配送点，将取货信息发给客户。客户可以通过人脸识别、输入取货码或点击手机应用程序链接三种方式完成取货。



图3.5.1 快递机器人

思考：

1. 这款快递机器人用到了哪些人工智能技术？这些技术用前面学习的哪些算法可以实现？

2. 如果想要搭建一个快递机器人，除了人工智能学科领域的相关知识，还需要哪些学科领域的技术支持？



微信公众号：电子课本大全

### 3.5.1 智能机器人简介

机器人将像个人计算机一样逐步进入家庭，改变我们的生活方式。目前，随着人工智能、机械制造、材料科学、电子技术、计算机科学、控制技术、传感技术和仿生学技术等多门学科领域的不断发展与学科融合，机器人技术不断取得进步，在社会服务、公共安全、危险作业和国防军事等领域具有广泛的应用前景。

**思考活动**

**体验身边的智能机器人**

人工智能之于机器人，更像是人脑之于人类。人工智能可以通过感知、学习、推理和规划等一系列的智能应用技术给机器人下达指令。工业时代，机器人只能通过固定指令帮助人类完成重复、枯燥的作业任务。人工智能时代，机器人将会拥有智慧，能够像人一样进行思考学习，完成作业任务。可以说：智能机器人是人工智能技术的集成化、产品化，是人工智能的一种具体表现形式，也是人工智能的科研平台。

思考：

1. 分组讨论，谈谈你在日常生活中接触过哪些智能机器人？
2. 查阅相关资料，分析人工智能技术是如何应用于该款智能机器人的。

#### 智能机器人的概念与兴起

“机器人”一词最早来源于1920年创作的科幻小说《罗萨姆的万能机器人》。多年来，科研人员一直致力于研发能够帮助人类完成各项任务的机器人。国际上对于机器人的定义见仁见智。美国机器人协会定义机器人为“一种用于移动各种材料、零件、工具或专用装置的，能够通过程序动作来执行各种任务，并具有编程能力的多功能操作机”。日本工业标准局定义机器人为“一种机械装置，在自动控制下，能够完成某些操作或者动作功能”。我国科学家将机器人定义为“一种自动化的机器，这种机器具备一些与人或生物相似的智能，是一种具有高度灵活性的自动化机器”。

随着机器人技术以及人工智能技术的不断发展，传统意义上的机器人已经无法满足未知和不确定环境下的作业任务，而具有感知、运动和决策能力的智能机器人成为当今各国研究的主要对象。我国国家标准将智能机器人定义为“具有依靠感知环境和（或）与外部资源交互、能够调整自身行为来执行任务的机器”。

总之，智能机器人是一种智能的、高度灵活的、自动化的机器，具备感知、规划、动作和协同等能力，是多种高新技术的集成体。智能机器人的“智能”特征体现在它具有与外部对象（即环境）和人的相适应、相协调的工作机能，能根据得到的信息进行加工、处理、决策，并对外界的环境改变作出反应性的动作。



微信公众号：电子课本大全

### 智能机器人的分类与典型应用

人工智能与机器人技术已广泛地应用在人们生产和生活的诸多领域。智能机器人可以分为工业机器人、服务机器人和特种机器人三大类。常见的服务机器人有医疗机器人、迎宾机器人、教育机器人、扫地机器人、快递机器人、聊天机器人和智能陪伴机器人等。这些形态各异的智能机器人已远远脱离了最初机器人所具有的实体模样，更加符合各种不同应用领域的特殊要求。

■ 工业机器人

现代汽车的自动生产线如图3.5.2所示，所有的机器设备都按统一的节奏运转，生产过程高度连续。生产线全面自动化的实现，得益于日趋成熟的人工智能和机器人技术。《中国制造2025》指出，到2025年，制造业重点领域将全面实现智能化，而人工智能则是提升工业制造系统智能水平的有效动力。



图3.5.2　工业机器人

■ 医疗机器人

现如今，医学上已经有手术机器人（图3.5.3）应用于临床心脏病手术的案例。基于人工智能技术，手术机器人控制端可将整台手术过程的二维影像实时还原成三维影像，由医生通过三维影像监控整个过程。在手术中，机器人的多支手臂各司其职，且灵敏度远超人类。医疗机器人可利用微创技术完成复杂的高难度手术。

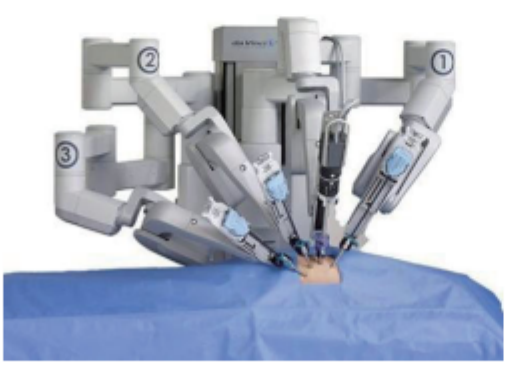



图3.5.3　医疗机器人



微信公众号：电子课本大全

另外，诊断机器人也是人工智能在医疗领域内的典型应用。诊断机器人运用疾病中心以患者基因组以及血液检查和图像诊断等大量信息为基础建立的数据库，对照医学论文等研究成果，给出诊断结果。

■ 迎宾机器人

迎宾机器人能够通过视觉系统观察、识别人类的表情，还能利用语音系统识别人类的语音、语调以及能够表现情感的特定词汇。与此同时，迎宾机器人利用人工智能技术对上述一系列人类的情感信息进行分析、判断、处理，并通过表情、动作和语音等与人类进行交流、反馈。有些迎宾机器人甚至能够跳舞、逗人开心等，还有些迎宾机器人可以根据客户在商场的消费记录等数据为客户推荐新款产品，如图3.5.4所示。

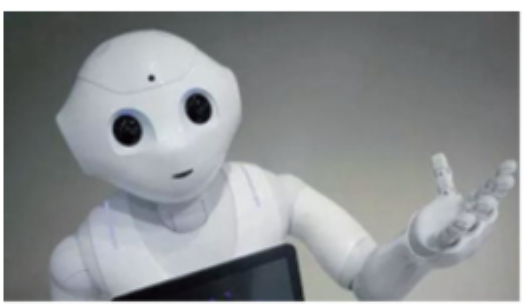


图3.5.4　迎宾机器人

■ 教育机器人

教育机器人由于其独特的形态、运动方式和智能交互功能，对青少年有较强的吸引力与启迪作用。它的出现开拓了课堂教育的新模式，成为一种新的学习平台。如图3.5.5所示，学生可以通过与智能机器人互动，学习编程技巧和科学知识，增强科学意识和创新思维，提高学习能力与动手能力。



图3.5.5　教育机器人

■ 扫地机器人

扫地机器人是一种智能家电，具有一定的人工智能，可以自动完成房间内的地面清扫任务，如图3.5.6所示。扫地机器人可以设定时间预约打扫、自行探索房间布局、即时定位与地图构建，能够实现自动避障、清扫和充电。



微信公众号：电子课本大全



图3.5.6　扫地机器人

■ 聊天机器人

聊天机器人具备模拟人类对话的功能，各大电商平台打造的智能客服机器人就是其中的一种。聊天机器人能与人们对话，回答人们提出的各种问题，解决人们的某些疑惑，如图3.5.7所示。这些看似“百问百答”的聊天机器人的背后，离不开大数据与人工智能技术的支撑。



图3.5.7　聊天机器人

## 阅读拓展

### 机器人酒店

有这样一家神奇的酒店，其服务团队皆由机器人组成。前台机器人接待员精通中、英、日三国语言，如图3.5.8所示。它们会帮助旅客办理入住手续，也会不时与旅客交流、互动。旅客经过大厅时，会有机器人主动帮助旅客寄存小件行李并将行李运送到指定房间。在房间门口，旅客需要通过“刷脸”进入房间。每个房间内都配备了小型机器人，可提供聊天服务，还可以根据客人的要求开关电视或提供天气信息。餐厅里的烹饪机器人负责制作煎饼、冰淇淋等食物，如图3.5.9所示。在这家机器人酒店，就连打扫卫生、维护绿植等工作，也都由机器人来完成，甚至连垃圾桶都是机器人。此外，酒店还配备了牙科、皮肤科兼内科等机器人诊室。这家酒店因其独特性，每年都吸引着世界各地的游客前往入住。



微信公众号：电子课本大全

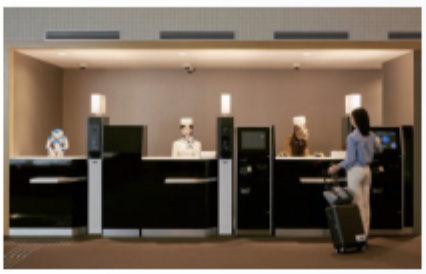


图3.5.8　机器人酒店前台



图3.5.9　摊煎饼机器人

可以看到，现代智能机器人正影响着我们生活的方方面面，而人工智能的发展在其中起着至关重要的作用。

### 3.5.2　智能机器人应用实践

现有的智能陪伴机器人主要是为儿童和老年人设计的，外貌大多是卡通或人物形象，可以实现语音交互、游戏教学、英语学习、亲子教育和情感表达等功能。智能陪伴机器人不仅能陪伴儿童和老人进行日常生活活动，有些机器人甚至能模拟家人的声音与儿童和老人进行智能交流。在本节，我们将利用前面所学知识搭建智能陪伴机器人。

#### 机器人硬件的搭建

物理形态机器人硬件的搭建是一个非常复杂的过程，涉及机器人学。机器人学是一门综合性学科，涉及领域广，主要涉及机器人本体机构、运动学和动力学、传感技术、控制技术、人工智能、信息交互、运动规划、应用工程以及多机器人协作等方面。机器人硬件的搭建包括机械结构设计及驱动、控制系统的建立、感知系统的建立、运动规划与控制这四个方面的内容。

■ 机械结构设计及驱动

机械结构就像是机器人的“骨骼”，支撑起整个机器人的外部形态。实际设计时，需要针对不同的作业任务，设计相应的机械结构。精巧的机械结构设计，能够拓展机器人的实际应用场景，有利于提高机器人对复杂环境的适应性。例如，现有的智能陪伴机器人外貌大多是卡通或人物形象，这样的设计往往更具亲和力，易被用户接受。机器人的下身往往选择轮式结构，因为相对足式结构，轮式结构可提供较快的移动速度，且稳定性较好，方便机器人在室内行走。

常见的驱动方式有液压驱动、气压驱动和电力驱动。针对不同的环境和应用场景，选择适当的驱动方式非常关键。液压驱动具有动力大、响应快速和易于实现直接驱动等特点，适用于承载能力大、惯量大的机器人，但液体泄漏会对环境产生污染，且工作噪声较大。气压驱动具有响应速度快、系统结构简单、维修方便和价格低廉等特点，但其驱动装



微信公众号：电子课本大全

置较大，且气体的可压缩性会降低定位精度。电力驱动是利用各种电动机产生力和力矩，直接或间接经过机械传动来驱动执行机构，以支持机器人的各种运动姿态。相较前两种驱动方式，电力驱动系统精度较高，并且因为省去了能量转换这一中间过程，电力驱动比液压驱动和气压驱动效率更高，使用更方便，且成本较低。由于智能陪伴机器人的工作环境以室内为主，同时对机器人操作的精度有一定要求，因此建议采用电力驱动的方式。

■ 控制系统的建立

控制系统是机器人的核心。机器人的智能程度和功能强弱通常与其控制系统的性能直接相关。机器人的控制系统主要负责处理指令信息和内外环境信息，并依据现有的模型与信息作出决策，产生相应的控制信号。最终通过驱动机器人各个关节按所需的顺序、沿确定的位置或轨迹运动，完成特定的作业任务。

■ 感知系统的建立

感知系统犹如机器人的“五官”，可以帮助机器人获取外部环境和内部状态的信息。为了适应复杂的环境，机器人往往需要通过多种类型的传感器，如力传感器、姿态传感器、触觉传感器和摄像头等来获取多样化的信息。另外，当工作环境复杂时，为了使机器人获取对环境相对完整的感知，通过多传感器信息融合来解决问题。

■ 运动规划与控制

机器人的运动规划指确定机器人的各关节在起点和终点之间走过的路径，以及在各路径点的速度和加速度。机器人控制技术研究在给定期望的运动规划前提下，机器人各关节如何快速响应并高效完成已经规划好的运动。

### 机器人系统的搭建

图3.5.10为智能机器人与人类交互的框架示意图。人类可以通过语音、图像与陪伴机器人进行交流，也可以通过游戏与机器人进行人机对弈。智能机器人则可以通过语音识别、语音合成、图像识别、认知推理和强化学习等技术完成与人类的沟通与交流。

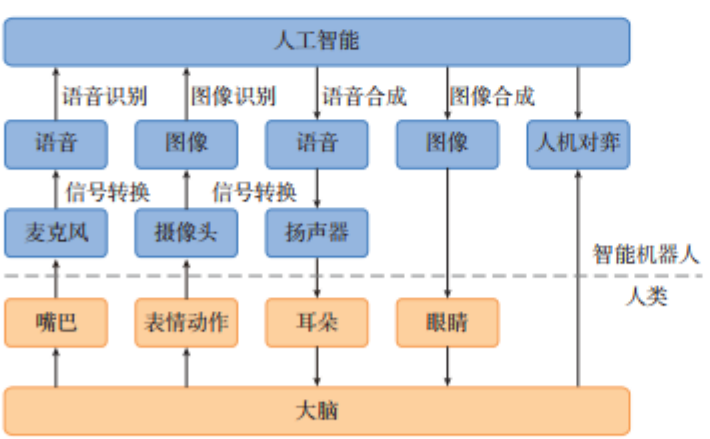



图3.5.10　智能机器人与人类交互框架示意图



微信公众号：电子课本大全

具体来说，机器人通过麦克风采集人类语音，经过语音识别，对人类语音进行转换、理解并产生应答信息，而后利用语音合成转换为人声并通过扬声器反馈给人类，完成与人类语音的交流与沟通。同理，机器人通过摄像头采集人类的图像，利用图像对人类的表情、动作加以识别和理解，再通过图像合成或语音合成反馈给人类。人机对弈则是机器人不断学习人类的游戏模式，并作出反馈的过程。

智能陪伴机器人通过语音和图像识别技术实现与人的交互。它能够观察感知周围环境，会看、会听、会说、会想，也会陪伴，可以与用户聊天和玩游戏等。它具有如下功能：

1. 能够识别用户的表情；

2. 能够与用户进行语音交流；

3. 能够与用户进行游戏。

图3.5.11所示为智能陪伴机器人的功能模块集成示意图。为完成上述功能，智能机器人需要集成视觉、语音、人机对弈三大模块。根据所要实现的功能，选择麦克风和摄像头作为智能机器人的外部传感设备。具体来说，视觉模块主要包括人脸检测、表情识别。语音模块主要包括自然语言处理与语音处理（主要包括语音识别与合成）。人机对弈模块主要体现在与用户进行游戏交互。

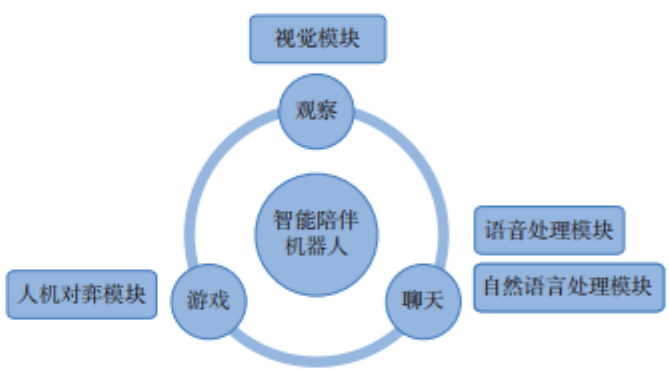



图3.5.11　智能陪伴机器人功能模块集成示意图

图3.5.12为智能陪伴机器人的主程序流程图，系统程序由Python编程语言实现。程序对用到的Python数据库及模块进行导入及初始化后，首先对摄像头数据进行读取，而后进入视觉检测识别模块，并对读取内容进行人脸检测、表情识别，接着调用语音模块对基于视觉模块检测和识别的结果进行反馈。语音模块对麦克风语音数据进行读取、转换和识别，调用应答模块进行反馈，并通过语音合成转换为人声进行播放。当聊天内容涉及游戏时，程序进入到对弈模块。对应的核心代码及注释如下：

```
from chatterbot import ChatBot          # 导入文本聊天模块
from speech import SpeechRecognizer     # 导入语音识别模块
from speech import SpeechSynthesizer    # 导入语音合成模块
import sounddevice                      # 导入语音设备模块
```

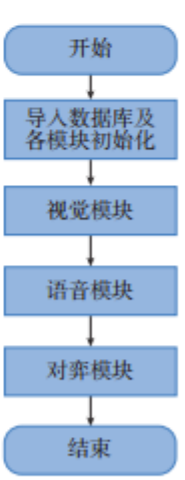



图3.5.12　智能陪伴机器人的主程序流程图



微信公众号：电子课本大全

```
from face import FaceDetector          # 导入人脸检测模块
from face import ExpressionClassifier # 导入表情分类模块
import cv2                             # 导入opencv模块

# 初始化各个模块
chatbot=chatterbot.ChatBot(
                           "Ron Obvious",
                           trainer="chatterbot.trainers.ChatterBotCorpusTrainer"
                          )
chatbot.train("chatterbot.corpus.chinese")
recognizer=SpeechRecognizer("speech_recognizer.model")
synthesizer=SpeechRecognizer("speech_synthesizer.model")

video_capture=cv2.VideoCapture(0)
face_detector=FaceDetector("face_detector.model")
expression_classifier=ExpressionClassifier("expression_classifier.model")
```

■ 视觉模块

视觉模块的流程如图3.5.13所示，程序首先对摄像头部位进行检测。如果摄像头故障，则跳出循环，结束程序，并要求用户检查和排除摄像头故障后重新开始；如果摄像头没有问题，则接着调用视觉模块进行人脸检测和表情识别。

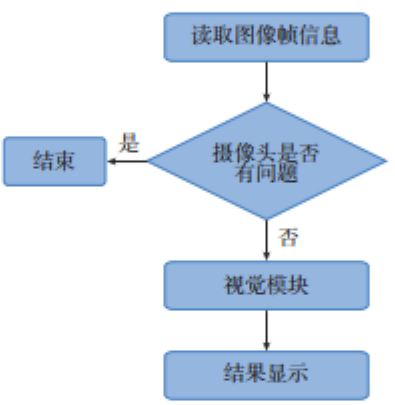



图3.5.13　视觉模块的流程图

核心代码及注释如下：

```
# 循环往复进行表情识别
while True:
    # 读取图像帧信息
    ret,frame=video_capture.read()
    if not ret or frame is None:
        break
    bbox=face_detector.detect(frame)  # 进行人脸检测
    face_image=frame[bbox[0].y:bbox[0].h, bbox[0].x:bbox[0].w]
    # 进行表情识别
    expression=expression_classifier.classify(face_image)
    # 每一帧处理后延时一段时间(毫秒)
    cv2.waitKey(5)
```

■ 语音模块

语音模块主要调用ChatterBot模块进行文本聊天，调用语音识别与合成模块进行语音处理。程序首先对语音进行检测和识别，将语音转为文本，然后调用文本聊天模块，获取响应文本，并调用语音合成及应答模块将响应文本转换为音频播放，完成整个交互。

语音模块的流程如图3.5.14所示，核心代码及注释如下：

```
# 调用语音设备模块的录音功能
input_audio=sounddevice.rec(int(duration * fs),samplerate=fs,channels=2)
```



微信公众号：电子课本大全

```
# 调用语音识别功能，将语音转换成文本
input_text=recognizer.recognize(input_audio)
# 调用文本聊天模块,获取响应文本
response_text=chatbot.get_response(input_text)

# 调用语音合成模块，将响应文本转换成响应音频
response_audio=synthesizer.synthesis(response_text)

# 调用语音设备模块的播放功能
sounddevice.play(response_audio,fs)
else:
    time.sleep(0.030)
```

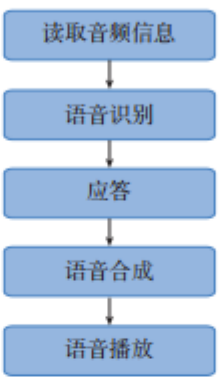



图 3.5.14　语音模块的流程图

■ 人机对弈模块

人机对弈模块主要利用强化学习算法教会机器人玩类似“入侵者”（Space Invaders）的这类游戏。强化学习中的“智能体”以“环境”提供的“奖励”作为反馈，学习一系列的环境“状态”到“动作”的映射，“智能体”在学习过程中掌握的基本规则是：如果某个“动作”带来了“环境”的正回报（“奖励”），那么这个“动作”就会被加强，反之则会被削弱。

“入侵者”游戏基于开源强化学习代码库，程序首先进行库函数导入和初始化，然后进行强化学习训练，最后由机器人自己完成“入侵者”游戏任务。核心代码如下：

```
import AIGame as game
game.play()
```

具体代码访问教学资源平台上的相关资源包。



微信公众号：电子课本大全

## 项目实施

### 定制智能陪伴机器人

一、项目活动

1. 根据本章所学知识，设计属于自己的智能陪伴机器人，并选择适当的传感器和功能模块进行整合。

2. 根据定制的智能陪伴机器人方案，选择合适的人工智能开发平台及工具。

3. 基于之前完成的素材和技术准备，完成自己的智能陪伴机器人搭建及展示。

二、项目检查

在“智能陪伴巧实践”项目中，小组展示项目作品，并完成组间互评。

## 练习提升

1. 尝试为已完成的智能陪伴机器人增加其他功能。

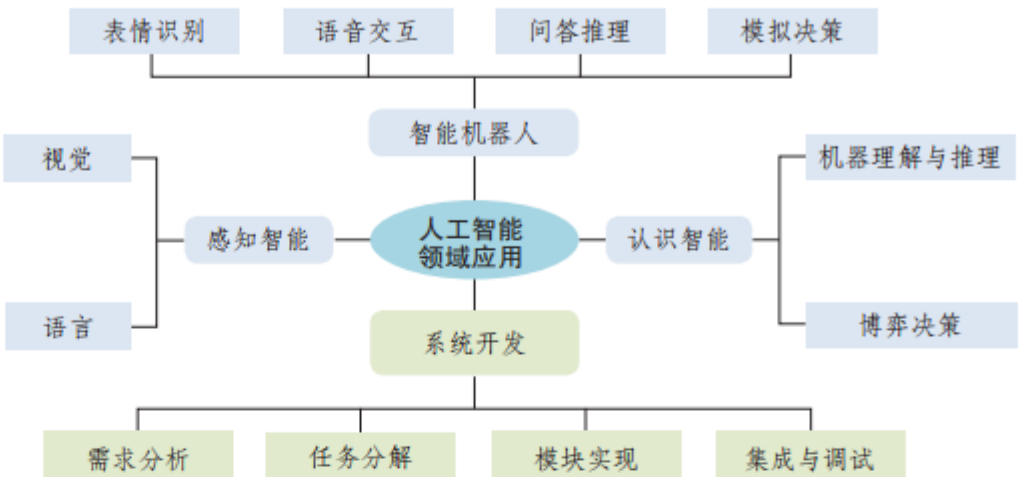
2. 编写作品说明书或者制作多媒体作品宣传册，对已完成的智能陪伴机器人进行功能和优缺点等方面的介绍。模拟开展一次班级机器人展览会，每组同学对自己的智能机器人产品进行展示。



微信公众号：电子课本大全

## 总结 评价

1. 下图展示了本章的核心概念与关键能力，请同学们对照图中的内容进行总结。




2. 根据自己的掌握情况填写下表。

| 学习内容 | 掌握程度 |
| --- | --- |
| 计算机视觉 | □不了解 □了解 □理解 |
| 自然语言处理 | □不了解 □了解 □理解 |
| 机器理解与推理 | □不了解 □了解 □理解 |
| 强化学习 | □不了解 □了解 □理解 |
| 智能机器人的概念 | □不了解 □了解 □理解 |
| 智能机器人的广泛应用 | □不了解 □了解 □理解 |
| 智能陪伴机器人的搭建 | □未完成 □部分完成 □完成 |



微信公众号：电子课本大全

# 第 4 章
# 人工智能发展

2018 年在天津举行的第二届世界智能大会上，通过图灵测试的机器人“小薇”担任主持工作，令人眼前一亮。当前，人工智能技术应用发展迅速，给我们的生产和生活带来了许多变化。

未来的世界会是什么样的？人工智能将怎样发展？人工智能与人类智能一样吗？机器人会超越人类吗……人工智能的发展引发了人们对人工智能未来的无限遐想。因此，了解人工智能的发展趋势，探讨人工智能的巨大价值和挑战，对我们来说非常必要。

本章我们将以“优势局限之我见”为主题开展项目活动，通过查阅资料，与同学探讨，完成一篇以“优势局限之我见”为题的小论文，然后分组选出代表进行辩论。共同探讨人工智能的应用价值，了解人工智能应用系统带来的伦理及安全方面的挑战，知道维护信息系统安全的重要性，增强我们在信息社会中的安全防护意识和责任感。



微信公众号：电子课本大全

# 4 主题学习项目：优势局限之我见

## 项目目标

人工智能技术走出了实验室，正在改变着我们生活的方方面面。我们无法预测人工智能的未来，但有必要了解它的发展趋势。人工智能为人类带来方便，也会带来问题和困扰。本章我们围绕主题“优势局限之我见”开展项目活动，以论文和辩论的方式进行全班交流。

1. 了解人工智能的巨大价值，开阔眼界和思路，培养科学探讨的兴趣。

2. 探讨人工智能的发展及其带来的挑战。在学习新技术、提高数字化学习与创新能力的同时，自觉维护和遵守人工智能应用的规范与法规。

## 项目准备

为完成项目，需做如下准备。

- 全班分成两个小组，开展辩论活动，明确目标与分工，最后每组选出4人参加辩论赛。
- 查阅相关资料，每人完成一篇小论文 。

## 项目过程

在学习本章内容的同时开展项目活动。为了保证本项目的顺利完成，要在以下各阶段检查项目的进度。

**1 了解价值和趋势**

小组同学通过查阅资料，了解人工智能的巨大价值和未来的发展趋势，完成论文第一部分。 P147

**2 了解挑战和局限**

小组同学通过查阅资料，了解当前人工智能带来的挑战和局限，完成论文第二部分。 P154

**3 确定正反方辩手**

每组推荐4人，作为正反方辩手，以“优势局限之我见”为主题，组织一场辩论赛。 P158

## 项目总结

通过查阅资料，每人完成一篇小论文，并在小组内开展论文交流与评价，总结出本方的观点，选出参加辩论赛的选手，帮助选手做相应的准备。体验小组合作、项目学习和知识分享的过程，进一步认识人工智能在信息社会中的重要价值。



微信公众号：电子课本大全

# 4.1
# 价值和未来发展

## 学习目标 ▶▶▶

- 了解人工智能对人类社会未来发展的巨大价值。
- 开阔眼界和思路，培养探讨科学的兴趣和把握新技术发展趋势的能力。

## 体验探索

### 人工智能同声传译

同声传译，又称“同声翻译”“同步口译”。博鳌亚洲论坛自2018年以来，启用了人工智能同声传译系统（图4.1.1）。该系统通过语音识别、自主学习、智能断句、去口语化和领域自适应等技术处理，为会议提供了实时翻译服务。




图4.1.1　人工智能同声传译

在国际化程度越来越高的今天，无论是在大型国际会议，还是在个人出境旅游等方面，同声传译的应用越来越普遍，人们对实时无障碍的交流要求也越来越高，将有力推动人工智能的进一步发展。

思考：

1. 查阅资料，了解还有哪些人工智能应用的案例，这些案例分别应用了哪些人工智能技术？

2. 你认为不久的将来会产生什么样的人工智能应用？



微信公众号：电子课本大全

### 4.1.1 人工智能的应用价值

人工智能是目前发展速度较快、发展前景较广阔的一门新兴技术，具有巨大的应用价值，将会给许多领域带来革命性的变革。人工智能正在极大地改变着社会生产方式、生活方式乃至休闲娱乐方式，它的发展与应用既给人类与社会的全面发展提供了契机，也带来了新的挑战。

从宏观的角度看，人工智能的应用价值主要体现在以下三个方面。

■ 提高社会的智能化程度，实现科学治理和智慧决策

党的十九大报告指出，“提高社会治理社会化、法治化、智能化、专业化水平”。提高社会治理智能化水平，契合当今时代信息化、智能化快速发展的需求。2016年，杭州市政府宣布打造城市数据大脑。两年后，我国多个城市相继开始建设和使用城市大脑，以提高社会治理的智能化程度。

城市大脑正在有效地改变着我们的生活。城市大脑可以将城市的基础设施、安全防空机制、交通调度管理和大气污染防治等各领域的信息融为一体，将所有人、车、路、水、电和气等数据都接入系统，通过人工智能技术，把庞大的数据转化为科学合理的业务模型，形成实时的城市大视图，借此来完成对城市的整体调度和管理。数据是协助城市运转和发展的重要资源。城市大脑利用采集的各类大数据资源，对城市进行全面分析，有效调配公共资源，不断完善社会的综合治理，实现城市的科学治理和智慧决策，从而推动城市的可持续发展。

■ 影响生产过程和生产方式，将人从部分生产劳动中解放出来

人工智能应用于传统的生产过程和生产方式，使机器具备了类似人的眼睛、耳朵和大脑等感应器官和思维器官的功能。这不仅可以将人从一些有毒、有害的危险工作环境中解放出来，还能代替人完成重复、单调和繁重的工作，让人们有更多可以自由支配的时间从事创造性的工作，发挥更大的才干。我们的社会也会因此得到更充分、更自由、更全面的发展。

■ 改变传统的学习和生活方式，成为人类的参谋和助手

人工智能正在改变着我们的学习方式。在教学过程中使用人工智能学习系统，可以帮助教育者提供个性化的教学，使“因材施教”成为可能。针对初学者，人工智能学习系统能够通过测试了解学习者的知识和能力水平；对于已经有学习记录的学习者，人工智能学习系统可以根据学习者的学习兴趣、学习能力和理解能力等方面的大数据分析结果，逐渐勾勒出每个学习者的学习方式和特点，从而自动调整教学内容、方式和节奏，为每个学习者提供个性化的学习方案，使每个人都能得到适合自己的教育。

此外，人工智能也在改变人们的生活方式。人工智能模仿人类工作，不是简单的模仿，而是一种启发式、创造性的模仿。它可以通过分析大量数据，帮助人们全面地掌握



微信公众号：电子课本大全

事实情况，并以此为基础帮助人类作出更好的选择和决策。事实上，人工智能正被应用于法律案件的量刑、债务纠纷的裁定和交通事故中责任的认定等领域。它正在成为人们生活的参谋和助手。

**实践活动**

**了解人工智能在各领域的应用**

上网查询人工智能在各领域的应用情况，并填写表4.1.1。

表4.1.1　人工智能在各领域的应用

| 序号 | 应用领域 | 应用情况 |
| --- | --- | --- |
| 1 | 工业 | |
| 2 | 农业 | |
| 3 | 医疗 | |
| 4 | 教育 | |
| 5 | | |
| 6 | | |
| 7 | | |
| ⋮ | | |

## 4.1.2　人工智能的未来发展

人工智能已经融入了人们的生活，它的发展对人类发展及社会进步产生了巨大的推动作用。根据人工智能应用的现状，可以将其分为三个层面：基础层、技术层和应用层，如图4.1.2所示。从这三个层面看，未来人工智能会有怎样的发展呢？




图4.1.2　人工智能应用的三个层面



微信公众号：电子课本大全

### 基础层

基础层主要包含半导体芯片、传感器、大数据和云服务。半导体芯片和传感器是人工智能的数据来源；大数据和云服务涉及数据的管理和传输，是人工智能的基础。基础层的研究将会影响人工智能的走向。

未来的芯片将是内建人工智能运算核心，并且是软硬件整合在一起的。最完美的架构是把中央处理器和视觉处理器（或其他处理器）结合起来，让增强现实技术成为人工智能的“眼睛”，两者相互补充，缺一不可。



## 思考活动

**认识芯片的重要性**

随着人工智能的广泛应用，人们越来越深刻地认识到芯片的重要性，芯片已成为各国竞相研发的项目。上网查询有关芯片的资料，将收集到的资料整理成演示文稿与同学们分享。

思考：

1. 什么是芯片？芯片最初是谁发明的？芯片为什么难以制造？
2. 芯片有多重要？自主研制芯片的意义何在？

### 技术层

技术层是人工智能的核心，包括计算机视觉、自然语言处理、语音处理和深度学习等，这些技术的发展会决定人工智能的走向。随着脑科学的发展，人类对自身智能机理了解越多，人工智能就越有可能接近人类智能。



## 阅读拓展

**脑科学与人工智能**

脑科学是研究人脑产生认知、情感和意识的工作机制的科学。对人工智能的进一步研究，使人们意识到自身对大脑工作机制的了解很有限，人类试图更深入地认识人类智能，以便进一步推动人工智能的发展。人工智能就是要发明模拟大脑的工具，因此，人工智能也属于工程学范畴。科学和工程相互交织、互相促进，从而对人类社会产生更大的影响。

人脑是一个输入输出信息的器官，视觉系统是人脑中最大的感官系统。人的整个视觉系统从眼睛开始直接连向大脑的内核，在大脑内部形成非常复杂的回路，这里面有很多组件——神经元，它们像是大规模集成电路中的一个个电容器。大脑的不同部分可以与视觉系统中的不同器官进行沟通。因此，要研究大脑的工作机制，需要综合心理学、解剖学和脑科学等多学科的知识，通过共同构建知识库，促进人工智能的进一步研究。



微信公众号：电子课本大全

### 应用层

应用层将应用技术层的人工智能相关技术集成到某个应用场景的产品和服务中。应用场景涉及金融、家居、医疗、安防和自动驾驶等诸多领域。

目前，人工智能的应用虽然提高了某些领域的生产效率，但其发展仍处于弱人工智能阶段，仅在某些方面具有智能。能否实现强人工智能，很大程度上取决于我们对人类智能本身的了解。

我国非常重视人工智能的研究和应用，已经取得了很多世界领先的技术成果。我国2017年发布的《新一代人工智能发展规划》将人工智能确定为引领未来的战略性技术。我国将在科技引领、系统布局、市场主导、开源开放的指导原则下进行人工智能的研究和应用。

当前人工智能正在从实验室走向市场，很多技术和应用还不成熟。人工智能的发展需要大量推动技术突破和开发创新性应用的高端人才。青年学生是国家的未来，希望能有更多的年轻人热爱新技术，投身到新技术的研究、开发和创新中来。

## 项目实施

### 完成论文（一）

一、项目活动

通过查阅资料，了解人工智能的巨大价值和未来的发展趋势，在有依据的基础上，形成个人的观点，完成论文第一部分。

二、项目检查

在小组中汇报已完成的论文第一部分，同学之间进行交流、研讨，加深对人工智能的认识。

## 练习提升

1. 你认为人工智能未来会是什么样的？强人工智能能实现吗？
2. 人工智能的发展会对人类社会产生什么影响？会影响到你生活的哪些方面？



微信公众号：电子课本大全

# 4.2
# 伦理及安全挑战

## 学习目标

- 了解当前人工智能的局限性，以及人工智能在隐私、安全和伦理方面给人们带来的挑战。
- 提高辩证认识人工智能的能力，培养多角度分析、思考的能力。

## 体验探索

### 网络空间的安全问题

人工智能有优势也有安全隐患。为了发现人工智能技术上的缺陷和漏洞，国际上每年都会组织国际安全极客大赛。在2017年的大赛上（图4.2.1），白帽黑客们（指用自己的黑客技术来维护网络关系公平正义的黑客，通过测试网络和系统的性能来判定它们能够承受入侵的强弱程度）上演了一场与人工智能的巅峰对决。他们的攻击对象包括当下流行的人脸识别、声纹识别以及使用银行卡在智能销售终端机消费等场景。一位女选手仅用两分半钟就破解了人脸识别系统。她利用系统漏洞直接获取系统控制权限、修改人脸信息，把设备中存储的评委人脸换成了自己的脸。这意味着人脸识别系统可以被任意人脸“蒙骗”。来自白帽黑客们令人惊叹的破解展示，说明人工智能存在安全隐患。



图4.2.1　2017年安全极客大赛场景

思考：

1. 查阅资料，了解人工智能技术会带来哪些安全问题。
2. 我们应该如何解决这些安全问题呢？



微信公众号：电子课本大全

### 4.2.1 人工智能的隐私挑战

目前，人工智能的发展是以大数据驱动为主导模式的，人工智能在使用大数据资源时，必然涉及对用户隐私数据的采集、传输、处理和显示等。隐私数据包括身份证号码、银行账户、密码、指纹、年龄、家庭、地址和健康状况等重要个人信息。这些信息如果被合理、合法地应用，会带来积极的影响；如果被非法利用，则会导致个人隐私被泄露，甚至带来巨大的损失和危害。



**思考活动**

**个人隐私的保护**

现实生活中，人们可能在不经意间就泄露了自己的隐私。例如，很多手机应用程序在使用前需要用户注册，这个注册过程往往就是用户授权提供个人信息的过程，其中一些应用程序还对用户信息的获取和使用等采取了“霸王条款”——如果不授权，用户就不能使用。

思考：

1. 使用应用程序及智能工具时，应当如何保护自己的隐私？
2. 如何提高对隐私泄露风险的防范意识？

一般来说，隐私权被侵犯主要出现在数据应用的以下三个环节。

■ 数据采集中的隐私侵犯

采集数据是许多智能系统的首要工作。例如，智能系统通过收集指纹、声纹、虹膜、步态和心跳等生理特征数据来辨别人的身份，通过收集人的锻炼情况、睡眠时间和质量以及人的体征变化等数据来判断人的身体健康状况。这就意味着我们把大量的私人信息都交给了智能系统。如果这些数据使用得当，就可以帮助人们提高生活质量。反之，就会造成隐私侵犯，给人们带来困扰和担忧，甚至还可能带来危害。

■ 数据存储和传输中的隐私侵犯

现在很多智能系统都是架构在网络之上的，这意味着数据必须在网络上传输及存储。云存储是一种新兴的网络存储技术，通过集群应用、网络技术或分布式文件系统等功能，将网络中大量、多种类型的存储设备通过应用软件集成起来，协同工作，共同对外提供数据存储和业务访问功能。由于云存储使用便捷、成本低廉，许多公司和政府组织选择将数据存储到云端。这些信息就容易遭到攻击和窃取，如果其中包含隐私信息，将会带来危害。因此，保护网络传输及云端存储中的数据安全就成为智能系统开发者必须要考虑和解决的问题。

■ 数据分析中的隐私侵犯

对大量的数据进行分析，抽取出有用的知识信息，这个过程就是知识抽取。知识抽取工具可以把很多看似不相关的数据通过人工智能技术整合在一起，从中找出有意义的信息。例如，人们每天的网络聊天和购物等行为，会被网站记录下来，形成各类数据，这些



微信公众号：电子课本大全

数据组合在一起，就可分析出一个人的兴趣、爱好和行为轨迹等。商家可以利用这些数据预测消费者的潜在需求，为消费者提供所需信息、产品或服务，给人们的生活带来便利。同时，这也意味着用户的个人隐私信息被挖掘和利用。因此，规范隐私保护的法律法规是需要与技术应用同步考虑的问题。

### 4.2.2 人工智能的安全挑战

作为新一轮产业变革的核心驱动力，人工智能为产业发展提供了新的机遇。同时，人工智能的广泛应用也带来了安全挑战。人工智能带来的安全威胁来自无意破坏和恶意破坏。无意破坏指系统本身存在功能缺陷，因获得的信息有误而作出错误决策。恶意破坏指人为的主观破坏，例如，一张猫的图片遭黑客攻击后被替换成一张狗的图片，这样就会造成后期的工作基础有误，得到错误的结果。面对安全挑战，只有制定和实施切实可行的应对策略才能让人工智能沿着健康的轨道发展。



**思考活动**

**人工智能应用领域的风险案例**

随着人工智能的不断发展，智能产品广泛应用于生产生活中，不仅提高了生产效率，也提高了人们的生活品质。作为一个新兴领域，人工智能也出现过一些风险案例。例如，国外某驾驶员驾驶一辆汽车，当启动自动驾驶模式后，与拖拉机车相撞而致人死亡。这是首次报道的关于自动驾驶模式致人死亡的事故。

思考：

1. 除此之外，人工智能的风险案例还有哪些？

2. 分析这些人工智能产品存在风险的原因。这些案例是否都是因为存在安全隐患造成的？安全隐患主要体现在哪些方面？

人工智能的安全挑战主要体现在以下四个方面。

■ 国家安全风险

人工智能在国家安全相关领域中的应用可能会带来影响国家安全的风险。人工智能技术对国家安全的影响，主要体现在军事、信息和经济三大方面。特别是在国防建设、基础设施和涉密系统等领域，风险巨大。

政府应注意管控人工智能带来的灾难性风险。管控措施主要包括：限制某些人工智能技术的应用；成立专门负责人工智能技术安全的机构；资助相关研究，开发人工智能系统防故障技术；采取相应措施，以防备人工智能生成伪造的音频、视频和文本文件等。

■ 社会安全风险

人工智能所带来的社会安全风险是多层面的。例如，人工智能技术应用于某些传统制造业，替代了大量以体力和重复劳动为生的工人，导致市场上该类劳动力的需求大幅



微信公众号：电子课本大全

下降，失业人员增加，从而影响社会安定。随着人工智能技术的发展，中高职业技术要求的劳动者的就业形势也会受到冲击。另外，有科幻预言指出，基因技术和人工智能技术的结合有可能会带来社会阶层的极端分化。这虽然是科幻预言，但在人类社会的正常发展过程中，这种未来可能发生的裂变及其带来的潜在危害仍不容小觑。

■ 网络安全风险

网络安全风险主要指网络传输过程中所产生的风险。例如，黑客常使用一些技术攻击或窃取服务器上的数据。网络安全风险还包括对人工智能算法、系统和应用进行恶意的网络攻击，利用干扰技术，使计算机在进行深度学习的过程中受到欺骗，以及利用数据欺诈等手段远程控制网络设备，使设备发生故障或停止工作等。

■ 人身安全风险

人工智能技术在给人类的生产和生活带来便捷的同时，也会给人类自身的安全带来风险。随着人工智能与物联网的深入结合，人们的衣食住行与智能产品之间的关联越来越密切，一旦这些智能产品（如智能医疗设备、自动驾驶汽车等）出现故障，就可能危及人身安全。例如，汽车的自动驾驶系统如果存在严重安全漏洞，乘车人员就可能有生命危险。

## 实践活动

### 容易被人工智能替代的职业及原因

1. 哪些职业比较容易被人工智能替代？说出理由，并填写表4.2.1（可在表中自行添加职业类型）。

表4.2.1　容易被人工智能替代的职业及原因

| 职业 | 是否容易被替代 | 理由 |
| --- | --- | --- |
| 司机 | □是　□否 | |
| 快递员 | □是　□否 | |
| 演员 | □是　□否 | |
| 教师 | □是　□否 | |
| 医生 | □是　□否 | |
| 记者 | □是　□否 | |
| 律师 | □是　□否 | |
| 会计 | □是　□否 | |
| ⋮ | □是　□否 | |

2. 哪些职业永远不会被人工智能替代？若不想被人工智能替代，人类应具备哪些能力？在小组内分享自己的看法。



微信公众号：电子课本大全

### 4.2.3 人工智能的伦理挑战

人类的思考和行动受社会规范、道德伦理和法律法规的约束。人工智能的目标是希望机器能像人一样理性地思考和行动。因此，让机器也能像人一样遵守社会规范、道德伦理以及法律法规成为当前人工智能领域研究和热议的问题。采取措施保障研究人员开发出的智能产品和智能系统与现有的法律、社会规范和道德伦理一致，确定人工智能产品或系统的法律主体、权利、义务和责任，是人工智能带来的伦理挑战。



**思考活动**

**假如与机器人一起生活**

智能产品已经应用到我们的现实生活中，例如养老院的老人护理机器人、家里的儿童陪伴机器人等。现在的机器人虽然还没有理想中那么完美，但是它们已经在改变着我们的生活。假设你的生活中有一个机器人，它将与你一起生活，它的身份可以是老师、保姆或厨师等。

思考：

1. 试想：你和机器人一起生活的日子会是怎样的？你们之间会是怎样的关系？

2. 人工智能会带来哪些伦理问题的挑战呢？

人工智能对伦理问题的挑战，主要表现在以下四个方面。

■ 对“什么是人”问题的新挑战

“什么是人”，这在以前是个不容置疑的问题。人是万物之灵，因其是地球上最有灵性（主观意识）的生命体而与万物不同。我们曾认为人的本质是“会思考”，但是，人工智能的出现打破了这一认识，正在实质性地改变着“人”的属性定义。因为，随着人机互补、人机互动、人机协同和人机一体技术的发展，智能机器也开始逐步具有人所特有的情感和创造性。智能器官的出现，人的自然身体与智能机器开始“共生”。例如，生物智能芯片植入人脑后，可以帮助人脑记忆、运算和表达。这样的“共生体”是人还是机器？智能机器人是人吗？人们不得不重新思考这些问题。

假如智能机器人在某种意义上可以被称为“人”，那么它能和我们人类拥有同等的权利吗？ 它是否像人类一样拥有人格和尊严？智能机器人之间能否像人类一样自由交往？一旦出现问题，承担相应行为后果的是智能机器人还是它的设计者？这类问题已经成为我们必须面对的新问题和新挑战。

■ 对传统伦理关系的新挑战

人工智能的出现带来了诸多的价值难题，包括对传统伦理关系的挑战。例如，当前



微信公众号：电子课本大全

有些青少年终日沉迷于各种智能终端而不能自控，他们对虚拟对象产生过分的眷恋和依赖，认为虚拟世界才是真实、亲切的。这种行为影响了他们人格的健康发展，打乱了传统的伦理关系，这类问题正在变得越发严重。又如，人工智能医生通过虚拟现实技术可以为患者实施手术或进行远程医疗，模糊了现实和虚拟世界之间的界限，使传统医患关系发生改变，可能会给医患双方带来心理上的隔阂。同样地，人工智能教师和保姆等也面临着相同的挑战。

另外，智能系统正在为许多社会组织提供管理服务，这有利于提高管理效率、减少人为失误、节省管理成本。不过，与传统管理方式相比，智能系统缺乏人类特有的同情心和人情味，也忽视了被管理者的文化传统和心理特征。随着具有自主意识的智能机器人的发展和应用，很多新的问题还会出现，如人与机器相比，谁的道德表现更为优异？谁能占据道德制高点？谁更有资格拥有教育、管理权力以及道德裁判权？ 这些都将成为对人类的传统伦理关系的新挑战。

■ 对原有社会秩序的新挑战

由于各个地区的生产力发展不均衡，不同地区的人接触人工智能的机会和方式是不一样的，对于人工智能产品的应用能力也不同，可能导致最先接触和使用人工智能技术的部分人获得较高的收入和社会地位，使原有的社会秩序被打乱。智能机器代替人来聊天、做家务、陪伴和辅导学习等，可能会导致智能机器人“取代”朋友、伴侣和孩子，使社会关系在一定程度上发生改变。此外，人类需要通过劳动获得自我肯定，实现自身价值，赢得社会尊严。但是，当越来越多的智能机器人取代人类劳动时，相关从业者就会失去职业价值，他们在精神上、心理上将承受巨大压力，这也将成为社会秩序所面临的新挑战。

■ 对人类未来命运的新挑战

只专注于完成某个特定任务的人工智能技术被称为弱人工智能，如语音识别、图像识别和翻译等。强人工智能指可以像人类一样思考问题、解决问题、抽象问题、布置计划和快速学习的人工智能技术。超级人工智能指通过相互学习、相互作用、自我完善、不断升级，最终超越人类智能水平的人工智能技术。

超级人工智能是否会出现？它是否会突破人类设计者的约束？人工智能是否会超越人类，甚至毁灭人类？这些问题目前还只是人类的思考和担忧。虽然现在还处于弱人工智能时代，但人类应未雨绸缪，防患于未然，人工智能也许会对人类的未来命运提出新的挑战。



微信公众号：电子课本大全

## 项目实施

### 完成论文（二）

一、项目活动

通过查阅资料，了解当前人工智能的挑战和局限，完成论文第二部分。

二、项目检查

在小组中汇报已完成的论文第二部分，同学之间进行交流、研讨，最后反思自己论文观点的价值。

## 练习提升

1. 查阅关于机器人“索菲亚”的资料。这类机器人的出现将会给人类带来怎样的挑战？它们会毁灭人类吗？

2. 人工智能还会给人类带来哪些挑战？



微信公众号：电子课本大全

# 4.3
# 法规与应用规范

**学习目标** ▶▶▶

- 了解与人工智能有关的法规与应用规范。
- 增强安全防护意识和责任感，自觉维护和遵守人工智能社会化应用的规范与法规。

## 体验探索

### 到底该不该发展自动驾驶汽车

自动驾驶汽车是通过车载传感系统感知道路环境，自动规划行车路线并控制车辆到达预定目的地的智能汽车，如图4.3.1所示。我国自主研制的红旗HQ3无人车，于2011年7月14日首次完成了从长沙到武汉286 km的高速全程自动驾驶实验。公众对自动驾驶汽车的发展并非一边倒地持支持态度，其中不乏反对者和观望者。反对者主要是基于安全方面的考虑，认为自动驾驶技术永远是将保护己方车辆和车内人员作为第一要务，而人类驾驶员则会综合考量自身和周围环境的情况，因此有时能够作出牺牲车辆以保护他人生命安全的判断。



图4.3.1　自动驾驶汽车

全自动驾驶汽车属于无人驾驶汽车的范畴。2018年3月，国外某汽车公司的一辆自动驾驶汽车发生交通事故，与一名正在过马路的行人相撞，导致行人在送往医院后不治身亡。这不是自动驾驶汽车的首次致死事故，但却是导致行人死亡的第一起事故。

这个事件引起了人们对人工智能的安全和法律责任的更多讨论，越来越多的人加入到对人工智能安全、法律法规和道德伦理的研究中。

思考：

1. 人工智能汽车与行人相撞，应该由谁来承担法律责任？
2. 如何保证人工智能设备安全地运作？



微信公众号：电子课本大全

### 4.3.1 法规与责任

人工智能技术是一把双刃剑，它的发展在给人类带来便利的同时，也带来许多问题。人工智能在设计、应用和法律法规等方面的很多研究才刚刚起步。尽管规范人工智能法律的路很漫长，但必须未雨绸缪。目前已经有一些大家公认的规则在起约束作用。

我国公布的《人工智能标准化白皮书（2018版）》中提出了人工智能应当遵循的原则：一是人类利益原则，即人工智能应以实现人类利益为终极目标；二是责任原则，即在技术开发和应用两方面都建立明确的责任体系，以便在技术层面可以对人工智能技术开发人员或部门问责，在应用层面可以建立合理的责任和赔偿体系。

■ 人工智能设计的规则

对于人工智能的设计者，制定法律法规约束其设计意图和行为很有必要。人工智能产品或系统的设计者在设计过程中应注意：第一，必须以为人类带来福祉为主要目标，以达到有助于社会可持续发展为目的；第二，要将人类的价值伦理体系、社会法律和道德规范等嵌入系统，保障人工智能系统遵守人类社会的伦理规范等；第三，不能利用性别歧视和种族歧视等算法决策信息。对此，社会要设立监管机制，监管人工智能相关算法以及算法决策。监管措施包括人工智能算法标准的制定，涉及性能标准、设计标准和责任标准等。由于人工智能算法很复杂，存储方式和分析方式都不固定，世界各国都在呼吁设计者将算法自身的代码以及算法决策透明化，以方便监管。对于算法决策，在确保透明性的基础上，要尊重用户的知情权，在人工智能产品或系统的设计中必须告知用户，并向用户提供相关解释，此外还须提供申诉的平台与管理机制。

■ 人工智能应用的规则

人工智能研发和应用应以辅助人类及社会发展为前提，在追求效率最大化的同时，不损害人的尊严，保障人的权利与自由。人工智能的发展应尊重隐私保护，加强数据安全措施，防止数据滥用，在符合规范和法律制度的前提下，进行个人数据的收集与使用。人工智能的应用应保障人身安全、财产安全及网络信息安全，建立和完善人工智能应用领域的监管机制，保障人工智能应用的安全，促进人类社会经济和文化的发展。

■ 人工智能责任的规则

我国当前的首要工作是尽快立法或制定法规，规范人工智能的责任，完善人工智能相关标准，使人工智能的研发和应用受法律监管。我国还要与其他国家加强人工智能研究的合作，共同探讨如何应对人工智能带来的挑战与风险，评估人工智能技术和产品的伦理影响，提出针对性的措施和预案。

■ 人工智能教育的规则

正确地引导公众学习人工智能相关知识。加强人工智能知识普及教育的同时，完善安全意识教育。不断完善教育体系，培养适应人工智能时代的新型人才。



微信公众号：电子课本大全

**实践活动**

**智能社会中人的责任**

人是人工智能的创造者和使用者，应担负相应的法律法规和伦理道德方面的责任。

查找资料，了解在智能社会中人应担负的责任、当前技术层面的问责体系，以及在应用层面的责任和赔偿体系。

### 4.3.2 规范与安全

与人工智能技术及其应用的快速普及相比，人工智能在规范与安全方面的研究却相对滞后。

目前，关于人工智能安全和伦理等问题的规范还没有定论。我国公布的《人工智能标准化白皮书（2018版）》对人工智能的安全、伦理和隐私保护等相关问题提出了标准规范。人工智能安全及伦理的标准，从广义来说涉及人工智能本身、平台、技术、产品和应用相关的安全标准，以及伦理、隐私保护规范。目前，人工智能安全与伦理标准主要集中在生物特征识别和自动驾驶等部分领域的应用安全标准，以及大数据安全和隐私保护等支撑类安全标准，但对人工智能自身安全或涉及各个领域的基础共性标准还比较少。

解决人工智能的安全问题，可以从两个方面进行：一方面，敦促设计者从安全、伦理和隐私保护等角度考虑产品设计，并限定产品的应用范围、自主程度和智能水平等；另一方面，加强科学家的社会责任感，对人工智能进行安全评估和管理，引导公众正确接纳人工智能。只有切实有效地保障人工智能的安全性，才能使之为人类带来福祉。

**实践活动**

**了解现有的人工智能发展原则内容**

在人工智能产生之初，就有人意识到人工智能安全和伦理的问题，一位科幻作家曾提出机器人三定律。2017年1月，国际上一些人工智能领域的科学家达成了23条人工智能发展原则。

查阅资料，了解机器人三定律以及23条人工智能发展原则的具体内容。

不管人工智能未来如何发展，我们都应具备信息安全意识和保护信息安全的能力，学会保护好自己的隐私数据，不给坏人可乘之机。我们应该遵守信息社会的法律法规、道德与伦理准则，不做任何有损他人的事情，同时也要积极接纳信息技术创新所产生的新观念和新事物，关注信息技术变革所带来的环境问题、法律问题与人文问题，既要有效地维护信息活动中个人的合法权益，又要积极维护他人的合法权益，保障社会公共信息安全。



微信公众号：电子课本大全

## 项目实施

### 完成论文及辩论赛

一、项目活动

每组各推选4名同学作为正反方辩手，以“优势局限之我见”为主题，展开一场辩论赛。

二、项目检查

1. 每人完成一篇以“优势局限之我见”为主题的论文，在小组中交流已完成的论文，同学之间进行研讨。

2. 全班组织一场辩论赛，各组推荐人选，组织参加辩论赛。

## 练习提升

1. 查阅资料，找到当前我国在人工智能规范与安全、法规与责任等方面的政策性文件。

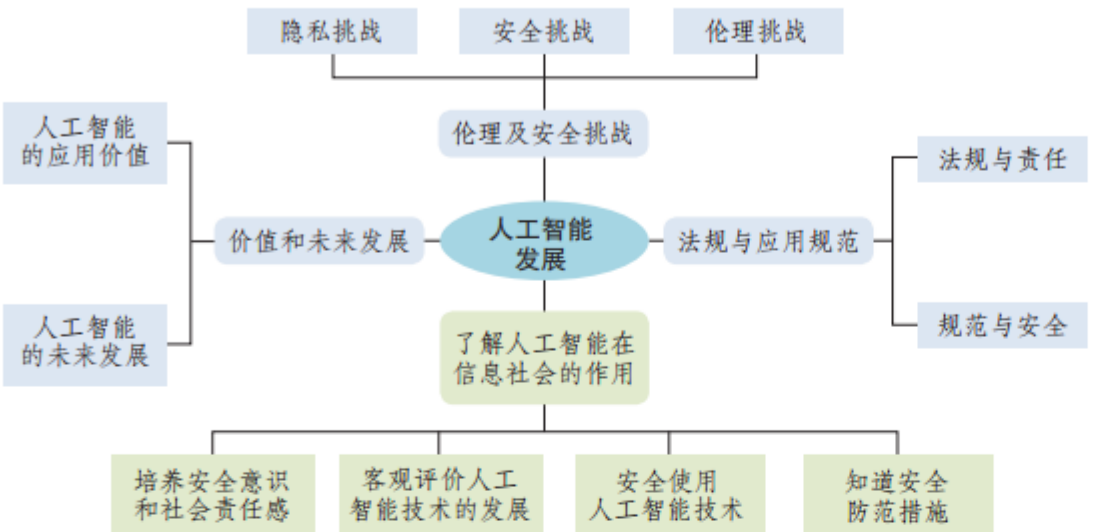
2. 讨论人工智能与人类智能的区别。简述自己对人工智能未来发展的展望。



微信公众号：电子课本大全

## 总结 评价

1. 下图展示了本章的核心概念与关键能力，请同学们对照图中的内容进行总结。




2. 根据自己的掌握情况填写下表。

| 学习内容 | 掌握程度 |
| --- | --- |
| 人工智能的应用价值 | □不了解 □了解 □理解 |
| 人工智能的未来发展 | □不了解 □了解 □理解 |
| 人工智能的应用挑战 | □不了解 □了解 □理解 |
| 人工智能的规则与安全 | □不了解 □了解 □理解 |



微信公众号：电子课本大全

## 项目评价

在完成项目活动后，请各组对项目完成情况进行评价。评价实施围绕项目主题、实施过程、分工合作、项目成果和展示交流五方面进行。根据项目评价中的评分参考，结合项目实际完成情况，确定各项评分结果，给出评分理由。同时，对项目活动进行全面梳理，指出需要进一步改进的地方。将评价内容如实填写到项目评价表中。

| 评价项 | 评分参考 | 评分（1~5分） | 评分理由 | 待改进之处 |
| --- | --- | --- | --- | --- |
| 项目主题 | 项目主题能反映出学科核心素养的要求（信息意识、计算思维、数字化学习与创新、信息社会责任）；主题任务与学习目标保持一致 | | | |
| 实施过程 | 项目研究计划详细，准备充分；实施过程完整，过程记录翔实，资料丰富；研究数据来源渠道多，出处明确，收集方式多样，质量高；研究方法得当，技术手段适宜 | | | |
| 分工合作 | 小组成员分工明确，态度积极，参与度高；善于提出问题，分析问题，解决问题能力强；踊跃分享观点，交流充分；能在完成自己任务的前提下，乐意帮助他组完成任务 | | | |
| 项目成果 | 项目活动成果丰富，内容具体，符合项目目标要求；研究结论清晰准确，有价值，有创新，具有指导及建设意义；项目报告或作品内容完整，论述充分，表述清楚，整齐美观 | | | |
| 展示交流 | 项目展示形式新颖，综合运用多种技术呈现成果，表现力强；语言表达清晰准确，逻辑性好 | | | |
| 项目总分 | | | | |



微信公众号：电子课本大全

# 后　记

本册教科书是中国地图出版社与人民教育出版社依据教育部《普通高中信息技术课程标准（2017年版）》，由双方共同组织团队联合编写的，经国家教材委员会2019年审查通过。

本册教科书的编写，集中反映了我国十余年来普通高中课程改革的成果，吸取了2004年版《普通高中课程标准实验教科书　信息技术》的编写经验，凝聚了参与课改实验的教育专家、学科专家、教材编写专家、教研人员和一线教师，以及教材装帧设计专家的集体智慧。本册教科书的编写人员还有聂璐、刘啸宇、武迪、张思、谷多玉、卢婧华；审校人员有吴劲松、胡志刚、杨奇、刘兆彬。为本册教科书进行装帧设计的有吕旻、李媛，摄影或提供照片的有新华社记者等。

我们感谢所有对教科书的编写、出版、试教等提供过帮助与支持的同仁和社会各界朋友。同时，我们还要感谢2004年版《普通高中课程标准实验教科书　信息技术》的编写人员。

本册教科书出版之前，我们通过多种渠道与教科书选用作品（包括照片、画作）的作者进行了联系，得到了他们的大力支持。对此，我们表示衷心的感谢！恳请未联系到的作者与我们联系，以便及时支付稿酬。

我们真诚地希望广大教师、学生及家长在使用本册教科书的过程中提出宝贵意见。我们将集思广益，不断修订，使教科书趋于完善。

联系方式

电　　话：010-83543863　　010-58758866

电子邮箱：sinomaps@yeah.net　　jcfk@pep.com.cn

中国地图出版社教材出版分社

人民教育出版社课程教材研究所信息技术课程教材研究开发中心

2019年4月

微信公众号：电子课本大全

PUTONG GAOZHONG JIAOKESHU

# XINXI JISHU



微信公众号：电子课本大全