

第1章 人工智能认知与科技伦理

【学习目标】

知识目标：理解人工智能、生成式 AI、机器学习、深度学习、自然语言处理、计算机视觉、大语言模型等基本概念，认识人工智能的发展脉络、主要类型与典型应用。

技能目标：能够结合学习、办公、制造、文旅、创意等真实场景，初步判断常见 AI 应用的技术类型；能够用通俗语言解释 AI “怎么学、怎么看、怎么听、怎么生成”；能够围绕隐私保护、算法偏见、AI 换脸等问题开展案例分析与讨论。

素质目标：树立科技向善、依法用智、责任共担、人机协同的基本观念，理解人工智能发展要服务高质量发展、服务人民美好生活、服务国家安全，在学习中自然融入文化自信、数字工匠精神和职业责任意识。

【情境导入】

小李同学早上用 AI 帮自己整理课堂笔记，中午在食堂刷脸支付，下午做课程汇报时用 AI 自动生成 PPT 大纲，晚上刷短视频时平台推荐的内容“准得有点吓人”。随后，他又在新闻里看到有人利用 AI 换脸和语音克隆技术实施诈骗。

这一天下来，小李突然发现：人工智能并不遥远，它已经悄悄进入了学习、消费、创作、管理、产业和社会治理等方面。对于高职学生来说，认识人工智能，不只是“知道一个新名词”，更是理解未来学习方式、工作方式和社会运行方式的变化。

【本章学习导航】

本章学习导航如图 1-1 所示。先认识 AI 是什么，再理解 AI 怎么工作，最后判断 AI 该怎样发展与使用，这就是本章的学习主线。

学习本章时，建议先抓住三条主线：①聚焦“人工智能与生成式 AI 概述”，帮助我们建立对 AI 发展脉络与典型应用的整体认识；②聚焦“人工智能基础理论”，用通俗类比理解机器学习、深度学习、自然语言处理、计算机视觉和大语言模型；③聚焦“AI 伦理安全与未来展望”，帮助我们形成技术向善、守护隐私、责任共担的底线意识。先看结构，再学细节，更容易把零散知识串成一张完整地图。图 1-2 所示为大学生一天中的 AI 接触场景。



图1-1 本章学习导航



图1-2 大学生一天中的AI接触场景

1.1 人工智能与生成式 AI 概述

1.1.1 人工智能的起源、发展与分类

人工智能,可以简单理解为:让机器完成过去主要依赖人类感知、判断、学习和生成的任务。这里的“智能”并不是说机器真的有了人的意识,而是说它在某些任务上越来越像“会思考、会判断、会创作”的人类。人工智能的应用形态多种多样,如人脸识别、语音输入、路线推荐、智能客服、AI 写作和视频生成等。



从发展过程看,人工智能大致经历了以下三个阶段。第一阶段是规则驱动阶段,这一时期的 AI 更像“按说明书办事的员工”,按照规则执行。第二阶段是机器学习阶段,这一时期机器不再完全依赖固定的规则,而是通过大量样本“自己找规律”。第三阶段是生成式 AI 与大模型阶段,这一时期 AI 不仅会判断“这是什么”,还会生成“新的内容”,如文字、图像、音频和视频。图 1-3 为人工智能发展阶段时间轴示意图。



图 1-3 人工智能发展阶段时间轴示意图

按任务能力来分,人工智能常见有三类:一是感知型 AI,负责“看”和“听”,如图像识别、语音识别;二是决策型 AI,负责“判断”和“推荐”,如导航、推荐算法、风险预警;三是生成型 AI,负责“创作新内容”,如写文案、做海报、生成短视频。

人工智能经历了从“靠规则”到“靠数据学习”再到“会生成内容”的发展过程。理解这条发展线索,有助于把复杂技术放回真实场景中去看:它不是突然冒出来的“黑科技”,而是一步步演进形成的能力体系。

【知识卡片】

人工智能不等于“电子人”。

它更像一套能完成特定智能任务的数字系统。

今天的大多数 AI 仍然属于“专才型”弱人工智能,而不是真正意义上的“全能型”强人工智能。

【想一想】

你每天接触的“会推荐”“会识别”“会生成”的软件,各自属于哪一类人工智能?

1.1.2 生成式AI的概念、特点与演进

很多学生第一次听到“生成式 AI”,会觉得这个词很抽象。其实通俗地说就是:它不只是会认、会判,还会“产出新东西”。传统 AI 更像阅卷老师,负责判断“对不对”;生成式

AI 更像内容助手,能根据要求写文章、画图片、做视频、生成代码。传统判别式 AI 与生成式 AI 对比如图 1-4 所示。



图1-4 传统判别式AI与生成式AI对比

生成式 AI 有三个显著特点。第一,会生成。它不仅能分析已有内容,还能组合并生成新的表达结果。第二,会多模态。越来越多的模型既能处理文字,也能理解图片、音频和视频。第三,会协同。它不只是回答一个问题,而是开始参与一整段任务流程,例如“先理解,后整理,又生成,再优化”。

生成式 AI 为什么会在近几年迅速发展? 原因主要有四个: 数据更丰富了,算法更强了,算力更充足了,场景需求更迫切了。随着教育、办公、制造、营销和创意设计等领域的数字化推进,社会越来越需要一种“会表达、会总结、会创作”的工具。

生成式 AI 的核心在于“基于已学到的规律,生成新的内容”。它既是 AI 能力升级的重要标志,也是后续智能写作、AI 绘画、智能办公、数字人和智能体应用的基础。

【知识卡片】

一句话读懂生成式 AI: 传统 AI 更擅长“分辨”,生成式 AI 更擅长“创造”。

【应用案例】

绍兴柯桥推出纺织印染行业垂类大模型“AI 布”,可用于花型设计、印染技术查找、找面料和找工厂等场景,显著提升传统纺织业的智能化协同效率。这个案例说明,生成式 AI 并不只是“写文章”,还可以真正进入产业链、设计链和服务链。

【想一想】

为什么说生成式 AI “像在创造”,但又不是完全无中生有?

1.1.3 人工智能与生成式AI的典型应用领域

人工智能已经渗透到社会生活的方方面面,正在深刻改变各行各业的工作方式。在



医疗健康领域, AI 辅助诊断系统能够帮助医生快速识别 CT 影像中的肺结节, 提高诊断效率和准确率, 缓解基层医疗资源不足的问题。在金融领域, AI 风控系统实时监测数百万笔交易, 在毫秒内识别异常行为, 防范金融欺诈。在教育领域, AI 个性化学习系统根据每个学生的知识掌握情况、学习风格和薄弱环节, 精准推荐学习内容和练习题目, 真正实现“因材施教”。在交通领域, 自动驾驶技术正在从封闭园区测试走向开放道路试点运营。

在产业场景中, AI 正加速走进实体经济。绍兴柯桥的“AI 布”推动纺织印染业加速迈入智能化; 诸暨珍珠产业已经出现 AI 珍珠精选机, 用于辅助识别珍珠大小、圆度、光泽和表面瑕疵, 大幅提升了分级效率; 古越龙山则在黄酒生产中推进酿造智能化、过程可视化和管理的数字化。

这里特别值得引出一个概念: 数字工匠精神。绍兴黄酒讲究“冬酿”, 看似是传统工艺, 背后其实体现的是对时间、温度、火候、原料的精确把握。AI 训练和数据治理也是一样, 数据差一点, 结果就可能偏很多。会点工具只是开始, 把数据做准、流程做稳、结果做实, 才是真正的数字工匠。

在商贸与跨境电商场景中, AI 正重塑工作方式。AI 数字人主播、多语种视频生成与智能选品技术, 帮助企业突破了语言与时空限制, 实现了全天候的跨国界营销。在文化传承与创意设计领域, AIGC 为传统文化传播提供了新路径。AI 可以辅助生成越剧人物形象、数字海报、文旅解说词, 还能在书法教学中模拟《兰亭序》笔意, 帮助学生直观理解传统艺术之美, 这些典型应用场景如图 1-5 所示。这并不是用技术代替文化, 而是让文化以更年轻、更多元的方式融入当代生活。



图1-5 人工智能典型应用场景

对于学习者而言, 理解 AI 的应用场景是掌握技术的第一步。在学习与办公场景中, AI 已成为得力助手: 它可以帮助梳理知识点、生成提纲、改写表达、总结长文, 也能自动撰写邮件、生成会议纪要、分析表格数据、搭建 PPT 框架、辅助客服问答。AI 最大的价值, 不是替人“偷懒”, 而是帮助人把精力从重复劳动中解放出来, 转向更重要的沟通、决策和创

造。理解这些应用,不只是为了“知道 AI 很厉害”,更是为了在未来学习和工作中找到“我怎样与 AI 协同”的入口。

【想一想】

结合你的专业,想一想 AI 可以在哪些方面帮助你未来的职业发展? 试着列出至少两个具体的应用场景。

1.2 人工智能基础理论

1.2.1 机器学习基础

机器学习听起来很专业,其实可以把它想成教幼儿认苹果,如图 1-6 所示。如果只告诉孩子“苹果是红的、圆的、能吃的”,他很可能把番茄也认成苹果。更好的办法是给他看很多苹果,也给他看很多不是苹果的东西。看多了,他就慢慢知道“什么是苹果,什么不是苹果”。机器学习也是一样:它并非由人逐条编写全部规则,而是给机器大量样本,让机器自己总结规律。



图1-6 机器学习像教幼儿认苹果

机器学习主要有三种方式:①监督学习,像学生做有标准答案的练习题;②无监督学习,像让学生自己给一堆资料分类;③强化学习,像打游戏闯关,做对了加分,做错了扣分。你现在不用死记这些概念,只要先明白一句话:很多 AI 不是“通过编程实现的”,而是“被训练出来的”。

【知识卡片】

机器学习的核心不是“背规则”,而是“从样本中找规律”。

1.2.2 深度学习与神经网络

如果说机器学习是“让机器看例子找规律”,那么深度学习就是把这个找规律的过程分成更多层并做得更细。



你可以把神经网络想象成一条流水线,如图 1-7 所示:第一位质检员看轮廓,第二位看颜色,第三位看纹理,第四位再综合判断。通常情况下,层数越多、分工越细,模型的表达能力越强,判断也越准确;但层数过多也可能带来训练困难和过拟合的风险。深度学习正是利用多层网络逐层提取特征,所以它特别擅长做图像识别、语音识别和视频理解这类复杂任务。

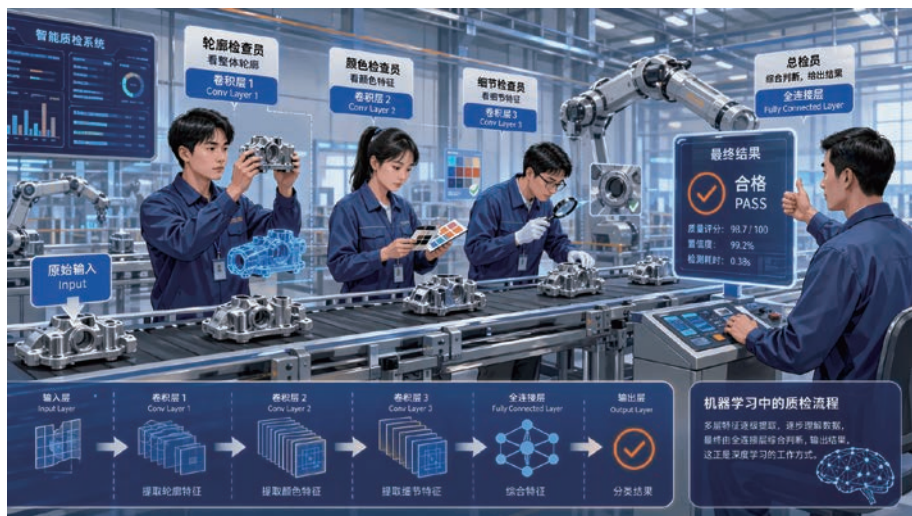


图1-7 深度学习像流水线质检员

当然,深度学习也不是没有代价。它往往需要更多数据、更多算力,训练好的模型在做出判断时更像一个“黑箱”——结果很好,但不一定一眼就说得清“为什么会这样判断”。这就提醒我们:技术越强,越要重视结果解释、应用边界和使用责任。

深度学习是当前 AI 最强大的“引擎”,大语言模型、图像生成、自动驾驶等前沿应用都建立在深度学习之上。如诸暨珍珠产业中的 AI 珍珠精选机,正是计算机视觉与深度学习结合的典型应用,它可以辅助识别珍珠的大小、圆度、光泽和表面瑕疵,把很多依赖经验的分拣环节做得更稳定、更高效。

深度学习是建立在神经网络基础上的更强学习方式。它像一条层层筛选的智能流水线,特别适合处理图像、声音和文本等复杂信息。

1.2.3 自然语言处理与计算机视觉

如果把 AI 看成一个数字世界里的“新人类”,它也需要自己的“耳朵”和“眼睛”,如图 1-8 所示。

自然语言处理就是机器的“耳朵和嘴巴”,它负责让机器读懂文字、理解语义、生成回答、完成摘要、翻译和对话。你用智能助手问问题、用 AI 改作文、用语音输入转文字,本质上都离不开自然语言处理。

计算机视觉就是机器的“眼睛”,它负责看图、识别人脸、分析视频、检测瑕疵、定位目标。手机刷脸解锁、工厂智能质检、景区人流识别、医学影像辅助分析等都属于计算机视觉的常见应用。



图1-8 机器的耳朵与眼睛示意图

自然语言处理和计算机视觉分别对应机器的“语言能力”和“视觉能力”，而多模态发展则让机器开始同时理解多种信息形式。今天更先进的系统，往往不是单独“会听”或单独“会看”，而是二者开始融合。你发一张图片给 AI，它能帮你写说明；你上传会议录音，它能帮你转成文字并总结重点；你输入一句话，它能直接生成一张图。这种同时处理文字、图片、声音、视频的能力，叫作多模态能力。

【知识卡片】

自然语言处理是机器“懂话、说话”的能力。

计算机视觉是机器“看图、认物”的能力。

多模态就是让机器把“眼睛、耳朵、嘴巴”一起用起来。

1.2.4 大语言模型基础认知

这两年最常听到的词就是大语言模型。你可以把它想象成一个博览群书、特别擅长“接话”的博学者，如图 1-9 所示。



图1-9 大语言模型像博览群书的博学者



它在训练阶段读过海量文本,慢慢学会了:什么词常和什么词一起出现,什么句式适合什么场景,什么问题通常怎么回答。所以当你输入一句话时,它会根据上下文预测“下一个最可能出现的词、短语或句子”,再一步步往下生成。

为什么它看起来“懂得很多”?因为它读过很多内容,能把不同领域的表达方式和常见模式联系起来。但一定要注意:它很会说,不等于它永远说得对。大语言模型有时会出现“幻觉”,也就是一本正经地给出并不准确的内容。所以,在涉及政策、法律、医学、财务、学术引用时,不能“AI一说我就信”,而要学会核验、比对和追问来源。

大语言模型是当前生成式 AI 的重要基础。它通过学习海量文本规律,实现理解和生成语言的能力,但生成流畅不等于事实必然准确,人类判断依然不可替代。

【知识卡片】

一句话理解大语言模型:它本质上是一个“特别会根据上下文接话”的语言生成系统。

【想一想】

为什么大语言模型写出来的话“很像真的”,但仍然需要人来最后把关?

1.3 AI 伦理安全与未来展望

1.3.1 AI伦理规范与国家安全

人工智能越强,越不能只问“能不能做”,还要问“应不应该做,怎样做才合规,出了事谁负责”,这就是 AI 伦理。

我国在人工智能治理上始终强调发展和安全并重、创新和治理并行、技术向善、以人为本。今天的 AI 安全,不只是“计算机会不会中毒”,还包括数据安全、网络安全、舆论安全、产业链安全和关键技术安全。人工智能已经成为发展新质生产力和推动科技自立自强的重要力量。

借用大禹治水的思想来理解 AI 治理。治水不是只靠堵,也不是只靠放,而是疏堵结合、系统治理。算法和模型治理也是一样:既不能放任不管,也不能因噎废食。要在鼓励创新与防控风险之间找到平衡。

AI 伦理不是技术发展的“刹车片”,而是技术健康发展的“方向盘”。只有坚持发展和安全并重,人工智能才能真正服务社会进步和国家发展。

【知识卡片】

“智能向善”不是一句口号,而是要求 AI 的发展目标、应用过程和治理方式都以增进社会福祉为导向。

1.3.2 算法偏见、隐私保护与责任归属

很多人以为,机器没有情绪,所以一定更公平。其实不然。如果训练数据本身就有偏

差,算法就可能把这种偏差“学进去”。这就是算法偏见。它往往不是机器“故意歧视”,而是现实中的不平等被技术重新放大了。

再看隐私保护。人工智能离不开数据,但数据不是想收就收、想用就用。以人脸识别为例,如果有其他非人脸识别方式可以达到同样目的,就不应把刷脸作为唯一验证方式。

如景区实行“限量、预约、错峰”管理,并采用分时预约、身份证或人脸识别入园等方式。技术上看,这确实提升了通行效率;但伦理上也必须追问:收集了哪些数据?游客是否被充分告知?有没有替代验证方式?数据保存多久?是否会被用于营销?

再看 AI 换脸和深度伪造。它们可以服务影视制作、数字人和创意表达,但一旦被用于诈骗、侵权和造谣,就会直接伤害公共利益和个人权益。

那么出了问题谁负责?答案很明确:不能把责任“甩”给 AI。真正承担责任的仍然是开发者、平台、运营者、使用者和相关单位。谁设计、谁提供、谁运营、谁使用,谁就不能只享受效率红利,而不承担治理责任。

算法偏见提醒我们:机器并不天然公正;隐私保护提醒我们:数据不能无限采集;责任归属提醒我们:出了问题不能怪机器。真正成熟的 AI 应用必须建立在公平、合规和可追责的基础上,技术发展与伦理治理的平衡如图 1-10 所示。



图1-10 AI伦理风险与治理平衡

【想一想】

如果你是平台运营者,你会怎样在“提高效率”和“保护隐私”之间划清边界?

1.3.3 人工智能的未来发展趋势与社会责任

展望未来,人工智能大致会沿着三条线继续往前走。第一,更强大。多模态、智能体、具身智能会进一步发展, AI 不只是会聊天,还会调用工具、执行任务、进入物理世界。第二,更深入。它会更深入地进入制造、教育、医疗、交通、文旅和公共服务。第三,更普及。模型效率提升、成本下降,意味着更多学校、企业和普通人都能更方便地用上 AI。



但越是这样,越要学会人机协同。未来真正有竞争力的人,不一定什么都亲力亲为,而是知道什么适合交给 AI 做、什么必须由人来判断。AI 可以辅助搜集资料、生成初稿、处理重复任务、创建短视频和图像,但价值判断、伦理选择、责任承担和建立信任关系仍然离不开人。

对于我们来说,真正重要的不是“害怕 AI 抢工作”,而是尽快成长为会与 AI 共事的人。你要会提问、会验证、会组合工具、会识别风险、会守住边界。这样, AI 越强,你越不会被代替,反而越能借力成长。

【知识卡片】

未来最重要的能力不只是“会用 AI”,而是“会与 AI 协同,并在关键处保留人的判断”。

【想一想】

未来进入职场后,你最希望 AI 帮你完成哪三类任务? 哪三类任务你认为必须由人来最终决定?

1.4 实 践 任 务

实践任务1：调研身边三个AI应用并分析其AI技术与社会价值

任务目标：认识身边 AI 应用的真实形态,分析其 AI 技术,并分析其社会价值与潜在风险。

任务描述：人工智能已悄然融入我们的学习、生活与工作。请你选择三个你真实接触过的 AI 应用,围绕“它解决了什么问题、用了哪些 AI 技术、它带来了什么价值、它可能带来什么风险”进行分析。

实施步骤：具体如下。

(1) 应用选取：观察并记录身边高频使用的三个 AI 应用,尽量涵盖不同领域的 AI 技术,如 AI 写作、短视频推荐、刷脸支付、智能客服、图像美化等。

(2) 记录体验：截图或拍照保留使用证据。

(3) 技术分析：通过网络检索或查阅相关资料,分析每个 AI 应用背后的核心 AI 技术。

(4) 汇总展示：将调研结果整理成图文并茂的调研报告。

成果要求：提交 800 ~ 1000 字的调研报告。

实践任务2：结合“鲁迅故里”游客数据采集场景开展AI隐私保护讨论

任务目标：理解智能文旅中的数据采集与隐私边界,培养合法、正当、必要、最小够用地正确使用数据的意识。

任务描述：以鲁迅故里预约入园、客流分析、智能导览为背景,从游客、景区管理者、技术公司、监管部门四个角色出发,讨论景区数据采集的必要性、风险点和保护方案。

实施步骤：具体如下。

(1) 识别数据：列出景区可能采集的身份、行程、行为等数据。

(2) 分析风险：判断哪些数据属于必要采集，哪些存在过度采集嫌疑。

(3) 角色讨论：围绕“是否必须刷脸、是否有替代验证方式、是否允许用于营销”等问题展开辩论。

(4) 形成建议：撰写“鲁迅故里智能文旅隐私保护建议书”。

成果要求：提交 1000 字左右建议书或课堂展示稿。

实践任务3：小组讨论AI换脸技术的伦理边界与法律规范

任务目标：理解深度伪造技术的双重属性，明确其合法应用边界与违法风险。

任务描述：围绕 AI 换脸、语音克隆、数字人视频等现象，分析其在影视制作、文旅传播中的正面用途，以及在诈骗、侵权、造谣中的风险，结合相关法规讨论平台责任、开发者责任和使用者的责任。

实施步骤：具体如下。

(1) 查找案例：每组收集 1 ~ 2 个真实的公开案例。

(2) 分类判断：分为正当用途、争议用途、明显违规三类。

(3) 对照法规：重点关注实名、审核、显著标识和内容管理责任。

(4) 小组陈述：形成统一结论并进行课堂表达。

成果要求：提交 800 字左右案例评析或讨论纪要。

本章小结

本章从“人工智能是什么”讲起，帮助大家认识了人工智能从规则驱动到机器学习、再到生成式 AI 和大语言模型的发展过程；又用生活化类比理解了机器学习、深度学习、自然语言处理、计算机视觉和大语言模型等基础概念；最后进入伦理、安全与未来展望，明确了人工智能必须坚持以人为本、智能向善、发展和安全并重。

学习 AI 不是为了盲目追热点，而是为了形成三种能力：看得懂、用得上、守得住。只有把技术能力、职业素养、法治意识和社会责任统一起来，才能真正成为智能时代需要的高素质技术技能人才。

复习本章时，可以重点抓住三类内容。第一类是关键概念，包括人工智能、生成式 AI、机器学习、深度学习、自然语言处理、计算机视觉、大语言模型、算法偏见、隐私保护与责任归属等。第二类是核心逻辑公式，可记作“人工智能三要素 = 数据 + 算法 + 算力”“机器学习基本链路 = 数据 → 训练 → 模型 → 预测”“大语言模型主流工作逻辑 = 上下文 → 预测下一个词 → 连续生成”“AI 治理平衡 = 发展与安全、效率与公平、创新与责任”。第三类是易错点，例如，把 AI 当成万能答案、把生成结果当成事实、把推荐算法当成天然中立、把便利凌驾于隐私之上、把责任全部推给机器等。把这些要点连起来，本章知识才算真正成为“有血有肉”的网络。

第2章 驾驭AI的第一步：提示词与高效对话

【学习目标】

知识目标：理解提示工程的核心概念、原则和价值；掌握提示词的关键构成要素；了解零样本提示与少样本提示的原理和应用场景；认识主流结构化提示框架；理解思维链及分步推理的机制；掌握迭代优化方法以及元问题、元指令的概念和作用。

技能目标：能够设计包含关键要素的结构化提示词；能够运用零样本、少样本提示方法引导 AI；能够通过思维链分步推理，拆解并解决复杂问题；能够运用迭代优化技巧改进和完善提示词；能够利用元问题和元指令与 AI 进行高效互动，明确需求并构建有效指令；能够综合运用多种提示工程技巧，为特定场景定制 AI 解决方案。

素质目标：树立用结构化思维和系统化方法与 AI 高效沟通的意识；培养通过迭代优化提升 AI 输出质量的耐心与精益求精的数字工匠精神；形成主动利用元问题和元指令，澄清需求、精准指挥的职业习惯，提升人机协同效率。

【情境导入】

小张是电子商务专业的大二学生，最近接了一个校内实践任务：为学校社团的“国潮文化周”设计一份线上推广方案。他听说用 AI 可以快速出方案，于是打开对话窗口，输入：“帮我写一个国潮文化周的推广方案。”

几秒钟后，AI 回复了一段四五百字的文字，内容虽然完整，但读起来像百度百科的介绍。小张挠了挠头，室友小李凑过来看了一眼，笑着说：“你这是在和 AI ‘随便问问’，它当然只能‘随便答答’。你得学会‘指挥’它——就像给一个很聪明但不了解你心思的实习生下任务，你要告诉它你是谁、要达成什么目标、受众是谁、限制条件有哪些，甚至可以先给它看个例子。”

小李接过键盘，写了一段长长的提示，完成提示词发送后，AI 生成了一份结构清晰、重点突出的方案。小李拍了拍他的肩膀：“这就是提示工程的魔力。”

【本章学习导航】

本章学习导航如图 2-1 所示。先认识提示词是什么，再理解如何设计高质量提示词，最后掌握高级思维引导和迭代优化，这就是本章的学习主线。

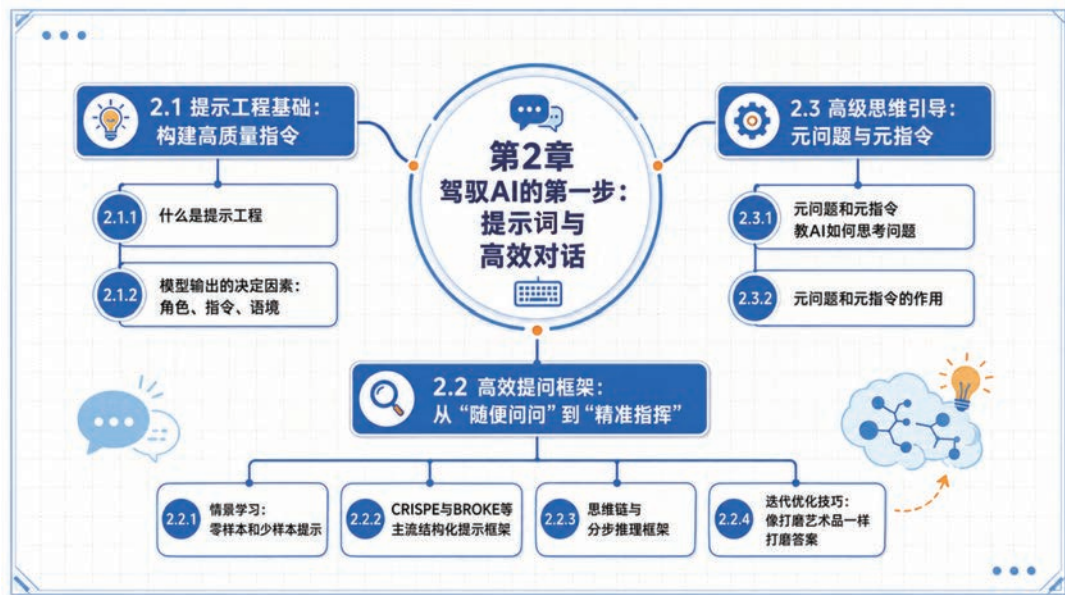


图2-1 本章学习导航

学习本章时,建议先抓住三条主线:①聚焦“提示工程基础”,帮助我们理解提示词的核心要素(角色、任务、背景、目标、格式)以及模型输出的决定因素;②聚焦“高效提问框架”,学习零样本/少样本提示、CRISPE与BROKE等结构化框架、思维链分步推理以及迭代优化方法;③聚焦“高级思维引导”,掌握元问题与元指令的概念和作用,提升人机交互效率和认知一致性。先掌握基础要素,再练习结构化框架,最后运用元思维优化交互,更容易把零散技巧串成一套实用的提示工程能力。

2.1 提示工程基础：构建高质量指令

2.1.1 什么是提示工程

提示工程(prompt engineering)是指通过设计和优化“提示词”(prompt),帮助生成式人工智能模型更准确地理解用户需求,并输出符合预期结果的一种方法。

假如现在你有一盏阿拉丁的神灯,灯神让你许三个愿望。首先我们会思考如何去表达我们的愿望,才能确保灯神可以理解。例如,我们想变成世界上最富有的人,结果愿望没说好,导致灯神误解了,把我们变成了世界上最贫穷的人。或者本来想让灯神给我1万亿美元,但对灯神说的是:请你给我1万亿,灯神可能就会随机给出一种货币,有可能是津巴布韦币(1万亿津巴布韦币=1美元)。显然,结果并不是我们想要的。

通过上面的例子不难看出灯神等于大语言模型,许下的愿望等于发送给大语言模型的内容等于提示词。而最终大语言模型能否很好地完成我们的任务,都取决于提示词的好坏。于是就诞生了一个新的学科——提示工程,这个学科就是研究如何写出更好的“提示词”。因此,提示工程可以看作人与人工智能之间进行高效沟通的一门技术。



【知识卡片】

提示工程可指导 AI 模型生成所需回答,可以将其视为一个路线图,引导 AI 朝着预想的特定输出方向前进。

2.1.2 模型输出的决定因素：角色、指令、语境

要写出一个好的提示词,就像写一篇小作文,它不是简单的词语的堆砌,而是需要包含一些核心要素。掌握这些要素,并学会灵活运用它们,就能让你与 AI 的沟通事半功倍。

我们通常会将一个有效的提示词拆解为以下几个关键要素。

要素一：角色 (role)

角色要素要求在提示中明确告诉 AI 应该“扮演”什么角色或者具备什么专业背景。如“你是一位资深的市场营销专家”“请你扮演一名高中数学老师”等。不同的角色代表不同的专业知识、表达方式和侧重点。设定角色能极大地影响 AI 输出内容的专业性和风格。

复述问题(错误的示范),提示词如下。

写一篇手机推广文案。

改进后的提示词如下(使用角色)。

请你扮演一位资深的市场营销专家,尤其擅长面向 Z 世代的校园推广。请为我写一篇推广文案。

要素二：任务 (task)

任务是提示的核心,它直接告诉 AI “你要做什么”以及“做到什么程度”。任务描述必须明确、具体、可执行。任务越具体, AI 的执行偏差就越小。这就像给了大厨一份详细的菜谱,而不是只说了“做道菜”。

复述问题(不够具体),提示词如下。

帮我写文案,介绍一下手机。

改进后的提示词如下(明确任务)。

请写一篇 300 字左右的微信朋友圈推广文案,要求:①突出“超长续航”和“超值性价比”两个卖点;②语气要活泼、有网感、能引起学生共鸣;③文案末尾需要包含一个号召性语句,比如“快来入手吧!”。

要素三：背景 (context)

背景信息是 AI 理解提示“语境”的关键。提供与任务相关的背景信息、数据、前提条件能帮助 AI 理解你的“潜台词”,避免产生误解。

复述问题(缺乏背景),提示词如下。

写一篇关于手机续航和性价比的文案。

改进后的提示(补充上下文)如下。

我们是一家新成立的手机品牌,产品定位是面向在校大学生。目标受众每天需要刷课、看视频、玩游戏,对电池续航时间很敏感,同时购买力有限。请基于这个背景写一篇关于续航和性价比的文案。

要素四：目标（goal）

告诉 AI 你写这段文案最终是为了什么，是提升品牌认知？增加购买转化？还是征集用户故事？不同的目标，文案风格和侧重点完全不同。

复述问题（目标模糊），提示词如下。

写文案。

改进后的提示（明确目标）如下。

这篇推广文案的核心目标是吸引大学生单击链接查看详情页，最终促成下单购买。所以文案要制造紧迫感，比如“限时优惠”“学生专享价”，并在结尾附上清晰的购买引导。

要素五：格式（format）

对于很多任务，你需要 AI 以特定的结构输出结果，比如表格、列表、代码块、大纲等。明确格式要求能让你直接得到可用的内容，节省二次整理的时间。

复述问题（无格式要求），提示词如下。

列出这款手机的优缺点。

改进后的提示（指定格式）如下。

请以表格的形式，对比这款手机和同价位竞争对手（比如红米 Note 系列、荣耀 X 系列）的优点和缺点，包括以下三个维度：屏幕、电池、处理器。表格需要清晰明了。

【案例 1】手机推广文案生成。

【任务描述】

你是某手机品牌的校园市场推广专家，对于刚发布的新产品“青禾 C5”，需要撰写一篇面向大学生的适合发布在小红书平台的推广文案。

【任务实施】

步骤一：根据提示词的构成要素编写提示词。

角色：你是一位资深的校园市场推广专家，非常了解大学生的消费心理和网络用语。

任务：撰写一篇面向小红书的推广文案。文案要突出“告别电量焦虑”和“用 1500 元买到 4000 元产品的体验”两个核心点；语气要活泼有趣，可以适当使用表情符号和网络热词。要求包含一个吸引人的标题（不超过 15 字）、正文（200 ~ 300 字），以及一个具有强号召力的结尾。

背景：我们是一家新创的手机品牌青禾，刚刚发布了一款主打产品青禾 C5。它的核心卖点是 6000mAh 超大电池和 1499 元的超值学生价。目标客户是 18 ~ 22 岁、预算有限但非常需要长续航的大学生。

目标：最大程度地吸引人，激发大学生的购买欲望，引导他们单击文案中的购物链接。

格式：直接输出完整文案，不需要额外解释。

步骤二：结果生成。

生成对应的内容，大模型生成结果如图 2-2 所示。



手机推广文案生成

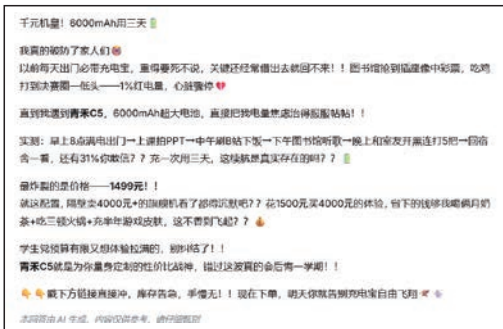


图2-2 DeepSeek模型生成结果（1）



2.2 高效提问框架：从“随便问问”到“精准指挥”

2.2.1 情景学习：零样本和少样本提示

人工智能模型在处理任务时展现出一种独特的“举一反三”能力。其中，零样本提示便是这种能力的一个典型体现。零样本提示是指我们在给 AI 模型下达指令时，不提供任何例子，仅仅依靠模型本身在预训练过程中已经学习到的知识、能力和推理逻辑来完成任务。此时，我们信任模型已有的“通用知识库”。我们假设模型已经“见过”足够多的类似场景，可以理解我们的抽象指令。

【应用案例】

(1) 情感分析。提示词如下。

判断以下评论的情感是积极、消极还是中性：“这家餐厅的菜品还不错，但服务员的态度有待提高。”

AI 输出为“中性”。

(2) 文本分类。提示词如下。

以下文本属于哪种类型：新闻报道、广告文案、科幻小说？“未来的城市，飞行汽车穿梭于高楼之间，人工智能管理着一切。”

AI 输出为“科幻小说”。

(3) 信息提取。提示词如下。

从以下句子中提取出人名和地点：“张华和李明在北京故宫博物院参观。”

AI 输出为“人名：张华，李明；地点：北京，故宫博物院”。

零样本提示的优势在于其操作的简单快捷性，用户无须额外准备示例数据，直接表述需求即可。然而，对于模型不太熟悉的高度专业领域知识，或是要求特定格式及复杂推理的任务，其效果可能不尽如人意。

与零样本提示不同，少样本提示为 AI 模型提供了一种“有样学样”的学习机制。当你学会了一个新技能，比如用一个新的软件修图。老师先给你演示了三张图片的修图步骤和效果，你依照着这几个例子，很快就掌握了修图的规律。AI 的少样本提示能力也是如此。

少样本提示的核心在于，用户在向 AI 模型提出任务请求时，会在提示语中包含少数精心挑选的输入—输出配对示例。当 AI 模型接收到少样本提示时，它会深入分析这些输入与输出之间的映射关系。例如，如果示例展示了将非正式语言转换为商务语言的模式，模型会从中学习这种转换规则，并将其推广到新的非正式语句上。这种深层理解使得 AI 模型能够更好地泛化到新的、未曾见过的输入数据上，从而精确执行用户意图。

【应用案例】

(1) 特定格式的文本生成。提示词如下。

请将以下公司名称转换为统一的缩写格式。

公司名称: Apple Inc. 缩写: AAPL

公司名称: Microsoft Corporation 缩写: MSFT

公司名称: Google LLC 缩写: GOOGL

公司名称: Amazon.com, Inc. 缩写: AMZN

公司名称: Tencent Holdings Ltd. 缩写: ……

AI 输出为 TCEHY。

(2) 自定义分类。提示词如下。

请根据客户邮件内容判断需求类型。

邮件: 我无法登录我的账户, 忘记了密码。 类型: 账户问题。

邮件: 我收到了一个损坏的产品, 想申请退货。 类型: 退货 / 换货。

邮件: 你们的最新产品什么时候发布? 类型: 产品咨询。

邮件: 我的订单号是 123456789, 想查询一下物流状态。 类型: 订单查询。

邮件: 我想更改我的收货地址, 可以吗? 类型: ……

AI 输出为“订单修改”。

少样本提示通过示例 AI 能够更精细地捕捉任务的微妙之处与具体要求。它还具备强大的适应性, 允许用户针对特定行业、风格或数据格式的任务进行个性化定制, 而无须进行耗时耗力的模型再训练。尽管如此, 少样本提示也存在一定的局限性。首先, 提示长度有限制, 过多的示例可能导致提示语超出模型的最大输入长度, 从而无法被完全处理。其次, 示例的质量至关重要, 提供的示例必须是高质量且能有效代表任务特征的, 否则反而可能误导 AI 模型的学习方向。最后, 虽然效果显著, 但毕竟是“少样本”, 对于那些极其复杂、需要大量专业知识或深层推理的任务, 少样本提示仍可能无法达到完美解决的程度。

2.2.2 CRISPE与BROKE等主流结构化提示框架

前面我们学习了提示工程的五大构成要素——角色、任务、背景、目标、格式。但很多学生可能会问: 这些要素该怎么组织在一起呢? 是不是每次都要凭灵感胡乱拼凑? 当然不是。在真实的工程实践中, 高手们会使用提示词框架——一种结构化的模板, 把各个要素按照逻辑顺序组织起来。这就像做菜有了菜谱, 盖房子有了蓝图, 你不再需要每次从头摸索。

大多数学生刚开始写提示词时, 容易犯一个错误: 用“写给人看的方式”写提示词。比如: “你是一个非常专业而且经验丰富的分析师, 现在我给你一段项目资料, 希望你能够帮我认真分析一下这个项目的优缺点、存在的问题以及未来可能的发展方向, 最好能从多个角度展开, 并给我一些有价值的建议。”这段话看起来很诚恳, 但对 AI 来说效率很低。因为 AI 不是人, 它不擅长“领会精神”, 它只擅长拟合结构、复制模式、延续格式。上面的提示词没有模块化, 没有边界, 没有稳定的输出结构, 而且不可复用——换一个项目, 你又得重新写一遍。

提示工程的第一原则是: 用结构代替语义, 用协议代替描述。好的提示词是用“框架”写出来的, 而不是靠“灵感”憋出来的。下面我们学习两种较为实用、经典的提示词框架。



1. CO-STAR 框架：通用任务型

CO-STAR 框架由 6 个组件构成,每个字母代表一个关键模块,各模块含义如表 2-1 所示。该框架特别适合知识工作类任务,如分析、写作、总结、评估,以及教学和探索型场景。CO-STAR 框架把人类在沟通中默认隐含的信息全部显式地写出来。平时我们和人说话时,大脑会自动补充场景、目的、身份、受众、格式等背景,但 AI 没有这些隐含假设,你必须一条一条、清清楚楚地告诉它。

表 2-1 CO-STAR 框架构成元素及其含义

字 母	含 义	解 释
C (context)	背景 / 状态 / 前提	告诉 AI “现在是什么情况”
O (objective)	总目标	告诉 AI “我们最终要达成什么目的”
S (style)	风格 / 角色	告诉 AI “你该用什么身份和语气”
T (task)	具体任务	告诉 AI “具体要做什么动作”
A (audience)	目标受众	告诉 AI “输出内容给谁看”
R (response)	输出格式	告诉 AI “以什么结构呈现答案”

【案例 2】使用 CO-STAR 框架对某创业项目进行评估。

【任务描述】

你正在参与一场创业项目评审会议,现在需要评估一个创业项目是否值得投资,并生成对应的评估结论。

【任务实施】

步骤一：根据 CO-STAR 框架编写以下提示词。

(1) context：你正在参与一场创业项目评审会议。项目资料如下。

项目名称：智链云—制造业供应链 AI 预测平台

阶段：天使轮

本轮融资额：800 万元人民币

核心产品：为中小型制造企业提供基于历史订单与外部数据的 AI 需求预测 SaaS,帮助降低库存成本。

关键数据：已签约付费客户 3 家(年费各 5 万元),正在 POC 客户 5 家;过去 3 个月 MRR (月经常性收入)为 2.5 万元,环比增长 20%;团队共 8 人(3 名算法,2 名销售,1 名产品,2 名运营)。

创始人：前中型软件公司销售总监,无 AI 技术背景。

CTO：应届博士生,研究方向为时间序列预测。

(2) objective：评估该项目是否值得进入下一轮尽职调查。

(3) style：你是一名极度保守的风控型投资人。

(4) task：请分析该项目的核心价值与主要风险。



CO-STAR
框架案例

(5) audience：投资决策委员会希望看到简洁、有数据支撑的判断。

(6) response：请按一句话结论、三个支持理由、三个关键风险、是否进入下一轮及原因的结构输出内容。

步骤二：结果生成。

大模型生成结果如图 2-3 所示。

一句话结论 该项目早期数据增长尚可，但团队结构性短板与产品验证不足导致风险远高于收益，不建议进入尽职调查。
三个支持理由 1. 市场需求真实：中小制造企业库存成本压力大，AI预测SaaS能直接降本，已获3家付费客户及5家POC，验证了初步痛点匹配。 2. 收入增速可观：过去3个月MRR从约1.7万元增长至2.5万元（环比+20%）。若维持该增速，年化ARR有望在12个月内突破50万元。 3. 细分切入点明确：聚焦制造业供应链预测，避开与通用ERP或大厂直接竞争，且利用外部数据（如天气、物流指数）有差异化潜力。
三个关键风险 1. 团队致命短板：创始人无AI技术背景，难以把控产品方向与客户信任；CTO为应届博士，缺乏工程化落地与产品商业化经验，时间序列预测模型在制造业实际噪声数据中极易失效。 2. 客户价值未量化：3家付费客户年费仅5万元（约4167元/月），客单价极低，且未披露实际降低库存成本的效果数据。POC转化率不明，当前MRR仅2.5万元，离规模化相距甚远。 3. 烧钱路径不清晰：天使轮要800万元，按团队8人（保守月运营成本25-30万）计算，仅够约24个月。但销售效率极低（2名销售3个月仅转化3家付费），获客成本预计远高于客户LTV，且无清晰市场扩张策略。
是否进入下一轮及原因 否，不建议进入尽调。 核心原因：团队能力与赛道要求严重错配（无AI背景的销售型创始人+无工业经验的算法博士），导致产品可靠性与商业化落地存在双高不确定性。当前数据仅证明“能签几张小单”，未证明“可规模化复制”。在天使轮估值不明的情况下，800万元融资额偏高，且后续存活概率低于20%。建议观察6-12个月，待团队补齐核心工程负责人或验证至少一个高价值标杆客户的实际ROI后再评估。

图2-3 大模型生成结果（2）

2. BROKE 框架：目标导向型

如果 CO-STAR 偏向通用任务理解，那么 BROKE 框架则更适合目标导向、需要量化结果的任务，比如项目管理、数据分析、标准化报告生成等。BROKE 框架各模块含义如表 2-2 所示。和 CO-STAR 相比，BROKE 更强调可量化和可衡量。它要求你把目标写成“销售额提升 10%”而不是“提升销售额”，把成功标准写成“找出 TOP3 问题环节”而不是“找出问题”。

表 2-2 BROKE 框架各模块含义

字 母	含 义	解 释
B (background)	背景与约束条件	任务所处的环境和限制
R (role)	角色定位	AI 该扮演什么职能
O (objective)	可量化的核心目标	要达成什么具体指标
K (key Results)	关键结果	判断任务是否完成了
E (execution)	执行要求	具体怎么操作