

西安交通大学桂小林教授主编

# 《人工智能基础与大模型应用》

**习题及其参考答案**

仅供参考

清华大学出版社

2026年7月

面向职业本科、职业专科

## 项目一：初识人工智能选择题

### 一、选择题

- 1、短视频 APP 的智能推荐系统主要核心问题是（ ）
  - A. 如何让视频播放更流畅
  - B. 推荐系统背后的智能逻辑是什么
  - C. 怎样增加视频的存储量
  - D. 如何设计更美观的界面
- 2、以下不属于人工智能核心分支演进内容的是（ ）
  - A. 从弱 AI 到强 AI
  - B. 从简单算法到复杂算法
  - C. 从专用 AI 到通用 AI
  - D. 从低智能到高智能
- 3、大模型被形容为人工智能时代的（ ）
  - A. “超级工具”
  - B. “超级大脑”雏形
  - C. “强大助手”
  - D. “智能核心”
- 4、以下哪个不是常见大模型（ ）
  - A. GPT
  - B. LLaMA
  - C. AlphaStar
  - D. 文心一言
- 5、在初识大模型的实践引导中，任务 1 是（ ）
  - A. 使用大模型生成个性化推荐语
  - B. 对比不同大模型的回答特点
  - C. 对大模型进行训练优化
  - D. 评估大模型的性能指标
- 6、人工智能的发展历程主要围绕（ ）展开。
  - A. 计算机性能提升
  - B. 算法不断改进与数据积累
  - C. 网络速度加快
  - D. 硬件设备更新
- 7、弱 AI 和强 AI 的主要区别在于（ ）
  - A. 弱 AI 只能处理特定任务，强 AI 具有通用智能
  - B. 弱 AI 运行速度慢，强 AI 运行速度快
  - C. 弱 AI 体积大，强 AI 体积小
  - D. 弱 AI 价格高，强 AI 价格低
- 8、短视频 APP 智能推荐系统“猜你喜欢”主要依据（ ）
  - A. 视频发布者的知名度
  - B. 用户的历史浏览行为等数据
  - C. 视频的拍摄地点
  - D. 视频的时长

- 9、以下关于大模型推动 AI 技术普及的说法，错误的是（ ）
- A. 降低了 AI 技术使用门槛
  - B. 提高了 AI 开发成本
  - C. 让更多人能接触和应用 AI
  - D. 促进了 AI 在各行业的落地
- 10、在体验主流大模型基础功能的实践中，对比不同大模型回答特点的目的在于（ ）
- A. 找出最贵的大模型
  - B. 了解各模型优势与不足
  - C. 淘汰回答不好的大模型
  - D. 确定哪个大模型最受欢迎

## 二、问答题

### 1、简述短视频 APP 的智能推荐系统是如何实现“猜你喜欢”的，其背后的智能逻辑是什么？

参考答案：短视频 APP 的智能推荐系统通过收集用户的历史浏览行为、点赞、评论、分享等数据，利用算法分析用户的兴趣偏好，然后根据这些分析结果为用户推荐可能感兴趣的视频，实现“猜你喜欢”。其背后的智能逻辑是基于大数据分析和机器学习算法，对用户行为数据进行挖掘和分析，建立用户兴趣模型，再根据模型进行个性化推荐。

### 2、人工智能有哪些核心分支，从弱 AI 到强 AI 的演进有什么重要意义？

参考答案：人工智能的核心分支包含从弱 AI 到强 AI 的演进等（也可提及专用 AI 到通用 AI 等相关内容）。从弱 AI 到强 AI 的演进意义重大，弱 AI 只能处理特定领域或任务，而强 AI 具有通用智能，能像人类一样理解和处理各种复杂问题，这种演进将极大地拓展人工智能的应用范围和深度，推动人工智能在更多领域发挥重要作用，甚至可能引发科技和社会的重大变革。

### 3、大模型为什么被称为人工智能时代的“超级大脑”雏形，它是如何推动 AI 技术普及的？

参考答案：大模型具有强大的语言理解、生成和推理能力，能够处理多种复杂任务，类似于人类大脑的综合处理功能，所以被称为“超级大脑”雏形。它推动 AI 技术普及的方式有：降低了 AI 技术的使用门槛，开发者无需从零开始构建模型，可直接基于大模型进行开发；提供了丰富的功能和应用场景，让更多人能接触和应用 AI；促进了 AI 在各行业的快速落地，提高了生产效率和创新能力。

### 4、请列举三种常见大模型，并简要介绍它们的特点。

参考答案：常见大模型有 GPT、LLaMA、文心一言等。GPT 以强大的语言生成能力著称，能够生成高质量、连贯的文本，在自然语言处理任务中表现优异；LLaMA 具有开源的特点，方便研究人员和开发者进行二次开发和研究，推动了 AI 技术的共享和进步；文心一言在中文理解和生成方面具有优势，能更好地处理中文语境下的各种任务，符合国内用户的使用需求。

### 5、在初识大模型的实践引导中，使用大模型生成个性化推荐语和对比不同大模型回答特点这两个任务分别有什么作用？

参考答案：使用大模型生成个性化推荐语的作用是让使用者亲身体验大模型在个性化推荐方面的能力，了解大模型如何根据输入信息生成符合特定需求的推荐内容，增强对大模型实际应用的认识。对比不同大模型回答特点的作用是帮助使用者了解不同大模型的优势和不足，以便在实际应用中根据具体需求选择合适的大模型，同时也促进对大模型技术差异和发展方向的理解。

## 项目二：理解机器学习

### 一、选择题

- 1、手机拍照场景分类功能中，机器“看懂”图像内容这一核心问题主要涉及以下哪项技术领域（ ）
  - A. 自然语言处理
  - B. 计算机视觉
  - C. 语音识别
  - D. 知识图谱
- 2、机器学习的定义是（ ）
  - A. 让机器自动编写代码
  - B. 让机器从数据中学习规律
  - C. 让机器制造工具
  - D. 让机器进行艺术创作
- 3、以下属于监督学习特点的是（ ）
  - A. 训练数据没有标签
  - B. 根据输入和输出数据学习映射关系
  - C. 主要用于发现数据中的潜在结构
  - D. 不需要预先定义好的输出
- 4、决策树属于哪种类型的学习算法（ ）
  - A. 监督学习算法
  - B. 无监督学习算法
  - C. 强化学习算法
  - D. 半监督学习算法
- 5、神经网络的基本结构单元是（ ）
  - A. 细胞
  - B. 神经元
  - C. 节点
  - D. 原子
- 6、激活函数在神经网络中的作用是（ ）
  - A. 增加网络的深度
  - B. 提高网络的计算速度
  - C. 引入非线性因素，使网络能够学习复杂模式
  - D. 减少网络的参数数量
- 7、以下不属于数据预处理基本方法的是（ ）
  - A. 清洗
  - B. 归一化
  - C. 分类
  - D. 标注
- 8、深度学习与传统机器学习的主要区别在于（ ）
  - A. 深度学习使用更简单的算法
  - B. 深度学习依赖人工特征工程更多

C. 深度学习能够自动学习数据的层次化特征

D. 深度学习只能处理小规模数据

9、在简单图像分类小实验中，任务 1 是（ ）

A. 运行基础图像分类模型并观察结果

B. 使用开源工具处理图像数据集

C. 对图像进行手动标注

D. 优化图像分类模型的参数

10、支持向量机算法主要用于（ ）

A. 数据降维

B. 图像生成

C. 分类和回归问题

D. 自然语言生成

## 二、问答题

1、简述手机拍照场景分类功能是如何实现的，其中机器“看懂”图像内容的关键是什么？

参考答案：手机拍照场景分类功能通过在拍照时利用计算机视觉技术，对拍摄的图像进行分析处理。首先收集图像数据，然后使用相关的算法模型对图像中的特征进行提取和识别，根据这些特征判断图像属于“人像”“夜景”“美食”等哪种模式。机器“看懂”图像内容的关键在于计算机视觉技术，它能让机器像人类一样对图像进行理解和分析，涉及到图像特征提取、模式识别等多个环节。

2、分别解释监督学习和无监督学习，并各举一个实际应用场景。

答案：监督学习是训练数据有标签，根据输入和输出数据学习映射关系的一种学习方式。例如，图像分类任务，给定大量带有类别标签（如猫、狗等）的图像作为训练数据，让模型学习图像特征与类别之间的对应关系，从而对新的图像进行分类。无监督学习是训练数据没有标签，主要用于发现数据中的潜在结构。例如，客户细分，电商企业拥有大量客户的购买行为数据，但没有对这些客户进行分类的标签，通过无监督学习算法可以挖掘出不同客户群体的特征和行为模式，将客户划分为不同的细分群体。

3、阐述神经网络中激活函数和反向传播的作用。

答案：激活函数的作用是引入非线性因素，使神经网络能够学习复杂模式。如果没有激活函数，神经网络无论有多少层，都只是对输入进行线性变换，无法处理复杂的非线性问题。激活函数可以让神经元对输入进行非线性映射，增强网络的表达能力。反向传播是一种神经网络的学习机制，它的作用是根据输出结果与真实标签之间的误差，从输出层向输入层逐层调整神经元之间的连接权重。通过计算误差对各层权重的梯度，利用梯度下降等方法更新权重，使得网络的输出逐渐接近真实标签，从而实现神经网络的学习和优化。

4、数据预处理包含哪些基本方法，它们分别有什么作用？

答案：数据预处理包含清洗、归一化和标注等基本方法。数据清洗的作用是去除数据中的噪声、错误值和重复值，提高数据的质量和准确性，确保后续分析和建模的可靠性。归一化是将数据按照一定的比例进行缩放，使其落在特定的范围内，例如 $[0, 1]$ 或 $[-1, 1]$ 。归一化可以消除不同特征之间的量纲差异，避免某些特征因为数值范围过大而对模型产生过大的影响，加快模型的收敛速度。数据标注是为无标签的数据添加相应的标签，对于监督学习任务，标注后的数据可以作为训练数据，让

模型学习输入数据与输出标签之间的映射关系，是模型训练的重要基础。

### 5、结合简单图像分类小实验，说明实践对于理解人工智能基础技术的重要性。

答案：在简单图像分类小实验中，通过任务 1 使用开源工具处理图像数据集，可以亲身体会数据预处理的过程，了解数据清洗、归一化、标注等操作在实际中的应用，明白数据质量对模型训练的重要性。任务 2 运行基础图像分类模型并观察结果，能够直观地看到模型如何对图像进行分类，理解机器学习和深度学习算法在实际任务中的工作原理和效果。通过实践，将理论知识与实际操作相结合，能够更深入地理解人工智能基础技术中机器学习、深度学习、数据处理等概念和方法，发现理论学习中可能忽略的问题，如不同算法在不同数据集上的表现差异、模型调参对结果的影响等，从而加深对人工智能基础技术的理解和掌握，提高解决实际问题的能力。

## 项目三：探究深度学习

### 一、选择题

1、智能写作助手快速生成专业报告，其核心问题是（ ）

- A. 如何快速输入需求
- B. 大模型为何能理解复杂指令并生成内容
- C. 怎样设计报告的排版
- D. 如何选择报告的主题

2、Transformer 的整体结构包含（ ）

- A. 输入层与输出层
- B. 编码器与解码器
- C. 卷积层与池化层
- D. 全连接层与激活层

3、自注意力机制在大模型中的作用是（ ）

- A. 加快模型的训练速度
- B. 增加模型的参数数量
- C. 让大模型“理解”文本
- D. 减少模型的计算量

4、多头注意力机制的主要作用是（ ）

- A. 降低模型的复杂度
- B. 使模型能够关注不同位置的不同信息
- C. 提高模型的训练效率
- D. 减少模型的内存占用

5、位置编码在 Transformer 中的作用是（ ）

- A. 标识文本中每个词的位置信息
- B. 对文本进行分类
- C. 增加文本的语义信息
- D. 对文本进行降噪处理

6、大模型的预训练阶段主要是（ ）

- A. 针对特定任务优化模型能力

- B. 在海量数据中学习通用知识
  - C. 对模型进行评估和测试
  - D. 调整模型的结构和参数
- 7、微调阶段的主要目的是（ ）
- A. 让模型学习更多的通用知识
  - B. 针对特定任务优化模型能力
  - C. 增加模型的训练数据量
  - D. 提高模型的预训练效率
- 8、提示工程的主要作用是（ ）
- A. 增加大模型的参数数量
  - B. 让大模型“听话”，提升生成内容质量
  - C. 减少大模型的训练时间
  - D. 改变大模型的核心架构
- 9、大模型的优势不包括以下哪一项（ ）
- A. 上下文理解能力强
  - B. 具备多任务处理能力
  - C. 不会出现幻觉现象
  - D. 能处理复杂的文本指令
- 10、在基于大模型 API 的文本生成任务中，任务 1 是（ ）
- A. 通过提示词优化提升生成内容质量
  - B. 调用大模型 API 生成定制化报告
  - C. 对生成的报告进行评估
  - D. 修改大模型的内部参数

## 二、问答题

1、简述智能写作助手输入需求后生成结构化报告的过程，并说明大模型能实现这一过程的关键因素。

参考答案：用户输入需求后，智能写作助手将需求转化为大模型能够理解的指令形式，大模型接收指令后，根据其内部存储的知识和训练得到的模式，对需求进行分析和理解，然后按照结构化报告的格式要求，生成相应的内容，包括标题、段落、图表等元素，最终输出完整的结构化报告。大模型能实现这一过程的关键在于其强大的语言理解和生成能力。这得益于大模型在海量数据上的预训练，使其学习到了丰富的语言知识和模式，能够理解复杂的指令和语义。同时，大模型的核心架构，如 Transformer 中的自注意力机制等，使其能够捕捉文本中的长距离依赖关系和上下文信息，从而生成符合要求的结构化报告。

2、详细解释 Transformer 中自注意力机制的工作原理，以及它为什么是大模型“理解”文本的关键。

参考答案：自注意力机制通过计算输入序列中每个元素与其他所有元素之间的相关性得分，来确定每个元素在处理过程中的重要程度。具体来说，对于输入序列中的每个元素，会生成三个向量：查询向量 (Query)、键向量 (Key) 和值向量 (Value)。然后计算查询向量与所有键向量的点积，并通过 softmax 函数将其转换为概率分布，这个概率分布表示了每个元素相对于当前元素的重要性。最后，根据这个概率分布对所有值向量进行加权求和，得到当前元素的注意力表示。

自注意力机制能够让模型在处理文本时，动态地关注输入序列中不同位置的信息，捕捉到文本中的长距离依赖关系和上下文信息。例如，在理解一个句子时，模型可以根据上下文准确地理解每个词的含义和作用，从而更好地理解整个文本的语义，所以它是大模型“理解”文本的关键。

### 3、阐述大模型预训练阶段和微调阶段的主要区别和各自的作用。

参考答案：训练数据：预训练阶段使用海量无标注的通用数据，如网页文本、书籍等，目的是让模型学习到广泛的语言知识和模式；微调阶段则使用特定任务的有标注数据，如针对智能写作助手的报告生成任务，会使用大量带有标注的报告数据。

训练目标：预训练阶段的训练目标是让模型学习到通用的语言表示，能够在各种语言任务中都有较好的基础表现；微调阶段的训练目标是针对特定任务优化模型的能力，使模型在该任务上达到更好的性能。

作用：预训练阶段为大模型提供了一个广泛的知识基础，使模型具备基本的语言理解和生成能力；微调阶段则是在预训练的基础上，让模型更好地适应特定任务的需求，提高模型在具体任务上的准确性和效果。

### 4、分析大模型面临的挑战，如幻觉、算力消耗与更新成本分别会对大模型的应用产生哪些影响。

参考答案：幻觉：大模型产生的幻觉现象，即生成的内容与事实不符或存在逻辑错误，会影响生成内容的可信度和可用性。在一些对准确性要求较高的应用场景，如医疗报告生成、金融分析等，幻觉现象可能会导致严重的后果，降低用户对大模型的信任度。

算力消耗：大模型的训练和推理需要大量的算力支持，这增加了使用大模型的成本。对于一些资源有限的企业或机构来说，可能无法承担高昂的算力费用，从而限制了大模型的广泛应用。同时，高算力消耗也会带来能源消耗和环境污染等问题。

更新成本：随着数据的不断更新和任务需求的变化，大模型需要定期进行更新和优化。然而，大模型的更新成本较高，包括数据收集、模型重新训练、评估和部署等方面的成本。频繁的更新可能会导致成本过高，使得一些应用难以持续进行模型的更新和改进。

### 5、结合基于大模型 API 的文本生成任务，说明如何通过提示工程提升生成内容的质量。

参考答案：在调用大模型 API 时，提供明确、具体的提示词，清楚地表达生成内容的要求和目标。例如，在生成定制化报告时，明确报告的主题、结构、内容要点等，让大模型能够准确理解需求。提供示例：给大模型提供一些与期望生成内容相似的示例，帮助大模型更好地理解生成的风格和格式。例如，提供一份优秀的报告示例，让大模型参考其语言风格、段落结构等。

如果生成的内容较为复杂，可以采用逐步引导的方式，先让大模型生成部分内容，然后根据生成的结果逐步调整提示词，引导大模型生成更完整、更符合要求的內容。

不同的提示词顺序和表述方式可能会影响大模型的生成结果。可以尝试调整提示词的顺序，或者使用不同的同义词、句式来表达相同的意思，观察生成内容的变化，选择最优的提示词组合。

## 项目四：实践大模型生成内容

### 一、选择题

1、企业客服机器人快速响应客户咨询的核心问题是（ ）

A. 如何设计机器人的外观

- B. 如何将大模型能力集成到实际业务系统
  - C. 怎样增加客服机器人的功能按钮
  - D. 如何选择客服机器人的语音
- 2、大模型 API 接口基础中，需要解析的关键要素是（ ）
- A. 请求参数与返回格式
  - B. 接口的版本号
  - C. 接口的调用次数
  - D. 接口的开发者文档
- 3、在大模型 API 调用中，认证与权限管理的主要作用是（ ）
- A. 提高 API 调用的速度
  - B. 确保 API 调用安全
  - C. 增加 API 调用的功能
  - D. 减少 API 调用的错误
- 4、以下属于常见大模型 API 调用工具的是（ ）
- A. Photoshop
  - B. Postman、Python 请求库**
  - C. Excel
  - D. Word
- 5、提示词工程中，指令设计需要遵循的原则不包括（ ）
- A. 清晰性
  - B. 具体性
  - C. 约束性
  - D. 模糊性
- 6、少样本提示与思维链提示的主要作用是（ ）
- A. 降低大模型的复杂度
  - B. 提升复杂任务的效果
  - C. 减少大模型的训练时间
  - D. 增加大模型的参数数量
- 7、检索增强生成（RAG）技术原理的核心是（ ）
- A. 让大模型直接生成内容
  - B. 结合大模型与外部数据库，提供更准确的回答
  - C. 增加大模型的训练数据量
  - D. 提高大模型的推理速度
- 8、本地知识库构建与更新的关键方法是（ ）
- A. 随机添加知识
  - B. 依赖大模型自动生成知识
  - C. 定期收集业务相关数据并整理入库
  - D. 手动输入所有知识
- 9、在开发简单智能问答机器人的实践中，任务 1 是（ ）
- A. 调用大模型 API 实现问答功能开发
  - B. 设计 FAQ 知识库与问答逻辑
  - C. 对机器人进行测试和优化
  - D. 选择大模型的类型
- 10、提示词模板设计与复用的主要优势是（ ）

- A. 降低提示词设计的难度
- B. 增加大模型的计算量
- C. 减少大模型的使用场景
- D. 提高大模型的训练成本

## 二、问答题

### 1、简述企业客服机器人客户咨询问题后精准回复的过程，并说明将大模型能力集成到实际业务系统的关键步骤。

参考答案：当客户向企业客服机器人咨询问题时，机器人首先接收客户的咨询内容，然后将内容转化为大模型能够理解的指令形式。大模型根据其内部的知识库和训练得到的模式，对咨询进行分析和理解，结合预设的业务逻辑和知识库，生成精准的回复内容，最后将回复内容返回给客户。

将大模型能力集成到实际业务系统的关键步骤包括：明确业务需求，确定需要大模型解决的具体问题；选择合适的大模型 API 接口，并进行认证与权限配置；设计提示词模板，将业务需求转化为大模型可理解的指令；结合业务数据库或知识库，通过 RAG 等技术增强大模型的回复准确性；进行系统集成和测试，确保大模型与业务系统的稳定交互。

### 2、详细解释大模型 API 接口的请求参数与返回格式分别包含哪些内容，以及认证与权限管理在 API 调用中的重要性。

参考答案：大模型 API 接口的请求参数通常包括模型名称（指定使用的大模型类型）、输入文本（需要大模型处理的内容）、温度（控制生成内容的随机性，温度越低越确定，越高越多样）、最大长度（限制生成内容的长度）等。

返回格式一般为 JSON，包含生成内容（大模型根据请求参数生成的结果）、状态码（表示 API 调用是否成功，如 200 表示成功）、错误信息（若调用失败，返回错误原因）等。

认证与权限管理在 API 调用中非常重要，它可以确保只有授权的用户或系统能够调用 API，防止未经授权的访问和恶意调用，保护大模型的安全和稳定性，避免数据泄露和资源滥用。

### 3、阐述提示词工程中少样本提示与思维链提示的工作原理，以及它们如何提升复杂任务的效果。

参考答案：

- 少样本提示：在提示词中提供少量与目标任务相关的示例，帮助大模型理解任务的要求和模式。例如，在文本分类任务中，提供几个已分类的文本示例，让大模型学习分类的标准。
- 思维链提示：要求大模型在生成最终答案前，先输出解决问题的思考过程，即“思考-回答”的链条。通过展示思维过程，帮助大模型更清晰地分析问题，提高复杂任务的推理能力。
- 提升效果：少样本提示通过示例引导大模型快速掌握任务模式，减少对大量训练数据的依赖；思维链提示则通过分解问题步骤，增强大模型的逻辑推理能力，从而提升复杂任务（如数学问题、逻辑判断）的处理效果。

### 4、分析检索增强生成（RAG）技术如何结合大模型与数据库，解决大模型应用中的哪些问题。

参考答案：

RAG 技术通过将大模型与外部数据库结合，当需要生成回答时，先从外部数据库中检索与问题相关的信息，然后将检索到的信息作为上下文输入大模型，大模型根据这些信息生成更准确、具体的回答。RAG 解决了大模型因训练数据滞后或知识范围有限导致的“幻觉”问题（生成与事实不符的内容），以及无法实时获取最新信息的问题。通过结合外部数据库，大模型能够利用最新的数据进行

回答，提高内容的准确性和时效性。

### 5、结合开发简单智能问答机器人的实践任务，说明设计 FAQ 知识库与调用大模型 API 实现问答功能开发的具体步骤。

参考答案：

- **设计 FAQ 知识库与问答逻辑**：首先收集企业常见的客户咨询问题 (FAQ)，整理问题与对应的标准答案，构建 FAQ 知识库。然后设计问答逻辑，确定当客户咨询的问题在 FAQ 知识库中时，直接返回标准答案；若不在知识库中，则调用大模型 API 进行生成回答。
- **调用大模型 API 实现问答功能开发**：选择合适的大模型 API 接口，配置认证与权限信息。根据设计的提示词模板，将客户的问题转化为 API 请求参数，调用大模型 API。接收 API 返回的生成内容，结合 FAQ 知识库的回答逻辑，将最终结果返回给客户。同时，对生成的内容进行校验和优化，确保回答的准确性和质量。

## 项目五：调用大模型进行应用开发

### 一、选择题

- 1、个人助手智能体管理日程与查询信息的核心问题是（ ）  
A. 如何设计智能体的外观  
B. 智能体如何实现多任务协同与自主决策  
C. 怎样增加智能体的功能按钮  
D. 如何选择智能体的语音
- 2、智能体的基本架构中，负责接收与解析用户输入的模块是（ ）  
A. 感知模块  
B. 决策模块  
C. 执行模块  
D. 存储模块
- 3、智能体的决策模块中，起核心作用的是（ ）  
A. 大模型作为智能体的“大脑”  
B. 传统的规则引擎  
C. 简单的条件判断逻辑  
D. 人工预设的决策树
- 4、工具调用能力中，让大模型“知道”可用工具的关键步骤是（ ）  
A. 工具注册与描述  
B. 函数调用格式规范  
C. 选择常见工具类型  
D. 测试工具的兼容性
- 5、函数调用格式的主要作用是（ ）  
A. 规范大模型的工具调用指令  
B. 增加工具调用的灵活性  
C. 减少工具调用的错误  
D. 提高工具调用的速度

- 6、以下属于智能体常见工具类型的是（ ）
- A. 绘画工具、音乐工具
  - B. 搜索工具、计算工具、API 工具
  - C. 办公工具、游戏工具
  - D. 社交工具、教育工具
- 7、多步骤任务分解方法的核心是（ ）
- A. 将复杂任务拆分为多个简单子任务
  - B. 直接一次性完成所有任务
  - C. 依赖大模型自动分解任务
  - D. 人工预设任务分解步骤
- 8、智能体的记忆机制中，短期记忆主要用于（ ）
- A. 存储长期的历史数据
  - B. 记录当前任务的上下文信息
  - C. 保存用户的个人信息
  - D. 存储大模型的知识库
- 9、在开发基础个人助手智能体的实践中，任务 1 是（ ）
- A. 优化智能体的任务规划逻辑
  - B. 实现日程提醒与天气查询功能集成
  - C. 对智能体进行测试和优化
  - D. 选择智能体的开发框架
- 10、智能体的任务规划与记忆机制设计中，长期记忆的主要作用是（ ）
- A. 存储当前任务的临时数据
  - B. 记录用户的日常习惯和偏好
  - C. 保存大模型的训练数据
  - D. 存储工具调用的历史记录

## 二、问答题

- 1、简述个人助手智能体用户指令后完成日程规划与信息整合的过程，并说明智能体实现多任务协同与自主决策的关键。

参考答案：

过程：当用户向个人助手智能体发出指令（如“规划明天的日程并查询天气”）后，智能体首先通过感知模块接收并解析指令，识别用户需求。然后，决策模块（以大模型为核心）分析需求，将任务分解为日程规划和天气查询两个子任务，并调用相应的工具（如日程管理工具、天气查询 API）执行。执行模块获取工具返回的信息后，整合结果，最终将规划好的日程和天气信息反馈给用户。

关键：智能体实现多任务协同与自主决策的关键在于其基本架构（感知-决策-执行）的协同工作，以及大模型在决策模块中的核心作用。大模型能够理解复杂指令，分解任务，并调用合适工具，同时通过记忆机制保留上下文信息，实现多任务的连贯处理和自主决策。

- 2、详细解释智能体基本架构中感知模块、决策模块、执行模块各自的作用及相互关系。

参考答案：

- 感知模块：负责接收用户输入（如语音、文本），并将其解析为智能体可理解的格式，是智能体与用户交互的入口。

- 决策模块：以大模型为核心，根据感知模块解析的信息，分析用户需求，制定决策（如任务分解、工具调用），是智能体的“大脑”。
- 执行模块：根据决策模块的指令，调用外部工具（如 API、计算工具）执行具体操作，并将结果返回给用户。
- 相互关系：感知模块为决策模块提供输入，决策模块指导执行模块操作，执行模块的反馈又可能影响感知模块的后续解析，三者协同完成智能体的功能。

### 3、阐述智能体工具调用能力中工具注册与描述、函数调用格式的具体内容，以及它们如何确保工具调用的有效性。

参考答案：

- 工具注册与描述：将可用工具的信息（如工具名称、功能、输入输出参数）注册到智能体中，并给出详细描述。这样大模型在决策时能“知道”有哪些工具可用及其用途，确保调用的工具符合任务需求。
- 函数调用格式：规范大模型调用工具时的指令格式（如指定工具名称、API ID、请求参数等）。通过统一格式，避免大模型生成不符合工具要求的指令，确保工具能正确执行，提高调用的准确性和可靠性。

### 4、分析智能体任务规划与记忆机制中多步骤任务分解方法和短期记忆、长期记忆设计的作用。

参考答案：

- 多步骤任务分解：将复杂任务拆分为多个简单子任务，降低处理难度。例如，规划日程并查询天气可拆分为“获取用户日程安排”“查询天气数据”“整合信息并生成日程”等步骤，使智能体能逐步完成，提高任务成功率。
- 短期记忆：记录当前任务的上下文信息（如用户之前的指令、已完成的步骤），确保任务处理的连贯性。例如，用户在规划日程时提到“明天下午 3 点开会”，短期记忆会保留这一信息，避免重复询问。
- 长期记忆：存储用户的日常习惯和偏好（如常用的日程时间、关注的天气城市），为智能体提供个性化决策依据。例如，长期记忆记录用户通常早上 8 点安排日程，智能体在规划时会优先这一时间段。

### 5、结合开发基础个人助手智能体的实践任务，说明实现日程提醒与天气查询功能集成的具体步骤，以及优化任务规划逻辑的方法。

参考答案：

- 实现功能集成：
  - 步骤 1：设计日程提醒功能，调用日程管理工具（如 Calendar API），注册工具并描述其功能（添加日程、查询日程）。
  - 步骤 2：设计天气查询功能，调用天气查询 API，注册工具并描述参数（城市、日期）。
  - 步骤 3：在感知模块解析用户指令（如“明天北京的日程提醒和天气”），决策模块调用对应工具，执行模块获取日程和天气数据并整合，反馈给用户。
- 优化任务规划逻辑：
  - 方法 1：引入多步骤任务分解，将复杂指令拆分为子任务（如先查询天气再规划日程），确保每一步都清晰。
  - 方法 2：利用短期记忆保留任务上下文，避免重复询问用户信息。
  - 方法 3：结合长期记忆的用户偏好，自动调整任务规划（如根据用户习惯优先安排重要日程）。

## 项目六：具身智能体与机器人

### 一、选择题

1. 大模型生成的虚假新闻在传播链条中，利用平台算法漏洞的主要目的是？

- A. 降低生成成本
- B. 实现精准触达目标用户
- C. 提升文本逼真度
- D. 规避内容审核

2. 以下哪项不属于大模型偏见的典型表现形式？

- A. 描述科学家时默认使用“他”
- B. 关联少数族裔与负面特征
- C. 生成内容时优先推荐高学历职业
- D. 根据用户需求生成多样化家庭分工场景

3. 对抗性攻击中，“多步诱导攻击”的核心策略是？

- A. 在输入中添加特殊符号干扰检测
- B. 通过逐步关联引导模型输出敏感信息
- C. 复制模型结构生成模仿模型
- D. 用噪声数据降低模型准确率

4. 欧盟《人工智能法案》将大模型多数列为“高风险”，要求企业必须完成？

- A. 开源模型代码
- B. 第三方合规评估
- C. 免费向公众开放 API
- D. 每季度发布用户数据报告

5. 以下哪种技术不属于数据静态脱敏方法？

- A. 用“用户 A”替换真实姓名
- B. 将“28 岁”泛化为“20-30 岁”
- C. 对数据添加差分隐私噪声
- D. 用生成式模型创建虚拟病例

6. 中国《生成式人工智能服务管理暂行办法》要求，生成内容需明确标注的是？

- A. 模型训练数据来源
- B. 企业营业执照编号
- C. “AI 生成”标识
- D. 开发者姓名

7. 大模型训练数据中的“历史偏见”主要来源于？

- A. 算法过度优化导致的误差

B. 社会固有偏见在数据中的体现

C. 开发者的主观恶意设置

D. 模型参数随机初始化的偏差

8. 以下哪项属于企业在大模型应用中的核心责任？

A. 要求用户无条件授权数据使用权

B. 优先追求模型性能而非合规性

C. 建立内部合规团队跟踪政策动态

D. 仅在用户投诉后改进隐私保护措施

9. 在内容安全审核中，针对“隐性仇恨文本”的检测主要依赖于？

A. 关键词匹配

B. 上下文语义分析

C. 数据格式识别

D. 图像特征提取

10. 差分隐私技术在数据安全中的主要作用是？

A. 完全删除敏感数据

B. 使模型无法定位单个数据样本

C. 加密存储用户身份证号

D. 限制数据访问权限

## 二、问答题

1. 请简述大模型生成虚假新闻的检测过程中，技术检测与人工核验各自的核心作用。

参考答案：技术检测通过文本特征分析（如困惑度计算）、语义一致性校验（如比对知识图谱）、图像溯源等识别 AI 生成痕迹；人工核验负责跨领域专家验证（如农业数据真实性）、信源追溯（如确认“专家”身份），并处置技术漏检的复杂案例（如隐性煽动内容）。

2. 大模型的隐私泄露风险主要体现在哪些场景？请列举至少三类。

参考答案：包括训练数据的“记忆提取”（如复现患者病历）、“提示词攻击”（如诱导输出隐私信息）、生成内容的“隐私嵌入”（如用户输入的银行卡号被存储）、跨境数据流动的隐蔽性等。

3. 企业在设计大模型隐私保护方案时，如何平衡“合规性”与“用户体验”？

参考答案：合规性方面，需实现数据最小化采集、明确授权流程、建立删除机制；用户体验方面，可简化授权步骤（如两步操作）、用通俗语言解释隐私措施、避免过度弹窗干扰，例如医疗 AI 可告知用户“姓名会被替换为代号，不影响诊断准确性”。

4. 请分析大模型训练数据的版权争议焦点，并列举一个典型案例。

参考答案：争议焦点是“未经授权使用受版权保护的作品训练模型是否构成侵权”，核心在于“转换性使用”的边界。例如，美国作家协会起诉 OpenAI，指控其未经授权使用数千本小说训练 GPT 模型，认为该行为超出“合理使用”范围。

5. 简述中国《生成式人工智能服务管理暂行办法》对内容安全的核心要求。

参考答案：生成内容需符合法律法规，禁止虚假信息和危害国家安全的内容；服务提供者需对生成内容进行审核；训练数据需遵守《数据安全法》和《个人信息保护法》；提供服务前需向网信部门备案。

人工智能基础&大模型应用