

# 人工智能实验 团队大作业

## 迷你聊天机器人助手 Mini Chatbot Assistant

2025 年春季学期

### 1. 作业说明

**组队要求：**请以 2-4 人为一组完成本次大作业，全组共享得分，占期末总评的 20 分。请于 **2025 年 5 月 16 日（周五）晚 23:59 前** 每组组长通过以下共享文档确定小组成员名单(16 号之后不可修改分组)，助教将根据名单在线教学平台中协助完成分组操作。

- **S 人工智能实验大作业分组\_2025春**
  - 每个小组选一个组长，负责作业提交和课堂演示
  - 分组完成后，各组需通过在线文档填写各自设计的 Chatbot 任务场景。填写后仍可在作业过程中进行修改与完善。但**后填写的小组所选任务场景不得与已有小组的内容高度重复**。
    - 说明：任务场景的“高度重复”是指核心内容几乎完全相同。若为相同类别（如都是古诗词），但在词牌、风格、作者等方面有明显差异，仍视为不同任务场景。如果不确定是否重复请咨询老师或助教。

**提交时间：**请于 **2025 年 6 月 13 日（周五）晚 23:59 前** 向在线教学平台提交完整作业。逾期提交将根据以下规则扣分：每逾期一天（以自然日计算）总分扣除 20%。例如：周二晚 23:59 前提交，扣 20%；周三晚 23:59 前提交，扣 40%；以此类推。

**提交方式：**通过**在线教学平台的作业模块**提交一个压缩包，命名方式为：`组员1姓名_组员2姓名_组员3姓名_组员4姓名.zip`（如：`张三_李四_王五_赵六.zip`）。**压缩包内容应包括：**

- **代码文件夹** `minimind/`：
  - 微调后的 LoRA 模型，保存在 `minimind/out/` 文件夹中。
  - 修改后的 WebUI 界面代码 `scripts/web_demo.py`，或你们自行开发的 WebUI 实现
- **大作业报告：**命名为 `大作业报告.pdf`，格式请参考附件提供的 `大作业报告.docx`
- **数据集文件夹** `dataset/`：包含你们收集和處理后的 `.jsonl` 格式文本数据。在线教学平台单个文件上传大小上限为 **100MB**，如全部作业压缩包较大，请将数据集单独压缩并命名为：`组员1_组员2_组员3_组员4_数据集.zip`。
- **说明文件** `README.txt`：说明你们**修改或新增的文件及其作用**；给出**如何运行 WebUI 的示例代码说明**；如为自定义 WebUI，请提供运行环境与配置说明
- **运行演示视频** `运行示例.mp4`：包括自我认知问题和自测问题的实际运行录屏过程，视频大小不超过 10MB (如果文件太大，可用免费的视频软件如 VLC 等压缩)

**问题交流：**

⚠ 注意事项:

- 请严格遵守提交说明命名文档
- **严禁抄袭与作弊**：一经查实，**作弊者与被抄袭者均记 0 分**
- **内容不得违反社会主义核心价值观、公序良俗**，否则成绩记为 0 分

## 2. 实验任务

大语言模型（Large Language Models, LLMs）是当前人工智能领域最前沿的技术代表，典型案例包括 ChatGPT、DeepSeek 等。这些模型已在国民经济、社会服务和科学研究等多个领域展现出颠覆性影响与巨大的经济价值。

本次团队大作业的目标是通过对小型语言模型的微调，帮助同学深入理解大语言模型的**基本原理、训练流程及实际应用场景**，并提升团队协作能力与工程实现能力。作业将基于开源项目 **Minimind** 进行实践，GitHub 项目地址：<https://github.com/jingyaogong/minimind>



请同学们仔细阅读项目资料，重点理解模型训练流程。本次作业将围绕项目中参数规模为 26M 的最小模型 `MiniMind2-Small` 开展微调。任务将分为三个部分，详情如下：

### 2.1 数据收集和标注（需写入“大作业报告.pdf”，总分 6 分）

本部分任务旨在帮助你深入理解大语言模型在不同应用场景下的问答数据组织与表示方式。你需要**定义一个 Chatbot 的任务场景**，并**收集并构建符合该场景的数据集**，以供后续模型微调使用。

#### (1) 任务目标

- 明确 Chatbot 的应用场景与功能目标（例如：唐诗问答、地理知识助手、历史小百科、个性化人物模拟等）。
- 在互联网上查找、整理与该功能相关的问答内容。
- 将数据转化为 Minimind 所需格式，并进行简单清洗与标注。

#### (2) 数据格式要求（仿照项目中的格式）

请仿照项目中给出的两个数据集文件：

- [https://www.modelscope.cn/datasets/gongjy/minimind\\_dataset/resolve/master/lora\\_identity.jsonl](https://www.modelscope.cn/datasets/gongjy/minimind_dataset/resolve/master/lora_identity.jsonl)
- [https://www.modelscope.cn/datasets/gongjy/minimind\\_dataset/resolve/master/lora\\_medical.jsonl](https://www.modelscope.cn/datasets/gongjy/minimind_dataset/resolve/master/lora_medical.jsonl)

构建一组“对话样本”，使用如下 JSON 格式（每行一条对话，结构化字段）：

- 自我认知场景：

- 该功能为必须完成的部分，可通过修改 `lora_identity.jsonl` 数据实现。

JSON

```
1 {"conversations": [{"role": "user", "content": "你叫什么名字?"}, {"role": "assistant", "content": "我叫minimind，是一名语言模型助手。"}]}
2 {"conversations": [{"role": "user", "content": "你是谁创造的?"}, {"role": "assistant", "content": "我的创造者是张三、李四、王五和赵六。"}]}
```

- 医疗问答场景：

- 不得直接使用提供的 `lora_medical.jsonl` 文件

JSON

```
1 {"conversations": [{"role": "user", "content": "颈椎病患者枕头多高合适?"}, {"role": "assistant", "content": "通常建议高度为8-12厘米..."}]}
```

- 唐诗问答场景（示例）：

JSON

```
1 {"conversations": [{"role": "user", "content": "床前明月光,"}, {"role": "assistant", "content": "疑是地上霜。"}]}
```

### (3) 数据构建流程建议（供参考）

- **定义任务目标与场景（写入报告）。**简要说明你希望 Chatbot 实现什么功能？回答什么类型的问题？适用于哪些人群或情境？明确回答风格（简洁 / 科普 / 口语化 / 文艺化）
- **制定数据边界。**确定数据涉及的知识范围（如只聚焦唐诗、不涉及宋词；或限定医学常识、不涉及诊断建议等）

- **搜索与采集原始问答。**可参考：百度百科、知乎、维基百科、问答网站、教材资料、公众号文章等公开信息来源。建议使用手动摘录或简单爬虫（如 Python + requests）工具辅助
- **转换为指定格式（JSON Lines 文件）。**每一组对话用一行 JSON 表示，推荐使用 UTF-8 编码，保存在 `dataset/your_dataset.jsonl` 文件中
- **示例样本说明（写入报告）。**选择 2-3 组具有代表性的对话样本，解释它们的设计思路以及代表的知识点或风格。

### ⚠ 提示与注意事项

- **分好组后，各组将通过在线文档填写自己的 Chatbot 任务场景，作业过程中可随时修改，但后填写的小组不得与先填写的完全相同，即 Chatbot 的任务场景不能完全重复。**
- 请**避免直接复制已有 ChatGPT 生成内容**，更鼓励基于可靠资料进行整理
- 建议同一小组的同学**协同处理不同类别或子主题**，提高数据多样性
- 我们不要求数据完美或全面，主要目的是让你**理解数据构造对模型微调的影响**
- 请不要收集太大或者太小的数据集，10 ~ 30MB 左右为宜，最大不超过 30MB

### 🎯 任务方向提示：

- 特定人物模拟（如古代诗人、动漫角色、科学家）
- 学科类助手（如语文知识、地理答疑、编程知识问答）
- 情感陪伴 / 励志助手（回答鼓励性话语）
- 特定情境小助手（如旅行问答、考试辅导等）
- 等等

### 📊 评分标准（满分 6 分）：

- **数据集(3 分)：**提交符合格式要求、语义合理、主题明确的数据集文件
- **报告说明(3 分)：**说明数据收集与整理流程，阐述期望功能及知识边界，并配典型样例说明

## 2.2 迷你聊天助手模型训练（需写入“大作业报告.pdf”，总分 8 分）

本次作业的重点是通过运行 **Minimind** 项目中的 **LoRA (Low-Rank Adaptation)** 微调流程，训练出一个具备你所设计功能的迷你聊天助手模型。你**不需要**完全理解大语言模型从零开始训练的全过程，只用**完成基于现有模型的微调**操作，并能结合代码进行基础理解分析。对技术细节感兴趣的同学，可阅读参考资料部分有关 LoRA 以及大语言模型的介绍博文。以下是模型训练的基本步骤

### (1) 数据集准备

确保你已经按照要求准备好了 `.jsonl` 格式的数据集文件，并命名如 `lora_medical.jsonl`，保存至 `dataset/` 文件夹。

- 训练时，你需要合并**自我认知类数据**（如 `lora_identity.jsonl`）与**任务类数据**（如诗词、动漫等）
- 合并数据时请**控制采样比例**（例如 3:1），否则模型可能无法学到“自我认知”能力。

## (2) 运行训练脚本（以下命令供参考，请按实际路径与命名修改）

请参考项目说明：<https://github.com/jingyaogong/minimind?tab=readme-ov-file#5-lora-low-rank-adaptation>。使用如下的命令即可开始训练，请根据你的实际情况传入对应参数

Bash

```
1 # 在 trainer/ 子文件夹下
2 python train_lora.py \
3   --lora_name lora_medical \
4   --data_path ../dataset/lora_medical.jsonl \
5   --out_dir ../out \
6   --epochs 20 \
7   --use_wandb \
8   --wandb_project chatbot_project
```

### ⚠ 提示与注意事项

- **训练轮数**（`--epochs`）：一般推荐设为 10~30，轮数越多效果越好，但训练时间也会增加。
- **W&B (Weights & Biases)**：推荐开启 `--use_wandb`，用于记录训练曲线（如 loss 曲线），可在 [wandb.ai](https://wandb.ai) 注册账户查看项目。
- **本地 CPU 训练** 可能需 6-10 小时。
- **Google Colab 免费 GPU** 可显著加快速度（约 1 小时）
- 我们鼓励有条件的同学尝试训练更大的模型或开发更复杂的功能模块，例如模拟类似 DeepSeek Reason 模型中的推理能力、链式思维、多轮对话等高级功能。这类探索有助于你加深对大模型架构与能力边界的理解，也有望提升项目实际效果。但请注意，**为了保证评分的公平性与可比性，这部分探索将不计入最终成绩加分**，不作为评分依据。你可以在报告中展示你的进阶成果，作为附加展示内容。

### 评分标准（满分 8 分）：

- **结合代码理解大模型训练基础原理。** (2 分)

- 请结合代码说明 minimind tokenizer 是如何工作的，并将 2-3 句自然语言映射为 token 序列。相关代码片段需写入报告中。
- 请结合损失函数部分的代码 `trainer/train_lora.py` 并画图示意，模型是如何计算训练损失的。即损失函数中的 `res` 和 `Y` 分别是什么，和 `X` 有什么联系。

```
47         res = model(X)
48         loss = loss_fct(
49             res.logits.view(-1, res.logits.size(-1)),
50             Y.view(-1)|
51         ).view(Y.size())
```

- **如实记录训练过程，展示必要细节。** (2 分)
  - 训练说明，包括训练轮数、batch size、学习率、使用平台（如本地/Colab）、训练时长等等
  - 训练日志与图表展示 loss 曲线图
- **模型自我认知测试。** (1 分)
  - 你的 Chatbot 需要能够正确回答“你是谁？”“创造你的人是谁？”等问题。请在 demo 视频中展示结果，并且在课堂演示中展示，课堂展示失败的不得分。
- **报告完成度与逻辑清晰。** (3 分)
  - 材料组织完整。报告中包含所有必要内容，章节齐全，引用准确；内容涵盖数据说明、模型训练、结果展示等核心部分
  - 表达清晰、逻辑严谨。语言通顺，术语使用准确，内容结构合理，条理分明；无明显重复、遗漏或逻辑混乱
  - 报告排版规范、美观。合理使用标题、子标题，字体大小统一，请用合适的工具画图，图表插入清晰，代码段格式整洁，整体美观度高

## 2.3 课堂演示

现在是 **Show Time!** 各小组将现场展示自己的 Chatbot 运行效果。我们将在理论课或实验课上安排统一的展示环节。课堂展示之前，请将你的所有代码以及模型文件，上传至在线平台（大小应该小于 100M），我们将把所有作业下载到老师或者助教的电脑，在 **本地断网状态下** 运行演示，确保 Chatbot 完全依赖本地模型作答。



模型设定调整

Number of Historical Dialogues

0

0

6

Max Sequence Length

256

8192

Temperature

0.60

0.85

1.20

选择模型来源

☒ 本地模型

☐ API

Models

MiniMind2 (0.1B)

Hi, I'm MiniMind2

内容完全由AI生成，请务必仔细甄别

Content AI-generated, please discern with care

大语言模型的原理是什么？

大语言模型（Language Model）是一种用于自然语言处理任务的机器学习模型。它通过学习大量文本数据来学习语言的结构、语法和语义，从而能够生成或理解人类语言。大语言模型的原理主要包括以下几个方面：

1. 数据收集：大语言模型需要大量的文本数据来训练。这些数据可以是文本数据、文本数据、语音数据等。数据的质量和多样性对于模型的性能至关重要。

2. 数据预处理：大语言模型需要对文本数据进行预处理，包括分词、去除停用词、词干提取等，以便于后续的语言处理。

3. 模型选择与设计：选择合适的模型架构，如Transformer、BERT等，用于处理大规模的文本数据。模型的结构和参数需要与大语言模型的训练过程相协调。

4. 模型训练：使用收集到的数据进行模型训练。训练过程中，模型会学习到语言的规律和特征，如词汇的多义性、上下文信息等，从而能够生成或理解人类语言的解析结果。

给 MiniMind 发消息

演示内容分为两个部分：

## (1) 自测能力展示

- 每组需设计并现场展示 **6 个自测问题及模型回答**。
- 自测问题应涵盖你们所训练的功能场景（如古诗预测、人物对话等），展示模型的代表性能力。

## (2) 随机交叉测试

- 教师将随机抽取除目标组以外的其他 3 个小组，作为“提问小组”，对目标组的 Chatbot 进行测试提问。目标组需在现场展示其 Chatbot 模型对提问小组问题的实时回答效果。
- 提问小组职责：**
  - 从自测用例中选择一个问题作为参考，根据该用例设计一个新测试问题。
  - 新问题应与原问题相似，不能差异过大。例如通过以下方式进行变形或改写：
    - 替换问题中的某个关键词或短语（例如：将“猫喜欢吃鱼吗？”改为“猫喜欢吃骨头吗？”）
    - 变更语序或句式结构（例如：将“猫喜欢吃鱼吗？”改为“鱼是猫喜欢吃的吗？”）
    - 改变问法但保留语义一致（例如：“猫喜欢吃鱼，对吗？”）
    - 使用同义替换 / 近义表达（例如：将“猫喜欢吃鱼吗？”改为“猫爱吃鱼吗？”）

- 添加少许干扰信息，但不改变核心问题（例如：“今天下雨了，猫喜欢吃鱼吗？”）
- 等等
- 由除目标组以外的所有学生负责现场打分。

### ⚠ 提示与注意事项

- 请确保上传的代码能通过**一行命令运行**，避免课堂演示出问题
- 建议使用默认 Streamlit WebUI 进行演示（位于 `scripts/web_demo.py`）。欢迎有能力的同学对 UI 做适当美化或功能增强。
- 你需要参考 `eval_model.py` 文件，对 `scripts/web_demo.py` 进行适当修改，使得 WebUI 能够正常调用训练出来的 LoRA 模型。

### 📊 评分标准（满分 6 分）：

- 自测演示 3 分，每小题 0.5 分。交叉测试，3 分，每小题 1 分。
  - 回答准确 or 有逻辑 or 内容与功能相关，均可得分(给分宽容一些~)
  - 明显错误、偏离主题太远、无输出或崩溃，该题不得分

## 3. 参考资料

- [1] LoRA (Low-Rank Adaptation) 详解: <https://zhuanlan.zhihu.com/p/663557294>
- [2] 从零开始训练大模型: <https://zhuanlan.zhihu.com/p/636270877>
- [3] 吴恩达 LLM 微调大模型系列教程: <https://www.bilibili.com/video/BV1c4i9YQEX8>

## 4. 致谢

本次大作业基于江苏大学研究生 **Jingyao Gong** 同学开源的项目 **Minimind** 开展。在此对 Jingyao 同学的无私奉献和对开源社区的支持表示**诚挚的感谢**。该项目为本课程提供了宝贵的实践平台，也为同学们深入理解大语言模型提供了良好基础。