

张桂生 - Agent开发工程师

男 24岁 15666867006 15666867006@163.com

教育经历

沈阳工业大学	- 软件工程 全日制研究生	2023年09月 - 2026年06月
德州学院	- 网络工程 全日制本科	2019年09月 - 2023年06月

专业技能

- 大语言模型基础**: 熟悉 Transformer 架构原理, 掌握自注意力机制、位置编码 (Sinusoidal、RoPE)、MHA/MQA/GQA 等注意力变体, 了解 Encoder-Only、Decoder-Only、Encoder-Decoder 三种架构的适用场景及主流模型 (BERT、GPT、T5 等)
- LLM 训练与优化**: 熟悉 Scaling Laws 及 Chinchilla 定律对训练资源分配的指导意义, 掌握 BPE、WordPiece 等 Tokenization 算法, 熟悉 GeLU、SwiGLU 等激活函数, 了解 MoE 混合专家模型的稀疏激活原理
- LLM 推理与解码**: 掌握 Greedy Search、Beam Search、Top-K Sampling、Nucleus Sampling 等解码策略的原理与优劣, 熟悉 KV Cache 机制及其对推理效率的影响
- 大规模训练工程**: 熟悉数据并行、流水线并行、张量并行等 3D 并行策略, 了解 ZeRO 显存优化技术, 掌握 BF16 混合精度训练、梯度裁剪、学习率预热等训练稳定性方法, 了解 DeepSpeed、Megatron-LM 等主流训练框架
- RLHF 与模型对齐**: 熟悉 RLHF 三阶段流程 (SFT、奖励模型训练、PPO 强化学习), 掌握 Bradley-Terry 模型及成对偏好损失函数, 理解 KL 散度惩罚项的作用, 熟悉 DPO 等简化对齐方法及奖励作弊 (Reward Hacking) 的成因与缓解策略
- 视觉语言模型 (VLM)**: 熟悉 CLIP 对比学习原理及双编码器架构, 掌握 LLaVA 等基于连接器的 VLM 架构设计, 了解视觉指令微调 (Visual Instruction Tuning) 流程, 熟悉 VLM 幻觉 (物体、属性、关系幻觉) 的表现形式及高分辨率图像处理方案
- RAG 系统**: 熟悉 RAG 完整流水线 (文档切块、嵌入、向量检索、重排序、生成), 掌握混合搜索、HyDE、多查询检索等高级检索优化技术, 了解 RAGAS 等评估框架, 熟悉 LangChain、LlamaIndex、RAGFlow 等主流 RAG 框架的选型策略
- LLM Agent**: 熟悉 Agent 的核心组件 (规划、记忆、工具调用), 掌握 ReAct、CoT、Tree of Thoughts 等规划范式, 熟悉 Function Calling 工具调用机制, 了解多智能体系统设计及 A2A 协议, 具备 Agent 微调与数据集构建经验
- 模型评估**: 熟悉 MMLU、HumanEval、GSM8K 等主流 LLM 评测基准, 掌握 LLM-as-a-Judge 评估范式及其位置偏见、冗长偏见等局限性, 了解 WebArena、AgentBench 等 Agent 专项评测框架, 熟悉红队测试 (Red Teaming) 在安全漏洞与偏见发现中的应用
- 模型微调与部署**: 熟悉 SFT、LoRA 等参数高效微调方法, 掌握 VLM 两阶段微调流程, 了解 vLLM、TensorRT-LLM 等高效推理框架, 熟悉线上服务持续监控、A/B 测试及数据飞轮 (反馈闭环) 的工程实践

实习经历

中国科学院沈阳自动化研究所

2024年05月 - 至今

2025.09-2026.01

智能装备测试体系一体化平台

项目介绍: 为解决工业控制与通信系统在不同标准和网络环境下兼容性验证成本高、人工参与重的问题, 基于 Qwen2.5-VL 多模态大语言模型与 LangGraph 工作流编排框架, 构建了面向工业协议规范的测试用例自动生成与质量验证系统。系统以技术规范文档 PDF 为输入, 通过多轮 Reflection 循环 (生成→验证→修订) 产出高质量标准化测试用例, 提升测试效率、降低人工参与成本, 并保障测试结果的准确性与可追溯性。

核心技术与方法:

- 模态工具链设计**: 将PDF解析、VLM推理、数学符号验证封装为职责单一的独立工具函数, 通过单例模式管理 Qwen2.5-VL 模型实例, 避免重复加载 GPU 资源, 工具接口统一采用 Dict[str, Any] 返回格式, 具备可测试性与可替换性。
- LangGraph状态机工作流编排**: 基于 StateGraph 构建五节点 DAG 工作流, 使用 TypedDict 定义强类型 AgentState, 状态字段区分输入、中间结果、输出与控制变量, 通过 add_conditional_edges实现动态路由, add_edge构建固定顺序边, 循环边支持反思迭代。
- Reflection 自反思机制**: Verify 节点使用与 Generate 节点相同的 VLM, 以"Principal Engineer / Bar Raiser"角色对生成结果执行四维检查 (技术深度、答案准确性、第一人称视角、语言规范), 输出结构化 JSON; Revise 节点将 feedback 注入新一轮 Prompt, 实现针对性自修正, 最多循环 MAX_ITERATIONS=3 次防止死循环。
- 模型推理控制与决策逻辑**: 决策函数读取全局状态, 返回路由键; 每个问题独立维护 status与 feedback 字段, 粒度精细到单题级别, 支持部分通过后仅对未通过题目继续迭代。
- 容错与JSON健壮性处理**: Generate 与 Verify 节点均实现三层 JSON 解析容错: ① 剥离 Markdown 代码块; ② 正则去除控制字

符；③ 宽松模式解析，确保 VLM 输出不规范时系统仍可降级运行而非崩溃。

6、LoRA 参数高效微调训练链路：实现参数高效微调训练链路，基于 PEFT + TRL SFTTrainer 对 Qwen2.5-VL 进行监督微调，采用 LoRA 低秩适配策略仅更新关键注意力模块，大幅压缩可训练参数量；自定义多模态 Batch 处理逻辑，对视觉 Token 区域屏蔽损失计算，使模型训练聚焦于文本生成目标；配置 Accelerate + DeepSpeed 多卡分布式训练，启用 bf16 混合精度，完成从数据构造到模型收敛的完整 SFT 工程链路。

7、SFT 训练数据构造与落库：以 ChartQA 视觉图表数据集为原始素材，设计双模型协作蒸馏的数据构造流水线——首先驱动 Qwen2.5-VL 对图表图片进行多模态理解并生成候选问答对初稿；随后通过 OpenRouter 调用 Claude 3.5 Sonnet 担任质量裁判，对初稿执行四维检查（技术深度、答案准确性、第一人称视角、语言规范），并在不达标时直接改写问答内容而非仅返回拒绝信号，实现强模型向弱模型的能力蒸馏；最终将图片、指令、目标回复格式化为标准 Chat Template 三元组结构，通过 HuggingFace Dataset 的 Features 定义强类型 Schema（ImageFeature 保障图片序列化一致性），落库为 Parquet 格式，完成可直接用于多模态 SFT 训练的数据集构建。

个人贡献

- 实现基于 LangGraph 状态机的多节点 Agent workflow，将 PDF 解析、多模态问题生成、质量验证、自动修订四阶段编排为有向图，通过条件路由与循环边实现 Reflection 自反思机制，支撑面试题自动化生成的全流程闭环；
- 构建多模态多工具体系，将 Qwen2.5-VL VLM 推理、PDF 图片化解析、SymPy 数学符号验证封装为独立工具节点，以单例模式管理 GPU 模型资源，设计三层 JSON 容错机制保障系统在 LLM 输出不规范时的稳定性；
- 设计细粒度状态驱动的决策控制策略，以强类型全局状态对象为信息载体，在单题粒度上维护验证状态与反馈字段，通过集中式条件路由模块读取全局状态动态决定 workflow 走向，兼顾质量达标时的快速收敛与迭代上限的安全兜底，显著提升 Agent 决策过程的可解释性与可控性；

2024.06-2025.09 工艺线管控MES系统

项目介绍：为某制造企业工艺线管控 MES 系统构建了融合本地知识库检索（RAG）与实时网络搜索的多模态智能查询 Agent，支持产线人员以自然语言对产品工艺流程配置、工艺物料参数、库存实时数据及设备运行状态进行智能检索与问答，显著提升产线生产执行效率与数据一致性，帮助一线人员快速获取准确的工艺信息与操作指导。

核心技术与方法：

- 1、意图理解与任务规划：**用户提问进入系统后，首先由规划 LLM（Qwen-Plus）分析查询意图，判断信息来源需求——是调用本地产品知识库（产品参数、车型对比等结构化信息），还是发起实时网络搜索（政策动态、竞品信息），并将复合问题拆解为可执行的子任务序列，动态决策工具调用顺序。
- 2、混合检索与本地知识召回：**本地检索采用 BM25 关键词匹配与向量相似度（text-embedding-v3，1024 维）的混合召回策略（权重 5%:95%），并引入智能回退机制：当严格阈值（min_match=0.3）下无结果时，自动降级至宽松阈值（min_match=0.1）重试，保障召回覆盖率；最终经 DashScope Rerank 模型对候选文档打分重排，Recall@10 从 53% 提升至 89%。
- 3、实时网络搜索与结果筛选：**网络搜索链路通过 Serper API 获取 Top 50 条结果，先用查询扩展（Query Expansion）与关键词拆解提升覆盖面；再构建 ChromaDB 内存向量库，基于相关度与时间权重二次过滤至 Top 32，将高质量信息传入后续生成环节。
- 4、多轮 Reflection 迭代精炼：**每轮检索结束后，Reflection 模块对已获取的上下文进行质量评估，判断信息是否充分；若不足，自动生成补充查询并再次调用对应工具，最多迭代 3 轮，直至信息完备再进入生成阶段。Memory 模块在迭代过程中持续积累检索结果，并在全局层面进行基于内容哈希的去重，避免冗余信息干扰生成质量。
- 5、多源融合生成与引用追溯：**最终由 DeepSeek-R1 对全部检索片段进行综合推理，生成结构化回答；答案中每处关键结论均通过混合相似度（阈值从 0.63 起自适应衰减）回溯至原始文档片段，插入内联引用标记，保证答案可追溯、可验证；同时基于当前对话语境生成 3 条推荐追问，引导销售深入沟通。

量化成果

- 系统每日为一线销售员提供超过 **500+ 次交互式培训与信息检索服务，答复准确率达 92% 以上**；
- 相比传统资料手册查询，人均沟通准备时间降低 40%，销售培训周期缩短 30%；

个人贡献

独立完成 Agent 核心链路设计与实现：包括意图规划模块、混合检索 RAG 管线（含回退策略与重排）、Serper 搜索链路、ReAct 多轮 Reflection 工作流及 Memory 去重机制、多源融合生成与引用插入。