提示工程实践教程

工具箱系列

2025 年 9 月 16 日

1 简介

提示工程是引导大型语言模型 (LLM) 产生高质量输出的系统化方法。优秀的提示设计能够显著提升模型的可靠性、事实性与可控度, 让我们在写作助手、数据分析、自动化客服等场景中快速构建可复用的智能能力。

在实际项目中, 提示工程扮演以下角色:

- **桥梁**: 让业务需求与模型能力产生精确映射。
- **控制台**: 通过约束语气、格式与推理路径, 控制模型输出的结构。
- **调优器**: 结合同步记录与回测机制, 持续改进提示并沉淀最佳实践。

2 入门

全面掌握提示工程的第一步是搭建稳定的实验环境, 随后通过小规模试验认识模型的响应规律。

2.1 环境搭建

建议按照表 **??** 准备基础设施, 以便快速开展实验。

将环境搭建过程固化为自动化脚本 (如 Makefile、PowerShell 或 Python 工具), 可以降低新成员接入成本。

2.2 小试牛刀

完成基础设置后, 通过最小可行任务感受 LLM 的行为。以下步骤在实践中十分高效:

1. **设定角色**: 将模型置于具体场景, 如 “你是一名资深技术写作者”。

表 1: 常见环境组件及建议

组件	要点
模型与接口	申请 OpenAI、Azure OpenAI、Anthropic 或本地开源模型, 记录密钥与速率限制。
开发工具	使用 VS Code、Cursor 等编辑器, 安装 Python/JavaScript SDK 与 API 调用脚本。
版本管理	使用 Git 管理提示与实验脚本, 通过分支记录迭代。
观察与记录	建立 Markdown/Jupyter 文档, 保留提示、响应、指标与反思。
团队协作	使用共享仓库或知识库整理最佳实践, 便于复用。

2. **描述目标**: 明确输入来源、任务边界与输出格式。

3. **提供范例**: 给出 1–2 个理想回答示例, 帮助模型学习风格。

4. **记录观察**: 从准确度、完整性、语气与潜在幻觉四个角度评价结果。

示例:

```
系统提示: 你是一名资深法律顾问, 擅长用简明方式解释合同条款。
用户输入: 请用不超过 120 字 summarise 下列条款的主要责任和免责点: ...
期望输出: 1. 主要责任; 2. 免责条件; 3. 风险提示。
```

通过更改语气、增加或删除示例、调整输出结构, 可以观察模型响应的差异, 逐步理解其敏感点。

3 指南

本章节依据 Prompt Engineering Guide 汇总常见提示模式, 并给出针对性的示例。

3.1 提示原则

设计提示时应确保信息充分、表达清晰、结构稳定。

1. **明确目标**: 说明任务、受众与输出质量标准。

2. **化繁为简**: 对复杂任务拆分步骤, 用编号或小标题控制逻辑顺序。

3. **锚定事实**: 将关键数据或引用直接嵌入提示, 提醒模型引用来源。

4. **设置约束**: 例如 “仅输出 JSON”、“避免主观评价” 等强约束描述。

示例:

```
任务: 分析安全事件报告并输出 JSON。
要求:
1. 识别根因, 需引用原文证据。
2. 按 {"impact":[],"root_causes":[],"actions":[]} 返回。
3. 若缺少信息, 使用 null 占位并说明原因。
```

3.2 如何迭代优化

优质提示往往经过多轮验证与精炼。

1. **建立回放集**: 为关键任务收集典型输入, 形成 “提示测试集”。

2. **单变量试验**: 每次只调整语气、结构或示例之一, 对比差异。

3. **量化指标**: 设计可检验的成功标准, 如正确字段数、事实准确率。

4. **自动回归**: 使用脚本批量调用模型, 记录每版提示的指标变化。

迭代日志示例:

```
v0 提示: 输出要点但缺少引用 -> 调整要求中加入 "引用原文"。
v1 提示: 引用过长 -> 在要求中限制引用不超过 30 字。
v2 提示: 结果稳定, 进入回归测试集。
```

3.3 文本总结

总结任务关注范围限定与写作角度。

设计思路:

- 指定摘要长度、目标读者与应包含的重点。
- 建议提供示范摘要, 用于传达语气与排版要求。
- 要求模型列出未覆盖的信息, 方便后续补充。

示例提示:

```
请阅读下列产品更新日志, 生成 150 字内的中文摘要, 面向产品经理:
- 强调对用户体验的影响
- 以条目形式列出
- 指出仍待验证的假设
原始日志: [...]
```

3.4 文本推断

推断任务常见于情感分析、意图识别与标签提取。
关键操作:

- 提供标签定义与互斥关系。
- 要求模型引用原文证据段落。
- 对不确定情况设置 “无法判断” 选项。

示例:

```
请判断评论的情绪标签，仅可选择 {"正面","中性","负面","不确定"}。
输出 JSON，包含字段:
- label: 标签
- evidence: 引用原文句子
- confidence: 0-1 之间的小数
评论: [...]
```

3.5 文本转换

转换任务强调格式控制与语义保持。
建议:

- 明确输入输出示例, 特别是 JSON 键名、表格列名等。
- 定义错误处理策略, 例如缺少字段时输出 “missing”。
- 在提示中提醒模型不要添加额外解释文字。

示例:

```
将下列 CSV 行转换为 JSON Lines。
输入示例:
name,email,role
Zhang Yan,zhang@example.com,Account Manager
输出要求: 每行一个 JSON 对象，字段 {"name","email","role"}。
```

3.6 文本扩展

扩展任务需要在创造力与一致性之间取得平衡。
实践要点:

- 明确扩展方向: 补充细节、拓展论证、延伸情节等。
- 设置语气、读者层次与篇幅上限。
- 要求模型指出新增内容与原文之间的联系, 防止偏离主题。

示例:

```
请将以下段落扩展为约 300 字，面向高校新生，语气鼓励:
- 保持原始观点不变
- 每个新增段落以主题句开头
原文: [...]
```

3.7 聊天机器人

设计聊天机器人需要构建角色、上下文记忆与安全策略。

操作清单:

- **人格**: 描述背景、口吻与知识边界。
- **对话状态**: 说明如何总结历史对话, 何时向外部工具提问。
- **拒绝策略**: 给出处理敏感或越权请求的流程。
- **记忆管理**: 规定合并旧对话或丢弃冗余信息的规则。

片段提示示例:

```
系统: 你是某银行的智能客服 Lucy，只能回答个人储蓄相关问题。
- 若问题涉及贷款或投资，请礼貌拒绝并推荐人工客服。
- 若用户超过 3 轮未提供关键信息，请总结目前信息并提出澄清问题。
用户: 我想了解信用卡增值服务...
```

3.8 总结

成功的提示工程流程可概括为 “设定目标 → 结构化表达 → 迭代优化 → 回归验证”。

为确保团队能力持续积累, 建议:

- 建立提示模板库与案例库, 支持跨项目复用。
- 持续维护指标仪表板, 监控提示质量与模型版本变化。
- 推动知识分享, 让团队形成共同的审核与改进标准。

参考资源

- Prompt Engineering Guide
- OpenAI 官方提示工程指南
- Prompting Guide