Promt设计常见错误与解决方案

错误1：Prompt过长，模型注意力分散

表现：1000+行超长Prompt，模型经常"忘记"关键指令

原因：模型注意力机制的限制，过长的Prompt导致关键信息被淹没

解决方案:

1 采用Multi-Agent架构，每个Agent只负责一个子任务

2 分层加载上下文，只加载当前步骤相关的信息

3 单个Agent的Prompt控制在500行以内

实战案例：将超长Prompt拆分为多个聚焦的小Prompt，每个控制在300-500行以内

错误2：状态管理混乱，多轮对话不连贯

表现：Agent"忘记"用户之前的诉求，重复提问，用户体验差

原因：依赖LLM从历史对话中推断状态，但LLM不擅长状态管理

解决方案:

状态显式传递：在Prompt开头明确告知当前状态

职责分离：LLM负责内容生成，代码负责状态管理

实战案例：在每个Agent的Prompt开头添加"## 当前状态"部分

错误3：边界case处理不当，误判率高

表现：相似意图经常混淆，如"为什么限制我的支付？"被误判为其他意图

原因：边界规则描述不清晰，缺少边界case的示例

解决方案:

1 用表格清晰展示边界规则

2 提供大量边界case的Few-shot示例

3 明确判断逻辑

错误4：输出格式不稳定，程序解析失败

表现：LLM有时输出JSON，有时输出自然语言，导致程序解析报错

原因：格式约束不够强，示例不够多

解决方案:

在Prompt中明确要求"严格遵循XML/JSON格式"

提供至少5个完整的输出格式示例

明确标注必填和可选字段

在输出要求中强调"不要输出分析过程，直接输出结果"

实战案例：在每个Agent的Prompt中添加"## 输出格式"部分，提供6-7个示例

6大核心原则：

单一职责：一个Agent只做一件事，做好一件事。

职责分离：LLM擅长创造性生成，不擅长确定性决策。

显式优于隐式：状态、规则、示例都显示，明确告知优于期待模型推断。

结构化优于自然语言：使用表格、列表、代码块展示规则、要求、示例。

示例优于说明：边界case、输出格式都要有示例而非说明。

测试驱动优化：建立测试用例集、准确率baseline，根据错误case分析优化。

各位彦祖亦菲，你学会了吗?

延展阅读：　Prompt设计六要素

写留言

腾讯云开发者 作者 3小时前 23

抱歉各位彦祖亦菲，标题手滑打错了，应该是 Prompt，这不是 bug，这是人类写作声明，🤦

置顶

angiie 浙江 2小时前 2

完了，AI 开始模仿人类的 bug 了（bushi）

4条回复

Ryan 海南 3小时前 5

搞prompt的就和巫术一样，区别是AI之神真的会回应你

编程挺好玩 湖南 1小时前

摸五休二 重庆 3小时前 2

有没有可能是 标题是 Prompt

腾讯云开发者 作者 3小时前

人类写作声明

郑小城 福建 3小时前 1

你们是怎么做到每天都有干货的，算是今年最值得关注的一个公众号。

hennessy 广东 3小时前 1

很有帮助，我到adp试试

士钧 北京 3小时前 1

很实用！

Mavis 北京 1小时前

多agent会造成每个agent出错概率叠加导致整体任务出错概率大幅增长吗 这个怎么解决

knight 湖北 2小时前

目前，想要用更深入的使用AI，还是要融入编程化思想在其中。只不过之前是代码程序员，现在是prompt 和工作流程序员

晨光光光 河南 2小时前

有实际应用的例子吗?

蓝莓科学家 重庆 2小时前

多agent是在哪里可以实现的？我用codex（vscode插件）好像实现不了

吴本立 上海 1小时前

在左边Github那个5.1mini可以实现

kelthas 上海 3小时前

问题是有些时候设定规则限制会很长，如何解决呢?

西门呀在吹雪 山东 3小时前
阿祖表示学到了

六月的雨 北京 3小时前
看到了彦祖亦非，我想到了：阿祖啊，你快收手吧！哈哈