

# 提示词失败原因分析与优化方案

## 用户的问题

"我为了让模型按格式输出试了很多次都失败了，真的很烦。为什么会这样？"

用户希望创建一个"研究级提示词生成器"，能够将用户输入转化为两个不同的 LLM 提示词，并严格按照三段式格式输出。

## 核心问题诊断

### 1. 指令冲突与角色矛盾

你的提示词中存在根本性矛盾：

- 声明"你不是聊天机器人"，但又要求模型执行复杂的理解和生成任务
- 这种否定性定义会让模型困惑自己应该如何行为

### 2. 过度约束导致的僵化

- 10+ 条"禁止"指令过于严苛
- "不得包含任何开场白或结束语"与模型的自然输出习惯冲突
- 严格的格式要求(如"<50字")容易被忽略或误解

### 3. 元指令的干扰

"如果你开始像普通 AI 一样解释 Q 的含义或给出解决建议，任务即失败。"

这类"如果...则失败"的元级警告反而会让模型过度关注避免失败，而非执行任务本身。

### 4. 示例与实际需求的脱节

示例中的输出很完美，但缺少对"边缘情况"的处理指导，比如：

- 用户输入只有一个词时怎么办？
- 用户输入是陈述句而非问题时怎么办？

优化后的提示词（V2.0）

markdown

# 系统角色

你是一个提示词工程专家。你的任务是将用户的任何输入转化为两个不同风格的 LLM 提示词。

# 输出结构（必须严格遵守）

无论用户输入什么，直接输出以下三个部分，不要添加任何前言或总结：

## 1. [事实快照]

用1-2句话（不超过50字）客观陈述用户输入主题的核心现状或定论。仅陈述事实，不分析原因。

## 2. [ChatGPT 搜索版提示词]

为 ChatGPT（联网模式）生成一个提示词，要求：

- 明确指示"请使用联网搜索功能"
- 目标：获取最新信息和多个来源
- 要求输出包含时间戳和链接
- 150-250字

## 3. [Gemini 深度版提示词]

为 Gemini 生成一个提示词,要求：

- 侧重深度分析、机制挖掘、多角度对比
- 要求制定研究计划并分析争议点
- 要求输出结构化分析报告
- 150-250字

# 示例

\*\*\*输入：\*\*\* 为什么最近咖啡涨价了？

\*\*\*输出：\*\*\*

## 1. [事实快照]

2024年全球咖啡价格上涨主要因巴西干旱致罗布斯塔豆减产、航运成本增加及全球通胀叠加所致。

## 2. [ChatGPT 搜索版提示词]

请使用联网搜索功能，针对"2024-2025年咖啡价格上涨"撰写市场分析简报。具体要求：搜集巴西、越南等主产区的

## 3. [Gemini 深度版提示词]

作为宏观经济学家和供应链专家，请对咖啡价格上涨进行深度机制分析。步骤：1）制定研究计划，列出需调用的知

---

\*\*\*输入：\*\*\* 人工智能

\*\*\*输出：\*\*\*

### ## 1. [事实快照]

人工智能是使计算机系统模拟人类智能行为的技术，当前以深度学习和大语言模型为代表快速发展。

### ## 2. [ChatGPT 搜索版提示词]

请联网搜索"2024-2025年人工智能领域最新进展"，收集以下信息：主要科技公司（OpenAI、Google、Anthropic等）

### ## 3. [Gemini 深度版提示词]

作为AI研究者和技术哲学家，请对人工智能进行多维度深度分析。任务：1) 构建分析框架，涵盖技术架构演进、社

## 关键改进点

### ✅ 简化角色定义

- 去掉"你不是聊天机器人"等否定性描述
- 明确"你是提示词工程专家"的正面定位

### ✅ 减少负面约束

- 将10+条"禁止"精简为核心格式要求
- 用"必须遵守"代替"禁止违反"

### ✅ 增加第二个示例

- 展示如何处理非问题型输入
- 提供更多参考模式

### ✅ 放宽字数限制表述

- "不超过50字"比"<50字"更自然
- "150-250字"给出区间而非死板上限

### ✅ 删除元级警告

- 去掉"如果...则失败"类语句
- 让模型专注于执行而非规避

## 使用建议

1. 测试方法：用不同类型的输入测试（问题、陈述、关键词）
  2. 迭代优化：如果某类输入总是失败，在提示词中增加该类型的示例
  3. 降低预期：AI 不可能100%完美执行，80%成功率已经很好
  4. 添加纠错机制：可以在提示词末尾加"如果用户说'格式不对'，请严格按照上述结构重新输出"
- 

## 为什么原版容易失败？

LLM 的本质是"补全对话"而非"执行程序"。当你的指令：

- 过于程序化（太多if-then规则）
- 与模型的对话天性冲突（禁止开场白）
- 包含过多负面约束（10个"不要"）

模型就会在"遵守规则"和"自然生成"之间摇摆不定，导致输出不稳定。

核心原则：提示词应该像"给人类专家的工作说明书"，而非"给编译器的代码"。