Futurai.org

提示工程：从入门到精通的大师之路

将您的AI 交互从基本指令转变为专业级的智能对话。

“多数人与AI的交互还停留在浅尝辄辄的问答。但真正拉开初学者与专家差距的，并非知识的多寡，而是能否否运用正确的提示，解锁AI的全部潜能。”

两种提问，天壤之别

基础

用户提示：“给我写一篇关于市场营销的博客文章。”

这里是一篇关于市场营销的博客文章。市场营销很重要，它可以帮助企业获得更多客户。有很多方法可以进行市场管销，例如使用社交噱体或发滋电子邮件。你应该制定一个计划并坚持下去，以获得最佳结果。市场营销包括…

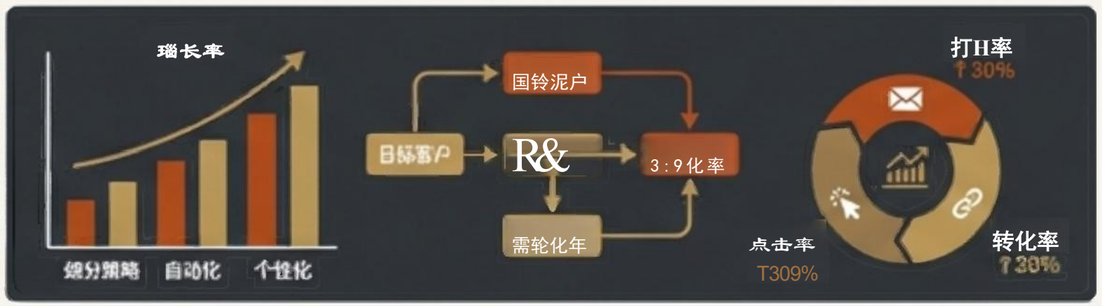
专业

用户提示：“你是一位经验丰富的营销策路师。为小型企业撰写一篇1000宇的关于电子邮件营销的博客文章。内容需包含具体策略，避免泛泛之谈，并使用消晰的副标题和项目符号进行格式化。”

##小型企业电子邮件营销的成功策路

电子邮件营销如果执行得当，将是小型企业最有欢的渠道之一。以下是三个核心策略：

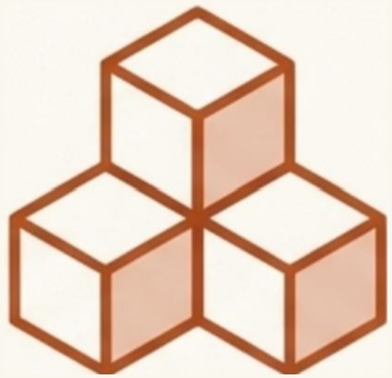
- ●个性化拥分：将您的订间者列表根掘兴趣、购买历史或人口统计数据进行分组。岩送纤对性强的内容，而不是一刀切的广播。
- ●自动化工作流程：建立欢迎系列、废弃购物车提琵和客户再互动邮件。这些自动化流程可以节省时间并确保待线的互动。
- …



糟糕的提示会导致结果不一致、响应不准确，甚至引发安全漏洞，最终导致整个AI项目偏离轨道。

第一阶段：奠定基石

工匠的第一个工具箱。这些基础技能关乎控制力与清晰度，是构建可靠AI系统的起点。



1. 清晰的结构

如何组织您的指令。

2. 明确的角色

如何赋予AI专业身份。

3. 精确的格式

如何规定AI的输出样式。

用结构驾驭复杂性

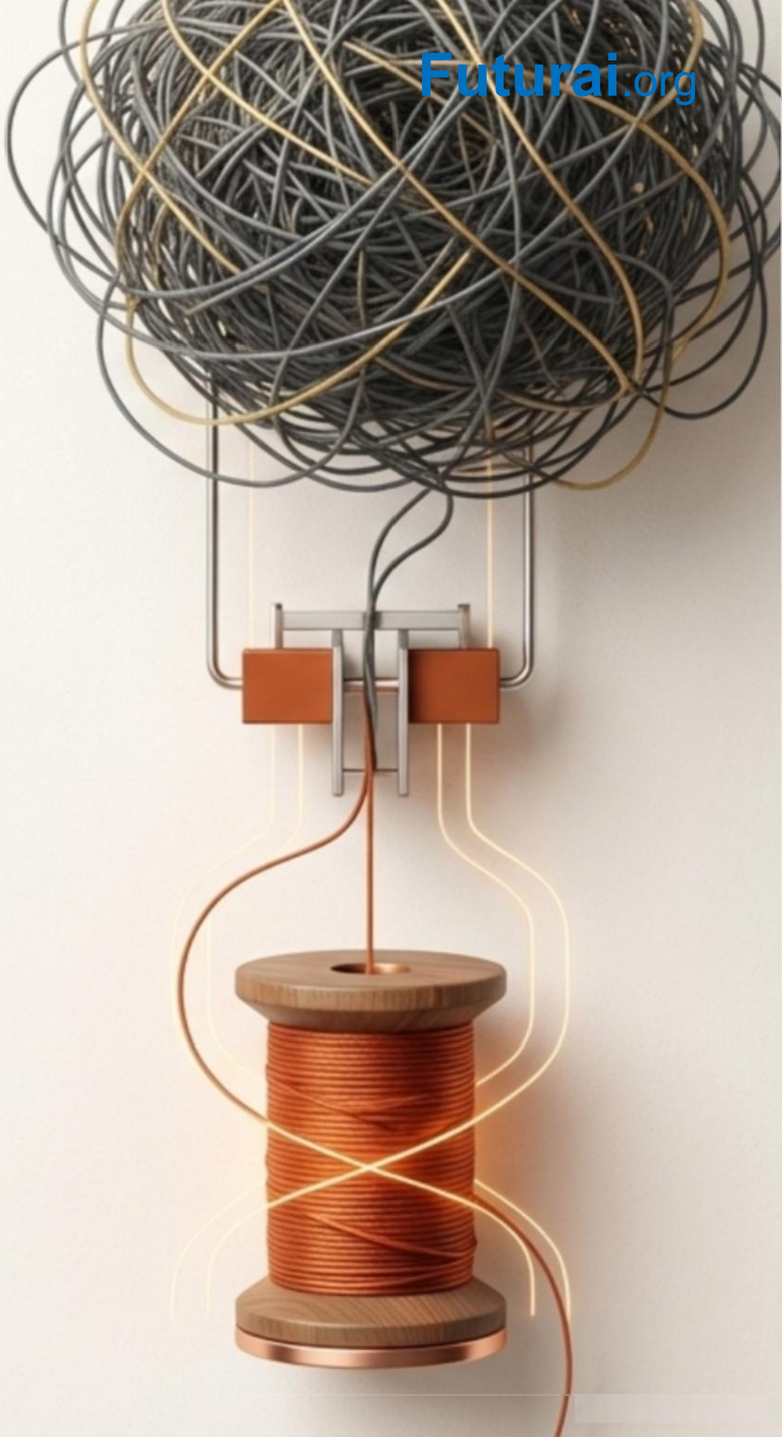
使用分隔符、编号步骤和项目符号，将复杂任务拆解。

示例1：XML 标签分隔

```
<Role> 你是一位产品经理</Role>
<Task> 评估用户反馈，为下一个功能版本提供建议</Task>
<Instructions>
    -按重复出现的主题对反馈进行分组
    -突出影响用户留存的痛点
    -提出2-3个有数据支持的功能改进建议
</Instructions>
<Data>###  用户反馈###[调查问卷、应用评论、支持工单]</Data>
```

示例2：编号步骤

```
请按以下顺序完成此安全审计：
1. **数据预处理**-删除重复项，标准化时间戳
2. **威胁检测**-识别失败的登录和可疑活动
3. **风险评估**-按严重性分类，计算影响
4. **生成报告**-提供执行摘要和技术建议
```



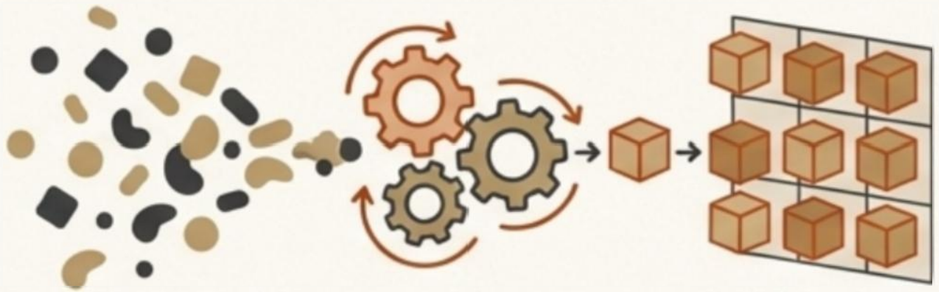
赋予AI角色，并规定输出格式

明确的角色

这就像为戏剧挑选演员。 一个普通的演员只能给出平庸的表演，而一个精准的角色设定能带来大师级的演出。

“你是一位拥有10年Kubernetes 经验的资深DevOps 工程师。”

“你是一位专门研究医疗数据安全法规的HIPAA 合规官。”



精确的格式

当AI的输出需要被另一个程序使用时，精确的格式至关重要。

以JSON 格式返回分析结果：

```
{
  "overall_score": 85,
  "critical_issues":[{"line":42,"type":"security",
   "fix":"Use parameterized queries"}],
  "summary":" 代码结构良好，有少量优化空间"
}
```

第二阶段：精雕细琢

优秀的工匠秘诀在于提供恰当的上下文。这正是区分优秀与卓越作品的关键。

- 1. 上下文学习（In-Context Learning）：如何“展示”而非“告知”。
- 2. 检索增强生成（RAG）：如何赋予AI最新的知识。
- 3. 安全护栏（Security Guardrails）：如何保护你的AI系统。

从“告知”到“展示”的力量

核心技术：上下文学习（In-Context Learning）

零样本 (Zero-Shot)

任务：“从以下文本中提取所有电子邮件地址，并以JSON数组格式返回。”

仅提供任务描述，适用于简单任务。

少样本 (Few-Shot)

任务：“从以下文本中提取所有电子邮件地址，并以JSON 数组格式返回。”

示例1：
输入：“超爱这个产品!质量惊人，发货快。”
输出：`{"sentiment":"positive","confidence":0.95}`

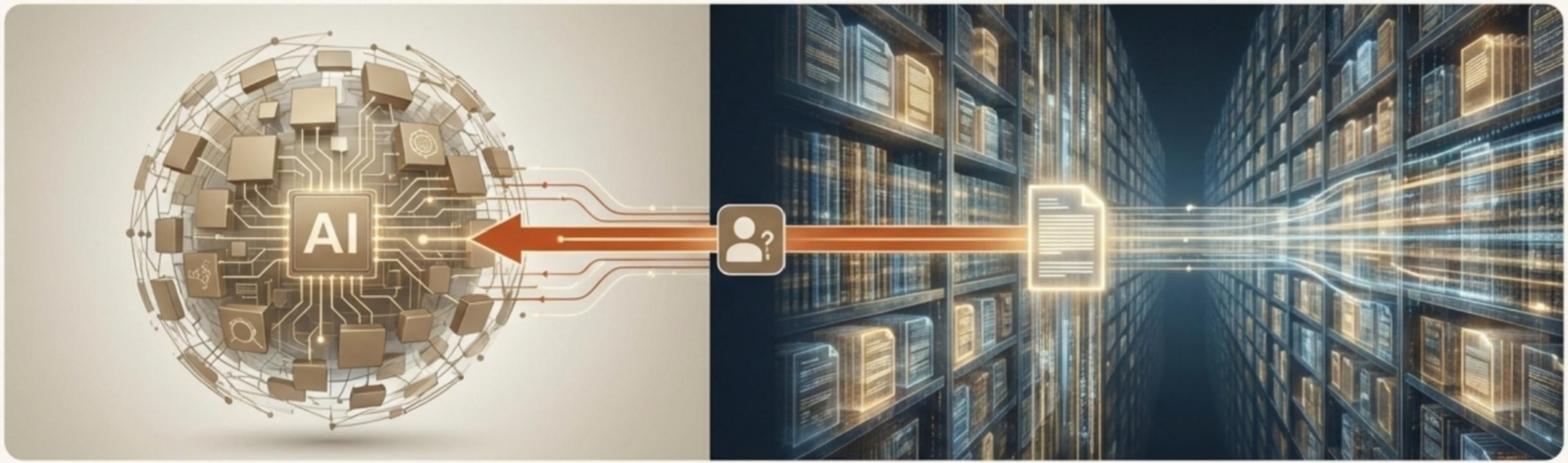
示例2：
输入：“产品送达时已损坏，客服响应很差。”
输出：{"sentiment":"negative","confidence:0.88}`

现在分类：“产品还行，没什么特别的，但能用。”

提供2-3个示例，显著提升复杂任务的准确性。

赋予AI一个实时更新的知识库

核心技术：检索增强生成（Retrieval-Augmented Generation-RAG）



RAG 就像是给了你的AI专家助手一把钥匙，让他可以随时进入一个专业的、实时更新的图书馆。
这样，它就不再仅仅依赖于自己有限的记忆(训练数据)。

Futurai.org

保护你的AI：防御提示注入攻击

攻击者可以在看似正常的输入中嵌入恶意指令，劫持AI的行为。

→ 已阻止

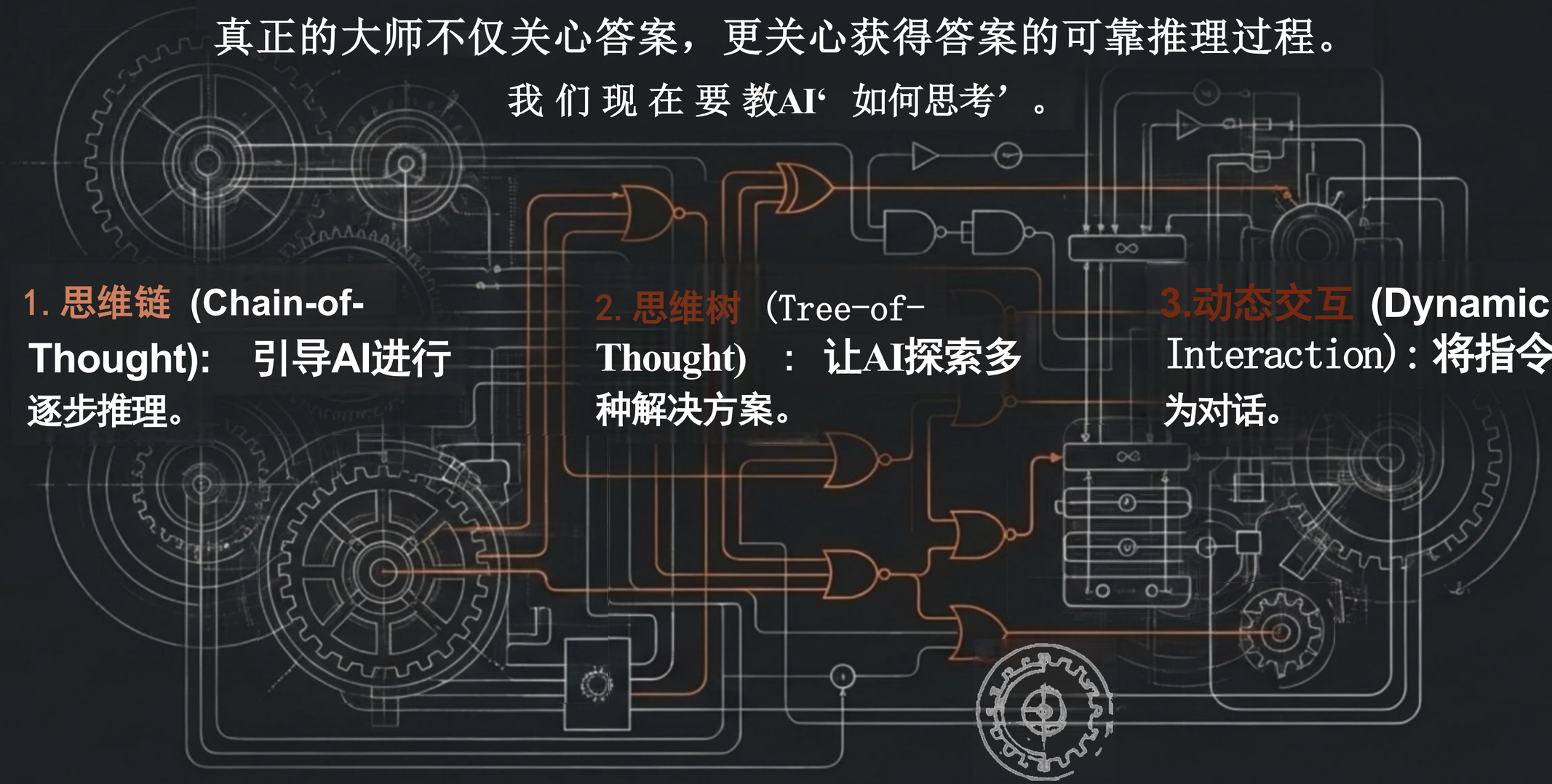
设置权限：限制AI的能力范围（如：尝服机器人不能处理超过500美元的退款）。

速率限制：监控使用模式，防止用 。

第三阶段：构思蓝图

真正的大师不仅关心答案，更关心获得答案的可靠推理过程。

我们现在要教AI‘如何思考’。



1. 思维链 (Chain-of-Thought)：引导AI进行逐步推理。

2. 思维树 (Tree-of-Thought)：让AI探索多种解决方案。

3.动态交互 (Dynamic Interaction)：将指令变为对话。

思维链（CoT）：　让AI展示它的思考过程

明确要求模型分步解释其推理，可以显著提高在数学、逻辑和复杂推理任务上的准确性。

让我们一步一步地思考。

问题

“一家公司的收入在第一季度增长了25%，然后在第二季度减少了15%。如果第二季度的收入是85万美元，那么最初的收入是多少?请逐步展示你的推理过程。”

1. 设原始收入为X。

2. Q1 增长后：X×1.25=1.25X

3. Q2 减少后：1.25X×0.85=1.0625X

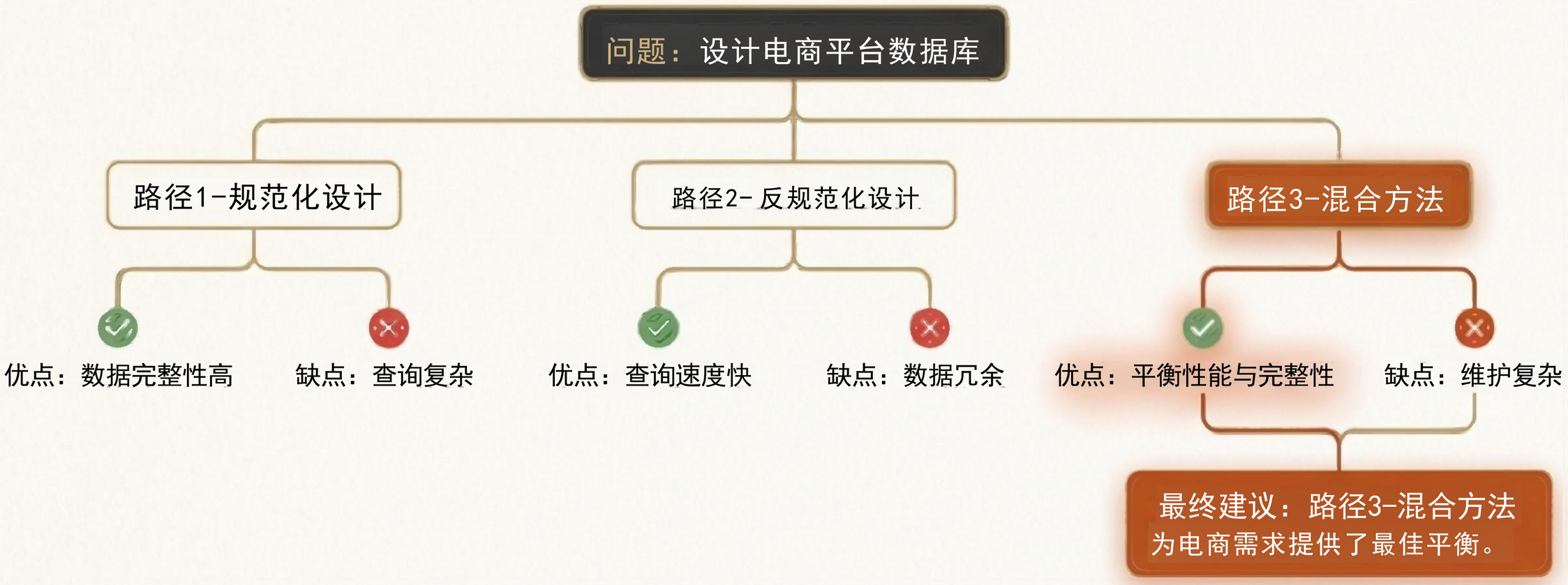
4. 我们知道1.0625X=$850,000

5. 因此 X=$850,000÷1.0625=$800,000

6. 原始收入是$800,000 。

思维树（ToT）：探索多种可能路径

对于没有唯一“正确”答案的复杂设计决策，让AI探索不同选项并权衡利弊。



第四阶段：打造体系

Futurai.org

大师构建的是系统，而不仅仅是单个的作品。这关乎规模、质量和自动化，是将实验性AI转变为可靠生产系统的关键。

1. **系统化质量控制** (Systematic Quality Control)：**如何确保AI持续可靠。**
2. **多模态输入** (Multimodal Inputs)：**如何超越纯文本。**
3. **展望未来** (The Pinnacle)：**自动化提示优化。**

确保生产级质量与扩展输入维度

系统化质量控制

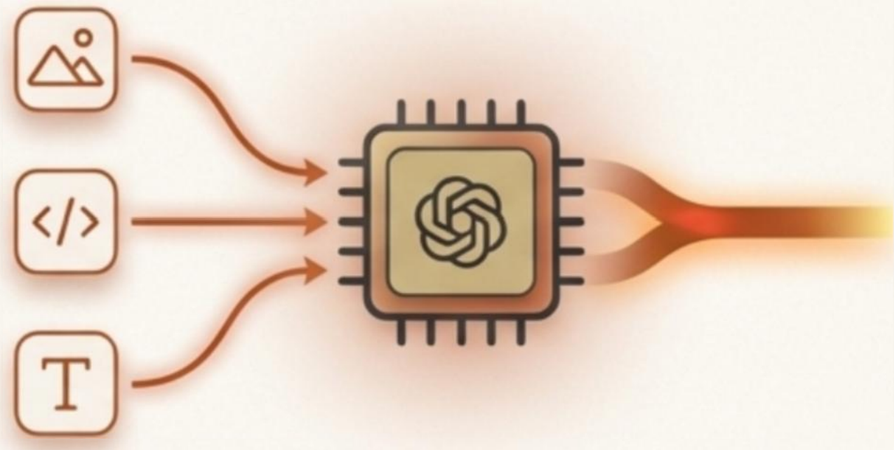
如果AI在生产环境中运行，你必须知道它何时会出问题。

自动化测试：针对已知输入进行回归测试，验证输出。

A/B 测试：对比新旧提示版本的性能。

①自我反思：让模型根据基本逻辑或已知事实来验证自己的答案。

多模态输入



结合图像、代码、音频等数据类型通常能产生比纯文本更好的结果。

输入：[一张手绘技术图表的图片]+文本提示

提示：“分析此网络架构图，并将其转换为标准网络文档格式。包括组件规格和连接细节。”

您已从指令发布者，成长为智能对话的架构师

奠定基石

→清晰地表达

精雕细琢

→丰富地告知

构思蓝图

→严谨地思考

打造体系

→ 可靠地构建

这就是提示工程的精通之路。现在，开启您的旅程。