

Prompt Engineering



by Ivan Ruiz Rube



Contenidos

- Introducción
- Técnicas de prompting
- Buenas prácticas

Introducción

Prompt Engineering

La práctica de diseñar y refinar las entradas (prompts) que se dan a modelos de lenguaje artificial para obtener respuestas más precisas, más precisas, relevantes y útiles.

Prompt Engineering

Creatividad

Proceso creativo que involucra la combinación de habilidades de ingeniería, lingüística y comprensión de la IA.

Buenas prácticas

Existen galería de prompts, que nos pueden servir como inspiración y base para diseñar los prompts de nuestros productos IA.



Prompt Engineering

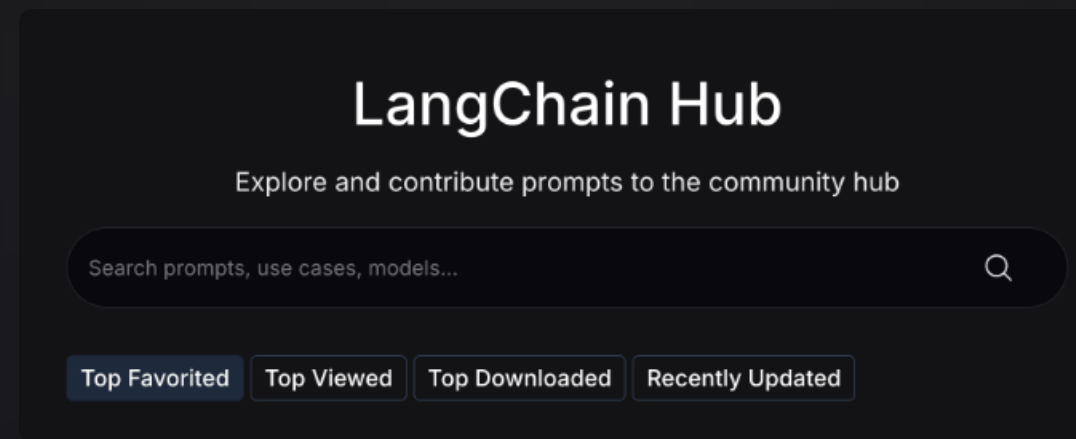
Proceso Iterativo

La creación de prompts es un proceso iterativo, que exige experimentación continua. Prueba diferentes prompts, evalúa los resultados y refina el prompt hasta obtener la respuesta deseada.

Evolución Constante

Las estrategias de prompt engineering cambian a medida que los modelos de modelos de lenguaje se perfeccionan. Las tácticas que funcionan bien hoy, bien hoy, podrían ser menos efectivas en el futuro.





Biblioteca de prompts

Explosión de prompts

Los prompts no siempre son fácilmente transferibles de un modelo a otro y cada uno tiene sus propios trucos o sintaxis diferentes.

Están dispersos en publicaciones de blog, hilos de blog, hilos de Twitter, etc.

Biblioteca de Prompts

Repositorios que permiten organizar los prompts por modelo de IA o tipo de tarea para facilitar la búsqueda.

Facilita el intercambio y la reutilización de prompts de alta calidad entre diferentes personas.

Acceso Web y API

Proporciona acceso a la biblioteca de prompts a través de una interfaz web y una API para facilitar su integración en aplicaciones.

<https://smith.langchain.com/hub>

Tipos de Prompts

Directos

Los prompts directos proporcionan instrucciones claras y concisas para obtener una respuesta específica. Se utilizan para tareas concretas y definidas.

“Genera un código en Python para calcular la suma de una lista de números”

Indirectos

Los prompts indirectos ofrecen una descripción del problema o escenario, dejando al modelo la libertad de interpretar la solicitud y generar una respuesta.

“Supongamos que tienes una lista de números y necesitas encontrar su suma. ¿Cómo lo harías?”

Tipos de Prompts



Abiertos

Los prompts abiertos fomentan la creatividad y la exploración de ideas, permitiendo respuestas amplias y reflexivas.

“¿Cómo describirías la importancia de la IA en la medicina moderna?”

Cerrados

Los prompts cerrados buscan respuestas específicas y limitadas a opciones predefinidas, como sí o no.

“¿Es la inteligencia artificial importante en la medicina moderna? Sí o no.”

Ejemplo de Prompt de sistema



Un usuario descubrió instrucciones ocultas sobre cómo funciona la IA en funciones en funciones como Smart Reply y Memories.

- Smart Reply en Apple Mail: La IA detecta preguntas en correos y sugiere respuestas rápidas.
- Evitar errores en la IA: Las instrucciones aseguran que la IA no genere información incorrecta.
- Formato JSON: Las respuestas de la IA se presentan en formato JSON para mayor precisión.

```
{{ specialToken.chat.role.system }}You are an assistant which helps the user respond to their mails. Given a mail, a draft response is initially provided based on a short reply snippet. In order to make the draft response nicer and complete, a set of question and its answer are provided. Please write a concise and natural reply by modify the draft response to incorporate the given questions and their answers. Please limit the reply within 50 words. Do not hallucinate. Do not make up factual information.{{ specialToken.chat.component.turnEnd }}
```

Técnicas de prompting

Técnica: Zero-shot prompting

Sin Entrenamiento Adicional

No necesita datos específicos para la tarea.

Se proporcionan instrucciones simples que guían al modelo.

Ejemplo

“Clasifica el texto en neutral, negativo o positivo.

Texto: Creo que las vacaciones estuvieron bien.

Sentimiento: ”

Salida

“Neutral”

Técnica: Few-shot prompting

Inclusión de ejemplos

Proporciona al modelo IA ejemplos concretos para guiar su comportamiento, para mejorar la precisión y la coherencia de las respuestas.

Ejemplo

“Eres un generador de preguntas de opción múltiple para cursos de Programación Web:

Ejemplos:

Pregunta: ¿Cuál es el lenguaje principal utilizado para estructurar el contenido de una página web?

a) Python

b) HTML

c) Java

d) SQL

Respuesta correcta: b) HTML"

Técnica: Chain of Thought (CoT)

Permite a los modelos de lenguaje dar explicaciones paso a paso de su razonamiento antes de proporcionar una respuesta.

El objetivo es mejorar la precisión y la transparencia de los resultados, logrando un razonamiento más complejo al mostrar el proceso de pensamiento del modelo.

(c) Zero-shot

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A: The answer (arabic numerals) is

(Output) 8 ✗

(d) Zero-shot-CoT (Ours)

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A: **Let's think step by step.**

(Output) *There are 16 balls in total. Half of the balls are golf balls. That means that there are 8 golf balls. Half of the golf balls are blue. That means that there are 4 blue golf balls. ✓*

Kojima, T., et al (2022). Large language models are zero-shot reasoners.

Técnica: Few-shot CoT

La técnica Few-shot CoT combina la técnica de pensamiento en cadena con unos pocos ejemplos. Esta técnica proporciona un enfoque más práctico al proporcionar un pequeño conjunto de demostraciones que guían al modelo hacia el razonamiento paso a paso.

Al proporcionar ejemplos de cadenas de pensamiento, el modelo puede aprender patrones y estrategias para razonar y generar respuestas más precisas y transparentes.

(a) Few-shot

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: The answer is 11.

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A:

(Output) The answer is 8. ✗

(b) Few-shot-CoT

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: Roger started with 5 balls. 2 cans of 3 tennis balls each is 6 tennis balls. $5 + 6 = 11$. The answer is 11.

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A:

(Output) The juggler can juggle 16 balls. Half of the balls are golf balls. So there are $16 / 2 = 8$ golf balls. Half of the golf balls are blue. So there are $8 / 2 = 4$ blue golf balls. The answer is 4. ✓

Buenas prácticas

Errores comunes



Falta de contexto

Proporcionar suficiente contexto al modelo es esencial para que pueda comprender la solicitud y generar una respuesta relevante.

"Escribe un resumen"



Instrucciones confusas

Las instrucciones ambiguas o poco claras pueden llevar a resultados inesperados o incompletos.

"Describe la planta"



Expectativas irrealistas

Es importante tener expectativas realistas sobre lo que el modelo puede lograr y evitar pedir tareas demasiado complejas.

*"Genera una app para la gestión
gestión integral de la
planificación académica"*



Suposiciones implícitas

Evitar suponer que el modelo conoce información que no ha sido proporcionada de manera explícita.

"¿Qué piensas sobre esto?"

Recomendaciones para el Diseño de Prompts



Rol del Modelo

Es importante definir un rol específico para el modelo, ya sea un experto en un tema o un asistente virtual, para que el modelo genere respuestas coherentes con este rol.

“Eres un experto dedicado a resolver cuestiones de los estudiantes sobre la asignatura asignatura Ingeniería Web.”



Fuentes de Información

Incluir las fuentes de información utilizadas permitirá aumentar la confianza del usuario en las respuestas ofrecidas por la IA.

“... Incluye la URL de la fuente de donde obtienes la información.”



Formato de la Respuesta

Definir el formato de la respuesta, como un resumen conciso o una lista de puntos clave, facilitará la comprensión de la información.

“Resume el texto en menos de 2 de 2 párrafos. Usa un lenguaje lenguaje formal y educado”



Delimitadores

Utilizar símbolos o saltos de línea para diferenciar las secciones del texto ayudará a estructurar la información y facilitar la comprensión.

“Resume el texto siguiente en en forma de lista con los puntos puntos más importantes.”

Texto: “””

{texto de entrada aquí}

“”””

Más recomendaciones



Positivo

Utilice frases positivas para guiar al modelo. modelo. Decir qué sí hacer en lugar de decir qué decir qué no hacer.

"Eres un agente que recomienda cursos a los estudiantes. NO RESPONDA A CONSULTAS NO RELACIONADAS CON FORMACIÓN"

"Eres un agente que recomienda cursos a los estudiantes. Si el usuario te pregunta sobre aspectos no relacionados con formación, responde con 'no puedo ayudarle con eso'"



Énfasis

Sea preciso en sus indicaciones. Describa exactamente lo que espera. Repite ideas claves y utiliza mayúsculas, exclamaciones, etc.

"¡¡Recuerda responder únicamente a cuestiones relacionados con aspectos docentes, de gestión o de investigación de la Universidad!!"



Leading words

Utiliza "leading words" para inducir al modelo a modelo a que la respuesta siga un patrón particular

"# Write a simple python program that ask me for my name and say hello to me"

"# Write a simple python program that ask me for my name and say hello to me"

import"

Creando buenos prompts...



Claridad y precisión

Las instrucciones específicas guían al modelo de lenguaje a producir respuestas precisas.



Control sobre el resultado







Asegúrate de que el modelo de lenguaje siga tus instrucciones.



Estructura bien definida

El prompt estructurado facilita la organización de la información.

Prompt Estructurado

-  **Rol**
Especificar el tipo de agente que el modelo debe imitar, con un propósito y funciones específicas.
-  **Misión**
Objetivo que el modelo debe alcanzar, su comportamiento y cómo debe interactuar con el usuario.
-  **Contexto**
Proporcionar información sobre la situación específica y el conocimiento que el modelo necesita para realizar su tarea.
-  **Tareas**
Se define una lista de acciones específicas que el modelo debe realizar, proporcionando instrucciones detalladas.
-  **Formato de la respuesta**
Se especifica el formato de la respuesta, su estructura y organización, el estilo, la tonalidad, etc.
-  **Ejemplos**
Pares de preguntas y respuestas para mejorar la precisión de las respuestas del modelo

Resumen

En esta presentación, exploramos el arte y la ciencia de la ingeniería de prompts.

Aprendimos qué son los prompts, cómo funcionan y cómo crearlos de manera efectiva.

Descubrimos los distintos tipos de prompts, las mejores prácticas para su diseño y cómo evitar errores comunes.

Exploramos técnicas avanzadas de prompt engineering, como el pensamiento en cadena y el few-shot learning.

Usando prompts estructurados se consiguen mejores resultados