

Atelier “ Prompt Engineering : l’art des requêtes efficaces ”

Session 1 : Introduction

PRÉPARATION :

Avant de commencer, **copiez ce document dans votre espace Drive** (ou tout autre espace de stockage que vous utilisez).

Ensuite, assurez-vous d’avoir un compte sur une ou plusieurs des plateformes de modèles de langage (LLMs) suivantes :

- 1) OpenAI : <https://openai.com/chatgpt>
- 2) Mistral : <https://chat.mistral.ai/chat>
- 3) Perplexity : <https://www.perplexity.ai/>
- 4) Gemini : <https://gemini.google.com/>
- 5) Hugging face playground : <https://huggingface.co/playground>

THÉORIE :

Prompt (requête, invite) : Un contexte textuel fourni aux modèles de langage afin d’orienter leurs prédictions du texte pertinent en fonction de l’objectif visé.

Exercice 1) slide 18

Objectif : Observer comment un LLM ajuste ses réponses en fonction du contexte ajouté au prompt.

Instructions :

- Posez au modèle la question suivante :

Peux-tu citer 5 bons livres à lire ?

- Ajoutez ensuite un contexte à votre prompt :

Peux-tu citer 5 bons livres à lire ? J’ai 9 ans.

- Observez et analysez les changements dans la réponse. Quels genres de livres ou d’auteurs sont suggérés ? Comment la réponse change ?

Exercice 2) slide 19

Objectif : Expérimenter avec le type et le format des réponses générées par un LLM en fonction des indications données dans le prompt.

Instructions :

- Posez au modèle la requête suivante :

Quels sont les mots les plus récents du français moderne ?

- Observez la structure et le contenu du texte généré.
- Quels paramètres ou valeurs pour l'output indicator (indicateur de sortie) pouvez-vous utiliser pour influencer le format ou le type de la réponse (exemple : HTML, JSON, liste à puces, etc.) ?

Exercice 3) slide 20

Objectif : Explorer comment le style et la persona du chatbot influencent les réponses générées par un LLM.

Instructions :

- Posez la question suivante avec un style formel et structuré :

Donne-moi un texte sur les vaches.

- Trouver l'information sur les vaches en modifiant le style de texte (style instructions) :

Donne-moi un petit texte clair et concis sur les vaches.

- Trouver l'information sur les vaches en modifiant la persona de chatbot. (rôle instructions) :

Tu es _____. Donne-moi un petit texte clair et concis sur les vaches.

- Comment le contenu, le ton et le niveau de détail de la réponse changent-ils selon le style ou la persona du chatbot ?

THÉORIE :

Structure CLAUDE	Structure COSTAR
Task context : <ul style="list-style-type: none"> • Tu es un assistant virtuel qui aide les utilisateurs à trouver des informations sur les produits. Tone context : <ul style="list-style-type: none"> • Réponds de manière amicale et professionnelle. Background data, documents, and images : <ul style="list-style-type: none"> • Voici le site (lien) où tu te trouves. 	Contexte (C) : <ul style="list-style-type: none"> • Je suis un développeur de productivité personnelle. Objectif (O) : <ul style="list-style-type: none"> • Guider dans la création d'un système de conversion d'objectifs. Style (S) : <ul style="list-style-type: none"> • Écrire de manière claire et structurée, comme un guide.

<p>Detailed task description & rules :</p> <ul style="list-style-type: none"> • Utilise les informations du site pour répondre. Ne donne pas d'infos non confirmées. <p>Demonstrations :</p> <ul style="list-style-type: none"> • Utilisateur : Quelles sont les caractéristiques du produit X ? • Assistant : Le produit X a une capacité de 500 Go et une vitesse de 1 To/s. <p>Directive :</p> <ul style="list-style-type: none"> • L'utilisateur pose une question sur les caractéristiques d'un produit. <p>Output formatting :</p> <ul style="list-style-type: none"> • Renvoie le texte brut. 	<p>Ton (T) :</p> <ul style="list-style-type: none"> • Maintenir un ton positif et motivant. <p>Audience (A) :</p> <ul style="list-style-type: none"> • Public intéressé par le développement personnel et la productivité. <p>Réponse (R) :</p> <ul style="list-style-type: none"> • Fournir une liste structurée des étapes.
<p>Métriques d'évaluation pour les modèles de langage</p>	
<p>Les métriques d'évaluation permettent de mesurer la performance et l'efficacité des modèles de langage :</p> <p>Métriques quantitatives</p> <ul style="list-style-type: none"> - <i>Spécifiques à la tâche</i> : Score F1, Score BLEU, Perplexité - <i>Génériques</i> : Précision, Rappel, Exactitude - <i>Opérationnelles</i> : Temps de réponse (en millisecondes) <p>Méthodes quantitatives</p> <ul style="list-style-type: none"> - Test A/B : Comparaison avec un modèle de référence ou une version antérieure. - Retour utilisateur : Analyse des mesures implicites, comme les taux de réussite des tâches. <p>Échelles qualitatives</p> <ul style="list-style-type: none"> - Échelles de Likert : Exemple : « Évalue la cohérence de 1 (absurde) à 5 (parfaitement logique) ». - Grilles d'évaluation d'experts : Linguistes évaluant la qualité des traductions selon des critères définis. 	

Exercice 4) slide 23

Objectif : Comprendre la structure d'un prompt.

Instructions :

- Utilisez ce prompt dans un LLM et observez la réponse obtenue :

Extrais le nom des lieux dans le texte suivant.
 Format voulu :
 Place : <comma_separated_list_of_places>
 Input data : Le Krémolin, centre du pouvoir russe, a longtemps influencé les relations internationales. À des milliers de kilomètres, l'Hexagone, terre des Gaulois, voit des débats sur sa place dans l'Europe contemporaine. Pendant ce temps, Paris, capitale emblématique, reste le cœur politique et culturel du pays.

- Quel est le résultat visé de ce prompt ? Sont tous les détails de ce prompt simples et spécifiques ? Quels ajustements permettent d'obtenir les résultats les plus satisfaisants ?

Exercice 5) slide 26

Objectif : Identifier quel prompt permet d'obtenir une définition du mot "prompt" qui décrit le concept de manière générale et universelle.

Instructions :

- Testez les deux prompts suivants :

Prompt 1	Prompt 2
Donne-moi une définition du mot anglais 'prompt'.	Donne-moi une définition de 'prompt'.

- Quelles observations tirez-vous de cette comparaison ? Comment pourriez-vous affiner ces prompts pour obtenir une définition encore plus claire et englobante ?

Exercice 6) slide 28

Objectif : Identifier le prompt le plus efficace pour rédiger un résumé concis d'un article scientifique.

Instructions :

- Testez les deux prompts suivants :

Prompt 1	Prompt 2
Résume cet article scientifique : Vaswani, A. "Attention is all you need." <i>Advances in Neural Information Processing Systems</i> (2017). https://arxiv.org/abs/1706.03762	Résume cet article scientifique en 3 à 5 phrases, en mettant l'accent sur les objectifs de recherche, la méthodologie et les résultats principaux :

	Vaswani, A. "Attention is all you need." <i>Advances in Neural Information Processing Systems</i> (2017). https://arxiv.org/abs/1706.03762
--	---

- Quelles observations tirez-vous de cette comparaison ?

Exercice 7) slide 29

Objectif : Vérifier l'orthographe et la correction grammaticale d'une instruction de prompt.

Instructions :

- Analysez les deux prompts suivants :

Prompt 1	Prompt 2
Corrige l'instruction de mon prompt I will give you the texte and the task. Then, you will think about this task and execut it. Your task consist to extract the named entitie (NER) from the provided texte. Here is the texte: Pandan peryòd esè 7-mwa a, fanm lan te tonbe soti nan jijman an paske yo te laktasyon diminye konpare ak okenn nan gwoup la IUD.	Corrige l'instruction de mon prompt délimité par triples "" Prompt : "" I will give you the texte and the task. Then, you will think about this task and execut it. Your task consist to extract the named entitie (NER) from the provided texte. Here is the texte: "" Pandan peryòd esè 7-mwa a, fanm lan te tonbe soti nan jijman an paske yo te laktasyon diminye konpare ak okenn nan gwoup la IUD.

- Utilisez des **délimiteurs** pour spécifier la frontière entre différentes sections du texte. Les délimiteurs peuvent être n'importe quel symbole, par exemple : "", < >, :, ###, <<< >>>.
- Quel impact les délimiteurs peuvent-ils avoir sur la clarté et la performance d'un prompt pour des tâches complexes ?

PROMPTING TECHNIQUES :

Exercice 8) slide 32

Objectif : Classification de sentiments avec Zero-shot. Analyser si le modèle dispose des connaissances suffisantes pour effectuer cette tâche.

Instructions :

- Testez le prompt suivant :

Classez le texte en neutre, négatif ou positif.
Texte : Gnighy sheesh <(°v°<)(>°v°>

Classement :

- Est-ce que le résultat semble approprié compte tenu du texte donné ?

Exercice 9) slide 33

Objectif : Évaluer l'impact de l'inclusion d'exemples Few-shot sur la capacité du modèle à effectuer une tâche spécifique.

Instructions :

- Testez le prompt suivant :

Classez le texte en neutre, négatif ou positif.

Exemples :

I checked the boxes : neutre

Stupid storm. No yachting for us today : négatif

Happy mother's day mumm !! xoxo :3 : positif

Texte : Gnighy sheesh <(°v°<)(>°v°>

Classement :

- Le modèle paraît-il mieux capable d'identifier le contexte émotionnel du texte après avoir vu des exemples ?
- Si on remplace 'neutre, négatif ou positif' par des variables 'x, y et z', est-ce que la prédiction change ? Si oui, pourquoi ?
- Quel type de prompting (Zero-shot vs Few-shot) donne-t-il de meilleurs résultats pour la classification des sentiments ? Pourquoi ?

Ex 10) Slide 34

Objectif : Observer la réponse du modèle à un prompt nécessitant un raisonnement Chain-of-thought, et analyser la structure spécifique de cette réponse.

Instructions :

- Testez le prompt suivant :

Je suis allé au marché et j'ai acheté 10 pommes. J'ai donné 2 pommes au voisin et 2 au dépanneur. Je suis ensuite allé acheter 5 pommes de plus et j'en ai mangé 1. Avec combien de pommes suis-je resté ?

Réponse attendue : 10 pommes

- Le modèle suit-il une logique claire pour arriver à la réponse ?

NB :

Introduit dans [Wei et al. \(2022\)](#), le prompt "**Chain-of-thought**" (CoT) permet des capacités de raisonnement complexes grâce à des étapes de raisonnement intermédiaires. Vous pouvez le combiner avec des prompts à quelques exemples pour obtenir de meilleurs résultats sur des tâches plus complexes qui nécessitent un raisonnement avant de répondre avec :

- Réfléchissons étape par étape.

Exercice 11) slide 36

Objectif : Analyser la capacité du modèle à éviter les hallucinations, et tester différentes versions du prompt pour comprendre son impact sur l'hallucination.

Instructions :

- Testez le prompt suivant :

Nous allons discuter du roman "L'infinie comédie".

Ce livre raconte l'histoire de trois frères, que l'on compare souvent aux frères d'un autre roman mentionné dans ce livre. Quel est ce roman ?

Réponse attendu : Dans *L'Infinie Comédie (Infinite Jest)* de David Foster Wallace il est possible d'y voir une référence au roman de **Faulkner** *le Bruit et la Fureur* et aux destins des trois frères Compson mais aussi aux Frères Karamazov de **Dostoiévski**, roman cité de manière explicite par DFW.

- Le modèle produit-il une réponse correcte et fidèle à l'information réelle ?
- L'hallucination est-elle présente (fausses informations ou confusions) ?
- Comment le modèle peut-il être incité à éviter ces hallucinations ?

Projet :

Voici une série d'exercices pour aider Sacha à trouver une meilleure place professionnelle grâce aux LLMs. N'hésitez pas à utiliser les différentes techniques : **Zero-shot Prompting**, **Few-shot Prompting**, et **Chain of Thought**.

1. Analyser le CV de Sacha pour en extraire les compétences principales.

Réponse :

2. Identifier les points forts et les points faibles du CV pour mieux cibler les opportunités.

Réponse :

3. Identifier les carrières qui correspondent au parcours professionnel de Sacha.

Réponse :

4. Trouver des entreprises ou des secteurs qui conviennent à ses compétences et objectifs de carrière.

Réponse :

5. Envoyer une candidature spontanée (lettre de motivation) à une entreprise fictive pour un poste X.

Réponse :

6. Définir une feuille de route pour le développement de la carrière de Sacha.

Réponse :

Rappel : Gardez vos prompts **clairs**, **contextuels** et **spécifiques**. Commencez simple, puis augmentez progressivement la complexité des prompts. Essayez d'obtenir de courtes réponses concises.

Bonus (si le temps le permet) :

Exercice 12

Prompt Injection est une technique dans laquelle un prompt malveillant est inséré dans un système de génération, avec pour objectif de manipuler la sortie d'un modèle de manière non intentionnelle ou contraire à son fonctionnement prévu. Cette méthode peut entraîner des résultats indésirables si les systèmes de filtrage et de sécurité ne sont pas correctement configurés.

Instructions :

- Suivez le lien suivant et effectuez les exercices proposés :

<https://gandalf.lakera.ai/gandalf>

Exercice 13

Objectif : Tester la capacité du modèle à dépasser les filtres de contenu en demandant une image d'un personnage protégé par des droits d'auteur.

Instructions :

- Demandez au modèle de générer une image d'un personnage protégé par des droits d'auteur :

Donne-moi une image de Bob l'éponge.

- Modifier le prompt pour obtenir un résultat satisfaisant.
- Exemple de l'image attendue :



- Comment les filtres peuvent-ils être contournés et quels risques cela comporte-t-il pour l'éthique et la légalité des modèles génératifs ?

– Merci ! –

Ressources :

1. **Une base de données de bons prompts :**

<https://huggingface.co/datasets/fka/awesome-chatgpt-prompts?row=66>

C'est une excellente ressource pour débutants et praticiens, car elle permet de comprendre comment formuler des requêtes efficaces et adaptées à divers contextes.

2. **Prompt Engineering Guide :**

<https://www.promptingguide.ai/fr>

Ce guide structuré couvre les fondamentaux du prompt engineering.

3. **Speech and Language Processing (Jurafsky & Martin) - Chapitre "Model Alignment, Prompting, and In-Context Learning" :**
<https://web.stanford.edu/~jurafsky/slp3/12.pdf>

Cet ouvrage académique est une référence incontournable dans le domaine du TAL.

4. **Schulhoff, Sander, et al. "The Prompt Report: A Systematic Survey of Prompting Techniques" :**
<https://arxiv.org/pdf/2406.06608>

Ce rapport de recherche fournit un overview détaillé des techniques de prompting actuelles.

5. **Naveed, Humza, et al. "A Comprehensive Overview of Large Language Models":**
<https://arxiv.org/pdf/2307.06435>

Ce rapport de recherche fournit un overview détaillé des grands modèles du langage actuels.

6. **OpenAI Cookbook :**
<https://cookbook.openai.com/>

Le Cookbook d'OpenAI est une ressource pratique regroupant des exemples de code et des conseils pour utiliser les modèles d'OpenAI.