|  |  |  |  |
| --- | --- | --- | --- |
| Une image contenant texte, Police, logo, graphisme  Description générée automatiquement | | **Ressource**  **Les assistants et l’Art-du-Prompt**  Luc Trunztler |  |
| CYCLE 4 | **COMMENT SECURISER L’ACCES AUX CASIERS DU COLLEGE GRACE A L’IA ?** | | NIVEAU QUATRIÈME |

# **Objectif**

Présenter les nouveaux assistants IA et les techniques de prompting pour bien les utiliser !

# **Quels assistants pouvons-nous utiliser ?**

Aujourd’hui les nouveaux assistants IA évoluent tous les mois, une façon de suivre les meilleurs assistants du marché en terme de performance « universelle » est de se référer au Leaderboard Arena : <https://leaderboard.lmsys.org/>

**En Septembre 2024** (attention cela peut naturellement évoluer), nous retrouverons dans le peloton de tête, **accessible librement** en Europe :

*Les 3 solutions sont américaines.*

* <https://chatgpt.com/> de OpenAI, accessible également via <https://copilot.microsoft.com/> (avec une surcouche Microsoft tout de même)
* <https://claude.ai/> d’Anthropic
* <https://gemini.google.com/> de Google

*Une solution française*

* <https://chat.mistral.ai/> est une autre alternative moins puissante voir détail ci-dessous

**ChatGPT**

* Permet d’analyser texte + image + tout autre type fichier (.docx, .pdf, .xlsx, ..).
* Version 4o accessible gratuitement pendant quelques conversations puis une fois ces crédits gratuits utilisés, il rebascule vers la version 3.5 beaucoup moins performance et non connectée à internet.
* La version 4o permet de faire des recherches sur internet (via le moteur Bing de Google).
* La version o1 intègre nativement la technique de prompting du chemin de pensée (voir plus bas).
* Accès à des GPT spécialisés (<https://chatgpt.com/gpts>). Les GPT spécialisés sont des assistants créés par OpenAI ou la communauté pour remplir de façon efficace une tâche bien particulière, par exemple pour rédiger un Post Linkedin pour le Rocket club ! (<https://chatgpt.com/g/g-oInQElZO1-post-rs>)  ou bien pour recevoir des conseils pour bien s’occuper de ses plantes (<https://chatgpt.com/g/g-6PKrcgTBL-planty>).

Pour préserver la confidentialité de vos échanges, pensez à créer des chats éphémères (= l’équivalent de la navigation privée sur les navigateurs web) :

Une image contenant texte, carte de visite, capture d’écran

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

**Penser également à désactiver, dans les paramètres, l’option « Améliorer le modèle pour tous »** pour s’assurer que les données ne seront pas utilisées pour le réentrainement du modèle et tombent alors dans le domaine public !

**Copilot**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* Propose des fonctionnalités très similaires à ChatGPT. En Août 2024, il s’agit cependant encore du modèle 4 et non 4o qui est disponible sur Copilot.microsoft.com
* Avec un compte entreprise, la protection des données personnelles est automatique :

**Claude IA**

* Offre des performances similaires à la 4o de ChatGPT à la différence que Claude.ia n’est pas connectée à internet pour vérifier ses sources. A noter que les modèles qui ne sont pas en capacité à vérifier leurs sources sur internet sont plus susceptibles à produire des hallucinations  (=réponse fausses générées par l’assistant mais données sur un ton très convaincant et affirmatif pouvant vous induire en erreur). Ce modèle reste cependant très performant pour traiter les données que vous lui communiquerez et sur lequel il y aura peu de risque d’hallucination.
* Comme la 4o de ChatGPT, il y a un nombre de crédit limité sur la version gratuite avant d’être bloqué. Les crédits se renouvellent également après x heures suivant la sollicitation de leur service.

**Gemini**

* Le modèle Gemini de Google est réputé très rapide. Il n’est cependant pas facile de construire des chemins de pensées (chain of thought) avec, une des plus importantes techniques de Prompting.
* D’expérience, Gemini est plus propice à des hallucinations lors de ses recherches d’informations.
* Depuis Août 2024, il est possible de générer des images via Gemini.

**Mistral**

* Le champion français. Malheureusement le modèle, comme Claude.ia, n’est pas connecté à internet.
* De nombreuses personnes affirment qu’il offre de meilleure qualité rédactionnelle en français que ces homologues américains car ces derniers, contrairement à Mistral, ont été entraînés exclusivement sur du contenu en anglais.

1. **Quels usages ?**

Il y a 2 principaux freins à l’usage des nouveaux assistants :

1. Ne pas parvenir à bien les utiliser
2. Ne pas savoir pour quels usages les utiliser dans son quotidien

Pour le **premier point**, plusieurs techniques de prompting existe ( voir ci-dessous) pour mieux les prendre en main.

Pour le **second point**, les 3 grands *usages de ces nouveaux assistants portent sur la Recherche d’information, la Génération de contenu et l’Analyse de documents*.

Ces 3 grands usages permettent de couvrir beaucoup d’usage métier mais aussi personnel.

1. **Quelles techniques ? L’art du prompting**
2. **La différence entre un assistant et un moteur de recherche**

S’entretenir avec un assistant comme ChatGPT n’a pas grand-chose à voir avec une recherche Google.

* Sur Google, la recherche se fait en utilisant quelques mots clefs pour obtenir +300 000 000 de résultats de sites web déjà créés avant la requête, le tout en 0,30 secondes. Les choix sont alors effectués et la navigation se fait à travers différents sites web, chacun présentant une structure qui lui est propre, à la recherche de la réponse.
* Sur ChatGPT, on entre dans une conversation pour co-construire, avec l'aide de l'assistant, une réponse. Cette réponse n'existe pas au préalable ; elle est littéralement construite au fil de l'échange. Si la demande est mal formulée, la réponse obtenue risque d'être médiocre. La qualité de la réponse dépend en grande partie de la qualité de la demande et de sa formulation. C'est ce qu'on appelle « l'art du prompting ».

1. **Anatomie d’un prompt**

Il est recommandé de préciser 4 informations dans un prompt :

* **L’expertise à embarquer dans la réalisation de la réponse**.

Suivant l’action demandée, il sera pertinent de demander à l’assistant d’endosser un rôle particulier (ex. Responsable marketing ou Responsable RH) afin qu’il puisse bien aborder la problématique avec l’expertise adéquate ! Par défaut, l’assistant risquerait de répondre de façon lambda à une problématique experte.

* **L’action** que doit réaliser l’assistant doit être claire et concise.
* **Le format de sortie** doit être précisé. Lors de la demande d'un résumé d'un document de 200 pages, il est possible d'obtenir différentes interprétations de ce que constitue un résumé. Cela peut varier : s'agit-il d'un résumé en 100 mots, en 2 pages, en 500 mots, ou d'une autre longueur ? Les attentes peuvent différer selon les formats de sortie souhaités.
* **Le contexte**. Le contexte est la partie **la plus importante**. Plus vous fournirez des éléments de contexte, plus l’assistant sera précis et pertinent par rapport à votre demande. Si vous pensez que vous oubliez des éléments de contexte, vous pouvez utiliser la technique de *l’auto-questionnement* pour compléter votre contexte

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. **Le chemin de pensée**

Le **chemin de pensée** est **la technique la plus importante** à connaître et la plus illustrative du fonctionnement d’un assistant.

Lorsqu'on sollicite un assistant, il est important de savoir qu'il dispose d'un temps de réflexion et d'exécution limité, généralement de quelques secondes à deux minutes maximum. Ainsi, si on demande à l'assistant de générer, par exemple, un post LinkedIn sur les bienfaits de la randonnée en entreprise pour renforcer l’equipe, il fera de son mieux dans le temps de réflexion qui lui est imparti. Cependant, étant donné que l'assistant est conçu pour être universel, il ne pourra pas atteindre un niveau d'expertise très élevé dans un laps de temps aussi restreint.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, document, Police

Description générée automatiquement

C’est là que la technique du *chemin de pensée* intervient.

La **technique du *chemin de pensée* (**ou *Chain of thought* en anglais) consiste à **diviser un prompt en plusieurs prompts** afin de faire monter en expertise l’assistant à chaque prompt.

Dans notre exemple, cela donne le découpage suivant :

**Prompt #1 :**

Une image contenant capture d’écran, texte, noir

Description générée automatiquement

Une image contenant texte, capture d’écran, document, lettre

Description générée automatiquement

**Prompt #2 :**

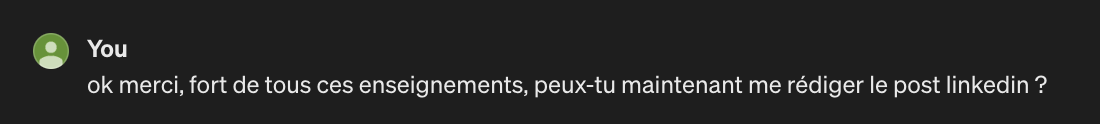
Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, document, Police

Description générée automatiquement

**Prompt #3 :**



Une image contenant texte, capture d’écran, document

Description générée automatiquement

Avec ce découpage, l’assistant va alors prendre plusieurs temps de réflexion (3 au total dans cet exemple) pour monter en compétence sur les différentes expertises sollicitées pour la rédaction du post pour pouvoir finalement produire un post Linkedin qui sera, tant sur la forme que sur le fond, plus performant que lors de la première itération avec un seul prompt :

1. **Les limites des assistants**

Une image contenant texte, capture d’écran, conception

Description générée automatiquementIl est important de savoir que les assistants ne raisonnent pas vraiment comme nous. Ils fonctionnent en copiant des raisonnements qu'ils ont appris pendant leur phase d'apprentissage, c'est-à-dire en lisant beaucoup d'informations sur Internet.

Pour comprendre la différence entre raisonner et copier un raisonnement, prenons l'exemple d'une énigme classique : comment faire traverser un loup, un mouton et une laitue d'une rive à l'autre d'une rivière avec une barque, en respectant trois règles :

* Le loup ne peut pas rester seul avec le mouton,
* Le mouton ne peut pas rester seul avec la laitue,
* La barque ne peut contenir que deux éléments à la fois.

Si tu demandes à un assistant de résoudre cette énigme, il pourra le faire car cette énigme est bien connue et expliquée sur Internet. Mais si tu changes les éléments de l'énigme, par exemple en remplaçant le loup par le Père Fouettard, le mouton par un enfant gourmand et la laitue par un panier de bonbons, l'assistant ne pourra probablement pas trouver la solution. Pourquoi ? Parce que personne n'a jamais posé cette énigme avec ces nouveaux éléments sur Internet, donc l'assistant n'a pas pu apprendre cette version.

En septembre 2024, une nouvelle version d'assistant, appelée o1, a été créée. Elle est peut-être capable de résoudre ce genre d'énigme, mais pour l'instant, ce n'est pas encore le cas.

En résumé, si ton problème utilise un raisonnement connu, l'assistant peut le reproduire. Sinon, il ne pourra pas le résoudre. La technique du chemin de pensée t'aide à réfléchir et à comprendre quelles sont les étapes et les connaissances nécessaires pour résoudre un problème correctement.