Jeudi 03 avril 2025

Aujourd’hui je suis de nouveau en maintenance “coffee break” à la cafétéria en bas du bâtiment de Gecina. Lundi, mardi et mercredi derniers, j’étais en journées de révisions pour avancer sur mes mémoires. Dimanche soir, j’ai préparé le programme de mes 3 jours dans l’espoir d’avancer un maximum sur le développement d’agent et la rédaction de mes mémoires (problématique, plan de rédaction, etc…). Cependant rien ne s’est passé comme prévu : lors de la première matinée j’ai cherché à corriger les problèmes liés à mon agent IA de rédaction de mémoire professionnel (rapport d’alternance), et pour accélérer le développement de cet agent, m’est venu à l’esprit de coder un MCP, Model Context Protocol, afin de remplacer claude-code que j'utilisais pour débugger mon code et corriger les erreurs de l’agent IA de rédaction.

J’ai donc effectué un développement en cascade : j’ai créé un nouveau repository, au quel j’ai connecté claude-code, au sein duquel j’ai fourni la documentation officielle de développement de MCP fournie par Anthropic, ainsi que la documentation de l’API Deepseek, afin qu’il puisse utilisait ces informations pour développer un MCP capable de débugger du code en local, lorsque connecté à un repo en local (ex: VS code/ Cursor).  
  
Cette démarche était dans le but de pouvoir se passer de claude-code, qui bien que révolutionnaire est bien trop coûteux, et que des APIs comme celle de Deepseek pourraient parfaitement répondre à mes besoins, pour une fraction du prix.

Cependant pour une raison que j’ignore, claude-code n’a pas réussi à développer cet outil, j’ai eu de très bref résultat mais le problème majeur se trouvait dans la réécriture des fichiers. Le workflow fonctionne de la manière suivante : je requête le MCP Deepseek directement en local dans un terminal ouvert sur mon projet de développement, ici l’agent de rédaction, je pointe une erreur visible sur l’interface de l’agent, premièrement l’erreur est traitée, comme une interaction LLM classique mais via le terminal, et lorsque l’erreur est identifié je demande au MCP d’intégrer les modifications qui pourraient corriger l’erreur directement sur le fichier responsable (ex : main.py). Le problème étant que le MCP n’était pas capable de réécrire le fichier en entier, et j’ignore la raison. Plusieurs suspicions : un mauvais paramétrage de la fenêtre de contexte, de la sécurité du fichier node.js de claude desktop, ou simplement un manque d’accuracy dans le développement. J’ai même suspecté que claude-code soit bridé au sujet du développement d’autres MCP décodeur / débuggeur, qui le placerait dans une mauvaise position compétitive, ce qui semble logic, mais shady de la part d’Anthropic et cette entreprise à plusieurs fois fait preuve d’une démarche à approche philantropic sur certain sujet d’IA, notamment concernant l’interprétabilité et l’alignement de l’IA, sujet qui sépare les doomers (ceux qui pensent que nous devrions ralentir le développement de l’IA dans le but de sécuriser et comprendre son utilisation) et les accélérationistes (qui eux veulent à tout prix développer l’IA le plus rapidement possible afin de générer divers bénéfices, monétaire ou médicaux