Aoyan Sarkar

Limitations of Generative AI

While Generative AI is very powerful, it is not perfect, and there are several key limitations that are stopping AI from replacing most humans from day-to-day jobs. The primary limitation of Generative AI is the tendency to hallucinate, or start generating text that is objectively not true. The larger the prompt seems to be, the higher the tendency there is for the AI to start hallucinating. Alternatively, giving AI more text than it can handle will usually cause it to “overflow” and start generating random text. The solution is to make more prompts that are smaller in scope, which stops it from getting overwhelmed as a single large prompt does.

Another key limitation is the inability for current Generative AI models to learn from live data without providing it as an input to a prompt. Unless I provide it context for an event, such as copy-pasting portions of a news article into the prompt, it does not know what happened after the data cutoff. For the lab, it would be impossible to generate a good “fake news article” about RPI’s new quantum computer just by prompting it, so I had to provide the input of the title of a news article on the topic. Related to this limitation is the inability for current AI models to be able to reliably browse the Internet, which means that currently humans need to copy-paste contents of a link instead of providing just the link.

A minor limitation is that AI models are unable to generate real URLs. They can generate URLs that seem plausibly correct but are incorrect. This means that for this lab, I had to give the URL in the prompt and ask it to echo it back. The final limitation is that there is no easy way to delete partial prompts from a ChatGPT history log, so if one of my prompts are erroneous, the error will carry over unless I explicitly make a prompt that specifically fixes the error that I made.