* Large language model (LLM) is a type of artificial intelligence (AI) program that can recognize and generate text, among other tasks.
* LLMs are trained on huge sets of data — hence the name "large."
* LLMs are built on machine learning: specifically, a type of neural network called a transformer model.
* LLM is a computer program that has been fed enough examples to be able to recognize and interpret human language or other types of complex data.
* Many LLMs are trained on data that has been gathered from the Internet — thousands or millions of gigabytes' worth of text. But the quality of the samples impacts how well LLMs will learn natural language, so an LLM's programmers may use a more organized data set.
* LLMs use a type of machine learning called deep learning in order to understand how characters, words, and sentences function together.
* Deep learning involves the probabilistic analysis of unstructured data, which eventually enables the deep learning model to recognize distinctions between pieces of content without human intervention.
* LLMs are then further trained via tuning: they are fine-tuned or prompt-tuned to the particular task that the programmer wants them to do, such as interpreting questions and generating responses, or translating text from one language to another.
* LLMs can be trained to do a number of tasks. One of the most well-known uses is their application as generative AI: when given a prompt or asked a question, they can produce text in reply.
* The publicly available LLM ChatGPT, for instance, can generate essays, poems, and other textual forms in response to user inputs.
* Any large, complex data set can be used to train LLMs, including programming languages.
* Some LLMs can help programmers write code.
* They can write functions upon request — or, given some code as a starting point, they can finish writing a program. LLMs may also be used in:

Sentiment analysis

DNA research

Customer service

Chatbots

Online search

* Examples of real-world LLMs include ChatGPT (from OpenAI), Bard (Google), Llama (Meta), and Bing Chat (Microsoft).
* GitHub's Copilot is another example, but for coding instead of natural human language.
* A main advantage of LLMs is their ability to respond to unpredictable queries.
* LLM can respond to natural human language and use data analysis to answer an unstructured question or prompt in a way that makes sense.
* LLMs can only be as reliable as the data they ingest. If fed false information, they will give false information in response to user queries.
* LLMs also sometimes "hallucinate": they create fake information when they are unable to produce an accurate answer. For example, in 2022 news outlet Fast Company asked ChatGPT about the company Tesla's previous financial quarter; while ChatGPT provided a coherent news article in response, much of the information within was invented.
* In terms of security, user-facing applications based on LLMs are as prone to bugs as any other application.
* LLMs can also be manipulated via malicious inputs to provide certain types of responses over others — including responses that are dangerous or unethical.
* One of the security problems with LLMs is that users may upload secure, confidential data into them in order to increase their own productivity. But LLMs use the inputs they receive to further train their models, and they are not designed to be secure vaults; they may expose confidential data in response to queries from other users.