気になるこの用語 第57回

消費生活相談の周辺用語を取り上げ、やさしく解説します。

嶋 是一　Shima Yoshikazu
NPO法人 日本Androidの会 理事長
MCPC 人材育成委員会 モバイルシステム技術検定プロジェクト 副主査
モバイル技術の普及促進活動として、KDDIテクノロジー CTOの任とともに、執筆、コンソーシアム、コミュニティー、大学非常勤講師などの活動に取り組む。趣味はストリートピアノ

チャットボット(2) プロンプト

ChatGPTを代表とする大規模言語モデル(LLM)を活用したチャットボットは、進化が著しい状況です。「プロンプト」を与えると、その指示に沿った動作を行う振る舞いが、日本の未来に有利に働く可能性があることについて紹介します。

はじめに

利用者が入力した文字に対して文章を自動生成し、応答を返してくれるサービスをチャットボットサービスと呼びます。最近は、生成AIの技術の1つである大規模言語モデル(LLM)を活用したチャットボットが利用されています。その代表的なサービスが「ChatGPT」です。

LLMは、世の中にあるさまざまな言葉を学習して作り上げられる情報の塊(モデル)です。このLLMに言葉を入力すると、学習している内容から最も確からしい「次に続く言葉」が選び出されます。ここで選ばれた言葉に続く言葉も、繰り返し選択し続けることで文章が生成され、これが返事として作成されます。

このLLMを作り出すには、「事前学習」と「ファインチューニング」の2つの学習が必要です。事前学習は、世の中のよろず事を片っ端から覚えて記憶脳を作るための学習です。一方、ファインチューニングは、応答に含める情報の選び方や応答時の振る舞い方など、主に「動作を習得」するための学習です。この2つの学習によって蓄えた知識を使い、「入力に対して自動応答する」という振る舞いを指示して、LLMをチャットボットとして動作させることができます。

創発現象の活用

LLMはあくまでも、学習した内容に従って、次に選ばれる文字を推測して並べているに過ぎません。事前学習で学習していない知識による応答文を生み出すことはできませんし、ファインチューニングで教えた挙動以外の動作を行うことは、基本的にありません。そのためLLMは、決められた内容だけに応答するルールベースのチャットボット(前回、「チャットボット(1)」参照)の機能を拡張する程度しか役に立たない、と考えられていました。ところが、ここ数年でこの状況が変わりました。

元々LLMは学習に含まれていない情報を入力すると、あり得ない情報を勝手に生成してしまう問題(ハルシエーションといいます)がありました。これを軽減する(知らないことを少なくする)ため、できるだけたくさんの情報を集めて、LLMに学習させる取組が継続されています。

そしてある時、学習するデータの量とそれを学習させるために使う計算量がある一定値を超えた所で「創発現象(Emergent Phenomena)」と呼ばれる挙動が見られるようになったのです。

この現象は、LLMが本来知らないはずの動作(ファインチューニングで学習させていない動作)なのに、新しい動作を指示する言葉を入力すると、あたかもその指示に従って処理したかのような振る舞いを行うというものです。まるで、指示された内容を今、理解し、その指示に従ったかのようです。まさにLLM自身が「理解する振る舞い」を得たような挙動を示し始めたのです。現在ChatGPTなどで話題になっているのは、この創発現象の応用により「人間の自由な指示で、(本来学習していないはずの)作業を完遂させる」ところにあります。

プロンプト

LLMへ入力する、動作の指示を含んだ入力文を**プロンプト**と呼びます。

LLMに対して最初に「次の文を翻訳して」とプロンプトを書くだけで、次の行から記載する外国語を翻訳してくれます。「要約をして」と書くだけで、文章のまとめを提供してくれます。「ブログの記事を作成して」と書くだけで、ブログの原稿を自動生成してくれます（ただし興味を引く文章の生成はとても難しいですが）。

通常このようなサービスは、ソースコードをプログラム言語（C言語やPythonなど）を使って書く必要がありました。ところが、LLMでは、プログラムの言語で書く必要がなく、日本語で「プロンプト」として指示を書くだけで、さまざまな内容を実行させることができます。まるで玉手箱のようなサービスとなっています。

ただ、単純な作業ならばシンプルなプロンプトでも期待どおりに動作しますが、少しでも複雑な作業となると、詳細に動作の指示を行わないと期待どおりに動きません。それらの動作指示すべてを「プロンプト」に含める必要から、複雑なプロンプトとなります。

プロンプトはアプリケーションに？

パーソナルコンピュータでは、WindowsなどのOS上にアプリケーション・ソフトウェア（例えば、WordやGoogle Chromeなど）をインストールしてさまざまな目的に利用します。また、スマートフォンでは、AndroidやiOSというOS上にアプリをインストールして、さまざまな機能を利用します。インターネット上のサービスは、AWS（Amazon Web Services）やGCP（Google Cloud Platform）といったクラウド開発基盤上でクラウド・アプリケーションとして開発され、提供します。

OSのような開発基盤上で、動作を作り出すしくみをアプリケーションと呼ぶならば、プロンプトは、「自然言語基盤上で動作を作り出せるアプリケーション」と考えられるようになるかもしれません。現状は、プロンプトに対してLLMが期待どおりに動作できる精度がまだまだ低いため、アプリケーションとして扱うには実用的ではありません。しかし、将来精度が向上するだろうこと、またプログラム言語ではなく自然言語（人間が使う言葉）で動作を定義（プログラム）できることを考えると、広くLLMのアプリケーションが普及することも夢物語ではないと感じます。

生成系AIと日本の未来

万能のように思えるChatGPTですが、精度はまだまだ十分ではありません。OpenAI社の論文によると、最新LLMバージョンのGPT-4を用いても、人間の期待する回答の6割ほどしか、応答の生成ができていないと報告されています。3回に1回は期待どおりの動作ではないため、ChatGPTが平然とウソをつくような振る舞いに目が行ってしまいます。そのため、OpenAI社は実用に耐え得る精度を獲得するため、改善を継続的に続けています。

そうしたなかで、世界から日本の生成系AIが注目されていることを、前回紹介しました。ChatGPTの開発元であるOpenAI社の開発拠点を日本にも設ける話や、GoogleのBardが他国言語を差し置いて日本語に対応するなど、日本への注目が集まっています。

英語に次いで日本語が優先的に改善され続けるとなれば、世界的にみても、いち早く高精度のチャットボットを自国語で活用できる稀有（けう）な国となります。例えば、人手だけに頼ることなく、24時間さまざまな所から消費者に対して情報やアドバイスを提供できる国になれるかもしれません。

ほかの国々に先んじて、精度が向上した実用的なLLMを、国民の多くが活用しやすい環境となること。それは競争力のある日本の未来につながるはずです。