近未来金融システム創造プログラム第 10 回講義レポート

第 10 回目となる本日は、東京大学大学院工学系研究科教授の松尾豊様より「金融と技術（各論Ⅱ） ディープラーニング」という題目で講義が行われた。生成 AI の現状、国内外の議論や政治の動き、各企業や組織がどう動いていくべきかについてお話しいただいた。

生成 AI の現状

AI は 1956 年にスタートした分野で、60 年の間にブームと冬の時代を繰り返している。そして、2010 年代に第三次 AI ブームに入る。第三次 AI ブームの中心はディープラーニングで、この背景にはデータ量の増加、マシンパワーの向上がある。

昨今注目を集める生成 AI もディープラーニングの一つである。AI と一口に言っても広い分野であり、その中に機械学習、またその中にディープラーニングが含まれている。

生成 AI には画像を生成する拡散モデルと自然言語を扱う大規模言語モデル（LLM）がある。ディープラーニングは、人間の脳の神経回路を模したニューラルネットワークを用いた手法の総称である。各ニューロンの重み和が一定以上であれば発火する。例えば、画像のピクセルの値でクラス分類をするとき、該当物にあたるニューロンが発火するか否かで出力する。出力が間違っている場合、出力側から入力側に誤差を戻す誤差逆伝播で学習をする。

2018 年から自然言語処理の精度が急激に向上した。この鍵となった 2 つの技術が「トランスフォーマー」と「自己教師あり学習」である。

「トランスフォーマー」は、入ってくる情報に応じてニューラルネットワークの中のどこの情報をどのように使うかを決める技術である。文章が会話文なのか説明文なのか等によって柔軟に学習できる。

「自己教師あり学習」は、文に対して前の部分から次の単語を次々と予測していく技術である。これをすることでトピックのつながりや文法、因果関係、知識まで学習できる。「自己教師あり学習」を行ってから翻訳や対話に適用させると精度が上がる。

パラメータの数を大きくするほどテスト誤差が下がる、つまり性能が上がる。データ量、モデルの大きさ、計算資源ともに大きければ大きいほど精度が上がることが分かり、大規模言語モデル（LLM）の研究開発が進んでいる。

大規模言語モデル（LLM）は従来の AI と何が違うのか。従来は翻訳モデル、要約モデル、対話モデルとそれぞれ分けてモデルを作成していた。一方で、大規模言語モデル（LLM）は、大量のデータで事前学習を行い汎用の LLM を作成し、事後学習で翻訳、要約、対話に適応させている。

大規模言語モデル（LLM）は言語空間だけで学習しており、実世界の情報に接地して学習してはいない。人工知能も人間と同様に、経験から効率的に外界の常識を学び、想像でき

るようになることが今後の発展の肝である。その基幹技術が世界モデルである。世界モデルとは、経験によって学習される脳の中のシミュレータ、つまり人間の「想像」にあたる部分である。例えば、グラスを落としたら割れるだろうといった現在から未来を予測する能力のことである。自己教師あり学習で因果関係を学習していく。

日本国内の議論や政策分野での動き、世界の動き

日本政府は ChatGPT を始めとする生成 AI に対する原則や方針を示すために急ピッチで様々な議論を実施している。昨年 11 月 30 日に ChatGPT が発表され、その約 2 か月後の 2 月 3 日には自民党により「AI の進化と実装に関するプロジェクトチーム」が発足した。

また、5 月 11 日に松尾教授が座長を務める政府の AI 戦略会議で議論が開始され、5 月 26 日に は「AI に関する暫定的な論点整理」が公表された。リスクへの対応、AI の利用、AI 開発力の 3 分野において、それぞれ論点が整理されている。

G7 においても「責任ある AI(人工知能)」の活用に向けた共同声明が採択され、今後日本が世界の標準ルールを取りまとめていくことが期待されている。各国において、欧州は非常に強い AI 規制の案を出す一方、米国は企業の自主規制としてイノベーションを重視している。

各企業や組織がどう動くべきか

企業においては、主に議事録の要約や情報収集のサポート・プログラミング、書類などの文書生成に ChatGPT が活用される事例が多い。

三豊市は松尾研究室と共同で ChatGPT を利用したゴミ出し案内を作成し、令和 5 年 6 月 1 日から、ChatGPT を利用した「ごみ出し案内」の実証実験を実施した。市長主導で初期の検討から約 1 ヶ月で実証実験開始となった。

自治体 HP にあるゴミ分別の説明ページがプロンプトに入っており ChatGPT が該当ページを参照しながら回答する仕組みとなっている。

LLM 活用の段階として 3 つのステップを踏んでいくことが考えられる。ステップ 1 では Chatbot を導入し執筆の支援やブレストなどを行う。ステップ 2 では組織専用 GPT を作成し、組織内文書を検索可能にし、組織内の文脈を踏まえて答えられるようにする。ステップ 3 では LLM を使った DX・業務改革を行い、本格的に利用するための開発、業務フローを変える。

今後の見通し

世界では、数千億から数兆パラメータのモデルを開発しているため日本の百億パラメー

タはそれより二桁少ない。LLM の研究開発は数兆円投資の戦いであるため、医療、金融、製造といった数十兆円の売上がある大きな業界に貢献できるようなものを開発し、利用・開発とリスクの対応バランスを取っていなかなければならない。日本全体として、大規模な学習データが必要であり、それをもとに学習してモデルを作成する。そのためには日本語データの拡充が求められる。また、大きいモデルを作るには実際にトライするしかなく、そのためにはかつてないほどのボリュームの計算資源（GPU）の確保が必要となる。物量戦争の時代に入ったと言ってもよく、現状、第三次 AI ブームから冬の時代を経ることなく、次の第四次 AI ブームに入ったと言っても過言ではない程のスピード感を持っている。

Q&A

Q1. 世界モデルについてブレイクスルーが起きないボトルネックは何か。
A1. 世界モデルはトランスフォーマーを使って自己教師ありで学習する手法のため、ブレイクスルーが起きておかしくない。大規模言語モデル（LLM）ではトークン数の制限があり、一定の範囲を超えると前のことを忘れてしまうことが課題である。

Q2. 海外の企業と比べると日本勢が確保している計算資源が少ない理由は何か。
A2. 百億パラメータを扱うのに必要な GPU 確保のための数千万から数億円の費用は大企業の一部署の部門長決裁で捻出することができる。しかし、一兆パラメータを作るとなると数十億から数百億円でも足りず、一般的な日本企業の決算では下りないことが理由である。政府の介入による資源の確保が必要である。

Q3. パラメータ数を増やして精度を上げることは、どこかの段階で頭打ちになるのか。
A3. データ量がボトルネックになり、恐らく数千から数兆パラメータで止まる。世間にはインターネット上に公開されているものより、インターネットに公開しないプライベートな情報の方が多いため、その情報を上手く学習できれば性能が上がる。プライベートな情報を学習できるようになると、より大きなモデルを作ることができる。

Q4. 仕事で機械学習を使用しているが、ディープラーニングまで精度を上げられていない。それが使われる未来が近くにあるのか。
A4. 人と AI が協調できる場面を探していくことが重要で、AI が人の作業を軽減し、段階的に全自動になることも出てくる。

Q5. 規模が大きくなるほど精度が上がる LLM は人口の多い中国やインドが開発に有利か。
A5. 中国はレベルが高い。インドは人口が多いが生成 AI に対する取り組みが進んでいるわけではない。世界的に見て開発が進んでいるのはアメリカの企業である。

Q6. 長年各国の企業が研究している中で、OpenAI の生成 AI がブレイクした要因は何か。
A6. OpenAI はスタートアップであるため世間に成果を公表したが、Google など大企業は、分かりやすい形で生成 AI を世間に公表する必要がなく、検索エンジンやソーシャルメディアにこっそり使っていけば良いと考えていたことが要因である。大企業は見えない形で研究を進めて行けば良かったが、OpenAI が世間に公表したことで走らざるを得なくなった。スタートアップの OpenAI は大逃げの状況である。企業規模を鑑みれば Google や Meta に差を詰められて逆転されるだろう。

Q7. プロンプトエンジニアリングは無くなるのか否か。また、プロンプトの工夫の余地はあるか。
A7. OpenAI の中には無くなると言っている人もいるが、自分は無くならないと思っていて、それに関しては両方の意見がある。現状の ChatGPT は対話の段階でビジネス用には作られておらず、ここから産業の要望に応じて形を変えていき、何年もかけて大きなビジネスになっていく。それにあたりプロンプトは調整され工夫されていく。

Q8. 情報漏洩の危険性はあるのか。
A8. インフラとなるものは法律で決められている場合もあるが、不文律で社会的信頼によって守られている部分もある。

Q9. 機械学習でブレイクスルーが起きるか。
A9. 人工知能は人間の知能にはまだ遠いため、いくつかのブレイクスルーが起こるだろう。LLM と人間の脳では仕組みが違うため、人間の知能を実現するためには課題があり研究の余地がある。

Q10. AI の発達でどのような未来が待っているか。
A10. ロボットがきちんと動くようになる。ロボットの学習能力や運動能力が上がれば活用の幅が広がる。