量子コンピュータに関する話題提供メモ　　2018/01/11　上崎

本日の話題、量子コンピュータに関するメモです。ただ、その理解度は、前回の AI 以下です。ご容赦ください。付録に前回、話したアルファ碁の最新バージョン（ゼロ）の話も載せています。

1)ちょっと現下（古典）のコンピュータ

①0-1 の単純な世界

現下（量子との対比では古典）のコンピュータは、Turing によってその動作原理が考案され、一般に「Turing Machine」と呼ばれている原理に基づくもの。

その動作原理は、読み書きできるテープ/読み書きできるヘッド/有限オートマトン（ふるまいのモデル)。

計算の基本単位を bit（binary unit)。それぞれが 0 か 1 の状態をとることにより 2 進数で数を保持、演算を行う。またこの bit は同時に 1 つの状態のみを表す。

1001+11=1100　　1101+101＝？

②スーパーコンピュータ

大規模で高度な科学技術計算をきわめて高速で行え、高性能の CPU を複数つなげて高速化を実現している。

CPU にはスカラー型（汎用性が高い）とベクトル型（高性能計算に特化）がある。

世界ランク(2017)/1，2 位は中国(93.01 ペタ(10^{15})フロップス、毎秒 1000 兆回の浮動小数点演算)。日本は 4 位の暁光（PEZY-SC2、例の斎藤なんとかさん、海洋研究開発機構横浜研究所)。

2)量子コンピュータ

ファインマン（アメリカのノーベル物理学者、1918～1988、ノイマンと同時期）が「量子力学的コンピュータを使えば任意の物理系を効率よくシミュレートできるのではないか」と考えたのが最初ではないかと言われている。

ところが効率よく計算できるアルゴリズムが存在しなかったため、しばらく量子コンピュータの研究は下火になっていた。

量子コンピュータを一躍世に広めたのは Peter　Shor の因数分解アルゴリズム（1994 年、私には全く理解できません)。元々桁の大きい整数の因数分解は、現行の古典コンピュータの苦手とするところで、Turing　Mchine で計算できることは示されているが、計算に膨大な時間が掛かる。

①動作原理

量子は、原子よりも小さいミクロの世界を説明する理論。

ミクロのモノは粒の性質と波の性質を持っており、ミクロの世界では、あらゆる物質は「状態の重ね合わせ」の現象がおこる。

動作の原理はこの「状態の重ね合わせ」がポイント。

「状態の重ね合わせ」とは同時に 2 つ以上の状態を表すことができる、直感的にいうとある状態が 1 でもあり、2 でもあり、3 でもあり、4 でもあるという感じで、確率的・・なので、量子コンピュータでは観測するごとに結果が違ってきたりする。

違う言い方をすると、ミクロの世界では、例えば一つの箱に一個の電子を入れて仕切ると、左右 50%づつの確率で「どちらにもある」のです(正直私にはこれも良く分かりませんが～～)。でも仕切った結果は、勿論左右どちらかにある。

要は、量子の世界では、観測のたびに変化する、その性質を利用する？。

また古典の Bit に対して、**量子ビット**(Quantum bit)が量子情報の最小単位である（興味があれば、各自学習してください。済みません、私の理解を超えています。|0〉,|1〉という状態以外に、|0〉,|1〉を重ね合わせた状態も保持できる。ブラ・ケット記法）

②量子コンピュータの方式

量子ゲート┬──スピン量子ビット型（IBM,インテル）
　　└──量子ビット型（IBM,グーグル）

量子イジングマシン┬──量子アニーリング型（D Wave　System、グーグル）
　　└──レーザネットワーク型（NTT）

因みにゲート方式は 0，1 の演算原理を基に、並列（重ね合わせを）で処理する方式。

③量子コンピュータの利点

状態の重ね合わせが実現できることによって、簡単にいうと「ある計算が効率よくできるということにつきる。

例えば、上記の因数分解の計算を実用的な時間で解くことができる。言い換えると現在使われている暗号系は簡単に解読されることが予想される。

④現状と課題など(IT Pro など)

IBM：

2016 年 5 月、量子ビット 5 個からなる量子コンピュータを操作できるクラウドサービス「IBM Quantum　Experience」を無償提供して話題を呼んだ。公開から約 1 年で 100 か国超の 4 万 5000 人が使い、約 30 万回の実験をこなした。

2017 年 5 月には量子ビット数を 16 個に増やした量子コンピュータのベータ公開を始め、17 個の「量子ビット」を備えたプロセッサを試作したとも発表した。同社初となる商用の量子コンピュータ用プロセッサの試作品となる。量子コンピュータの商用化へ本気で取り組み始めた。

また IBM Research の研究グループも 2016 年 8 月に 100 量子ビット機が近い将来に実現するとの論文を発表しているし、「近い将来」を 5 年以内と仮定すれば、2021 年までには 100 量子ビットを実現でき、その計算能力は、単純計算でスパコンの 9000 兆倍。

米 Gogle：

人工知能（AI）の演算を高速化できるとみて開発を進めている。

その他インテル、マイクロソフトなども積極的に取り組んでいる。

応用面としては、ジョン・マルティニス教授（量子ゲート方式の権威として知られる米カリフォルニア大学サンタバーバラ校）は 2016 年 6 月、分子の性質をシミュレーションする「量子シミュレーション」と呼ぶアルゴリズムであれば、50 量子ビットの量子コンピュータでスパコンの性能をしのぐ「量子の超越性」を実証できると学会で発表している。

ただ、「産業的な貢献があるかは、正直言って分からない」（1999 年に初めて超電導回路の量子ビットを作った東京大学の中村泰信教授）。

また量子コンピュータが扱う問題は「人類が初めて計算する問題であり、どんな使い道があるかが見えてくるのはこれから」（西森教授）。量子ゲート方式の計算能力はアルゴリズム次第だ。IBM が自社の量子コンピュータをクラウドに公開したのも「研究者を増やして産業応用できるアルゴリズムの発明を促す狙いがありそうだ」（中村教授）。

アルゴリズムの発明は「前触れもなく突然訪れる」。そう話す東京大学の小芦雅斗教授は、2014 年に新たな量子暗号通信のアルゴリズムを発表した張本人。30 年間議論もされなかった通信方式を「偶然見つけた」（小芦教授）という。新しいアルゴリズムが見つかれば、明日にも量子コンピュータが産業利用できるかもしれない。

このほか、シリコンバレーにある航空宇宙局の「エイムズ研究センタ」で開催された Q2B Conference では、ドイツの Volkswagen（VW）や米 Goldman Sachs（GS）、欧州 Airbus などが研究に取り組んでいる。VW は実機を使った検証やアルゴリズムの開発を進めている。カナダの D-Wave System での検証結果を発表したり、グーグルと量子コンピュータ用のアルゴリズム開発など、GS はモンテカルロシミュレーション（金融機関のリスク計算に欠かせない）への適用（現状は大規模なスパコンシステムを利用）を、AirBus は航空機設計のシミュレーションへの適用（現状スパコン）を試行している。

⑤整理してみて

良く分かりませんでした。多分並列処理が可能、そして量子の世界からさらに精神エネルギー（今科学的に理解できない）的な世界の解明につながるような気がします。

【付録】

アルファ碁ゼロ

人間の棋譜は学ばず、AI どうしが対局を繰り返して上達し、独自の[定石]を見つけたという（以前のバージョンは[定石]を棋譜情報から学んだ）。碁のルールだけから始めた強化学習で、韓国の李九段などを破ったバージョンにも圧勝した（2017/10/19）。

量子暗号化

誰かが量子を観察した時点で別のものに変貌するため、他者によって観察されたかどうかがすぐわかる。この原理を利用して暗号鍵を共有しようとするものである。

現在の暗号化技術の基本は、送りたいデータに数学的な処理を行うことで複雑で判読できない別のデータに書き換えるというもの。