計算限界解明の意義--現代の鳥瞰

Significance of Exploring Limit of Computation - A Modern Overview

徳山 豪

１．検証と求解：智と計算の融合に向けて

智とは何かという問題は、ギリシア哲学からの大きな学究目的である。絶対智の典型は数学であり、『幾何学を知らざる者はこの門をくぐるべからず』というプラトンの警句に代表される。古代ギリシアの計算はコンパスと定規を用いた作図で行われ、計算可能性を問う三大作図問題（立方体倍積問題、円積問題、角の三等分）は、無理数、複素数、三角関数、極限などの概念や、方程式や数学記号、座標幾何などの手法を生み、2 千年以上、科学全般を先導した。一方で、絶対智である数学に比べると人間の持つ智はより複雑であり、深い哲学的対象である。

さて、現代の計算は、計算機にプログラミングされたアルゴリズムで行い、人間が記録し活用する情報はすべて基本的に計算機で扱うことができる。すなわち、ギリシア時代に区別された絶対智と人間生活における智が、情報処理に融合され、互いに近いものになっている。

では、人間の智はどこまで計算機によって代替できるのだろうか。また、智と計算を融合した、未来の計算モデルや計算手法はどのようなものだろうか。この哲学的かつ現実的な問いに、数理的にチャレンジするのが計算理論、より限定すると計算限界の解明であり、古代ギリシアの三大作図問題と同様に学術の原動力である。

計算機科学分野で名高いチューリング賞に加えて、1993 年より、過去 10 年の最も優れた計算理論の研究成果にゲーデル賞が毎年 1 件贈られている。その受賞の歴史を紹介しながら、計算限界の解明の意義を考察しよう。

紹介する技法の発想は自然で人間的であり、現実の情報社会の未来を導く。賞に名を冠する A. Turing と K. Gödel がそうだったように、計算限界の解明は情報社会の水先案内人であり、そこに最大の意義がある。

本稿は鳥瞰を目的とし、専門的な厳密性を犠牲にした記述を含む。教科書(文献(1))や技術解説(文献(2))、また登場人物については Web 等を併せて参照されたい。

1.1 問題の難しさと計算量

アルゴリズムを設計して問題を解くときには、計算量の解析という作業がある。「計算機実験はどんな具合？」「昨日から計算中です」「こら、計算量の解析はやったの？」というような会話は日常茶飯事である。アルゴリズムの計算量が例えば $O(n^2)$であるとは、計算時間の増加が、n^2という入力サイズ n の多項式関数に比例する形以下で抑えられるという事であり、このようなときに多項式時間アルゴリズムと呼び、クラス P の問題であると言う。多項式時間でない、例えば指数時間の計算量は問題のサイズを増やすと爆発的に膨張するので、極力避けないといけない。ところが残念なことに、重要問題でも多項式時間アルゴリズムが知られていないものが多い。

２．計算限界の解明の意義とその波及効果

2.1 NP 問題：実社会で解けそうな問題

まず、人間が工夫して解決している多くの現実問題の特徴を捉えてみよう。ある事実が正しいことを示す作業を検証と呼ぶ。検証ができないと、その事実の正当性を理解させることができない。実験や人間による検証も世の中にはあるが、ここでは、数理的な検証を考えよう。

判定問題と呼ばれる、Yes－No を答える問題に特化する。解が Yes である時に、それを多項式時間で検証できる証拠が存在する問題を NP 問題(非決定的多項式時間可解問題)と呼び、多くの現実の重要問題を含む。たとえば、近年流行している数独パズルを考えよう。「与えられた数独問題に解があるか？」という問題は NP 問題であり、数独の解（数の埋まった表）を証拠として与えられれば、その検証は容易である。

人間の実社会では、検証が容易な課題は、工夫したり熟練したりすると達成できることが多い。つまり、NP 問題は、「人間が智恵を使って解く」問題の典型である。

残念なことに、NP 問題の最悪ケースの計算量は一般

には指数時間かもしれないのが現状で、本質的に多項式時間アルゴリズムが設計できないNP問題があるだろうと予想される。これが計算理論の最大のチャレンジであるP≠NP予想であり、その解決は研究者の夢である。

夢にトライする一方で、NP という計算クラスを考えることの現実社会的な意義はなんだろうか？ NP 問題は一言でいうと、「運よく解を発見すれば、それを検証して解ける」問題である。したがって、バックトラック法や遺伝アルゴリズムなどの『発見的解法（ヒューリスティクス）』と呼ばれる手法が通用する。ＮＰというモデルがあって、発見的解法の意味が明確になり、実用的に優れた手法が開発されるのである。

2.2 難問を解く計算モデルとその実現

では、NP 問題より難しそうな問題はどうだろうか？ たとえば将棋では、「この局面は先手が優勢です」とプロ棋士が解説しても、膨大にある組合せを全部列挙しない限り、厳密な証拠にはならず、検証することが難しい。将棋や囲碁(ルールに付加条件が必要だが)のような問題をモデル化したものが PSPACE(多項式空間クラス）であり、PSPACE は NP を含むクラスである。PSPACE の問題は指数時間で解けることが知られており、指数時間で解ける問題のクラス EXP に含まれる。つまり、P⊂NP⊂PSPACE⊂EXP である。この 4 つはそれぞれ異なると予想されているが、現在判明しているのは P≠EXP だけである。

さて、通常のモデルのアルゴリズムや発見的解法では PSPACE の問題に太刀打ちできない。これを克服するために、人間の智と計算機の計算力を融合させた新しいモデル作りがされている。乱択計算、通信複雑度、量子計算など豊かな新分野を開拓した、2000 年のチューリング賞受賞者 A. C. Yao の思想に倣い、コミュニケーションと乱択（ランダム性の利用）を通して見てみよう。

2.2.1 対話証明：教師の力とコミュニケーション

人は良い教師に導かれて成長する。この時に大切なのは、教師の答えを盲信するのではなく、自分で検証して納得する事である。一方で、教師の方では、自分が正しいことを相手に納得させるには工夫が必要である。

そのような人間生活を模倣した計算モデルが、L. Babai らによって提案された対話証明である（1993 年ゲーデル賞）。IP(Interactive Proof)と呼ばれるモデルでは、全ての問題を解けるふりをする先生(証明者と呼ぶ）と、多項式時間の計算能力を持つ生徒(検証者）がおり、問題に対して、答えが Yes か No かを先生が答える。生徒はその答えが正解か、あるいは先生が嘘をついているかを対話により検証するのである。

A. Shamir（暗号理論の業績で 2002 年チューリング賞）によって、IP は PSPACE 問題を解くことが示され、さらに 2 名の証明者に質問できる MIP モデルでは、NEXP という、EXP を超えて困難な問題群まで解いてしまうことが判っている。

本稿では厳密な議論はできないが、問題を対話で楽に解く例を紹介しよう。2 組のジグソーパズルセット A と B がある。この 2 組の完成図が微妙に異なると、あなたより百倍速くパズルを解く先生が言うのだが、嘘でないことを確かめたい。でも、楽しみが減るので、完成図は見たくない。どうすればいいだろうか？ あなたは、ランダムにどちらかのセットを取って、パズルピースをかき混ぜて「これは A ですか B ですか？」と先生に聞けばよい。もしも同じセットなら、あなたがどちらを選んだのか先生には判断がつかなくて返答に困るだろう。何回か質問して毎回正解なら、信用できる。

現実に対話証明のシステムを利用するには、証明者をシミュレートする仕組みが必要である。少し比喩的だが、人間の智の財産である膨大な将棋記譜データを使った、将棋の証明者構築を例に説明しよう。証明者は、「評価関数」という数値関数と、計算機の計算力をフルに生かした深い探索を融合した、一種の計算回路で表現される。評価関数は記譜データから機械学習で求めて自動補正し、探索の深さが評価関数の力の弱さを補う役割を受け持つ。検証者は不安なときには、『もう少しここの先を調べて』と要求できる。さらに、複数のシステムの合議は能力をより高める。理論的なモデルと、専門棋士と勝負している現実のソフトウエアをそのまま比べるのは妥当ではないが、思想は共通しており、合議手法である AdaBoost 法は 2003 年ゲーデル賞、機械学習の理論基盤を築いた L. Valiant は 2010 年のチューリング賞を受けている。

更に乱択の力を示したのが戸田誠之助の戸田理論であり、PSPACE に近い PH というクラスの問題が、PP という理想的な乱択モデルを使って多項式ステップで解けることを示し、1998 年にゲーデル賞を受けた。この研究は次節の PCP 理論につながる新時代の幕開けだったのだが、最近では、モンテカルロ法という、戸田理論の思想を髣髴させる仕組みが囲碁のプログラムで利用される。これは実用化の難しい PP モデルを、膨大な数の実戦シミュレーションを用いて模倣するものあり、計算機パワーの向上で初めて可能なものである。

2.2.2 確率的検証証明：検索と乱択の力

我々はインターネット時代を生きている。何か知りたいとなったら、まず Web を検索してみるだろう。Web は、書き込みをする人々から湧く、知識の泉を整理した

「証明の書」のようなものであり、我々は Web 上の記述を検証しながら利用している。評判の良い複数のサイトを見て矛盾がなければ、検証できたということになる。これに近いモデルが PCP（確率的検証証明）である。

PCP では、対話証明と同様に証明者と検証者を考えるが、証明者は問題の答えが Yes であることを主張し、その証拠を記述する（これを証明とよぶ）。検証者は証明に対して検索を行い、正しさを納得する。証明者に騙されないように、検索の時には乱択手法を使って、証明者に予測されない場所を読めるようにし、偽証明ならば、高い確率で検証者は偽りを告発できる証拠を握る。

PCP は、検索回数と乱択に用いる乱数の長さを用いて計算階層を細分化できる利点を持つ。実際、多項式回の乱択検索を行えば IP より強く、MIP と同等の力になる。

さらに重要なのは、NP 問題に対して、証明の定数ビットを検索すれば検証できる PCP が構築できることである。これは不思議な仕組みである。たとえば数独は NP 問題であるが、定数ビットの情報ではその解自体は漏洩しない。一方で「解がある」ことは、納得させられるのである。なお、この「情報を漏洩せずに納得させる」手法は暗号通信の世界ではゼロ知識証明と呼ばれ、開発者の S. Goldwasser と S. Micali は 2012 年にチューリング賞を受けている。

2.3 インターネットとビッグデータ時代への貢献

PCP の成果の出た 90 年代初頭には、まだインターネットは現在のような知識の泉ではなかった。1992 年に筆者は IBM の Watson 研究所に海外赴任したが、PCP でゲーデル賞を 2001 年に受けた 9 人衆（S. Arora, U. Feige, S. Goldwasser, C. Lund, L. Lovász, R. Motwani, S. Safra, M. Sudan, M. Szegedy）のうちで Sudan が博士号を取って着任したばかりであり、Feige がワイツマン研究所からポスドク研究員として来ていた。彼らは、乱択手法で高名な P. Raghavan（彼らを集めた張本人）らを交えて、PCP のような仕組みを現実の世界で活かすことを真剣に議論していた。後に Sudan は PCP で開発した誤り訂正符号の画期的な手法を拡張して、通信理論でも活躍し、Raghavan は Web 解析のパイオニアとしてヤフーとグーグルの技術部門トップを歴任した。

このように、計算理論の思想や道具を引っ提げて現実の情報社会を変革していく研究者は数多い。9 人衆の中でも白眉は急逝した Motwani で、彼はグーグルの創始者である指導学生 2 名とともにページランクという Web 検索手法を開発してグーグルを成功させ、他にも PayPal など多数のベンチャー起業のメンターとして活躍した。

また、Arora は有名なユークリッド巡回セールスマン問題に多項式時間近似スキーム（任意の精度の近似解を多項式時間で計算する手法）を与えた。「ユークリッド巡回セールスマン問題の解決」というニュースは世界を駆け回り、二度目のゲーデル賞を 2010 年に受けた。

計算限界の解明では、指数サイズである巨大な情報をコンパクトに凝縮し、乱択や検索などを用いて、一見不可能に見える問題解決を行う。これは、到来しつつあるビッグデータ時代でのデータ処理に必要な思想である。

事実、データを格納せずにストリーム形式で読むストリームアルゴリズム理論では、9 人衆の Szegedy などの成果が 2005 年のゲーデル賞を受けた。更に、グラフの性質を対数多項式時間で検査する手法や、データを圧縮したままで検索や加工を行う、魔術のような手法が開発されており、堀山貴史による多面体の展開図検索カタログ（文献(3)）では、3 垓=300 エクサ＝3×10^{20} 以上(同形分類すると 312 京程度)あるサッカーボールの展開図を圧縮したまま列挙生成し、検索構造化している。

計算限界の解明が新しい問題解決のモデルを作り、さらに計算限界解明で開発された手法がビッグデータ時代を切り開く、それが今現実化しているのである。

文　　献

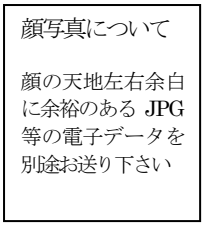
(1) M. Sipser（渡辺治、太田和夫監訳）計算理論の基礎, 1999 共立出版［第二版(三分冊) 2008］

(2) 徳山 豪、計算下界の解明―その意義とシナリオ(前編、後編)，情報処理 54-4、54-5 (2013)

(3) http://www.al.ics.saitama-u.ac.jp/horiyama/research/unfolding/catalog.new/index.ja.html

顔写真について

顔の天地左右余白に余裕のある JPG 等の電子データを別途お送り下さい



徳山　豪（フェロー）会員番号0014362

昭60年、東京大学理学系大学院・数学博士課程卒. 昭和61年日本ＩBM入社、同社東京基礎研究所研究員. 平成11年東北大学大学院情報科学研究科教授、理学博士. 本学会フェロー、情報処理学会フェロー、日本ＩBM科学賞、船井情報科学振興賞などを受賞。

徳山豪　フェロー　東北大学大学院情報科学研究科
E-mail アドレス　tokuyama@dais.is.tohoku.ac.jp
Takeshi Tokuyama　member,　(Tohoku University, Japan)

電子情報通信学会誌　Vol.00,　No.00　pp.000-000　20XX 年 00 月