

計算論の現在：P vs NP 問題とは何か？

照井 一成 （国立情報学研究所）terui@nii.ac.jp

はじめに

西暦 2000 年、アメリカのクレイ数学研究所は現代数学における 7 つの難問を提示し、それぞれの解決に 100 万ドルの賞金を懸けた。いわばヒルベルトの 23 問題の現代版である。その中の一つに P vs NP 問題と呼ばれる問題がある。1971 年にクックにより提起されたこの問題は計算機科学の根本問題の一つであり、(実的な意味での) 計算の限界に関わるという点で、計算可能性に関するチャーチ・チューリングらの探求に比肩しうるものである。

本発表においては、この P vs NP 問題を中心として現代の計算論、特に計算の複雑さの理論 (theory of computational complexity) と呼ばれる分野の紹介を行い、その意義を検討する。時間があれば、P vs NP 問題の解決に向けたいくつかのアプローチも紹介したい。

古典的計算論の主要成果

- (1) 計算可能な関数 (決定可能な問題) の数学的定式化 (チャーチのテーゼ)
- (2) 半決定可能かつ (全) 決定不能な問題の発見 (チューリング機械停止問題の決定不能性)

(1) は広く受け入れられているテーゼである。すなわち、関数が計算可能である (問題が決定可能である) とは、それが再帰的である、あるいはその関数を計算するチューリング機械が存在することとする取り決めである。

(2) について注意：単に計算不能な関数や決定不能な問題が存在することは当たり前であり (自然数上の関数：非可算無限、チューリング機械：可算無限)、チューリングの功績は、半決定可能 かつ決定不能な問題を見つけたところにある。証明は対角線論法による。

計算可能性から計算の複雑さへ

これらの成果により、関数や問題の計算可能性・決定可能性を調べるといふ一つの研究方針が確立した。しかしこの道具立てだけで十分かといえば、もちろんそうではない。古典的な計算可能性理論は計算の複雑さ (計算に要する実行時間 = ステップ数、空間 = 使用メモリ量) を考慮に入れていないからである。

計算の複雑さはプラクティカルな観点からいって重要である。特にしばしば問題にされるのは、与えられた関数が実際に計算可能 (feasibly computable) かどうか、すなわち現実的に許容できる時間内で計算できるかどうかである。

また、計算の複雑さは理論的な興味の対象でもある。関数には、それに固有の計算の複雑さが本性的に備わっており、複雑さの度合いに応じて階層づけられているように見えるからである。つまり関数空間は計算論的に言って決して一様ではない。その構造を探ることは理論的に興味深い問題であろう。

計算の複雑さの理論の主要課題

(3) 実際的に計算可能な関数(実際的に決定可能な問題)の数学的定式化

(4) 実際的に検証可能かつ実際的に決定不能な問題はあるか?

実際的計算可能性のテーゼ

上で見たように「実際的に計算可能」という概念はプラクティカルな重要性を持つため、それに対して数学的な定式化を与えることは重要である。しかし、「100時間で計算可能なこと」とか「チューリング機械で100億ステップで計算可能なこと」などとアドホックに取り決めることはもちろんナンセンスである。幸いなことに、それよりは満足のいく定式化が1960年代にコブハム、エドモンズ、ラビンらにより提唱され、現在ではほとんど全ての計算機科学者の間で受け入れられている(ただし量子コンピュータが実用化されれば、事情が大きく変わる可能性がある)。いま、チューリング機械で多項式時間で計算可能な関数(問題)のことをP関数(P問題)と呼ぶことにする。このとき、実際的に計算可能な関数(実際的に決定可能な問題)とはP関数(P問題)のことに他ならない(実際的計算可能性のテーゼ)。本発表ではこのテーゼをチャーチのテーゼと比較し、その妥当性を検討する。

実際的検証可能問題

(4)について注意:(2)の場合と同様に実際的に決定不能な問題があることは当たり前である(例:停止問題)。全く自明でないのは、実際的に検証可能という但し書きがついた場合である。

話を簡単にするために、「~を満たすものは存在するか?」という存在疑問の形の問題に焦点をしばらく。多くの重要な計算論的課題がこの形をとる。例えば、「命題論理式Aは充足可能か?」という問い(充足可能性問題)は、「Aを真とする真理値の割り当ては存在するか?」と言い換えることができ、「地図Mは三色で塗り分け可能か?」(三色塗り分け問題)は「地図Mを三色で塗り分けるような各国に対する色の割り当て方は存在するか?」と言い換えることができる。

さて、このタイプの問題には共通して、あるトリヴィアルな解法が存在する。それはしらみつぶしあるいはguess & checkなどと呼ばれる方法である。たとえば三色塗り分け問題なら、まず地図を三色で適当に塗ってみて(guess)、それが正しい塗り分けになっているかどうかを調べてみる(check)。もし正

しい塗りわけになっていればそれでよし、さもなければ、全ての可能な塗り方について、しらみつぶし的に上の手順を繰り返すというものである。

しかしこのような解法は、地図のサイズが大きいたくにはあまり実用的とはいえない。国の数に対して塗り方の数は指数関数的に増加するからである。実際、国の数が何百何千のオーダーになると、現在のどんなに早いコンピュータでさえ、全ての可能性を「しらみつぶす」のに何億世紀あっても足りない。また、そのようなアルゴリズムは計算論の美学から言って全く満足のいくものではない。もっとこう、すばやく、エレガントに、一発でスパッと解を求める合理的な方法が望ましいのである。そのような方法は存在するのだろうか？

しらみつぶしアルゴリズムは実用的には役に立たないが、ある問題のクラスを同定するには役に立つ。まず最初に指摘すべきことは、具体的な計算論的問題を考えると、上の check のプロセスは簡単に計算可能であることが非常に多いということである。三色塗りわけ問題が典型例である。正しい塗りわけ方を見つけるのは非常に難しいが、与えられた塗りわけ方の候補が正しいかどうかを検証するのは非常に簡単である。

このことを一般化しよう。いま、ある問題に対してしらみつぶしアルゴリズムが存在し、そのうち check の部分が実際に計算可能なとき、すなわち与えられた guess が正しいかどうかを実際的に検証可能なとき（かつ各 guess のサイズが多項式で抑えられるとき）その問題を実際的に検証可能問題（feasibly verifiable problem）と呼ぶことにする。ここで「実際的に」ということで「多項式時間」を意味するとするならば、その問題は NP 問題であるという。この定義が重要なのは、経験的にいって、現場のプログラマは「しらみつぶしをすれば簡単なんだけど…」という状況に頻りに直面するからである。多くの重要な計算論的課題が NP 問題なのである。

P vs NP 問題

さて、このようにして、実際的に決定可能ということで P を、実際的に検証可能ということで NP を意味するとするならば、(4) がまさに P vs NP 問題に他ならない。P vs NP 問題とは、P 問題のクラスと NP 問題のクラスは一致するかという数学的問いである。言い換えれば、しらみつぶしが必要だが check プロセスは簡単にできるような問題は、常にしらみつぶしなしに一発でスパッと解けるか？という問題である。

大方の予想はノーである。すなわち、世の中には本質的にしらみつぶしによらなければ解けないような問題が存在し、そのような問題に対して合理的なアルゴリズムを見つけることは不可能であろうというのである（もちろんバックトラックや何らかのヒューリスティクスを用いることで多少の効率化を図ることはできるだろうが、それは大きな助けにはならない）。予想の根拠は、これまで多くのアルゴリズム学者やプログラマが充足可能性問題や三色塗りわけ問題など、NP 問題の中で「最も難しい」問題（NP 完全問題）に対してうまいアルゴリズムを発見しようと努力してきたが、それが叶わなかつ

たという経験的な事情によるところが大きい。

みんなが一生涯懸命頑張ってそれでも NP を P に還元できなかったのだから、きっと P と NP は異なるクラスに違いない! というわけだが、いざそれを証明しようとなるとそれが実に難しい。すぐに思いつくのは (2) の証明に用いられた対角線論法を転用することだが、これはどうも簡単にはうまくいきそうにない。実際、対角線論法破りとでもいうべき返し技が存在することが知られている。P vs NP 問題の解決のためには、使い古された対角線論法ではなく、何か根本的に新しい手法が必要とされているのである。

おわりに

P と NP は同一か? 言い換えれば粗暴な「しらみつぶし」は合理的なアルゴリズムで常に置き換えることができるか? この問いは、計算可能性の限界に対するチャーチ・チューリングらの問いを実際の計算可能性の限界に対するものへと置き換えたものと見なすことができる。その一方で、「多項式時間」などの量的側面や「しらみつぶし」(あるいは非決定性)などの質的側面に言及し、その解決のためには根本的に新しい手法を要するという点で全く異なる問いでもある。

強調しておくが、P vs NP 問題は決してプラクティカルな関心のみから興味を持たれているのではない。その解決は、計算概念の本質について何事かを明らかにし、関数空間の計算論的見取り図の作成に大きく寄与するはずである。また、グラフ論・整数論・論理学など多くの数学分野に対して重要な帰結をもたらす。この美しく、難しく、根源的な問題は、セイレーンの歌声のごとく多くの数学者を惹きつけ、虜にしている。

References

- [1] S. Cook. The P versus NP Problem. Clay Mathematics Institute, 2000. クック自身により書かれたミレニアム問題のオフィシャルステートメント。
<http://www.claymath.org/millennium/>よりダウンロード可能。
- [2] M. Garey, D. Johnson. *Computers and Intractability. A Guide to the Theory of NP-Completeness*, Freeman & Co, 1979. 古典的名著。数百の NP 完全問題のリストで有名。
- [3] C. H. Papadimitriou. *Computational Complexity*. Addison and Wesley 1993. 丁寧にかかれた入門書。
- [4] M. Sipser. The history and status of the P versus NP question. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 603–618. ACM, 1992. P vs NP 問題のサーヴェイ。