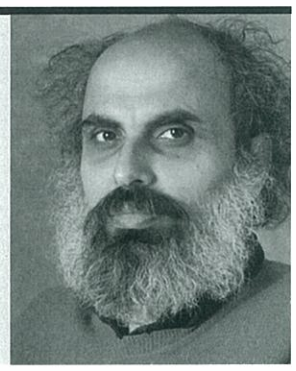
P ≠ NP予想, 代数的計算量

垂井 淳
◉電気通信大学大学院情報理工学研究科

Message from a World Expert



Ketan Mulmuley
(University of Chicago)

Geometric Complexity Theory (GCT) is an approach towards the P vs. NP problem and related problems via algebraic geometry and representation theory. It has been shown recently that derandomization of Noether's Normalization Lemma (NNL), which lies at the heart of the problem of classifying algebraic varieties, is essentially equivalent to black-box derandomization of polynomial identity testing. This essential equivalence between the foundational problems of geometry and complexity theory reveals that these two fields are two sides of the same coin. It also reveals that the foundational problems of these two fields share a common root difficulty, namely, the problem of overcoming the existing EXPSPACE vs. P gap in the complexity of derandomizing NNL for arbitrary explicit varieties. This gap is called the GCT chasm. To cross it, a deep synthesis of geometry and complexity theory seems necessary.
By geometric complexity theory (GCT) we mean any approach to cross this chasm based on a synthesis of geometry and complexity theory in some form. One such approach has been proposed by the existing GCT program. It has revealed deep connections of complexity theory with several outstanding problems of algebraic geometry and representation theory. The ongoing work in GCT focuses on understanding these connections.

1. 定規とコンパス vs. 多項式時間アルゴリズム

問題1 定規とコンパスによって，与えられた角度を3等分することは可能か？

問題2 定規とコンパスによって，与えられた半径の円と同じ面積の正方形を作ることは可能か？

問題3 多項式時間アルゴリズムによって，与えられたグラフが3彩色可能かどうか判定することは可能か？（グラフとは頂点n個と異なる頂点を結ぶ向きのない辺m本からなるもので，3彩色可能とは各辺の両端が違う色になるように各頂点を赤か青か黄にぬることができること.）

問題1と問題2は，ギリシャの3大作図問題のうちの2つである.（あとの1つは与えられた立方体の倍の体積の立方体の作図.） ギリシャ時代の数学者によって提示され，3つとも作図不可能であることが19世紀に証明された．問題3が不可能であるというのがP ≠ NP予想であり，未解決である.

作図問題は単純で美しく面白い問いであって，結

果的には「体の拡大」や「代数的数 vs. 超越数」といった重要な概念が関係しているものだった．しかし，問いに答えをだすことそのものの重要性に関しては，P ≠ NP 予想のほうが上だと言えるだろう．「多項式時間アルゴリズムで解く」というのは荒っぽく言うと「使うものは何でもありの計算で実際に答えを出す」ということだ．それで，もしNP問題すべてが実際に解けるのならば，実世界に大革新がもたらされる．このようにとらえると「定規とコンパスで角が3等分できるか？」という問いより「多項式時間アルゴリズムでNP問題すべてが解けるか？」という問いのほうがより根源的な問いだと言えるだろう．

2. 超越数 vs. 超多項式計算量

整数を係数としてもつ1変数多項式の根となる複素数を代数的数という．代数的数でない複素数を超越数という．上記の問題2は，πが超越数であることから作図不可能性がわかる．超越数に関する議論を次のように段階にわけて考えてみよう．

（1） 整数係数の1変数多項式は全部で可算無限個しかないけれど，複素数は非可算無限個ありずっと多いので超越数が存在することがわかる．区間$[0,1]$から一様ランダムに実数を選べば確率1で超越数である．この議論では存在はわかるけれど，具体的な数が超越数であることについて何もわからないことに注意する．

（2） 超越数を具体的に構成してみせる．

（3） 自然な数，たとえば，eやπが超越数であることを証明してみせる．

（4） 適当に与えられた数，たとえば，$e+\pi$が超越数であることを証明してみせる．

超越数であることの証明については，現在ステップ(3)までできているようだ．以上の段階と比べると計算量理論ではステップ(1)しかできていないと言える．クラスPに属さない問題の存在は対角線論法を使えばわかる．また，n-ビット入力1-ビット出力のブール関数が全部で2^{2^n}個あることとサイズsの回路が全部で$s^{O(s)} = 2^{O(s \log s)}$個しかないことを比べることによって，ほぼ1の確率でランダムなブール関数の回路計算量が指数的であることがすぐわかる．しかし，超多項式計算量であるものに関して具体的なことは現在何も示せない．P ≠ NP 予想の証明はステップ(3)に対応づけられるだろう．

3. 問題の還元, NP完全性

n個の頂点とm本の辺からなるグラフGが与えられたとしよう．3彩色可能性について改めて考える．各頂点iに対して，$X_{i,\mathrm{red}}, X_{i,\mathrm{blue}}, X_{i,\mathrm{yellow}}$の3つの0か1の値をとる変数を用意する．頂点$i$を赤くぬることを$X_{i,\mathrm{red}} = 1$に対応させようとしている．$n$個の頂点それぞれについて$X_{i,\mathrm{red}} \vee X_{i,\mathrm{blue}} \vee X_{i,\mathrm{yellow}}$という論理式を作り，辺で結ばれている頂点$i$と頂点$j$のペアそれぞれについて，$\overline{X_{i,\mathrm{red}}} \vee \overline{X_{j,\mathrm{red}}}$，$\overline{X_{i,\mathrm{blue}}} \vee \overline{X_{j,\mathrm{blue}}}$，$\overline{X_{i,\mathrm{yellow}}} \vee \overline{X_{j,\mathrm{yellow}}}$という3つの論理式を作る．ここで$\vee$はORの演算で，$\overline{x}$は$x$の否定をとるNOTの演算である．（$\overline{x}$の値は$x = 1$のとき0で，$x = 0$のとき1である．）

$3n$個の変数の値を適当に0か1に決めて，このように作った$n+3m$個の論理式**すべて**を満たすことができるだろうか？ 頂点iに対応する論理式が満たされるのは頂点iに少なくとも1つの色が割り当てられているときである．辺に対応する論理式3つが同時に満たされるのはその辺の両端に同じ色が使われていないときである．すなわち，グラフGが3彩色可能であることと，以上の論理式すべてが**充足可能**であることは同値である．（論理式を充足する0-1割り当てにおいて1つの頂点が2色以上で塗られていることがありうるが，その場合は色を任意に1つに絞り込めばいい．）

今度は，**論理式が充足可能かどうか**という形から複数の**多変数多項式の共通零点が存在するかどうか**という形に変換してみよう．任意の体Fを固定する．標数はpでも0でもいい．有限でも無限でも

いい．代数的閉体でもそうでなくてもいい．次のように連立方程式を作る．2行目の式は辺で結ばれている頂点ペアすべてについて作り，以下ではredについてだけ書いているがblueとyellowについても同様に作る．3行目の式は$X_{i,\mathrm{red}}$などの$3n$個の変数すべてに対して作る．

$$(1-X_{i,\mathrm{red}})(1-X_{i,\mathrm{blue}})(1-X_{i,\mathrm{yellow}})=0$$

$$X_{i,\mathrm{red}}X_{j,\mathrm{red}}=0$$

$$X_{i,\mathrm{red}}^2-X_{i,\mathrm{red}}=0$$

以上の連立方程式に対して解が存在することは，もとの論理式が充足可能であることと同値である．3行目の式により，存在する場合に解は0か1に限定されるので解の存在は方程式をどの体上で考えるのかに依存しない．

答えのyes/noを保存するような問題Aから問題Bへの多項式時間計算可能な変換が存在するとき，AはBに**還元可能**と言う．問題SがクラスNPに属し，かつ，クラスNPに属する任意の問題XについてXがSに還元可能なとき，問題Sを**NP完全**という．NP完全な問題はクラスNPのどの問題とくらべても同じかそれ以上に難しいという性質をもつ．以上でとりあげた3彩色可能性判定と充足可能性判定と0-1解の存在判定は，すべてNP完全問題である．この3つの問題はどれをどれに還元することもできる．

4. NP≠coNP予想

判定問題がクラスNPに属することの定義は，答えがyesのときに多項式時間で検証可能な証拠が存在することである．グラフGが3彩色可能なときは実際に彩色条件を満たす3彩色が証拠として存在する．論理式が充足可能なときは充足させる0-1割り当てが証拠となり，連立方程式に対して0-1解が存在するときは解が証拠となる．彩色条件を満たしていることなどの検証は多項式時間でできる．

このようにクラスNPに属する場合だけを見ていると単純な話に見えるかもしれないが，実はクラスNPの定義の扱いにはある程度の注意が必要となる．ここでは厳密な議論はバイパスして話を続ける．

以上の3つの問題のどれをとりあげても話は同じなのだが，答えがnoのときにnoであることの証拠で多項式時間で検証可能なものが必ず存在するだろうか？ 3彩色不可能なn頂点グラフに関して考えてみよう．頂点n個に対する3色の割り当てを3^n通りすべて列挙し，それぞれについて満たしていない彩色条件を挙げるという形の証拠は，サイズが大きすぎて多項式時間検証可能とは言えない．もしグラフの小さな一部分をとりだして「ローカルにこの部分だけですでに3彩色不可能」といえるのであれば，それはその特定のグラフに対する効率的検証可能なコンパクトな証拠と言える．しかし，小さなローカルな部分はすべて3彩色可能だけれど全体は3彩色不可能であるグラフも存在する．

任意の3彩色不可能グラフに対して多項式時間検証可能な3彩色不可能性の証拠が存在するかと言えば，そのような証拠が存在しない場合があるということの計算量クラスを用いた表現がNP≠coNPであり，このように予想されている．NP≠coNPという予想はP≠NP予想より強い予想である．

5. 証明の複雑さ：零点定理，ZFC

Fを任意の有限体とし，$p_1,\cdots,p_m\in F[x_1,\cdots,x_n]$とする．さらに，$x_i^2-x_i$という形の$n$個の多項式はすべて$\{p_1,\cdots,p_m\}$に含まれているとする．第3節の連立方程式は以上のシナリオに含まれている．このとき，弱い形のヒルベルト零点定理により，多項式p_jの共通零点がF^nにないことと$\sum_{1\le j\le m}p_jq_j=1$を満たす$q_1,\cdots,q_m\in F[x_1,\cdots,x_n]$が存在することは同値である．通常，零点定理は代数的閉体に対して述べられるが，$x_i^2-x_i=0$によって解が0か1に限られることなどから以上のように言える．

すなわち，$\sum p_jq_j=1$を満たす多項式$q_1,\cdots,q_m$を多項式$p_1,\cdots,p_m$が共通零点をもたないことの**証明**と考えるとき，この証明系は健全で完全である．もしこのようなq_jの最大次数を常に低くとれるのであれば，NP≠coNP予想に反することになる．有

限体上で次数が低い n 変数多項式はすべての項の係数を列挙する素朴な方法によりコンパクトな表現が可能なので，以上の零点定理に基づく証明系については，q_j の次数を高くとらざるを得ないような p_j の構成が知られている．

NP ≠ coNP 予想に関連して**証明の複雑さ**を考えるとき，証明系の中で特に重要なものが ZFC（ツェルメロ-フレンケル集合公理系＋選択公理）である．通常のすべての数学をその上で展開できると考えられている公理系の中でもっとも標準的なものだという理由で ZFC に固定して話をしている．任意の 3 彩色不可能なグラフに対して，ZFC の中で彩色不可能性のコンパクトな証明が存在するかという話は，つまり，どんな数学的推論を使っても OK で，コンピュータによる計算を用いても OK というシナリオのもとでコンパクトな証明があるかという話である．予想されている通りに NP ≠ coNP ならば，このシナリオのもとでコンパクトな証明が存在しない場合があることになる．

6. 行列式 vs. パーマネント

まず n 次の正方行列 $X = (x_{i,j})$ の行列式 $\det(X)$ とパーマネント $\mathrm{perm}(X)$ の定義式を書く．

$$\det(X) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{1 \le i \le n} x_{i,\sigma(i)}$$

$$\mathrm{perm}(X) = \sum_{\sigma \in S_n} \prod_{1 \le i \le n} x_{i,\sigma(i)}$$

ここで，S_n は $\{1, \cdots, n\}$ の置換の集合（または n 次対称群）を表し，$\mathrm{sgn}(\sigma)$ は置換 σ の符号を表す．ベースとする体または可換環を K で表し，話を単純にするため $K = \mathbb{Z}, \mathbb{Q}, \mathbb{C}$, または $\mathbb{F}_p$ とする．ここで，$\mathbb{F}_p$ は p 個の要素からなる有限体で，p は奇素数とする．標数が 2 の体上では $+1 = -1$ なので $\det(X) = \mathrm{perm}(X)$ となり以下の話があてはまらない．

$\det(X)$ と $\mathrm{perm}(X)$ については，n^2 個の変数からなる多項式，すなわち多項式環 $K[x_{1,1}, \cdots, x_{n,n}]$ の元としても考えるし，また，各 $x_{i,j}$ に K の特定の要素が与えられて $\det(X) \in K$，$\mathrm{perm}(X) \in K$ が決まるという文脈でも考える．特に，$\det_n$ と perm_n はそれぞれ n^2 個の変数からなる多項式としての det と perm を表すとする．

$\det(X)$ の計算は簡単であるが，$\mathrm{perm}(X)$ の計算は難しいと予想されるというのがここでの基本的ストーリーである．$\det(X)$ の計算は，たとえばガウスの消去法によって効率的にできる．ただし，ガウスの消去法は $x_{i,j}$ の値が固定された場合に $\det(X)$ の値を求める方法として考えるのが普通だ．しかし，多項式として $\det_n$ を計算する（作る）ことも効率的にできる．また，素朴なガウスの消去法は逐次的アルゴリズムだが，並列化して $O(\log^2 n)$ の並列時間で計算を終えるようにすることもできる．$\det(X)$ の計算が簡単であることは K をどのようにとっても同じ話となる．

ここで $f \in K[x_1, \cdots, x_s]$，$g \in K[y_1, \cdots, y_t]$ とする．多項式 f が多項式 g のプロジェクションであるとは $f(x_1, \cdots, x_s) = g(a_1, \cdots, a_t)$ となるような $a_1, \cdots, a_t \in K \cup \{\pm x_1, \cdots, \pm x_s\}$ が存在することと定義する．すなわち，g の変数 1 つ 1 つに対して f の変数どれか 1 つまたは K の元を代入して f が得られるときに f は g のプロジェクションと言う．f が g のプロジェクションであるとき，f を計算したければ，代入を実行して g を計算すればいい．すなわち，f の計算を g の計算に還元できる．このことをふまえて，**f が g のプロジェクションであること**を**f を g に埋め込める**とも言うことにしよう．（埋め込むという表現は，読者がイメージしやすいのではないかと思いつつ，この原稿のために作って使っている．）

多項式 perm_n を多項式 $\det_m$ に埋め込むために $m = m(n)$ をどれぐらい大きくとらなければならないかを考える．$n = 2$ のときをまず考えてみると，$m = n = 2$ として埋め込めることに気づく．$n = 3$ の場合ですでに話がけっこう複雑になる．そもそも m を十分大きくとったら必ず埋め込めるということが自明でないのだが，m を 2^n ぐらいまで大きくとれば埋め込めることはわかっている．次が基本的で重要な予想である．

予想[Valiant]　$m = m(n)$がnに関して多項式的増大度であるならば，十分大きいすべてのnについてperm_nは$\det_m$に埋め込めない．(「十分大きいすべての」を「無限に多くの」に変えると弱い形の予想となる．)

この予想を見て，次のような疑問が浮かぶかもしれない．

（1）　埋め込みで使うことができるのが代入だけという制限は強すぎないか？　埋め込むターゲットが$\det_m$に固定されているのも強すぎる制限ではないのか？　すなわち，perm_nの計算が実は簡単なのだけれど以上の意味での$\det_m$への埋め込みはできないという可能性はないのか？

（2）　なぜperm_nについて考えるのか？　perm_nの計算が難しいという予想に対する何らかの根拠はあるのか？

結論だけ言うと，以上の疑問に表出されている心配は不要ということがわかっている．

以上の予想は，$\mathrm{P} \neq \mathrm{NP}$予想よりは弱い予想である．(より正確には，以上の予想は非一様な話なので$\mathrm{P} \neq \mathrm{NP}$と比較することができない．)　計算量理論の一部の研究者はこの予想について$\mathrm{P} \neq \mathrm{NP}$予想の前に解決されるべきものだと考えている．この点については意見が分かれるだろうが，以上の予想の解決が非常に大きなブレークスルーとなることは確かだ．

改めて以上の予想を眺めてみよう．アルゴリズムや計算といったものに比べるとかなり話が単純化されたようにも見える．時間とともに計算が進んでいくといった動的な話はなくなり，埋め込めるかという静的な話だけになっている．代数の言葉だけで語れる話になっている．これらのポジティブな印象はすべてもっともな話ではあるのだけれど，問題の難しさの本質はそっくりまだ残ったままだと考えるのが妥当だと思われる．

7. 幾何的計算量理論, GCT

メッセージを寄せてくれたKetan Mulmuleyは第6節で説明したValiantの予想を表現論や代数幾何を用いて解こうとする枠組みを研究し続けており，この枠組みのことを幾何的計算量理論(Geometric Complexity Theory, GCT)と名付けている．最近，GCTに真剣な興味をもつ表現論や代数幾何の専門家が増えており，GCTに関する研究集会において参加者の半数以上が純粋数学者ということもよくあるようだ．計算量理論の研究者は難しそうな数学を展開させることの必要性・必然性がまだはっきりしないようにも思われるので静観している人が多そうだ．

筆者は今年の3月に東京で開催された計算量理論に関する研究集会を世話する機会があった．Mulmuley氏は招待講演者の一人であり，また彼はGCTに特化したサテライト集会でも話をしてくれた．このときには有木進氏(大阪大)や徳山豪氏(東北大)のご尽力により国内の数学者との交流も実現した．GCTの枠組みの意味や見込みについて筆者はわかっていない．興味をもたれた読者が自分で探られることを期待したい．

◉── 参考文献

本を3冊あげておく．[1]は計算量理論に関する現時点での標準的レファレンス本である．[2]は特に統計物理と計算量理論の境界領域に関する説明が詳しく，また全体的に面白い．[3]は計算量理論と証明論の両分野における第1人者によりごく最近出版されたもの．面白い．

[1]　Sanjeev Arora and Boaz Barak: *Computational Complexity: A Modern Approach*, Cambridge Univ Press, 2009.

[2]　Cristopher Moore and Stephan Mertens: *The Nature of Computation*, Oxford Univ Press, 2011.

[3]　Pavel Pudák: *Logical Foundations of Mathematics and Computational Complexity: A Gentle Introduction*, Springer Monographs in Mathematics, Springer, 2013.

[たるい じゅん]