経 済 学 研 究 *59−4*
北 海 道 大 学 2010. 3

Nash 均衡の計算複雑度について

田 中 嘉 浩

1 はじめに

von Neumann and Morgenstern [27] によって 1944 年に著された名著 *Theory of Games and Economic Behavior* を嚆矢とするゲーム理論に於いて，1950 年に Nash [18] が導入した重要概念である Nash 均衡の計算が「効率的解法」を持たず，従来の NP 完全と違った，PPAD 完全というクラスの問題に属するという結果を，Daskalakis, Goldberg and Papadimitriou 等は国際計算機学会（ACM）の *Communications of the ACM* 誌 2009 年 2 月号に掲載された論文 [8] “The complexity of computing a Nash equilibrium” で彼等自身の研究を中心に紹介した。

更に，21 世紀に解決されるべき数学の 7 大未解決問題（ミレニアム懸賞問題）の一角である Poincaré 予想が 2002〜2003 年に Perelman によって解決されたからかどうか分らないが，未解決問題を含む計算量に関する話題が最近脚光を浴びつつある。*Communications of the ACM* 誌 2009 年 9 月号に Fortnow 氏によるサーベイ論文 [11] “The status of the P versus NP problem” が出て以来大変な反響を受けており，それを受けて更に一般紙でも *The New York Times* 紙（10 月 7 日）に一般向けに的を得た解説が為されている。

本稿では計算量に関する概念や最近の研究を概観し，多くの重要な応用を持つ Nash 均衡の計算量に関する論文 [8] の結果を示す。

2 計算量の理論の発展

2.1 定 義

Turing [25] が Turing マシンを提案し，Church により計算可能という概念が 1936 年に定義されて以来，先ず「何が計算可能か？」ということが問題にされ，Cantor によって実数が有理数と違って不可算であることを示すことに用いられた対角線論法による Turing マシンの停止判定問題が計算不可能であることの証明 [25] 等の理論的結果が初期の段階で得られている。

それ以降は「効率的解法」に関する研究から計算複雑度に関する理論が，特に 1971 年の Cook の充足可能性判定問題（Satisfiability; SAT）が NP 完全問題に属することの証明 [7]，Karp [14] による多項式時間帰着可能による NP 完全の証明法を嚆矢にして大きく発展してきた。

簡単に説明すると，クラス P とは多項式時間アルゴリズムで判定できる問題の集合であり，クラス NP とはインスタンスが与えられた時に YES であることを多項式時間で判定できる判定問題の集合である。判定問題 B 顥 NP は，NP に属する他の全ての問題が B に多項式変換可能な時に NP 完全（NP Complete）という。NP 完全問題はその定義からクラス NP の中で最も難しい部類の問題である。

クラス P に属する代表的な問題を示す。

・素数判定問題

この問題は多項式時間で効率的に判定できることが保証されている。判定問題ではないが,

- ・ソーティング
- ・最小木問題
- ・辺数最大マッチング問題
- ・最大フロー問題
- ・行列の積や連立一次方程式
- ・割当問題
- ・線形計画問題

等の探索問題は多項式時間のアルゴリズムが知られている。辺数最大マッチング問題はこの中では特殊な問題だが，親しい者同士が分っている集団でペアの組み方を考える問題であり，Edmonds［10］が 1965 年に効率的な多項式時間アルゴリズムを考えている。なお，最小木問題の様にマトロイド(matroid)という特定の構造をもつ問題は貪欲算法によって効率的に解けることが分っている。

ところで，線形計画問題(の許容解の判定)や素数判定問題は，YES に対する問題も NO に対する問題もどちらも多項式時間で判定でき，良い特徴付けをもつ(NP 瓦 coNP に属する)クラスの問題であることが分っている。このクラスの問題で線形計画問題が 1979 年に，素数判定問題が 2004 年に多項式時間アルゴリズム［1］が発見されたことは興味深いが，P＝(NP 瓦 coNP)？問題は未解決問題である。

NP 完全に属する代表的な問題を示す。

- ・充足可能性判定問題(SAT)
- ・点カバー問題(Vertex Cover)
- ・Hamilton 閉路問題(Hamilton Circuit)
- ・クリーク問題(Clique)
- ・３次元マッチング問題(３DM)
- ・分割問題(Partition)

定義から NP 完全に属する問題のどれか１つにでも多項式時間アルゴリズムがあれば，NP のすべての問題が多項式時間で判定できることになるが，現在のところそういうアルゴリズムは発見されておらず，寧ろ存在しないと信じられている。多項式アルゴリズムが存在しなければ変数の数が増大するにつれて計算量の爆発が起き，どんなにコンピュータのハード面が進歩しようが大きなサイズの問題は急に解けなくなる。P＝NP？問題が 21 世紀に解決されるべき数学の未解決問題の１つとして解決を嘱望されている所以である。

最適化問題若しくは判定問題 B 纇 NP は，NP に属する他の全ての問題が B に多項式変換可能な時に NP 困難という。NP 困難問題はその定義からクラス NP の中で最も難しい問題と少なくとも同程度に難しい同等である。整数計画問題や巡回セールスマン問題(TSP)は NP 困難であるが，相転移のイジングモデルの基底状態を見つける問題等も NP 困難として知られている。

2.2　P 莞 NP への試み

Razborov［21］は 1985 年に回路計算量に関して，大きなクリーク問題を解く，NOT ゲートを含まない AND と OR からなる小さな(単調)回路が存在しないことを示し，回路を一般化して P 莞 NP の証明となることが期待されたが，後に NOT ゲートを含めば旨く行かないこと等が彼等自身の研究で示されている。

トートロジーかどうかを判定する問題が NO となる為には，そういうインスタンスを代入すれば分るが，YES となる為にはすべてのインスタンスを考えることになる。導出(resolution)はトートロジーを証明する標準的な方法だが，1985 年に Haken は鳩巣原理を表すトートロジーを短い導出法で示せないことを示した。しかしながら，この結果は P 莞 NP を示すのに必要であるが，十分ではない。

2.3　困難の扱い

NP 完全の問題を実際に解かなければならない場合，仮に P 莞 NP ならばそういう方法論が本流になるが，幾つかのアプローチが知られている。

先ず最適に近い近似解を求める近似アルゴリ

ズムを考える試みが為されており，例えば，最大重みカット問題（NP 困難）では Goemans and Williamson［13］は半正定値計画を用いて 1.139-近似アルゴリズム（但し，k-近似アルゴリズムとは，最小化問題（最大化問題）では最適解の k 倍以下（$\frac{1}{k}$ 倍以上）の解を多項式時間で求めるアルゴリズム）を得ている。

2.4 節に関連するが，近似率 k 噂 1 が定数である時にその様な近似アルゴリズムは APX，更に，任意の å 瓜 0 に対して k 厩 1茨å とできる時に PTAS と定義されている。

巡回セールスマン問題（NP 困難）で辺長を地図上の距離で与える時（Euclidean TSP），三角不等式が成立するので近似可能と知られているが，Arora［3］は平面の再帰的分割に基いた PTAS を与えている。

計算量の理論では通常は最悪時間を問題にするが，平均時間を扱えればより実態に合っていることも多いが，Levin［15］は特定の確率分布を考えて P ＝ NP？問題の確率版を定義しているが，NP 完全が最悪時間で成立する時に平均時間でも成立するかどうかは未解決問題である。

2.4　対話的証明と近似不可能性

問題 A に対して，任意の解 x をその全てのビットではなく，入力のビット数を n として長さ r廓較の乱数を用いて，q廓較個のランダムビットを用いて検証することを考える。x が真に YES の時に x を YES と判断する確率が 1 であり，x が真に NO の時に x を NO と判断する確率が $\frac{1}{2}$ 以上であるときに，問題 A は PCP 廓廓較q廓輳數に属するという。

次の定理が成立する。

定理 1（*PCP* 定理）［2］　NP ＝ PCP（log n,1）　■

PCP 定理を用いてクリーク問題から生じる最大クリーク問題に対して次の結果が得られている。

定理 2　*cf.*［2］　最大クリーク問題は P 莞 NP ならば *APX* を持たない。　■

一方，分割問題から生じる最小 2 分割問題には PTAS が存在することが知られている。

2.5　P 莞 NP？の応用

P ＝ NP ならば計算量の爆発の為に解けないでいた多くの重要な問題が一気に高速に解ける様になり，人類は大きな恩恵を受けることは間違いない。しかしながら，P 莞 NP がもっともらしいと思われているが，だからこそ，計算の困難性は積極的に応用されている。

暗号，特に日常的に認証や電子署名で良く使われる公開鍵暗号では，P 莞 NP を仮定して成立しているのだが，それだけではなく，素因数分解の平均複雑度に関する仮定も必要である。そこで公開鍵でなく，例えば認証では，NP 完全問題を用いて，証明者がその解を知っていることを検証者にゼロ知識証明で分らせる，という様な応用を考えることができる。

2.6　量子コンピュータと NP完全問題

素数判定問題は 2004 年に多項式時間アルゴリズム［1］が発見されたが，合成数の素因数分解の効率的なアルゴリズムはまだ知られておらず，現代暗号は素因数分解等の問題の困難さに基いて成立しているものである。

Shor［24］は 1997 年に素因数問題や離散対数問題を効率的に解く仮想的な量子コンピュータを提案したが，ハードでの実現を目指した研究方向も進んでいる。

しかしながら，素因数問題も離散対数問題も NP 完全問題よりは易しいクラスであり，NP 完全問題を量子コンピュータだけで効率的に解けるとは思われていない。

2.7　更なる方向性

問題を１ステップで解く概念上の装置をオラクル(oracle)というが, Baker, Gill and Solovay [5] はオラクル付きのチューリングマシンを考えることにより，P と NP が等しくなる様にも P と NP が等しくならない様にも相対化(relativize)できることを示した。停止問題が計算不可能である証明に用いられた対角線論法, ひいては集合論的方法は相対化を利用しそうなので P＝NP？解決に無力と思われている。

Razborov and Rudich [22] は“natural”という概念を提案し,

「一般の(単調でない)回路に対する超多項式下界は，暗号の様に逆関数の計算が困難な一方向性関数の存在の仮定の下で,“natural proof”は存在しない」という結果を得ている。

Mulmuley and Sohoni [17] は幾何学的計算量の理論(Geometric Complexity Theory; GCT)を用いて P＝NP？を扱う方法を提案している。彼等は或る代数的変数上での群表現に基いた高次元多面体 P_n を考え，もし全ての n に対して P_n が整数点を含むならば，入力 n の Hamilton 路が多項式でない $O(n^{\log n})$ 下界を持つことが示され，P $\neq$ NP となることを示している。彼等自身は理論の完成には 100 年掛かると言っているが，代数幾何を用いる方法は有望視されている。

3　Nash 均衡の計算複雑度

3.1 背　景

von Neumann 等によって 1940 年代に創始されたゲーム理論は経済学だけでなく政治学, 行動科学等重要な応用を持っている。

Nash [18] は非ゼロ和非協力ゲームに於いて, プレイヤー i ($i=1, \ldots, n$) の混合戦略を s_i, 利得関数を f_i とする時に,

「各プレイヤー i に対して，他のどのプレイヤーも混合戦略を変える動機がない，即ち,

$E f_i(s_1, s_2, \ldots, s_i, \ldots, s_n) \geq E f_i(s_1, s_2, \ldots, s_i', \ldots, s_n)$ となる」

時に 混合戦略の組 $(s_1, s_2, \ldots, s_i, \ldots, s_n)$ を 均衡(Nash 均衡)と定義し,

「混合戦略の範囲で少なくとも１つは均衡点が存在する」

ことを，角谷の不動点定理を用いて証明した。しかしながら非ゼロ和対称２人ゲームでさえ, Nash 均衡が２つ以上あるかどうか判定するのは NP 完全問題 であることが分っている [12]。

NASH： 混合戦略の範囲で Nash 均衡を１つ求めよ。

と定義する。NASH は，ゼロ和ゲームでは 1920 年代に von Neumann によって線形計画に定式化できることが示されているので高速に解ける。しかしながら，非ゼロ和(双行列)ゲームでは Lemke-Howson のアルゴリズムがあるものの，多項式時間アルゴリズムではない [23] ことが知られており，効率的な解法が知られていない。そこで効率的な解法の探求と共に，その計算量に関する研究が進展してきた。

3.2　全探索問題

第２節では判定問題に対するクラスを紹介したが，探索問題，しかも必ず解を持つ探索問題には，単に NP 完全を探索問題に拡張した FNP や必ず解を持つ探索問題に拡張した TFNP だけではない，より細かいクラスを考えれる。

「有向グラフで入次数と出次数の違う点があれば，必ずもう１つそういう点がある」

という事実を用いて解の存在を示し，正確にはもう１つの点を求める線終端問題(END OF THE LINE)に帰着される全ての探索問題は PPAD(Polynomial Parity Argument in a Directed graph)と定義される。PPAD は完全問題を持つことが分っており，それを PPAD 完全という。

PPADは FP と FNP の間にある複雑度の問題であるが，実験結果からは効率的なアルゴリズ

ムはないと信じられている。

3.3　Nash 均衡と PPAD

Daskalakis, Goldberg and Papadimitriou [8] は次の結果を示している。この節の定理自体は前に Papadimitriou [19] によって単独に得られているが，別証明の [8] のアイディアを示す。

定理 3 [8]　NASH は PPAD 完全である。　■

これを証明する為に彼等は間に次の不動点を求める問題を考えている。

BROUWER：リプシッツ連続関数 F:擞,1郭^3 臆 擞,1郭 に対して，精度 å 瓜 0 が与えられた時に d廓F廓較 x較閏 å を満たす x 顥 擞,1郭 を求めよ。

BROUWER が PPAD であることが，三角分割，色付け，等の手法により Sperner の補題を用いて，BROUWER が線終端問題（PPAD 完全）に帰着されることから示されている。

NASH が BROUWER に帰着されることは，均衡点でなければ，現戦略を他戦略に変えようとする不満足なプレーヤーが存在するので戦略から戦略への選好関数を構成することで示せる。これで NASH が PPAD であることは示された。

次に，NASH をクラス PPAD で完全であることを示す為に，線終端問題のグラフを対応するゲームに変換する。まず，線終端問題のグラフを 擞,1郭^{3}に埋め込むことで BROUWER に変換できることから次の定理が成立する。

定理 4 [8]　BROUWER は PPAD 完全である。　■

BROUWER の F を計算するのに，加算，乗算，比較等の演算子を組合わせて構成するのだが，それらの各演算子はプレイヤーの “go” の確率（混合戦略）を表す変数と媒介プレイヤーへの利得を考えることによって実現される。各点 x 顥 擞,1郭^{3}を 3 人プレイヤー X_1, X_2, X_3 の “go” の確率を並べた点と考える。Nash 均衡点 廓y_1, y_2, y_3較で終わる様に X_1, X_2, X_3 に利得を与えることにより，BROUWER を 3 人ゲームの NASH で計算できる様に構成できる。よって定理 3 は証明された。

3.4　近似計算について

Nash 均衡を効率的に解くアルゴリズムは知られておらず，幾つかの近似アルゴリズムが考えられている。近似アルゴリズムに於いて，± 近似 Nash 均衡とは各々の戦略が ± 近似最適反応戦略であることを言う。

NASH の近似アルゴリズムは例えば Daskalakis, Mehta and Papadimitriou [9] による多項式時間 0.38 近似アルゴリズムが得られており，APX が存在するとは言える。

NASH の近似アルゴリズムで，任意の å 瓜 0 に対しては，Lipton, Markakis and Mehta [16] は n 人ゲームに対して準指数時間 O廓$^{\log n 慰^2}$較の近似アルゴリズムを提案している。しかしながら，PTAS が存在するかどうかはまだ未解決問題である。

4　終わりに

Nash 均衡解の計算はゼロ和 2 人ゲームの場合でさえ，戦略数が非常に多く，混合戦略の空間次元が高くなって扱いにくい問題があるが，Peña [20] はその混合戦略の単体に対して知られている近接関数（prox-function）を用いて滑らかな問題にしてから非線形計画の手法である勾配法を適用する提案やポーカーへの応用を示している，

Papadimitriou [19] は [8] の論文より前に，必ず解を持つ探索問題に対して PPAD だけでなく幾つかの重要なクラスを提案している。
その中では，

「有向グラフで閉路を持たないものは必ず終点を持つ」
という事実に基いて解の存在を示す PLS (Polynomial Local Search)というクラスと,
「グラフで奇数次数の点があれば必ずもう１つ奇数次数の点がある」
という事実に基いて解の存在を示す PPA (Polynomial Parity Argument)というクラスも定義されており，PLS が完全問題を持つことや，PPAD 盈 PPA が成立すること等が示されている。

次の定理が成立することも興味深い。

定理５ 交換均衡問題(*Exchange Equilibrium*)や競争均衡問題(*Competitive Equilibrium*)は PPAであり，更にPPAD 完全である。

［証 明］ 交換均衡については［19］Lemma 4 の Corollary。競争均衡については，同 Corollary から角谷の不動点を求める問題が PPAD 完全であることと，角谷の不動点を応用して競争均衡が求まること［4］と，単位球面 $S^{n\text{芋}1}$ 上に $\dot{p}$ の方向に矢印で方向付けれることから PPAD 完全であると言える。 ■

いずれにしても Nash 均衡解の計算という重要な問題のクラスが Brouwer や角谷の不動点の計算と同じ特定の計算の困難なクラスの PPAD 完全であるという結果が確立されたことは意義深い。

参考文献

［1］ Agrawal, M., Kayal, N., and Saxena, N., "PRIMES is in P" *Ann. Math.* 160, 781-793 (2004).

［2］ Arora, S., "Probabilistic checking of proofs and the hardness of approximation problems," Ph. D. thesis, UC Berkeley, (1994).

［3］ Arora, S., "Polynomial time approximation schemes for Euclidean traveling salesman and other geometric problems," *Journal of the ACM* 45, 753-782 (1998).

［4］ Arrow, K.J., and Debreu, G., "Existence of an equilibrium for a competitive economy," *Econometrica* 27, 265-290 (1954).

［5］ Baker, T.P., Gill, J, and Solovay, R., "Relativizations of the P=? NP Question," *SIAM Journal on Computing* 4, 431-442 (1975).

［6］ Conitzer, V., and Sandholm, T., "New complexity results about Nash equlibria," *Games and Economic Behavior* 63, 621-641 (2008).

［7］ Cook, S.A., "The complexity of theorem proving procedures," *Proc. 3rd Annual ACM Symposium on the Theory of Computing*, New York, 151-158 (1971).

［8］ Daskalakis, C., Goldberg, P.W., and Papadimitriou, C.H., "The complexity of computing a Nash equilibrium," *Communications of the ACM* 52, 89-97 (2009).

［9］ Daskalakis, C., Mehta, A., and Papadimitriou, C.H., "A note on approximate Nash equilibria," *Proc. 2nd WINE*, 297-306 (2006).

［10］ Edomonds, J., "Paths, trees and owners," *Canadian J. Math*. 17, 449-467 (1965).

［11］ Fortnow, L., "The status of the P versus NP problem," *Communications of the ACM* 52, 78-86 (2009).

［12］ Gilboa, I, and Zemel, E., "Nash and correlated equilibria: Some complexity considerations," *Games and Economic Behavior* 1, 80-93 (1989).

［13］ Goemans, M.X., and Williamson, D.P., "Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming," *Journal of the ACM* 42, 1115-1145 (1995).

［14］ Karp, R.M., "Reducibility among combinatorial problems," in: *Complexity of Computer Computations*, Miller et al. Eds., Plenum, 85-103 (1972).

[15] Levin, L., "Average case complete problems," *SIAM J. Computing* 15, 285-286 (1986).

[16] Lipton, R.J., Markakis, E., and Mehta, A., "Playing large games using sample strategies," *Proc. 4rd EC*, 36-41 (2004).

[17] Mulmuley, K., and Sohoni, M., "Geometric complexity theory I: An approach to the P vs. NP and related problem," *SIAM Journal on Computing* 31, 496-526 (1975).

[18] Nash, J., "Noncooperative games," *Ann. Math.* 54, 289-295 (1951).

[19] Papadimitriou, C.H., "On the complexity of the parity argument and other inefficient proofs of existence," *J. Comp. Syst. Sci.* 48, 498-532 (1994).

[20] Peña, J., "Nash equilibria computation via smoothing techniques," *Optima* 78, 12-13 (2008).

[21] Razborov, A., "Lower bounds on the monotone complexity of some Booloean functions," *Soviet Mathematics Doklady* 31, 485-493 (1985).

[22] Razborov, A., and Rudich, S., "Natural proofs," *J. Comp. Syst. Sci.* 55, 24-35 (1997).

[23] Savani, R., and Stengel, B., "Hard-to-solve bimatrix games," *Econometrica* 74, 397-429 (2006).

[24] Shor, P., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing* 26, 1484-1509 (1997).

[25] Turing, A., "On computable numbers, with an application to the Entscheidungsproblem", *Proc. London Math. Soc.*, 42 230-265 (1936), 43 544-546 (1937).

[26] Uzawa, H., "Walras's existence theorem and Brouwer's fixpoint theorem," *Econ. Stud. Quart.* 13, 59-62 (1962).

[27] von Neumann, J., and Morgenstern, O., *Theory of Games and Economic Behavior*, Princeton Univ. Press, Princeton, (1944).