

「P v s NP」問題の解決：最終章

The solution of " PvsNP" problem: The final

山口人生
Jinsei Yamaguchi

1、序論

計算量理論における「P v s NP」問題はTM基準の言語認識問題として設定されている。しかし、言語Lの認識アルゴリズムで最短なものを追及するには、“可能な、有りとあらゆるアルゴリズム”を考察する必要がある。その中で、特に、“発見可能な総ての決定問題の実現アルゴリズム”は論考の対象から外せない。ここでの論点は“総ての決定問題”である。これは数学の枠内に収まるものであろうか？例えば、ZF集合論上で決定問題を考える。この場合、ZF+ACベースの決定問題とZF+ADベースの決定問題は共存できるか？(ZF+AC+ADは矛盾する。)この問題意識が「P v s NP」問題最終解決の糸口になる。

2、融合 term

集合論の言語として、
 <1> 固体定数： \emptyset, ω 、及び、必要に応じて有限個の追加定数
 <2> 集合記号： $\{x \mid \}$
 <3> 述語記号： $\in, =$
 を指定する。この時、

定義

集合論の“融合 term”とは、
 1. 固体定数と変数は融合 term
 2. 融合 term だけを用いて定義される、 x を自由変数に持つ述語論理の formula $f(x)$ に対し、 $\{x \mid f(x)\}$ は融合 term
 3. 以上で構成されたものだけが融合 term \dashv

この定義の下、
 $\Delta = \{x \mid x \text{ は融合 term で表現される集合論のオブジェクト}\}$
 とすると、

ヤマグチのパラドックス

1. Δ への所属を決定するアルゴリズムがある。
2. Δ は集合論 (、つまり数学) の対象外。 \dashv

証明は、[6]参照。このパラドックスは歴史的

新発見。これを“ヤマグチのパラドックス”と名付ける。事態は集合論 v s アルゴリズム論の境界争いにまで発展する。例えば、 Z を $\{1,0\}$ 順序対の集合とし、 Δ と Z の関係 μ を考える。集合論的には、このような μ は証明対象外。一方、融合 term の $\{1,0\}$ コードは、 Δ の表現と Z の関係を付ける。これが融合 term の“表現 v s 実体”問題である。

この二重性を分析するため、対象領域を数学の各種決定問題を考究する第一層と、そのRFアルゴリズムを論考する第二層と、 $\{1,0\}$ 言語認識問題をTMで考察する第三層に階層化する。従来の素朴計算量理論では、「P v s NP」問題は第一層を無視して議論できると思われてきた。ところが、第二層も第三層も、理論として公理的集合論が土台になっている。よって、計算量理論でも融合 term を無視できない。以下、この結果が「P v s NP」を直撃することを示していく。

3、計算測度理論

TM基準の計算量理論とは別に、第一層の決定問題をベースにした“計算測度”なる概念を定義する。そのため、 $D\$ = \{x \mid x \text{ は決定問題の正規入力 (=各種 term 表現された数学対象)}\}$ を考える。当然、 $Z \cup \Delta \subset D\$$ 。ここでは、判り易さを優先させて $Z \cup \Delta$ をベースにする。各決定問題 Q は $Z \cup \Delta$ の部分クラス (Q の入力クラス) を正解クラス $Y(Q)$ と不正解クラス $N(Q)$ に分離する。

(以下、“クラス”は“集合”込みとする。)我々の意図は、 $\{1,0\}$ 正則 (両方向多項式時間変換) コード σ に対し、

「決定問題 Q の計算測度が $P \Leftrightarrow (Y(Q), N(Q))$ 決定アルゴリズムで、 σ コードのTM計算が入力サイズに対し多項式時間で収まるものがある」が成立するような理論化。定義中、 σ を陽に指定している点に注意せよ。同様にして、NPやEXPも定義できる。

計算測度は言語認識問題として定義していない。これが計算量概念との相違である。一見すると、この概念は、 $(\sigma(Y(Q)), \sigma(N(Q)))$ に対する決定アルゴリズムとして第二層+第三層だけでも定義可能に見える。しかし、第一層のセマンティクスが本質的に作用する問題設定ができる。これが計算量とは根本的に異なる点。ところが、

定理

「P v s NP」問題と同値な計算測度ベースの Δ セマンティクス問題が定義できる。

証明：

各融合termは集合やクラスの表現である。そして、同一集合、クラスに対し、異なる融合term表現ができる。特に、任意の $K = \{x \mid f(x)\}$ に対し、いくらでも長い融合term表現 $\{x \mid f(x) \wedge t_1 = t_1 \wedge t_2 = t_2 \wedge \dots \wedge t_n = t_n\}$ が存在する。

(各 t_i は融合term) さて、任意の $\{1,0\}$ 順序対 w に対し、 (w, K) なる入力を考えることで、言語認識問題 L から次のような新決定問題 $L(K)$ を作ることが可能。

$(w, K) \in L(K) \Leftrightarrow w \in L \wedge K \neq \emptyset$

ここでのポイントは“ $K \neq \emptyset$ ”のチェック。一般には、このチェックは困難。(アルゴリズムが存在しない可能性すらある。)しかし、 K が \emptyset でないと判明している場合、これは trivial に成立する。このようなケースに限定した問題設定が可能。つまり、 $K \neq \emptyset$ のチェックが trivial になるアルゴリズムのみ有効になる自己アルゴリズム言及問題。([5] 参照。) ここでは、実現アルゴリズムに対する制約と K のセマンティクスを関連付けている点に注意せよ。この意味で、 $L(K)$ は K のセマンティクスに依存した決定問題になっている。さて、今、 L の計算量がNPだとする。この時、 K の融合 term 表現として、比較的 (σ コード) サイズが小さなものを固定すれば、 $L(K)$ の計算測度もNPになる。ところが、各 w に対し、 $|w|$ の冪サイズの融合 term 表現 $k(w)$ を対応させる入力 $(w, k(w))$ を取ることができる。このような入力を選択した場合、 $L(K)$ の計算測度はPになる。つまり、同一 K に対し、決定問題 $L(K)$ の計算測度は二つの可能性が生じる。これを、(言語認識問題の) K による“2系統化”と名付ける。

(私のオリジナル。 [1],[2]を参照せよ。) これにより、

「計算量の意味でNP言語 L がPになる $\Leftrightarrow L(K)$ の計算測度は、 K の融合 term 表現に依存せず、Pに一意決定可能」

が成立する。その結果、「P v s NP」問題は、 K に依存した計算測度の一意決定可能性問題「 $P = NP(K)?$ 」と同値になる。 \dashv

4、パラドックスによる消滅

「P v s NP」問題を考える場合、TM計算の定義で許容される範囲であれば、どのようなアルゴリズムでも使用できる。つまり、「P v s NP」問題には、使用可能アルゴリズムに関する制限は設定されていない。当然、融合 term 入力の決定問題のアルゴリズムも σ コードすることで想定

対象になる。ならば、 Δ の決定アルゴリズム (σ コード) は使用できるのか? この不可思議さが議論のポイントである。従来は、TM基準で抽象化することで、これを誤魔化してきた。これを“半純性”と呼ぼう。ここでは、同値な「 $P = NP(K)?$ 」問題を使用することで、計算量理論の間に潜むパラドックスを暴く。まず、

補題 Δ 消滅

「P v s NP」問題は Δ 消滅する。

証明：

$K = V (= \{x \mid \neg(x \in x)\})$ を採用すると、 $V \neq \emptyset$ は trivial に成立。ところが、 V はクラスだから、数学証明の枠外。よって、「 $P = NP(K)?$ 」問題も数学証明の枠外。よって、同値な「P v s NP」問題も数学の枠外。 \dashv

では、可能的決定問題の範囲として、数学の枠内で扱えるものだけを考えればどうか? この方向を精緻に分析するため、仮に、ある形式公理体系 T を決めるとする。(具体例としては、第二層+第三層のアルゴリズム論の公理化。) この場合、

定理 制限独立

「P v s NP」は T から独立した問題。

証明：

T を超える集合 J は必ず存在する。よって、 $K = J$ とすることで「 $P = NP(J)?$ 」は T の枠外問題。 \dashv

これは、通常の独立性証明とは違う、新しい手法。これを“制限独立”と名付ける。ここで重要なのは、

「 T の枠外だから J を考えない」

という言い逃れはできないという点。それは、独立集合を認可しないという未熟で誤った考えになる。この結果は、具体的な T に依存せず成立することに注意せよ。以上の準備の下、

最終解決

「P v s NP」問題は消滅する。

証明：ある形式公理体系 T を証明場に考える。 K の選び方次第で「 $P = NP(K)?$ 」は T 外問題になる。ところが、「P v s NP」問題設定に関し、公理的集合論(数学)の枠内であれば、 K に対する制限は無い。つまり、どんな T を選んでも、ある K が存在して、「P v s NP」は T の枠外。かくして「P v s NP」は数学の枠外問題であることが判明した。 \dashv

以上で、「P v s NP」問題は最終解決されたことになる。この種の論法を“メタ論理的矛盾”に基づく解決と呼ぼう。この概念もオリジナル。史

上初なので、把握困難な査読者向けに、消滅とメタ論理的矛盾の論点を鮮明しておく。

「通常の数学問題QをTで解く場合も、T外Kを採用することで、T外問題Q(K)化できるのでは？」

ここでの課題は、“一般のQの場合、QとQ(K)は同値になるのか？”普通は同値にならない。例えば、T内でYes、Noが証明できるQの場合、同値にはならない。では、QがTで独立なケースでは、どうか？このケースには、弱いKを選べば同値の可能性はある。それでも、T+Q外のKを採用すれば同値にはならない。ところが、「P v s NP」問題の場合、集合論で許容される範囲の、どんなKを採用しても同値になるのだ。ここがポイント。この事実を別の観点から見れば、

「どのような理論Tを採用しても、「P v s NP」はT外問題になり、TでYes、Noが証明できない」ということ。これが“消滅”という用語の定義。かくして、我々は史上初の数学解法第四カテゴリーを発見したことになる。即ち、“Yes、No、独立”に加え、“消滅”する問題があるのだ。数学用語で定義されているが、証明を考えた時、数学の枠外に出る問題のこと。この枠外性をメタ論理的矛盾と名付けた。

ここで使用した“表現 v s 実体”テクニックは枠内の強制法を超えている。(ACと同値な二つの問題の同値性証明はZFで可能という感触、より一般的に言えば、ACの独立性証明がZFで可能という感覚と比較せよ。)「 $P=NP(K)?$ 」との同値性証明は、指定 σ の下でT外Kを考えると意味では、T+Kで実施されている。しかるに、実質的には、コード結果だけに依存している。つまり、 σ 指定はバーチャル。更に、 σ が表現に対し定義されているのに対し、数学(集合論)は実体を扱うというダブルスタンダード問題も発生している。ここに、枠外 Δ における表現と実体の二重性が関与してくる。「P v s NP」問題は、数学の枠外・枠内問題を無視した問題設定になっているという意味。かくして、この消滅は(Δ のような)数学的実体としての側面と形式的表現の側面の不可分性に起因していることが判る。従って、より一般的に言えば、アルゴリズム理論は集合論ベースの数学と相克を起し、パラドックスが発生することになる。この真理が「P v s NP」問題設定者には見えなかった。この意味で、計算量理論は、歴史的に見れば、消滅という新解法登場の契機となった。

5、まとめと展望

では、コードを駆使するアルゴリズム論で証明作業はできないのか？そんな馬鹿なことはない。

ここで証明したのは、“問題によってはパラドックスが発生するケースがある”という真理。アルゴリズム論の場合、第一層が干渉し始める問題が設定され得る。その結果、パラドックスが発生し消滅する問題もあるということ。消滅するかどうかを証明するのも問題解決法なのだ。これが新発見の思想的背景。TM計算だけで考えていると、こういう現象は発見できない。これは、集合論、より広く言えば、決定問題のセマンティクスが、受理言語の抽象的なシンタックスにより隠されてきたことが原因。ここで、従来の常識の何処が駄目なのかを指摘しておく。

「言語認識問題は極めてハッキリした普遍領域。そこに曖昧性が発生する余地はない。」従来の普遍派は全員こう考えていた。これこそが根本的な認識違い。ハッキリしているのは、“言語が認識できるかどうか？”のレベル。つまり、アルゴリズムの存在(∃)問題。ところが、計算量では、可能な総てのアルゴリズムを考える必要が発生する。即ち、全称(∀)問題であり、別次元の話題。“言語認識問題”という用語を使用したため両者を混同してしまった。これこそが、消滅解決法が、これほど理解困難な理由である。

従来の“Yes、No、独立”解決の視点から見れば「P v s NP」のような問題設定はグローバル過ぎるのだ。ならば、「SATはP？」問題なら消滅しないか？これに関する議論も[2],[6]を参照せよ。ここから、Cookの定理の証明の真偽問題に発展する。([3],[4]参照。)いずれにせよ、以後、問題消滅に注意！但し、問題消滅後も、数学 v s 情報科学の境界問題は、依然、残る。実は、

究極メタ定理

第一層+第二層+第三層は普遍枠外理論で状況依存。+

が証明できる。詳しい証明は[2],[6]参照。

参考文献

- [1]山口人生、「 $P=NP$ 」:最終解決、第6回情報処理学会全国大会論文集、2002年3月。
- [2]山口人生、計算量理論の存亡(1):「 $P=NP?$ 」問題の解決、I.I.I., 2002年10月。
- [3]山口人生、SATはNP完全か?:Cookの証明は間違っていた!, FIT2004, 2004年9月。
- [4]山口人生、SATはNP完全か?:Part 2, FIT2005, 2005年9月。
- [5]山口人生、「 $P=NP?$ 」問題の解決:Part 2, FIT2006, 2006年9月。
- [6]山口人生、「 $P=NP?$ 」問題の解決、I.I.I.社サイト新着情報(<http://www.int2.info/news1.htm>), 2001年~2007年。