A-020

「ＰｖｓＮＰ」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「ＰｖｓＮＰ」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「ＰｖｓＮＰ」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：∅、ω、及び、必要に応じて有限個の追加定数
＜２＞集合記号：｛ｘ｜　｝
＜３＞述語記号：∈、＝
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｜ｆ(ｘ)｝は融合 term
３．以上で構成されたものだけが融合 term　⊣

この定義の下、
Δ=｛ｘ｜ｘ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。　⊣

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ｖｓ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ｖｓ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、「ＰｖｓNP」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「ＰｖｓＮＰ」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$＝｛ｘ｜ｘは決定問題の正規入力（＝各種 term 表現された数学対象)｝を考える。当然、Ｚ∪Δ⊂Ｄ$。ここでは、判り易さを優先させてＺ∪Δをベースにする。各決定問題ＱはＺ∪Δ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　⇔ (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、(σ(Y(Q)), σ(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

㈱I.I.I.　代表取締役会長

「ＰｖｓＮＰ」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｜f(ｘ)｝に対し、いくらでも長い融合term表現｛ｘ｜f(ｘ)∧ｔ$_1$＝ｔ$_1$∧ｔ$_2$＝ｔ$_2$∧・・・∧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)∈L(K) ⇔ w∈L ∧ K≠∅

ここでのポイントは“K≠∅”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∅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≠∅”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 ⇔ 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、「ＰｖｓＮＰ」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。 ┤

４、パラドックスによる消滅

「ＰｖｓＮＰ」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、「ＰｖｓＮＰ」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（のσコード）は使用できるのか？こ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、計算量理論の闇に潜むパラドックスを暴く。まず、

補題　Δ消滅

「ＰｖｓＮＰ」問題はΔ消滅する。

証明：

Ｋ＝Ｖ（＝｛ｘ｜￢(ｘ∈ｘ)｝）を採用すると、Ｖ≠∅ 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「ＰｖｓＮＰ」問題も数学の枠外。┤

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

「ＰｖｓＮＰ」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。┤

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

「ＰｖｓＮＰ」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、「ＰｖｓＮＰ」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、「ＰｖｓＮＰ」はＴの枠外。かくして「ＰｖｓＮＰ」は数学の枠外問題であることが判明した。┤

以上で、「ＰｖｓＮＰ」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にしておく。
「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がある。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、「Ｐｖｓ 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、「ＰｖｓＮＰ」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ｖｓ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を考えるという意味では、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。「ＰｖｓＮＰ」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こし、パラドックスが発生することになる。この真理が「ＰｖｓＮＰ」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「ＰｖｓＮＰ」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ｖｓ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６４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？：Ｐａｒｔ２，ＦＩＴ２００５，2005 年 9 月。
[5]山口人生、「Ｐ＝ＮＰ？」問題の解決：Ｐａｒｔ２，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。