「Ｐ＝ＮＰ」：最終解決

4W−06

山口　人生
神奈川大学理学部情報科学科

1　はじめに

「Ｐ＝ＮＰ」問題は、従来の計算量理論（以下、これを“古典計算量理論”と呼ぼう）の枠組み内で定義可能なため、“古典計算量理論で肯定、または否定的に解決可能であろう”とプロの間で想定されてきた。しかし、私は、この常識を打ち破った。つまり、

「古典計算量理論の枠組みでは、この問題に関するＹｅｓ、Ｎｏの解答は得られない」

ことを示す。

但し、この結果は（平行線の公理のように）“「Ｐ＝ＮＰ」が古典計算量理論から独立した命題である”ということを意味しない。

そうではなく、

「古典計算量理論では、ＳＡＴは（アルゴリズムを速くしなくても、）ＮＰと同程度の意味でＰになる」

という意味である。

（全くの新概念。比喩で言えば、“光は波動且つ粒子”と言っているようなもの。）

そして、これこそが、古典計算量理論における「Ｐ＝ＮＰ」問題の最終解決である。

2　Ｂ(λ,Ｓ)－ＳＡＴ

最初に、準備概念の定義をしておく。

定義２－１

(1)ＣＮＦ：ＳＡＴで使用する論理式全体の集合。
(2)Ｂ(m)：次数（アトム数）mのブール代数。
(3)ＣＮＦの要素αが“Ｂ(m,Ｓ)－充足可能”：α内の各命題変数にＢ(m)の適切な要素を代入して、αの値がＢ(m)の部分集合Ｓに属するようにできること。
(4)Ｂ(m,Ｓ)－ＳＡＴ：“Ｂ(m,Ｓ)－充足可能性”に一般化したＣＮＦの充足可能性問題。　┤

ここで注意してほしいのは、入力としての真理値領域Ｂ(m)のサイズである。これが2^mであって、mでないという点は、αのサイズが、αの次数（アトム数）ｎではないという事実と同じ理由による。この定義に従えば、通常のＳＡＴは、Ｂ(1,{1})－ＳＡＴになる。

さて、上のＢ(m,Ｓ)－ＳＡＴは、各αに対し、真理値領域がＢ(m)に固定されているが、これを以下のように相対化することができる。

定義２－２

(1)ＢＰ＝(∪{Ｂ(m)|ｍ≧１})の冪集合
(2)λをＣＮＦから自然数全体ℕへの写像とし、Ｓ∈ＢＰの時、“Ｂ(λ,Ｓ)－ＳＡＴ”：各α毎に、真理値領域をＢ(λ(α))に変動させた“Ｂ(λ(α),Ｓ∩Ｂ(λ(α)))－充足可能性”に基づくＣＮＦの充足可能性問題。　┤

以下、こちらの相対化された概念を使用する。定義により、“Ｂ(λ,Ｓ)－ＳＡＴ”の入力サイズは“α”だけではなく、“Ｓ∩Ｂ(λ(α))”にも依存する。これにより、次の性質が成り立つことが確認できる。

「λやＳの選び方により、“Ｂ(λ,Ｓ)－ＳＡＴ”をαの判定問題としてＰにすることができる。」

（∪{Ｂ(m,Ｓ)－ＳＡＴ|ｍ≧１}に対する対角線論法）

λやＳを抽象的に選んでＰにすると集合論の選択公理が顔を出す。しかし、λやＳを具体的に定義することで、これを避けることができる。例えば、

定理２－３

δ(α)＝“αの次数（αに登場するアトム数）”なる特別なδを採用すると、“Ｂ(δ,Ｓ)－ＳＡＴ”はＳ∩Ｂ(δ(α))がＢ(δ(α))のultrafilterになる時、Ｐになる。■（証明省略）

勿論、これ以外にも、様々な“Ｂ(λ,Ｓ)－ＳＡＴ”をＰにすることができる。例えば、ζ(α)＝“αの次数＋１”なるζでもＰになるｅｔｃ。しかし、以下では、この特別なδに限定して話を進める。

このようにδを指定した場合でも、依然、Ｓは入力になっている。ここが以下の議論のポイントである。

3　Ｊｉｎｓｅｉの同値変換

この節では、ＳＡＴからＢ(δ,Ｓ)－ＳＡＴへの同値変換を考える。

まず、ＣＮＦレベルでは、各αにα自身を対応させる。問題は、ＳＡＴにおけるαの解の探索木が、Ｂ(δ,Ｓ)－ＳＡＴでは、どのような探索木に写されるかである。以下、これについて論じる。

「Ｐ＝ＮＰ」: the final solution
Jinsei Yamaguchi
Dept. of Information Science, Kanagawa University

上述のように、ＳＡＴとは、正確に言えば、Ｂ(1,{𝟙})－ＳＡＴのことである。よって、次数ｎのαに対応する真理値領域Ｂ(ｎ)をある ultrafilterＵで類別して、商代数Ｂ(ｎ)/Ｕにおける付値が元のＢ(1)での付値と一致するようにαのＢ(ｎ)値化を考える。

つまり、α内のアトム（命題変数）$A_1,\cdots,A_n$に対し、元のＳＡＴで真理値$𝕥_1,\cdots,𝕥_n$が代入された枝Ｌに対し、Ｂ(ｎ)では、$𝕓_1,\cdots,𝕓_n$を対応させる。ここで、各$𝕥_i$に対し、

$𝕥_i=𝟙$ならば$𝕓_i\in U$、　$𝕥_i=𝟘$ならば$𝕓_i\notin U$

とする。

また、真理値$𝕥_1',\cdots,𝕥_n'$が代入された別枝Ｌ'に対し、Ｂ(ｎ)では、$𝕓_1',\cdots,𝕓_n'$を対応させる。ここで、各$𝕥_i'$に対し、

$𝕥_i'=𝟙$ならば$𝕓_i'\in U$、　$𝕥_i'=𝟘$ならば$𝕓_i'\notin U$

とする。

以下、同様である。

この付値では、同じA_iが、（枝によって、）異なる３個以上のＢ(ｎ)の要素に対応する可能性もあることに注意！

このような対応を、“{𝟙,𝟘} のＢ(ｎ)/Ｕ化”と名付けよう。この概念のポイントは、

「Ｕは任意だが固定された ultrafilter である」

という点である。この対応により、

定理３－１

ＳＡＴでαの各アトムに対するある {𝟙,𝟘} 代入がαの値を𝟙にする

ｉｆｆ

Ｂ(δ,Ｕ)－ＳＡＴでαの各アトムに対する、“{𝟙,𝟘} のＢ(δ(α))/Ｕ化”により、αの値はＵに属する。

■（証明省略）

これで「Ｊｉｎｓｅｉの同値変換」が定義できた。

ところで、この同値変換は、ＳＡＴからＢ(δ,Ｕ)－ＳＡＴへの還元とみなすことができる。この還元はＰで実行可能であろうか？以下、この点をチェックしてみよう。

今、次数ｎのαの探索木を考える。ＳＡＴ側の {𝟙,𝟘} 代入のある枝に対し、対応するＢ(δ,Ｕ)－ＳＡＴ側の枝の各ノードは、Ｂ(ｎ)の元が対応している。ここで、Ｂ(ｎ)の各要素は、“{𝟙,𝟘} のｎ項順序対”として定義できる。よって、サイズはｎのオーダー。そして、枝の深さは、ＳＡＴ側の枝の深さと一致する。つまり、ｎ。従って、枝全体も、やはり、ｎのＰサイズで計算できる。最後に、枝の葉値がＵに属するかどうかのチェックは、ＵがＢ(ｎ)のアトムから生成される ultrafilter であるという事実によりｎのＰサイズで計算できる。

以上により、αに(α,Ｕ)を対応させる還元はＰで実行可能であることが判る。Ｕのサイズ自体は2^nであるが、Ｕが主 filter である点が、このマジックの種である。

（ブーリアンシンタックス）

４　計算量的パラドックス

Ｃｏｏｋの還元では（論理式が変化するため）探索木が巨大化した。一方、Ｊｉｎｓｅｉの還元では、探索木の構造自体は変化せず、各ノードが複雑になった。それゆえ、同じ入力αに対し、ＳＡＴよりも計算量は増えている。にもかかわらず、理論的には入力Ｓの所為でＰになる。実は、このような現象こそ、古典計算量理論の特質なのである。

一見単純な上の証明中、入力Ｕのサイズに関し、議論が沸騰するであろう。一般的な定理では、Ｕのサイズは2^n。一方、実際に計算する場面では、ｎサイズで処理可能。つまり、全く同じ計算処理をしている入力Ｕに対し、一方ではサイズを2^nのオーダーとみなし、他方ではｎのオーダーとみなしていることになる。この種の“混同”を避けるため、果たして、どちらに決めたらよいのか？

実は、この決定が古典計算量理論の枠内では、“原理上できない”のである。（記号・実体問題）

計算量理論では、その他にも、様々な興味深い「概念定義問題」が発生するが、ここでは詳しく論じない。これらを総称して、古典計算量理論の「計算量的パラドックス」と呼ぼう。これは、新種のパラドクッスである。つまり、一方と同等の理由で、他方も成立する（ことを認めざるを得ない）。そして、ＳＡＴがＢ(δ,Ｕ)－ＳＡＴに還元できる以上、この種のパラドックスは不可避である。

何れにせよ、上の“「Ｐ＝ＮＰ」の証明”は見かけほど単純なわけではない。その特質により、「Ｐ＝ＮＰ」は現代数学・計算機科学の（中核ではなく）最辺境の新成果を駆使せねば解決不可能なのだ。そして、私は成功した。

この成果を理解するには、古典計算量理論を完全にマスターし、さらに、それを乗り越える才能を備えていることが前提になる。

５　まとめ

計算機分野における難問「Ｐ＝ＮＰ」は、従来、否定的な見解が大勢を占めていた。しかし、私は、これを「計算量的パラドックス」という全く新しい形で解決した。証明の詳しい内容は論文にして出版する。また、一般読者向けの解説が、まもなく、本の形で出版される予定である。

上の還元は「Ｐ＝ＮＰ」の解決という目的に特化したものである点に注意してほしい。実は、Ｓ＝Ｂ(δ(α))－{𝟘} を採用することで、より高速のアルゴリズムが実現可能になる。(ｎ葉同時ベクトル処理＋・・・) これに関する議論は、また別の機会に。