A-035

ＳＡＴはＮＰ完全か？
（Cook の証明は間違っていた！）
Is SAT NP- complete?
(Cook's proof is wrong!)

山口人生
(Yamaguchi Jinsei)

１．序論

計算量理論の専門家ではなくても、そして、その内容は知らなくても、情報科学の分野に「Ｐ＝ＮＰ？」という難問があることは、この業界の研究者ならば聞き及んでいるはずである。特に、２０００年に、クレイ数学研究所がミレニアム難問の一つとして１００万＄の懸賞金を懸けてからは、一気に有名になった感がある。

これに関連して、

「ＳＡＴ（充足可能性問題）はＮＰ完全である」…（１）

という結果も聞いたことがあると思う。これは、S. Cook（[1]）によって、１９７１年に発表された仕事であり、それ以来、計算量理論の根幹を成してきたものである。当然、従来の「Ｐ＝ＮＰ？」問題に対する挑戦は、全て、この基本原理（１）に則ってアプローチされてきた。

しかしながら、私は

「Cook の証明には本質的な誤りがある」

ことを発見した。今回の発表により、計算量理論は根本的改革を迫られることになろう。

２．Ｃｏｏｋ還元再考

以下、“決定問題”、“論理式”、“充足可能性”、“ＳＡＴ”、“計算量”、“クラスＰ”及び“クラスＮＰ”、“（非）決定性ＴＭ（チューリングマシン）”、“受理言語”、“（多項式）還元”、“ＮＰ完全”、等の最低限の用語は周知のこととする。詳細を確認したい方は、計算量理論系の教科書か、この分野の辞典を参考にしてほしい。

さて、Cook が（１）の証明で用いた Cook 還元の定義を厳密に調べてみよう。ここでは、紙幅の関係で詳細には言及できないが、あの定理の証明で採用した還元には基本的欠陥があることが判る。それは、

「Cook 還元では、不正解入力の行き先指定ができていない」

という点である。きちんと言えば、

定理１．

Cook 還元は還元になっていない。

証明：

ある（ＮＰ）問題から別の（ＮＰ）問題への“多項式還元”とは、

「元の問題の入力全体を定義域とする写像」

の内、特に、

１、入力に対する正否の判定が、元の問題と写像後の問題とで一致する（還元性）

２、写像が、元の問題の入力サイズに対し、多項式時間で構成できる（多項式性）

場合のことを言う。

しかるに、Cook の定理で提示した対応関係は、

「元の問題の正解集合全体を定義域とする写像」

に過ぎない。

よって、還元にはなっていない。

従って、

系２．

Cook の証明はＳＡＴのＮＰ完全性証明にはなっていない。

よって、ＳＡＴのＮＰ完全性を主張するには、不正解入力の行き先を追加指定する必要がある。問題は、

「Cook の証明を修正して、無事、定義域を入力全体に拡張できるかどうか？」

である。この為、例えば、不正解入力に対し、常に、（特定の）充足不能論理式を対応させればどうか？正解集合と不正解集合は disjoint だから、一瞬、これで拡張できたように見える。しかし、この種の拡張は、

「正解入力と不正解入力が写像の時点で区別できている」

という前提が必要になるのだ。この前提が、不自然なことは、

『事前に区別できているのならば、

「正解は全て、（特定の）tautology に対応させ、不正解は全て、（特定の）充足不能論理式に対応させる」

ような写像でＳＡＴに還元できることになる。』

という事実から明白であろう。区別が多項式時間で可能になるのならば、「Ｐ＝ＮＰ」ということである。つまり、この前提は仮定できないのだ。よって、この種の拡張は、拡張になっていない。

となると、最後に

「Cook の証明とは全く異なる方式で、ＳＡＴがＮＰ完全になることが証明できる可能性はないのか？」

という疑問が湧くはずである。これに対する否定的見解が次節で提示される。

３．層化還元問題

“論理式 α が充足可能である”とは、α を論理変数の {1,0} 真理値関数（ブール関数）として見た時、

（$\exists\theta$ ：代入）（$\alpha\theta=1$）

が成立することを言う。この時、以下の疑問を提示することができる。

「α が充足可能な場合、代入 θ を具体的に計算する必要があるのか？」…（２）

これが有効な論点になるためには、

「θ の具体的計算抜きで、α の充足可能性がチェックできるアルゴリズムが存在する」…（３）

ことが必要になる。果たして、このようなアルゴリズムは

（株）Ｉ．Ｉ．Ｉ．代表取締役会長

存在するのであろうか？実は、このタイプのアルゴリズムが実在することを私は証明した。即ち、

定理３.

（３）は成立する。

証明：

長くなるので省略。

この証明中に使用した技術が“ワープ（瞬間移動）”というテクニックである。ここでは、この方面の詳しい議論は割愛するが、要点を単純化して言えば、

「論理式の変形過程を、補題使用により、省略する」というアイデアが核になっている。

さて、（２）の問題意識により、従来ＳＡＴと呼んできた決定問題とは別に、次のような決定問題を定義できることが判る。

「任意の論理式αに対し、αの充足可能性を保証する代入θが（少なくとも一つ）計算できた時、Yes。それ以外はNo。」…（４）

ここで注意すべき点は、

「代入が計算できないＳＡＴアルゴリズムは、この決定問題のアルゴリズム候補にはなり得ない」

という点である。一般に、この種の問題を“witness 計算問題”と呼ぶことにする。そして、特に問題（４）をＣＡＴと呼ぶことにしよう。そして、ＣＡＴとＳＡＴの相違を際立たせるため、ＣＡＴの入力を$(\alpha, c(\alpha))$の形にする。ここで、$c(\alpha)$は

「αが充足可能な場合、その witness 代入（の一つ）を具体的に計算する関数」

に対応した形式的記号である。これで、ＳＡＴとＣＡＴの受理言語が異なった。この場合、“$(1,\theta)$”なる計算結果が得られた時に Yes、“(0,0)”なる結果の時は No となる。

ここでの課題は、ＣＡＴをＳＡＴに還元できるかどうかである。これに関しては、ＣＡＴの定義により、通常の還元手法では無理なことが判る。即ち、

定理４.

“$(\alpha, c(\alpha)) \Rightarrow \alpha$”対応では、ＣＡＴはＳＡＴに還元不能。

証明：

この手法で還元したら、具体的代入が計算できないＣＡＴアルゴリズムが登場し、ＣＡＴの定義（セマンティクス）に反する。

この結論により、ＣＡＴからＳＡＴへの還元の難しさが理解できよう。しかし、何らかの特殊な還元手法を採用すれば、ＣＡＴの witness 計算がＳＡＴの論理式で知識表現できる可能性は残っている。その場合、問題は、

「その還元が多項式時間で可能かどうか？」

である。Cook 還元の場合は、還元性が保持できていなかったが、この特殊還元（知識表現）の場合には、多項式性が課題になる。例えば、冪オーダ時間の対応を許容すれば、この種の知識表現は可能になることが（私なら）証明できる。しかし、それでは、ＮＰ完全性の保証にはならない。かくして、ＳＡＴのＮＰ完全性は、未だに、open problem のままなのである。

実は、この問題に関連し、計算量理論の存亡に関わる大問題が発生する。即ち、

「従来の（素朴）計算量理論は、パラドックスを内包した非厳密理論である」

ことが証明できるのである。つまり、

『「ＣＡＴはＳＡＴに多項式還元可能かどうか？」の解答が、Yes, No で得られる』

と無邪気に考えてはいられなくなってきたのだ。更に、このパラドックスは、「Ｐ＝ＮＰ？」問題の解答にも影響を及ぼす。即ち、

『「Ｐ＝ＮＰ？」問題は“Yes, No”、もしくは、“独立”で解決できる』

という、従来の想定が破綻してくるのである。この話題に関しては、別の機会に発表する。

この種のパラドックス分析過程を通じ、

「従来のＳＡＴと、今回提示したＣＡＴとは、カテゴリーの異なるＮＰ問題になる」

ことが発見できる。そして、ＣＡＴは、ある種の witness 計算問題グループ内では、相互に多項式還元可能になる。これは、ＳＡＴ（と相互多項式還元可能な）問題が一群のＮＰ問題グループを成している事実からの帰結である。つまり、

「ＮＰは少なくとも２つの（還元ベース）階層に分かれている」

とみるのが自然なのだ。これが、この節の題で使用した“層化還元”という概念の由来である。

４．まとめと展望

ＳＡＴのＮＰ完全性は証明できていないことを示した。ここから、従来の素朴計算量理論の綻びが徐々に露呈してくることになる。そして、最終的には、理論に内在するパラドックスの発見にまで繋がってくる。そのパラドックスが「Ｐ＝ＮＰ？」問題を直撃するのである。その結果、「Ｐ＝ＮＰ？」問題は、思いもよらない方法論により解決されることになる。

実は、私は去年の春の段階で「Ｐ＝ＮＰ？」問題を解決している。([2],[3],[4]参照。) しかし、証明手法の斬新さの所為で、あの時点では、誰も理解できなかった。それ以来、１年以上に渡り、証明の詳細な説明をサイト

http://www.int2.info

で続けた。そろそろ、その解説も終了を迎えようとしている。今回の発表は、その内容のまとめ第一弾である。

参考文献

[1]S. Cook, The complexity of theorem-proving procedures, *Conference Record of Third Annual ACM Symposium on Theory of Computing*, 151-158, 1971.

[2]山口人生、「Ｐ＝ＮＰ？」問題の解決、*Proceeding of IPSJ 64,* Vol.1, 183-184, 2002.

[3]山口人生、計算量理論の存亡（１）:「Ｐ＝ＮＰ？」問題の解決、*Ｉ．Ｉ．Ｉ．*, 2002.

[4]J. Yamaguchi, A proof of P≠NP: toward the axiomatic computational complexity theory, *http://www.int2.info*, 2003.