

解の存在が保障されている組合せ 探索問題について

京産大・理 岩間一雄 (Kazuo Iwama)

1. まえがき

NP-完全性の理論は、解を具体的に求めることを要求する探索問題に対してでなく、解が存在するかどうかを問う決定問題を対象に構築されている。しかし、ほとんどの場合、決定問題は対応する探索問題より易くなるということが示せるので、一般性は失われていないとされている(例えば[1])。このことは、探索問題の方が決定問題より何となく難しそうだという漠然とした“常識”があるからと見えてくる理屈であろう。その常識の正当性を問う直すことが本稿の主目的である。関連して、線型に近い時間計算量を有する1テープTMについての2,3の話題にも触れる。

2. 問題集の直観的説明

例として、和積型論理式の充足可能性問題(SAT)と、論理式の値を真にするような変数への真偽の割当て(解)を具

体的に求める問題 (ASSIGN) を考えてみよう。ここで、通常の前程は、双方のインスタンス集合は等しい、つまり、ASSIGN に対しても解を有しない論理式が入力されるというものである。この前程のもとでは、確かに ASSIGN は SAT 以上の難しさを有している。(実はよく知られているように双方は同じ程度の複雑さを有する。) しかるに、ASSIGN の真の目的が純粋に真偽の割当てを求めることにありと考える存す、対象とするインスタンスは常に少なくとも1つの解を有するという制限を付したもの (ASSIGN* で表わす) も十分意味を持ちかつ実際的であろう。ASSIGN の場合と同様の結論 (ASSIGN* も SAT 以上の難しさである) が可能であろうか。

ある人はこの問に対して、「もし ASSIGN* を解く決定性多項式時間 TM M (M はある多項式 $T(n)$ に対し $T(n)$ 時間限定である) が存在する存す SAT を解く同様の TM N を以下の様に容易に構成できるか? 結論できることは明か。」と答えるかもしれない。 M は長さ n の入力 (解を持つ論理式) に対して、 am^b ステップ (a, b は定数) 以内で停止するとする。 N は与えられた長さ m の (解を持たないかもしれない) 論理式 E に対し、それをそのまま M の入力として M の動作を模倣し、同時に M のステップ数を数える。もし M が am^b ステップ以内に停止して解を出したとすれば本当に正しい解

であるか (Eを真にするか) を検算し (これは多項式時間で可能である), 正しいければ (正しくなければ) Eは充足可能 (不能) と答を出す. $a \cdot m^b$ ステップを超えても停止しなければ充足不能と答を出す.

この主張はかなりの厳密さに欠けており, よくみればいくつかの重要な問題集を含んでいる. オ1に整数 a と b が降っていったように出て来ている点である. 与えられた M に対し a と b が計算できるのならばだが, それが不可能なことはほとんど自明である. より形式的には次の事実が成り立つ. k -ステップ決定性多項式時間 TM M と整数 a と b に対し, M がすべての入力 x に対し, $|x|^b$ ステップ以内で停止するかという決定問題は, $k=b=1$ の場合を除いて非可解である. (なお, $k=b=1$ の場合は可解になり, こゝろの方は自明ではない. 関連の話題も含め5. で簡単に触れてみた.) オ2の問題集は, ある問題 A に対する多項式時間アルゴリズム M が存在するならば別の問題 B に対する同様のアルゴリズム N が構成できるという議論の中の構成法に関してである. 容易に気付くことであるが, 上で述べたような N の構成ができるためには (たとえ a と b が与えられたとしても) M がプログラムブックとして与えられるのでは不十分で (ステップ数の計測が不可能), 具体的に与えられる必要がある. M の存在を否

定しようという目的にたじみかどうが疑問の残るところであ
らう。

このように、 $ASSIGN^*$ がSAT以上の難しさを有するかどう
かについては、軽々に結論することはできない。こうして考
えてくると、問題間の変換可能性 (reducibility) の概念の便
利さ (上の様なめんどうを起さず) が改めて実感であ
る。それは本報告の目的にも適合すると思われる。

3. 問題とその変換可能性

問題 P は、(1) インスタンスの集合 $I(P)$ と、(2) 個々のイン
スタンス $x \in I(P)$ に対する解 $P(x)$ の記述より成る。例え
ば、SAT の場合、インスタンス集合は和積型の論理式の全体、
インスタンス x に対する解は、 x が充足可能 (不能) なら
 yes (no) である。ASSIGN については、インスタンス集合
は同じであるが、 x に対する解は、 x が充足可能であるとい
はる真偽割当て、不能のときは no である。ASSIGN * は
インスタンス集合が充足可能な論理式だけに制限された ASSIGN
である。問題 P_1 が、問題 P_2 をオラクルとするある決定性多項
式時間 TM によって解くことができるなら P_1 は P_2 へ変換可能
であるといひ、 $P_1 \leq P_2$ とかく。この TM はオラクルを参照
するときは、必ず $I(P_2)$ に属するインスタンスをパラメー
タにしなければならぬといふことは言うまでもない。 $P_1 \leq P_2$ で

かつ $P_2 \leq P_1$ であるとき $P_1 \equiv P_2$ とかく。

4. 解の存在が保障されている探索問題の複雑さ

SAT \equiv ASSIGN であることはよく知られており、2つの問題はある意味で等しい複雑さを有する。この系として、 $ASSIGN^* \leq SAT$ が得られる。この逆はどうか。もし、 $SAT \leq ASSIGN^*$ なる $ASSIGN^*$ をオラクルとする TM M が存在する。

そこでその M のオラクルの部分（オラクル入力テープ上の論理式のある真偽割当てを仮想的に1ステップでオラクル出力テープに出す）を、与えられた論理式の解をヤス（これを確認した上で出力テープに出す非決定性サブルーチン（明らかに多項式時間）で置き換えた M' とする）というのだろうか。容易に判るように、 M' は与えられた論理式に対して、 Y_{es} （充足可）と答を出すのも n_0 （不可）と答を出すのも共に非決定性多項式時間（ヤスが当たれば多項式時間という意味）である。このことに気付けば次の定理の証明は易しい。

[定理1] $SAT \leq ASSIGN^*$ なる $NP = co-NP$ である。

従って、 $SAT \leq ASSIGN^*$ である可能性はほとんどなく、 $ASSIGN^*$ は SAT よりある意味で易しいといえる。 $P \neq NP$ かつ $NP \neq co-NP$ を仮定すると、 $ASSIGN$ に対する多項式時間アルゴリズムは存在しないことが結論できるが、 $ASSIGN^*$ に対しては、多項式時間アルゴリズムが存在すると仮定しても

現時点では矛盾は生じていない。(ただし、2.の議論から明らかなように、そのアルゴリズムとステップ数の上界を与え子多項式を具体的に求めることができないことを仮定すると矛盾が生じる。) 与えられた論理式は必ず解を持つという性質が、解を求める上で、決定的なヒントになる可能性を(少いにしても)残しているのである。

さらにインスタンス集合を制限して、例えば唯一つの解を持つものだけに制限(これを UNIQUE ASSIGN で表わす)したらどうだろうか。UNIQUE ASSIGN \leq ASSIGN* は自明であるが逆については現在のところ何もわかっていない。しかし、唯一の解を持つ論理式は、えうとは限らない論理式にはない、利用できるかもしれないいくつかの性質を有している。例えば、 $f(x_1, \dots, x_n)$ を元の論理式としたとき、 x_1 (別にどの x_i でもよい) を 0 に固定した式 $f(0, x_2, \dots, x_n)$ と 1 に固定した式 $f(1, x_2, \dots, x_n)$ を考えたとき、必ず一方は奇数個他方は偶数個の最大項をおおうことがわかる。(もちろん奇数個の方に解がある。) 和積型の論理式がすべての最大項をおおうかどうか、あるいはおかない最大項はどれかといった質問に比べ、おおう最大項の数が奇数かどうかの質問の方が直観的には易しく、本質的なヒントになりうる可能性もある。

インスタンス集合を制限することが以上の様な効果をおよ

が成り立つこともある。1-インスタンス集合は $ASSIGN^*$ と同じだが、極大の解 (解 (a_1, \dots, a_n) が極大であるとは、 $a_1 \leq b_1, \dots, a_n \leq b_n$ であるような (b_1, \dots, b_n) も解で $a_1 = b_1, \dots, a_n = b_n$ に成り立つこと) を求める問題は $MAXASSIGN$ とある。

[定理2] $MAXASSIGN \equiv SAT$. (証明略)

このことは、 $ASSIGN^*$ に対する良いアルゴリズムを発見したと思っても、もしそれが常に極大 (極小でも同じ) の解を出してくるようなものは $ASSIGN^*$ の定理1の性質をそのまま利用して成り立つことを証明したことになる。

5. $n \log n$ より少ない時間計算量を有する 1テープ

TM について

線型時間に近い 1テープ TM (この章では常に 1テープであるが以後こゝから成り立つ) について判っていることはそれほど多くなく、筆者の知る限りでは、線型時間の場合には正規集合しか受理できない、決定性 $O(n \log n)$ 時間で受理できる非正規の言語が存在することぐらいである。 $T(n)$ 時間限定 TM の定義はいくつかの異なったものが知られている。ほとんどの場合においてこれらの違いは問題に成り立つものに対し、ここではそれが無視できる。先ずは、 $T(n)$ 時間限定 TM は、もし入力が受理されるような受理に至る任意の計算過程 (非決定性の場合には2つ以上ありうる) が $T(n)$ ステップ以

内に終了するという定義(例えば(2))の場合を考える。次の補題が中心である。

[補題1] 状態数 a の TM M の入力 x で次の条件を満たすものを考える。 x に対する通過列 (crossing sequence) の最大長が k であり、かつ $n-1$ 以下の長さ ($n=|x|$) の w が存在する入力に対しても通過列の最大長が k に存在する w に対する受理に至る計算過程が存在しない。(つまり x は長さ k の通過列が現れうる最短の入力。) このとき、 x に対する上の計算過程のステップ数は、少なくとも $\frac{n}{8} \log_a \left(\frac{n}{8}\right)$ である。 (証明略)

より直観的にいうと、もし M の通過列の最大長が入力の長さにつれて制限なくいくつでも大きくなっていくようなら、(補題の制限を満たす x はいくつでも長いものが存在するから) M の時間計算量は $\Omega(n \log n)$ である。このことを使って2.3の事実が証明できる。

[定理3] $O(n \log n)$ 時間限定 TM は正規集合しか受理できない。

[定理4] TM M と整数 a, b に対し、 M がすべての入力 x に対し、 $a|x|+b$ ステップ以内に停止するかどうかは可解である。

補題1が主張している内容は、TM の別の定義に対しては

意味を失ってしまふ。つまり、例えば(3)では、 $T(n)$ 時間限定 TM (非決定性) は、入力 x に対し、受理に至る最短時間の計算過程のステップ数が $T(n)$ 以下なように、前の定義に比べて制限がゆるく、また非決定性操作の基本的考え方により合致していると思われる。しかし、この場合もやはり、 M の計算時間は線型な形式 $T(n)$ より $\Omega(n \log n)$ で増加すること強く予想される。これらについては稿を改めて述べる。

6. 注意

インスタンス集合を制限して問題を易しくすることは、解が存在するかどうかを問う決定問題の場合も教知れが行われている。しかし、決定問題の場合には全く意味を持たない制限が存在し、その一つが本稿で論じた "常に解を持つインスタンス集合" に制限することである。このこと一つとつても決定問題だけで十分であるという一般に広まっている考え方の問題点を示している。

定理 3 は東工大小林によっても最近独立に発見された。東工大渡辺は 2. に関して、「 $ASSIGN^*$ を解く多項式時間 TM M が存在するならば SAT を解く同様の TM N も存在する」ことには正しいことを指摘した。貴重な御意見をいただいたり、また共に議論していただいた両先生に深謝いたします。本研究は一部文部省科学研究費による。

文献

- (1) M. Garey and D. Johnson, Computers and Intractability, W.H. Freeman (1979).
- (2) J. Hopcroft and J. Ullman, Introduction to Automata Theory, Languages and Computation, Addison-Wesley (1979).
- (3) H. Lewis and C. Papadimitriou, Elements of the Theory of Computation, Prentice-Hall (1981).