数理解析研究所講究録
556巻 1985年 250-259

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しくなるということがないことが示せるので，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"があるからこそ出てくる理屈であろう．その常識の正当性を問い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. 問題点の直観的説明

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う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ると考えるなら，対象とするインスタンスは常に少くとも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）が存在するならSATを解く同様のTM Nを以下の様に容易に構成できるから結論できることは明らか自明だ。」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，an^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，それをかまわずMへの入力として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an^bステップ以内に停止して解を出したらそれが本当に正しい解

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），正しければ（正しくなければ）Eは充足可能（不能）と答を出す．an^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．

この主張はかなり厳密さに欠けており，よくみればいくつかの重要な問題点を含んでいる．第1に整数aとbが降ってわいたように出て来ている点である．与えられたMよりaとbが計算できるのならすだよいが，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．チューリング決定性多項式時間TM Mと整数aとbに対し，Mがすべての入力xに対し，$a|x|^b$ステップ以内で停止するかどうかの決定問題は，$a=b=1$の場合を除いて非可解である．（なお，$a=b=1$の場合は可解になり，こちら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い．）第2の問題点は，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がブラックボックス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の存在を右

定しようという目的になじむかどうか疑問の残るところであろう.

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こさない) が改めて実感できる. 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, (i) インスタンスの集合 I(P) と, (ii) 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) なる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きはある真偽割当て, 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い, $P_1 \propto P_2$ とかく. このTMはオラクルを参照するときには, 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ないことは言うまでもない. $P_1 \propto P_2$ 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．この逆はどうであろうか．もし，SAT $\leq$ ASSIGN* なら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上に出す）を，与えられた論理式の解をゲスしてそ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）で置き換えたら（M'とする）どうであろうか．容易に判るように，M'は与えられた論理式に対して，yes（充足可）と答を出すのも no（不可）と答を出すのも共に非決定性多項式時間（ゲ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* なら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。（たゞし，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る多項式を具体的に求めることができることまで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，解を求めるまでで，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UNIQUEASSIGNで表わす）したらどうであろうか。UNIQUEASSIGN ≤ 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，そ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，$f(x_1,\cdots,x_n)$をそのような論理式としたとき，x_i（別にどのx_iでもよい）を0に固定した式$f(0,x_2,\cdots,x_n)$と1に固定した式$f(1,x_2,\cdots,x_n)$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，あるいはおおわ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ほう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

ぼさないこともある．インスタンス集合はASSIGN* と同じだが，極大の解（解 $(a_1,\cdots,a_n)$ が極大であるとは，$a_1 \leq b_1$，$\cdots$，$a_n \leq b_n$ であるような $(b_1,\cdots,b_n)$ も解なら $a_1=b_1,\cdots,a_n=b_n$ になることをいう）をめる問題をMAXASSIGNとする。

［定理2］ MAXASSIGN ≡ 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ら，それはASSIGN* の定理1の性質をすこしも利用していないことを証明したことになる．

5. $n\log n$ より少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テープであるから以後ことわらない）について判っていることはそれ程多くなくて，筆者の知る限りでは，線型時間の場合には正則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則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ったものが知られている．ほとんどの場合においてそれらの違いは問題にならないのにたして，ここではそれが無視できない．先ずは，$T(n)$ 時間限定TMは，もし入力 x が受理されるなら受理に至る任意の計算過程（非決定性の場合は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q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であるような受理に至る計算過程が存在し，かつ$n-1$以下の長さ（$n=|x|$）のいかなる入力に対しても通過列の最大長がkになるような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，少くとも$\frac{n}{8}\log_q(\frac{n}{8})$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らでも大きくなっていくようなら，（補題の制限を満たすxはいくら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．このことを使ってこれら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にたして，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

意味を失ってしまう．つまり，例えば(3)では，$T(n)$ 時間限定TM（非決定性）は，入力文に対し，受理に至る最短時間の計算過程のステップ数が $T(n)$ 以下なるよく，前の定義に比べて制限がゆるく，また非決定性動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の計算時間は線型でないだろう $\Omega(n\log n)$ で増加することが強く予想される．これらについては稿を改めて述べたい．

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数知れず行われている．しかし，決定問題の場合に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1つとっ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ついている．

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SATを解く同様のTM Nも存在する」ことは正しいことを指摘した．貴重な御意見をいただき，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).