Chin. Ann. of Math.
9B (4) 1988

THE STRUCTURE OF RELATIVIZED *P* AND *NP* QUESTIONS

YE HHNG (叶 红)*

Abstract

First, based on the work of [5] a new property on the structure of P and NP is proved. Then, using the notions of mitotic and non-mitotic defined by R. E. Ladner[6], the author defines similar concepts in the relativized classes P^X, NP^X and constructs a recursive oracle. In the constructions, an NP-non-mitotic set is obtained by using the simple priority argument and the coding strategy which Robert I. Soare[8] used to prove the density results in the r.e. degrees.

§1. Introduction

Since [1] introduced the relativized P and NP problems, many questions which are quite difficult to deal with in P and NP have been solved in relativized classes P^X and NP^X.

Almost at the same time of [1], [5] introduced the structure of the degree of P and NP.

We will prove some new results on the structure of relativized classes P^X and NP^X.

In this section, we will give some notations.

We fix the alphabet $\Sigma=\{0, 1\}$ as the alphabet in which all $(P)NP$ sets are encoded, so that a $(P)NP$ set is simply a subset of Σ^*.

Let $<$ be the natural order on Σ^* ($\lambda<0<1<00<01<10<11<000<\cdots$), where λ represents the empty string.

If $x\in\Sigma^*$, we let $|x|$ denote the length of x.

We define a 1−1 and on-to function f which maps Σ^* into N as follows: f: $\Sigma^*\to N$. Σ^*: λ 0 1 00 01 10 11 000 $\cdots$,

N: 0 1 2 3 4 5 6 7 $\cdots$,

i. e. $f(\lambda)=0$, $f(0)=1$, $f(1)=2$, $f(00)=3$, $\cdots$.

For each set A and string x, according to the natural order of Σ^* we define

$$A\upharpoonright x=\{y\,|\,y\leqslant x \text{ and } y\in A\}.$$

Manuscript ereceived August 17, 1985. Revised January 2, 1987.

* Department of Computer Sciece and Technology, Beijing University, Beijing, China.

The definition of P, NP, P^A, NP^A are the same as [1].

Let $\{P_i^B: i\in N\}=P^B(\{NP_i^B: i\in N\}=NP^B)$ be a standard enumeration of the polynomial time bounded oracle deterministic (non-deterministic). Turing machines with oracle set B, and we let $\{P_i: i\in N\}$ be a recursive sequence of polynomials such that P_i bounds the run time of $P_i^B(NP_i^B)$ for each oracle B. when $B=\phi$, P_i^ϕ, P^ϕ, NP_i^ϕ and NP^ϕ are abbreviated to P_i, P, NP_i, and NP respectively.

We say

$$A\leqslant_T^P B \text{ if } \exists i \text{ such that } A=P_i^B,$$

$$A\leqslant_T^{NP} B \text{ if } \exists i \text{ such that } A=NP_i^B,$$

$$A\equiv_T^P B \text{ iff } A\leqslant_T^P B \text{ and } B\leqslant_T^P A,$$

$$A\equiv_T^{NP} B \text{ iff } A\leqslant_T^{NP} B \text{ and } B\leqslant_T^{NP} A,$$

$$A<_T^P B \text{ iff } A\leqslant_T^P B \text{ and } B\nleqslant_T^P A,$$

$$A\Big|_T^P B \text{ iff } A\nleqslant_T^P B \text{ and } B\nleqslant_T^P A,$$

$$A<_T^{NP} B \text{ iff } A\leqslant_T^{NP} B \text{ and } B\nleqslant_T^{NP} A.$$

We use Gödel numbering of $N\to N^4$, Which can be encoded and decoded within polynomial steps.

$N\to N^4$ means $t\to(i, j, k, l)$ where $t=(i, j, k, l)$ denotes $(((i, j), k), l)$.

For every number $\underline{n}$, n denotes the n-th string in the natural order of Σ^*, i. e. $f(\underline{n})=n$.

We encode each finite sequence of binary strings $x_1, \cdots, x_m$ into the binary string $(x_1, \cdots, x_m)$ that is obtained from the string $x_1{}^*\cdots{}^*x_m$ (over the alphabet $\{0, 1, *\}$) by replacing each occurence of 0, 1, $*$ by 00, 01, and 11, respectively.

Both the encoding and decoding can be performed in time bounded above by a linear function of $|x_1|+\cdots+|x_m|$. Note that $|x_i|<|(x_1, \cdots, x_m)|$ for every $i\leqslant m$.

Suppose B is a given oracle, we define the following:

A set A is P-mitotic in P^B if $A\in P^B$ and there are two sets C, $D\in P^B$, such that $C\cup D=A$, $C\cap D=\emptyset$, $C\equiv_T^P A\equiv_T^P D$. We say that (C, D) is a P-mitotic splitting of A.

A set A is NP-mitotic in NP^B if there are sets C, $D\in NP^B$ such that $C\cup D=A$, $C\cap D=\emptyset$ and $C\equiv_T^{NP} D\equiv_T^{NP} A$. We say (C, D) is an NP-mitotic splitting of A.

A set A is NP-non-mitotic in NP^B if for all C, $D\in NP^B$, (C, D) is not an NP-mitotic splitting of A.

A set A is P–non–mitotic in P^B if for all C, $D\in P^B$, (C, D) is not the P–mitotic splitting of A.

The existence of P–mitotic set is trivial. In particular, in class P, for all $A\in P$, ϕ, A split A and $\phi\equiv_T^P A\equiv_T^P A$ (We can compute A within polynomial steps without oracle).

The existence of NP–mitotic set is trivial. For each set A, if A is P–mitotic then A is NP–mitotic.

§2. Another Dense Result

R. E. Ladner's density result[5] tells us that for all A, B, if $A<_T^P B$ and A, B are computable, then there exist computable sets C_1 and C_2 such that $A<_T^P C_i<_T^P B$ for $i=0, 1$, and $B\equiv_T C_0\oplus C_1$, where

$$A\oplus B(2x)=\begin{cases}1 & \text{if } x\in A,\\ 0 & \text{if } x\notin A,\end{cases}\qquad A+B(2x+1)=\begin{cases}1 & \text{if } x\in B,\\ 0 & \text{if } x\notin B.\end{cases}$$

Using the method of coding strategy which encodes a segment of strings of A into a piece of D, we prove the following theorem.

Theorem 2.1. *For all sets A, B, C such that $C<_T^P B<_T^P A$ there exists a set D such that $C<_T^P D<_T^P A$ and $D\Big|_T^P B$.*

(In particular, if $NP\neq P$, such A, B, C exist, according to [1], we get an oracle E, which is recusive, such that $P^E\neq NP^E$ and clearly, in such NP^E, A, B, C exist.)

Proof We construct D in such a way that for every $j\in N$, the following requirement is satisfied:

R_j: $j=4i$, $A\neq P_i^D$, $j=4i+1$, $D\neq P_i^C$, $j=4i+2$, $B\neq P_i^D$, $j=4i+3$, $D\neq P_i^B$,

$$\text{let } D_0=\{(\underline{0}, x)\,|\,x\in C\},\quad n_0=0.$$

Construction of D

stage j

$j=4i$ (satisfy $A\neq P_i^D$)

$$\text{let } x=\mu y(A(y)\neq P_i^{D_j}(y) \text{ and } |y|>n_j),$$

where $\mu yP(x_1, \cdots, x_n, y)$ means the least y such that the property $P(x_1, \cdots, x_n, y)$ holds with respect to the standard enumerations of the strings.

(Such y exists, otherwise $A\leqslant_T^P C\cup$ a finite set, i.e. $A\leqslant_T^P C$. This contradicts the fact $C<_T^P A$.)

let $n_{j+1}=n_j+\sum_{0^{n_j}<y\leqslant x} P_i(|y|)$

$D_{j+1}=D_j$,

$j=4i+1$ (satisfy $D\neq P_i^C$)

let $A_j=\{(\underline{i+1}, x)\,|\,x\in A$ and $|x|>n_j\}$. Clearly $A_j\leqslant_T^P A$.

let $x=\mu y(A_j((\underline{i+1}, y))\neq P_i^C((\underline{i+1}, y))$ and $|y|>n_j)$

(Such x exists, otherwise $A\leqslant_T^P C$. This contradicts the fact $C<_T^P A$).

let $n_{j+1}=n_j+\sum_{0^{n_j}<y<x} P_i(|(\underline{i+1}, y)|)$,

$A_{j+1}=\{(\underline{i+1}, x)\,|\,x\in A$ and $|x|>n_{j+1}\}$,

$D_{j+1}=D_j\cup(A_j-A_{j+1})$.

$j=4i+2$ (satisfy $B\neq P_i^D$) let $x=\mu y(B(y)\neq P_i^{D_j}(y)$ and $|y|>n_j)$.

(Such x exists, otherwise $B\leqslant_T^P C\cup$ a finite set, i. e. $B\leqslant_T^P C$. This contradicts the fact $C<_T^P B$).

let $n_{j+1}=n_j+\sum_{0^{n_j}<y\leqslant x} P_i(|y|)$,

$D_{j+1}=D_j$.

$j=4i+3$ (satisfy $D\neq P_i^B$)

let $A_j=\{(\underline{i+1}, x)\,|\,x\in A$ and $|x|>n_j\}$.

let $x=\mu y(A_j((\underline{i+1}, y))\neq P_i^B((\underline{i+1}, y))$ and $|y|>n_j)$

(Such x exists, otherwise $A\leqslant_T^P B$. This contradicts the fact $B<_T^P A$).

let $n_{j+1}=n_j+\sum_{0^{n_j}<y\leqslant x} P_i(|(i+1, y)|)$,

$A_{j+1}=\{(\underline{i+1}, x)\,|\,x\in A$ and $|x|>n_{j+1}\}$,

$D_{j+1}=D_j\cup(A_j-A_{j+}\cdot)$.

End of the construction of D, $D=\bigcup_{j=1}^{\infty} D_j$.

Clearly, for every j, R_j has received attention and no string queried by the oracle machine restrained from D is later added to or deleted from D. We can conclude that $C\leqslant_T^P D$.

It is sufficient to show that $D\leqslant_T^P A$.

Lemma 2.2. $D\leqslant_T^P A$.

Proof First we define the following:

$In\text{-}k=\{(\underline{k+1}, x)\,|\,n_{4k+1}<|x|\leqslant n_{4k+2}$ or $n_{4k+3}<|x|\leqslant n_{4k+4}\}$,

In- segment $=\bigcup_k In\text{-}k$.

For eeach x, where $x=(\underline{i}, y)$, if $i=0$,

then $x\in D$ iff $y\in C$. We can decide if $y\in C$ within polynomial steps with oracle set A (because $C\leqslant_T^P B\leqslant_T^P A$),

If $i\neq 0$,

then we can decide if x is in In-segment within $|y|$ steps according to the construction.

$x\in D$ iff $x\in In$-segment and $y\in A$.

It follows that $D\leqslant_T^P A$. The proof of Theorem 2.1 is completed.

Corollary 2.3. *For all sets A, C, B_i $i=1, \cdots, n$, such that $C<_T^P B_i<_T^P A$, $i=1, \cdots, n$, there exists a set B_0 such that $C<_T^P B_0<_T^P A$ and $B_0 |_T^P B_i$, $i=1, \cdots, n$.*

Proof Using the same method as Theorem 2.1 we can construct such B_0 piecewisely. We construct B_0 in such a way that for every $k\in N$, the following requirement is satisfied:

$$\begin{aligned} R_j:\ & j=(2n+2)k: && A\neq P_k^{B_0}, \\ & j=(2n+2)k+1: && B_0\neq P_k^{C}, \\ & j=(2n+2)k+2i: && B_i\neq P_k^{B_0}, \quad i=1, 2, \cdots, n, \\ & j=(2n+2)k+2i+1: && B_0\neq P_k^{B_i}. \end{aligned}$$

We omit the detail.

§3. The Existence of $P(NP)$-non-mitotic Set in Relativized Classes P and NP

Theorem 3. 1. *There is a recursive oracle B such that there is a set A such that $A\in P^B$ and A is P-non-mitotic.*

Proof We construct $A=B$.

We let B_t contain the elements of B at the the end of the stage t. i.e. B_t is the approximation of B at the end of the stage t.

We can construct B in such a way that the following requirements are satisfied:

for all t: R_t: $t=(i, j, k, l)$, at least one of the followihg is not true:

(1) $P_i^B\cup P_j^B=B$,

(2) $P_i^B\cap P_j^B=\emptyset$,

(3) $B=P_k^{P_j^B}$,

(4) $B=P_l^{P_i^B}$.

The construction of B. let $n_0=0$, $B_0=\emptyset$.

stage $t+1$ $t+1=(i, j, k, l)$ (satisfy R_t).

let $m_t = \max\{n_t, p_i(n_t), p_j(n_t), p_i(p_k(n_t)), p_j(p_l(n_t))\}+1$.

if there exists a string x, where $|x| \leqslant m_t$, such that

(1) $(P_i^{B_t} \cup P_j^{B_t})(x) \neq B_t(x)$

or (2) $x \in P_i^{B_t} \cap P_j^{B_t}$

or (3) $B_t(x) \neq P_k^{P_i^{B_t}}(x)$

or (4) $B_t(x) \neq P_l^{P_j^{B_t}}(x)$,

then we restrain the strings which were asked in the (1)—(4) computation fromiB and let $n_{t+1} = \max\{m_t, p_i(|x|), p_j(|x|), p_i(p_k(|x|)), p_j(p_1(|x|))\}$.

If (1)—(4) are not true, then the following holds:

$$(P_i^{B_t} \cup P_j^{B_t}) \upharpoonright 1^{m_t} = B_t \upharpoonright 1^{m_t}$$
$$\text{and} \quad P_i^{B_t} \cap P_j^{B_t} \upharpoonright^{m_t} = \emptyset$$
$$\text{and} \quad B_t \upharpoonright^{m_t} = P_k^{P_i^{B_t}} 1^{m_t}$$
$$\text{and} \quad B_t \upharpoonright 1^{m_t} = P_l^{P_j^{B_t}} \upharpoonright 1^{m_t}.$$

We enumerate string 0^{n_t} into B, i.e. $B_{t+1} = B_t \cup \{0^{n_t}\}$. There are two cases:

Case 1 P_i^B and P_j^B really split B. One of P_i^B and P_j^B must accept 0^{n_t}, but not both.

If 0^{n_t} enters P_i^B, then $P_j^B \upharpoonright 1^{m_t} \neq P_j^{B_t} \upharpoonright 1^{m_t}$, therefore $P_l^{P_j^{B_t}} \neq B$ via 0^{n_t}.

If 0^{n_t} enters P_j^B, then

$P_k^{P_i^B} \neq B$ via 0^{n_t}.

let $n_{t+1} = m_t$.

Case 2 P_j^B and P_i^B do not split B via a string x, where $|x| \leqslant m_t$.

We set $n_{t+1} = \max\{m_t, P_i(|x|), P_j(|x|)\}+1$,

End of the constructionres Finally we let $B = \bigcup_{t \in N} B_t$.

From the construction it is clear that when R_t has received attention, it can not be destroyed forever. All R_t has received attention in the construction. Therefore B is the required set and orale.

Theorem 3.2. *There is a recursive oracle B, such that there is a set A, $A \in NP^B - P^B$ and A is NP-non-mitotic.*

Proof We will construct B such that $A = \{0^n |$ There is a string x, such that $|x| = n$ and $x \in B\}$ and B satisfies the following requirements:

for all $t \in N$

R_t: (NP-non-mitotic requirement), *where* $t = (i, j, k, l)$, at least one of the following is not true:

(1) $NP_i^B \cup NP_j^B = A$,

(2) $NP_i^B \cap NP_j^B = \emptyset$,

(3) $A = NP_k^{NP_i^B}$,

(4) $A=NP_l^{NP_j^B}$.

S_t: $A\neq NP_t^B$.

The priority of the requirements is $R_0S_0R_1S_1R_2S_2\cdots$.

We say S_t, R_t require attention if they have not received attention.

We say S_t, R_t are satisfied if they have already received attention.

The construction of B

$$\text{let } B_0=\phi.$$

stage s

$s+1=2(t+1)$ (R_t receives attention) $t+1=(i, j, k, l)$,

$$\text{let } m_t=\max\{n_t, p_i(n_t), p_j(n_t), p_i(p_k(n_t)), p_j(p_l(n_t))\}+1.$$

If there exists a string x, where $|x|\leqslant m_t$, such that

(1) $NP_i^{B_s}\cup NP_j^{B_s}(x)\neq A_s(x)$

or (2) $x\in NP_i^{B_s}\cap NP_j^{B_s}$

or (3) $A_s(x)\neq NP_k^{NP_i^{B_s}}(x)$

or (4) $A_s(x)\neq NP_l^{NP_j^{B_s}}(x)$,

then we set

$$n_{s+1}=\max\{m_t, p_i(|x|), p_j(|x|), p_j(p_k(|x|)), p_j(p_l(|x|)\}+1.$$

(Clearly, in this step, we restrain all strings that will destroy the computation of the string x from B).

If such x does not exist, the following is true:

$$(\#)\quad\begin{cases} NP_i^{B_s}\cup NP_j^{B_s}\restriction 1^{m_t}=A_s\restriction 1^{m_t} \text{ and } NP_i^{B_s}\cap NP_j^{B_s}\restriction 1^{m_t}=\emptyset, \\ \text{and } A_s\restriction 1^{m_t}=NP_k^{NP_i^{B_s}}\restriction 1^{m_t} \text{ and } A_s\restriction 1^{m_t}=NP_l^{NP_j^{B_s}}\restriction 1^{m_t}, \end{cases}$$

then we enumerate 0^{n_s} into B, i.e. $B_{s+1}=B_s\cup\{0^{n_s}\}$. There are two cases:

Case 1 NP_i^B and NP_j^B really split A, one of the $NP_i^{B_{s+1}}$, $NP_j^{B_{s+1}}$ must remains unchanged because 0^{n_s} can only enter one of them.

If 0^{n_s} enters $NP_i^B(NP_j^B)$, then

$NP_l^{NP_j^B}\neq B$ via 0^{n_t} ($NP_k^{NP_i^B}\neq B$ via 0^{n_t}),

let $n_{s+1}=m_t$.

Case 2 $NP_i^{B_{s+1}}\cup NP_j^{B_{s+1}}\restriction 1^{m_t}\neq A_{s+1}\restriction 1^{m_t}$ via a string x, where $|x|\leqslant m_t$.

$$\text{let } n_{s+1}=\max\{m_t, p_i(|x|), p_j(|x|)\}+1.$$

$s+1=2t+1$ (Satisfy S_t)

Choose $n>n_s$ so large that $p_t(n)<2^n$, run query machine p_t with oracle B_s on input 0^n. If $p_t^{B_s}$ accepts 0^n, then place nothing into B at this stage.

If $p_t^{B_s}$ rejects 0^n, then add to B the least string x of length n not queried during the computation of $p_t^{B_s}$ on input 0^n, i.e. $B_{s+1}=B_s\cup\{x\}$.

End of the construction Fnially we let $B=\bigcup_{s\in N} B_s$.

It is clear that for all t, R_t, S_t receive attention and are not destroyed by other requirements. Therefore $A \in NP^B - P^B$ and A has NP-non-mitotic property.

I would like to thank professor Yang Dongping for his guidance. Thanks are also due to Miss Xu Yiqing for some helpful discussions.

References

[1] Theodore Baker, John Gill and Robert Solovay, Relativizations of the P=? NP Questions, *SIAM J. Comput.*, **4**: 4(1975), 431—442.

[2] Timothy, J. Long, Strong nondeterministic polynomial-time reducibility, *Theoretical Computer Science*, **21**(1982), 1—25.

[3] Robert, I. Soare, Recursively enumerable sets and degrees: The study of computable functions and computable generated sets.

[4] Steven Homer & Wolfgang Maass, Oracle dependent properties of the lattice of NP sets.

[5] Ladner, R. E., On the structure of polynomial time reducibility, *J. Assoc. Comput. Mach.*, **22**(1975), 155—171.

[6] Ladner, R. E., Mitotic recursively enumerable sets, *J. Symbolic Logic*, **38**: 2(1973), 199—211.