INFORMATIQUE THÉORIQUE ET APPLICATIONS

KER-I KO

A note on separating the relativized polynomial time hierarchy by immune sets

Informatique théorique et applications, tome 24, nº 3 (1990), p. 229-240

<http://www.numdam.org/item?id=ITA_1990__24_3_229_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 24, n° 3, 1990, p. 229 à 240)

A NOTE ON SEPARATING THE RELATIVIZED POLYNOMIAL TIME HIERARCHY BY IMMUNE SETS (*)

by Ker-I Ko [1]

Communicated by J. Diaz

Abstract. – *A set A is $\mathscr{C}$-immune if A is infinite and does not have an infinite subset in $\mathscr{C}$. It is proved that for any $k>0$, there exists as set A such that $\Sigma_k^p(A)$ contains a $\Sigma_{k-1}^p(A)$-immune set.*

Résumé. – *Un ensemble A est $\mathscr{C}$-immunisé si A est infini et ne contient pas de sous-ensemble élément de $\mathscr{C}$. On montre que pour tout $k>0$, il existe un ensemble A tel que $\Sigma_k^p(A)$ contienne un ensemble $\Sigma_{k-1}^p(A)$-immunisé.*

1. INTRODUCTION

The concept of immunity in complexity theory arises from the need to understand the structural relationship between complexity classes. Let $\mathscr{C}$ be a complexity class. A set A is said to be *$\mathscr{C}$-immune* if A is infinite and A does not have an infinite subset in $\mathscr{C}$. A proof for $A \notin \mathscr{C}$ demonstrates only a worst-case lower bound in the sense that no algorithm of type $\mathscr{C}$ can solve the problem A completely, while a proof for A being $\mathscr{C}$-immune is much stronger such that any algorithm of type $\mathscr{C}$ intended for a subproblem of A can only recognize a finite number of instances in A – thus no better than a simple table lookup algorithm. In the following we will call a proof of the existence of a set $A \in \mathscr{C}_2 - \mathscr{C}_1$ a *simple separation* (of the class $\mathscr{C}_2$ from the class $\mathscr{C}_1$) and a proof of the existence of a set $A \in \mathscr{C}_2$ which is $\mathscr{C}_1$-immune a *strong separation* (of the class $\mathscr{C}_2$ from the class $\mathscr{C}_1$).

A number of strong separation results have appeared in the literature. A typical result is that of Balcázar and Schöning [4]: there exists a set A in

(*) Received April 1988, revised October 1988.
Research supported in part by the NSF Grants CCR-8696135 and CCR-8801575.
(1) Department of Computer Science, State University of New York at Stony Brook, Stony Brook, NY 11794, U.S.A.

EXP (the class of sets computable in time $2^{O(n)}$) such that both A and $\bar{A}$ are P-immune. Since no simple separation result is known to this date about complexity classes between *PSPACE* and P, all known strong separation results about these complexity classes are proved in the relativized form. For instance, Bennett and Gill [5], Homer and Maass [8] and Schöning and Book [13] proved that there exists an oracle A such that $NP(A)$ contains a $P(A)$-immune set. Homer and Maass [8] and Balcázar [2] proved that there exists an oracle B such that $co\text{-}NP(B)$ contains an $NP(B)$-immune set. Other strong separation results concerning relativized probabilistic complexity classes can be found in Balcázar and Russo [3], Russo [12] and Ko [9].

It is interesting to observe that the proofs of the above relativized strong separation results about complexity classes P, NP and $co\text{-}NP$ all assume a very simple form of delayed diagonalization. Within this simple setting of delayed diagonalization, the real diagonalization process becomes a routine translation of the diagonalization involved in the corresponding simple separation proof. Even for more complicated proofs involving probabilistic complexity classes, the proofs still follow this form of delayed diagonalization. In this note, we give more explicitly this general setting of delayed diagonalization for relativized strong separation, and demonstrate how the strong separation of relativized polynomial time hierarchy can be proved in this setting so that the complicated combinatorial arguments used in the simple separation can be translated into this setting without extra difficulty.

Our main results include

THEOREM 1: *For every $k>0$, there exists a set A such that $\Sigma_k^P(A)$ contains a set which is $\Sigma_{k-1}^P(A)$-immune.*

THEOREM 2: *There exists a set A such that PSPACE (A) contains a set which is $\Sigma_k^P(A)$-immune for every $k \geqq 0$.*

THEOREM 3: *For every $k>0$, there exists a set A such that $\Sigma_k^P(A)=\Pi_k^P(A)$* and *$\Sigma_k^P(A)$ contains a set which is $\Sigma_{k-1}^P(A)$-immune.*

These results extend the simple separation results of Yao [15], Hastad [7] and Ko [10] for the relativized polynomial time hierarchy. Theorem 1 also extends the result of Balcázar [2] and Homer and Maass [8] that there exists a set A such that $NP(A)$ contains a simple set.

The above results, together with earlier strong separation results, seem to suggest that most simple separations can easily be modified to strong separations and these strong separation results by immune sets do not reveal more about the difference of the complexity classes under consideration. Perhaps an even stronger separation by, for example, bi-immune sets (*cf.* Torenvliet and van Emde Boas [14]) may provide more insight into the structural relationship between the complexity classes.

NOTATION: In this paper, all sets A are sets of strings over the alphabet $\Gamma=\{0, 1\}$. For each string x, let $|x|$ denote its *length*. Let Γ^n be the set of all strings of length n. Let $\langle i, j\rangle$ be a standard pairing function on two integers. For each set A, let χ_A be its characteristic function. Let A be a set; then $P(A)$, $NP(A)$ and $PSPACE(A)$ denote the classes of sets computable by oracle machines with oracle A in deterministic polynomial time, nondeterministic polynomial time, and polynomial space, respectively. For $k\geqq 0$, we let $\Sigma_k^P(A)$ be the k-th level of the polynomial time hierarchy relative to A; that is, $\Sigma_0^P(A)=P(A)$, and $\Sigma_k^P(A)$, $k>0$, is the class of sets computable by a nondeterministic polynomial time oracle machine relative to a set in $\Sigma_{k-1}^P(A)$. The relativized polynomial time hierarchy $PH(A)$ is the union of all $\Sigma_k^P(A)$, $k\geqq 0$.

We will consider constant-depth circuits. These circuits have a fixed number of depth of AND or OR gates, with unbounded fanin in each gate. A circuit computes a function on its variables. In this paper, each variable is associated with a string $x\in\Gamma^*$, and is denoted by v_x. Let V be the set of variables occurred in a circuit C. Then a *restriction* ρ of C is a mapping from V to $\{0, 1, *\}$. For each restriction ρ of C, $C\lceil_\rho$ denotes the circuit C' obtained from C by replacing each variable v_x with $\rho(v_x)=0$ by 0 and each v_y with $\rho(v_y)=1$ by 1. Let B be a set of strings. Then, there is a restriction ρ_B associated with B: $\rho_B(v_x)=1$ if $x\in B$ and $\rho_B(v_x)=0$ if $x\notin B$.

2. A GENERAL SETTING FOR RELATIVIZED STRONG SEPARATION

Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be two complexity classes. Assume that there exists an oracle A such that $L(A)\in\mathscr{C}_2(A)-\mathscr{C}_1(A)$ for some set $L(A)$ having the following properties:

PROPERTY A: There exists an effective enumeration of machines $\{M_i\}$ such that $\mathscr{C}_1(A)$ is exactly the class of sets $L(M_i, A)$, $i\geqq 1$, where $L(M_i, A)$ is the set of strings accepted by M_i with oracle A. Also, each machine M_i on an input w of length n can only access to the oracle A strings of length $\leqq q_i(n)$ for some strictly increasing recursive function q_i.

PROPERTY B: The set $L(A)$ has the property that whether a string w of length n is in $L(A)$ depends only on the set $A\cap W(n)$, where $W(n)$ is a window such that $W(n) \subseteq \{x \mid m_1(n) \leq |x| \leq m_2(n)\}$ for some functions m_1 and m_2 and that $W(n_1) \cap W(n_2) = \varnothing$ for different n_1 and n_2.

Further assume that the proof of $L(A) \notin \mathscr{C}_1(A)$ has the following standard form of diagonalization:

Diagonalization. The set A is constructed by stages. By the end of stage $i-1$, the memberships in A of strings up to length l_i have been determined and $A(i)$ is set to be $\{x \mid |x| \leq l_i \text{ and } x \in A\}$. In stage i, machine M_i is considered and a sufficiently large integer $n = n_i > l_i$ is chosen such that the window $W(n)$ is free from the interference of construction of earlier stages (*i.e.*, $m_1(n) > q_{i-1}(n_{i-1})$ and $m_1(n) > l_i$), and that the following property is satisfied:

PROPERTY C: There exists a set $B \subseteq W(n)$ such that $0^n \notin L(B)$ if and only if $M_i^{A(i) \cup B}$ accepts 0^n.

Then, $A(i+1)$ is set to $A(i) \cup B$. The set A is defined to be $\bigcup_{i=1}^{\infty} A(i)$.

Examples. (*a*) Baker, Gill and Solovay [1] have used this simple form of diagonalization to prove that there exists a set A such that $L(A) \in NP(A) - P(A)$, where $L(A) = \{0^n \mid A \cap \Gamma^n \neq \varnothing\}$. That is, the window $W(n)$ is simply Γ^n and the existence of set B for Property C is shown by a simple counting argument which asserts that a polynomial-time deterministic machine cannot query, on input 0^n, about every string of length n.

(*b*) In a more general case, Hastad's proof [7] for the existence of set A such that $L(A) \in \Sigma_k^P(A) - \Sigma_{k-1}^P(A)$, $k > 0$, also has this form of diagonalization. Namely, the set $L(A)$ is defined to be the set of all 0^n such that

$$(\exists y_1, |y_1| = n)(\forall y_2, |y_2| = n) \ldots (Q_k y_k, |y_k| = n)\, y_1 y_2 \ldots y_k \in A$$

(where $Q_k = \exists$ if k is odd, and $= \forall$ if k is even), and so the window $W(n)$ is equal to Γ^{kn}. The key combinatorial lemma here is that any depth-k circuit with small bottom fanins cannot compute the predicate "$0^n \in L(A)$". This lemma then is translated to Property C above by Furst, Saxe and Sipser's observation [6] of the relationship between constant-depth circuits and Σ_k^P-predicates.

From the above diagonalization of simple separation results, we can describe a typical strong separation result which proves that, in addition to the above result, $L(A)$ is $\mathscr{C}_1(A)$-immune. To do this, we need some more assumptions about classes $\mathscr{C}_1(A)$ and $\mathscr{C}_2(A)$:

First, the above Property C need be generalized into

PROPERTY D: For any finite collection of machines $M_{j_1}, \ldots, M_{j_p}$ for class $\mathscr{C}_1(A)$, there exists a set $B \subseteq W(n)$ such that $0^n \notin L(B)$ if and only if $\exists r$, $1 \leqq r \leqq p$, $M_{j_r}^{A(i) \cup B}$ accepts 0^n.

Furthermore, we assume that the class $\mathscr{C}_1$ and set $L(A)$ satisfy

PROPERTY E: There exists an infinite number of indexes j such that $L(M_j, X) = \varnothing$ for all oracles X, and

PROPERTY F: $L(A)$ has the property that $0^n \notin L(A)$ if $A \cap W(n) = \varnothing$.

The basic setup is the same as the setup for the simple separation proof. The main difference is that we also maintain a set U of "uncanceled" indexes. Before stage 1, U is set to $\varnothing$. In stage i, we first add i into set U, then consider all machines M_j whose index j is in U. We also pick a sufficiently large integer $n = n_i$ and consider the input 0^n and the window $W(n)$. There are two cases:

Case 1: There exist an $j \in U$ and *a* set $B \subseteq W(n)$ such that $0^n \notin L(B)$ and $M_j^{A(i) \cup B}$ accepts 0^n.

Then, j is canceled (*i.e.*, $U := U - \{j\}$), and $A(i+1)$ is set to $A(i) \cup B$.

Case 2: Not Case 1.

Then, by Property *D*, there exists a set $B \subseteq W(n)$ such that $0^n \in L(B)$ and for all $j \in U$, $M_j^{A(i) \cup B}$ rejects 0^n. Set $A(i+1)$ to be $A(i) \cup B$.

This completes stage i. Set A is defined to be $\bigcup_{i=1}^{\infty} A(i)$. The above construction achieves the following two goals: (*a*) $L(A)$ is infinite, and (*b*) for each j, $L(M_j, A)$ is not an infinite subset of $L(A)$.

First note that by the choice of integers n_i and Property *B* of $W(n)$, the conditions established in stage i such as $0^n \in L(A(i+1))$ or $M_j^{A(i+1)}$ accepting 0^n also hold for set A.

Next note that by Property *E*, which asserts that for infinitely many indexes j, M_j^A rejects 0^n for all n, we know that the limit of set U is infinite. Since in each stage we add at most one index into set U, the limit of U is infinite only when Case 2 occurs infinitely often in the above construction. That is, an infinitely many 0^n have been made to be in $L(A)$. This shows that goal (*a*) is established.

For the goal (*b*), we consider machine M_j. If j is canceled in stage i, then we must have $0^n \notin A(i+1)$ and $M_j^{A(i+1)}$ accepts 0^n. Therefore, 0^n is a witness that $L(M_j, A) \subseteq L(A)$. So, we may assume that j is never canceled. Then, for any $n \geqq n_j$, if $0^n \in L(A)$, then $n = n_i$ for some integer $i \geqq j$, and in stage i, Case 2 occurs [if $n \neq n_i$ for all i then $A \cap W(n) = \varnothing$ and hence, by Property F, $0^n \notin L(A)$]. This means that $M_j^{A(i+1)}$ rejects 0^n. Therefore, $L(M_j, A) \cap L(A)$ must be a finite set. These arguments establish the goal (b).

The above proved the following metatheorem.

METATHEOREM: *If $\mathscr{C}_2$ and $\mathscr{C}_1$ have a relativized simple separation satisfting Properties A-F, then $\mathscr{C}_2$ and $\mathscr{C}_1$ have a relativized strong separation.*

Remarks: (1) In the above proof, Property F is not really necessary. It is added only for the purpose of convenience. All we need, actually, is a simple condition on $A \cap W(n)$ such that $0^n \notin L(A)$ if $A \cap W(n)$ satisfies this condition. Then, in the stage i, we first expand $A(i)$ into $A'(i)$ to make $A'(i) \cap W(n')$ satisfy this condition for every $n' \neq n$ which is $\leqq q_i(n)$, and construct B to satisfy Property D with respect to the new $A'(i)$.

(2) The referee pointed out that in earlier proofs, such as in [13], it is often required that, in Case 1, the smallest index j satisfying the property is cancelled. Our proof above does not require this since it is less constructive and relies more on Property E which implies that Case 2 occurs infinitely often.

3. PROOFS OF THEOREMS 1 AND 2

We now apply the above metatheorem to the polynomial time hierarchy. We first consider Theorem 1.

THEOREM 1: *For every $k > 0$, there exists a set A such that $\Sigma_k^P(A)$ contains a set which is $\Sigma_{k-1}^P(A)$-immune.*

Let $k > 0$. Let

$$L(A) = \{ 0^n \mid (\exists y_1, |y_1| = n)(\forall y_2, |y_2| = n) \ldots (Q_k y_k, |y_k| = n)\, y_1 y_2 \ldots y_k \in A \}.$$

Then $L(A) \in \Sigma_k^P(A)$ and satisfies Property B with $W(n) = \Gamma^{kn}$. By the standard enumeration of polynomial-time alternating machines with at most k alternations and the enumeration of polynomial functions, we get an enumeration $\{M_i\}$ of Σ_k^P-oracle machines satisfying Property A. Furthermore, Properties E and F are obviously satisfied by this enumeration and set $L(A)$. Thus, for the proof of Theorem 1, we only need to verify Property D, which is quite simple in terms of lower bounds for constant-depth circuits established by Yao [15] and Hastad [7].

For any integers k and t, let $\Sigma\text{-}CIR(k, t)$ be the collection of all depth-$(k+1)$ circuits with its top gate an OR gate, its fanin $\leqq 2^t$, and its bottom fanin $\leqq t$. Also recall that for any set $B \subseteq \Gamma^*$, the restriction ρ_B is defined to be $\rho_B(v_x)=1$ if $x \in B$ and $\rho_B(v_x)=0$ if $x \notin B$.

LEMMA 4 [6]: *Let M_i be a Σ_k^P-oracle machine, with a polynomial time bound q_i. Then, for each string x of length n, there exists a circuit $C=C_{i,x}$ in $\Sigma\text{-}CIR(k, q_i(n))$ such that its variables are those associated with strings of length $\leqq q_i(n)$ and for each set $B \subseteq \Gamma^*$, $C\lceil_{\rho_B}=1 \Leftrightarrow M_i^B$* accepts x.

Let D_k^n be the depth-k circuit with the following property: the fanin of D_k^n is exactly 2^n for every gate; the top gate of D_k^n is an OR gate; and all other gates are alternatively OR and AND gates. Also let the variables of the circuit D_k^n be exactly those associated with strings of length kn, occurring in the circuit in the increasing order. Then, it is clear that $D_k^n\lceil_{\rho B}=\chi_{L(B)}(0^n)$ for all sets B.

LEMMA 5 [7, 15]: *For any $k>0$, there exists an integer n_k such that for all $n>n_k$, no circuit C in $\Sigma\text{-}CIR(k-1, n^{\log n})$ computes exactly the same function as D_k^n.*

LEMMA 6: *For any k, p, $m>0$ there exists an integer $n_0>m$ such that for all $n>n_0$ and all sets A of strings of length $\leqq m$, there exists a set $B \subseteq \Gamma^{kn}$ such that $0^n \notin L(B)$* if and only if there exists a machine M_j, $1 \leqq j \leqq p$, such that $M_j^{A \cup B}$ accepts 0^n.

Proof: Let ρ be the restriction on variables associated with strings of length $\leq \sum_{j=1}^{p} q_j(n)$ defined as follows:

$$\rho(v_x)=\begin{cases} \chi_A(x), & \text{if } |x|<kn; \\ 0, & \text{if } |x|>kn; \\ *, & \text{if } |x|=kn. \end{cases}$$

Then, for each j, $1 \leqq j \leqq p$, define the circuit C'_j to be the circuit $C_{j,0^n}\lceil_\rho$, where $C_{j,0^n}$ is the circuit of Lemma 4, corresponding to machine M_j and string 0^n.

From Lemma 4, it is clear that for all sets $B \subseteq \Gamma^{kn}$, $C'_j\lceil_{\rho B}$ outputs 1 if and only if $M_j^{A \cup B}$ accepts 0^n. Let $C=\bigvee_{j=1}^{p} C'_j$. Then, C is in $\Sigma\text{-}CIR(k-1, n^{\log n})$ for sufficiently large n (*i.e.*, if $n^{\log n}>\sum_{j=1}^{p} q_j(n)$). (Note that the top gates of C'_j's are OR gates.) By Lemma 5, C does not compute the function computed by D_k^n. That is, there exists a set $B \subseteq \Gamma^{kn}$ such that $C\lceil_{\rho B}$ outputs 1 if and only if $D_k^n\lceil_{\rho B}$ outputs 0 if and only if $0^n \notin L(B)$. Since C is the OR of the circuits C'_j, $1 \leqq j \leqq p$, the lemma follows from the above relation and the relation between C'_j and M_j. $\square$

Remark: The above proof can be modified to prove that $\Sigma_k^P(A)$ contains a $\Pi_k^P(A)$-immune set. To see this, we first note that Lemma 5 can be strengthened so that no C in Π-CIR$(k, n^{\log n})$ computes the function as circuit D_k^n, where Π-CIR(k, t) is the collection of circuits of the same structure as those in Σ-CIR(k, t) but having top AND gates. Then, in Lemma 6, each circuit C'_j is in Π-CIR$(k, q_j(n))$, and we need to show that $C = \bigvee_{j=1}^{p} C'_j$ is still in Π-CIR$(k, n^{\log n})$. Write $C'_j = \bigwedge_{r=1}^{q_j(n)} C'_{j,r}$, with each $C'_{j,r}$ in Σ-CIR$(k-1, q_j(n))$. Then, by DeMorgan's law, C can be expressed as the AND of $\prod_{j=1}^{p} q_j(n)$ many circuits, each of the form $\bigvee_{j=1}^{p} C'_{j,r}$ and hence each being in Σ-CIR$(k-1, \sum_{j=1} q_j(n))$. For sufficiently large n such that

$$n^{\log n} \geqq \prod_{j=1}^{p} q_j(n) + \sum_{j=1}^{r} q_j(n), \qquad C \in \Pi\text{-CIR}(k, n^{\log n}).$$

Next we consider Theorem 2.

THEOREM 2: *There exists a set A such that PSPACE(A) contains a set which is $\Sigma_k^P(A)$-immune for every $k \geqq 0$. (The following proof actually establishes a stronger result: the class $\oplus P(A)$ contains a set which is $\Sigma_k^P(A)$-immune for every $k \geqq 0$; where $\oplus P$ is the class of sets accepted by nondeterministic machines with an odd number of accepting paths* [11].)

The proof for Theorem 1 extends easily to Theorem 2. First, the enumeration of machines for the class $PH = \bigcup_{k=0}^{\infty} \Sigma_k^P$ can be done by enumerating $M_{\langle k, j \rangle}$ where $M_{\langle k, j \rangle}$ is the j-th machine in the enumeration of Σ_k^P-oracle machines. It is obvious that this enumeration satisfies Properties A and E. Next, let $L_{\text{odd}}(A) = \{ 0^n \mid \| A \cap \Gamma^n \| \text{ is odd} \}$.Then, the window is $W(n) = \Gamma^n$ and $L_{\text{odd}}(A)$ and $W(n)$ satisfy Properties B and F. For Property D, we use Yao's result [15] that a constant-depth, subexponential-size circuit does not compute the parity function.

LEMMA 7 [15]: *For any* $k>0$, *there exists an integer* n_k *such that for all* $n>n_k$ *no circuit* C *in* Σ-$CIR(k, n^{\log n})$ *computes the (odd) parity of* 2^n *variables.*

LEMMA 8: *Let* $m>0$, *and* $M_{\langle k_1, j_1 \rangle}, \ldots, M_{\langle k_p, j_p \rangle}$ *be a finite collection of PH-oracle machines. Then, there exists an integer* n_0 *such that for all* $n>n_0$ *and for all sets* A *of strings of length* $\leqq m$, *there exists a set* $B \subseteqq \Gamma^n$ *such that* $\| B \|$ *is even if and only if* $\exists r$, $1 \leqq r \leqq p$, $M^{A \cup B}_{\langle k_r, j_r \rangle}$ *accepts* 0^n.

Sketch of Proof: The proof is essentially the same as that of Lemma 6. All we need is to let $k=\max\{k_r \mid 1 \leqq r \leqq p\}$ and construct a circuit C in Σ-$CIR(k, n^{\log n})$ such that for all sets B, $C\lceil_{\rho B}$ outputs 1 if and only if at least one of $M^{A \cup B}_{\langle k_r, j_r \rangle}$, $1 \leqq r \leqq p$, accepts 0^n. Then, the lemma follows from Lemma 7 that the circuit C does not compute the parity of B. □

4. PROOF OF THEOREM 3

Homer and Maass [8] constructed an oracle set A such that $NP(A)=co$-$NP(A)$ and that $NP(A)$ has a $P(A)$-immune set. Theorem 3 generalizes this result to every level of the polynomial time hierarchy.

THEOREM 3: *For every* $k>0$, *there exists a set* A *such that* $\Sigma^P_k(A)=\Pi^P_k(A)$ *and* $\Sigma^P_k(A)$ *contains a set which is* $\Sigma^P_{k-1}(A)$-*immune.*

First we observe that the construction of a set A such that $\Sigma^P_k(A)=\Pi^P_k(A)\neq\Sigma^P_{k-1}(A)$, $k>0$, does not follow exactly the general form of diagonalization outlined in Section 2. To make $\Sigma^P_k(A)=\Pi^P_k(A)$, we need to ensure an additional condition that $K^k(A)\in\Pi^P_k(A)$ be satisfied, where $K^k(A)$ is a complete set for $\Sigma^P_k(A)$. It is more convenient if we also assume that $K^k(A)$ has the property that the question of whether a string x is in $K^k(A)$ depends only on the set $A \cap \{w \mid |w| < |x|\}$. In the following we give an outline of the construction of an oracle A for the simple separation $\Sigma^P_k(A)=\Pi^P_k(A)\neq\Sigma^P_{k-1}(A)$. For details, *see* Ko [10].

Fix an integer $k>0$. First we translate all the requirements into requirements on circuits. We modify the set $L(A)$ in the proof of Theorem 1 into

$$L'(A) = \{0^n \mid (\exists y_1, |y_1|=n)(\forall y_2, |y_2|=n)\ldots(Q_k y_k, |y_k|=n)\, 0^n y_1 y_2 \ldots y_k \in A\}.$$

Thus the window $W(n)$ is $\{0^n y \mid |y| = kn\}$. Let G_k^n be the depth-k circuit on variables associated with strings in $W(n)$ such that $G_k^n \lceil_{\rho A}$ outputs 1 if and only if $0^n \in L'(A)$. Next, for each w, $|w| = n$, define a circuit H_k^w on variables associated with strings of length $(k+1)n+1$ such that for each set A, $H_k^w \lceil_{\rho A}$ outputs 1 if and only if $(\exists z_1, |z_1| = n)$ $(\forall z_2, z_2| = n) \ldots (Q_k z_k, |z_k| = n)$ $1 w z_1 z_2 \ldots z_k \in A$. Note that G_k^n and H_k^w's are depth-k circuit whose fanin of each gate is exactly 2^n. Now the extra requirement that $K^k(A) \in \Pi_k^P(A)$ can be satisfied if we select A such that for each w, $H_k^w \lceil_{\rho A}$ outputs 1 if and only if $w \notin K^k(A)$.

In stage i, assume that we have determined $A(i)$ of the memberships of strings x in A up to length l_i. We consider the i-th $\Sigma_{k-1}^P(A)$-oracle machine M_i. Choose a large $n = n_i > l_i$, and expand $A(i)$ into $A'(i)$ of strings of length up to $n-1$ and make $H_k^w \lceil_{\rho A}$ outputs 1 if and only if $w \notin K^k(A)$ for all w, $|w| < n$. Next let $W'(n) = W(n) \cup \{1z \mid |z| = (k+1)m, n \leq m \leq q_i(n)\}$, and prove the following property.

PROPERTY C′: This exists a set $B \subseteq W'(n)$ such that

(i) $0^n \notin L'(B) \Leftrightarrow M_i^{A'(i) \cup B}$ accepts 0^n, and

(ii) $(\forall w, n \leq |w| \leq q_i(n))\, H_k^w \lceil_{\rho_{A'(i) \cup B}}$ outputs $1 \Leftrightarrow w \notin K^k(A'(i) \cup B)$.

To prove this property, we first convert the condition $M_i^{A'(i) \cup B}$ accepting 0^n into a condition on depth-k circuit. Namely, the circuit $C = C_{i, 0^n}$ is defined to be the circuit corresponding to the computation of M_i on input 0^n, with the following extra assignments to variables: if $|x| < (k+1)n$ the assign value $\chi_{A'(i)}(x)$ to the variable v_x, and if $|x| \geq (k+1)n$ and $x \notin W'(n)$ then assign value 0 to the variable v_x. This circuit C is in Σ-$CIR(k-1, q_i(n))$. Then, the following lemma shows that Property C' can be satisfied if n is sufficiently large.

Let C be a circuit with variables V. Let ρ be a restriction on V such that $C\lceil_\rho$ computes a constant function 0 or 1. Then, we say that ρ *completely determines* C.

LEMMA 9 [10]: *For every $k \geq 2$ there exists a constant n_k such that the following holds for all $n > n_k$. Let G_k^n and H_k^w, $n \leq |w| < n^{\log n}$ be circuits defined above. Let C be a circuit in Σ-$CIR(k-1, n^{\log n})$ whose variables are a subset of those of G_k^n and H_k^w's. Then, there exists a restriction ρ on variables of C such that ρ completely determines C but it does not completely determine any H_k^w, $n \leq |w| < n^{\log n}$, nor the circuit G_k^n.*

Property C' is satisfied by first finding ρ which completely determines $C_{i, 0^n}$ but none of G_k^n or H_k^w, and then extend ρ to ρ' which completely determines G_k^n but having value $G_k^n\lceil_{\rho'} \neq C_{i,0^n}\lceil_{\rho'}$, and then further extend it to ρ'' such that each H_k^w is completely determined by ρ'' and having value $H_k^w\lceil_{\rho''}=1$ if and only if $w \notin K^k(A'(i) \cup B)$. Finally, let B be the set of all strings x with $\rho''(x)=1$. The above forms the proof of the simple separation result: $\exists A\, \Sigma_k^P(A)=\Pi_k^P(A)\neq\Sigma_{k-1}^P(A)$.

Now, for Theorem 3, we need to verify additional Properties D, E and F. First, Properties E and F are easily seen to be true. (Also, for Property B, note that $W'(n_1) \cap W(n_2)=\varnothing$ if $n_1 \neq n_2$ and so the construction in one stage will not affect the construction in other stages.) Next, we need to strengthen Property D into

PROPERTY D′: For any finite collection of Σ_k^P-oracle machines $M_{j_1}, \ldots, M_{j_p}$, there exists a set $B \subseteq W'(n)$ such that

(i) $0^n \notin L'(B) \Leftrightarrow \exists r,\ 1 \leq r \leq p,\ M_{j_r}^{A'(i) \cup B}$ accepts 0^n, and

(ii) $\forall w,\ n \leq |w| \leq q_i(n))\ H_k^w\lceil_{\rho_{A'(i) \cup B}}$ outputs $1 \Leftrightarrow w \notin K^k(A'(i) \cup B)$.

Note that by the above discussion, $M_{j_r}^{A'(i) \cup B}$ accepts 0^n if and only if $C_{j_r,0^n}\lceil_{\rho B}=1$, where $C_{j_r,0^n}$ is a circuit in Σ-$CIR(k-1, q_{j_r}(n))$ corresponding to the machine M_{j_r} and input 0^n. Thus the OR of these circuits forms a circuit C' in Σ-$CIR(k-1, n^{\log n})$ for sufficiently large n. Apply Lemma 9 to circuits C' and G_k^n and H_k^w's to find a restriction ρ which completely determines C' but none of H_k^w nor G_k^n. Then, similarly to the above discussion on Property C', we can extend ρ to define the set B. Thus, Property D' is satisfied. This completes the proof of Theorem 3.

REFERENCES

1. T. BAKER, J. GILL and R. SOLOVAY, *Relativizations of the P=?NP Question*, S.I.A.M. J. Comput., Vol. 4, 1975, pp. 431-442.
2. J. BALCÁZAR, *Simplicity, Relativizations, and Nondeterminism*, S.I.A.M. J. Comput., Vol. 14, 1985, pp. 148-157.
3. J. BALCÁZAR and D. RUSSO, *Immunity and Simplicity in Relativizations of Probabilistic Complexity Classes*, R.A.I.R.O. Theoretical Informatics and Applications, Vol. 22, 1988, pp. 227-244.
4. J. BALCÁZAR and U. SCHÖNING, *Bi-Immune Sets for Complexity Classes*, Math. Systems Theory, Vol. 18, 1985, pp. 1-10.
5. C. BENNETT and J. GILL, *Relative to a Random Oracle A*, $P^A \neq NP^A \neq co\text{-}NP^A$ *with Probability* 1, S.I.A.M. J. Comput., Vol. 10, 1981, pp. 96-113.
6. M. FURST, J. SAXE and M. SIPSER, *Parity, Circuits and the Polynomial-Time Hierarchy*, Math. Systems Theory, Vol. 17, 1984, pp. 13-27.
7. J. HASTAD, *Almost Optimal Lower Bounds for Small Depth Circuits*, Proc. 18th A.C.M. Symp. on Theory of Computing, 1986, pp. 71-84.

8. S. Homer and W. Maass, *Oracle Dependent Properties of the Lattice of NP Sets*, Theoret. Comput. Sci., Vol. 24, 1983, pp. 279-289.

9. K. Ko, *Nonlevelable Sets and Immune Sets in the Accepting Density Hierarchy in NP*, Math. Systems Theory, Vol. 18, 1985, pp. 189-205.

10. K. Ko, *Relativized Polynomial Time Hierarchies Having Exactly k Levels*, S.I.A.M. J. Comput., Vol. 18, 1989, pp. 392-408.

11. C. Papadimitriou and S. Zachos, *Two Remarks on the Power of Counting*, Proc. 6th GI Conf. on Theoretical Computer Science, Lecture Notes in Computer Science, Vol. 145, 1983, pp. 269-276.

12. D. Russo, *Structural Properties of Complexity Classes*, Ph. D. dissertation, University of California, Santa Barbara, 1985.

13. U. Schöning and R. Book, *Immunity, Relativizations and Nondeterminism*, S.I.A.M. J. Comput., Vol. 13, 1984, pp. 329-337.

14. L. Torenvliet and P. van Emde Boas, *Diagonalization Methods in a Polynomial Setting*, Proc. Structure in Complexity Theory Conf., Lecture Notes in Computer Science, Vol. 223, 1986, pp. 330-346.

15. A. Yao, *Separating the Polynomial-Time Hierarchy by Oracles*, Proc. 26th I.E.E.E. Symp. on Foundations of Computer Science, 1985, pp. 1-10.