

On the Power of Unambiguity in Alternating Machines*

Holger Spakowski[†]

Institut für Informatik
Heinrich-Heine-Universität Düsseldorf
40225 Düsseldorf, Germany
spakowsk@cs.uni-duesseldorf.de

Rahul Tripathi[‡]

Department of Computer Science and Engineering
University of South Florida
Tampa, FL 33620, USA
tripathi@cse.usf.edu

Abstract

Unambiguity in alternating Turing machines has received considerable attention in the context of analyzing globally-unique games by Aida et al. [ACRW04] and in the design of efficient protocols involving globally-unique games by Crâsmaru et al. [CGRS04]. This paper explores the power of unambiguity in alternating Turing machines in the following settings:

1. We show that unambiguity based hierarchies—AUPH, UPH, and UPH —are infinite in some relativized world. For each $k \geq 2$, we construct another relativized world where the unambiguity based hierarchies collapse so that they have exactly k distinct levels and their k 'th levels coincide with PSPACE. These results shed light on the relativized power of the unambiguity based hierarchies, and parallel the results known for the case of the polynomial hierarchy.
2. For every $k \geq 1$, we define the bounded-level unambiguous alternating solution class $UAS(k)$ as the class of all sets L for which there exists a polynomial-time alternating Turing machine N , which need not be unambiguous on every input, with at most k alternations such that $x \in L$ if and only if x is accepted unambiguously by N . We construct a relativized world where, for all $k \geq 1$, $UP_{\leq k} \subset UP_{\leq k+1}$ and $UAS(k) \subset UAS(k+1)$.
3. Finally, we show that robustly k -level unambiguous alternating polynomial-time Turing machines, i.e., polynomial-time alternating Turing machines that for every

*A preliminary version of this paper appeared in *Proceedings of the 15th International Symposium on Fundamentals of Computation Theory (2005)* [ST05].

[†]Supported in part by the DFG under grants RO 1202/9-1 and RO 1202/9-3.

[‡]Supported in part by NSF grant CCF-0426761. Work done in part while affiliated with the Department of Computer Science at the University of Rochester, Rochester, NY 14627, USA.

oracle have k alternating levels and are unambiguous, accept languages that are computable in $P^{\Sigma_k^e \oplus \mathcal{A}}$, for every oracle \mathcal{A} . This generalizes a result of Hartmanis and Hemachandra [HH90].

Keywords: structural complexity, unambiguous computation, alternation, relativization.

1 Introduction

Chandra, Kozen, and Stockmeyer [CKS81] introduced the notion of *alternation* as a generalization of nondeterminism: Alternation allows switching of existential and universal quantifiers, whereas nondeterminism allows only existential quantifiers throughout the computation. Alternation has proved to be a central notion in complexity theory. For instance, the polynomial hierarchy has a characterization in terms of bounded-level alternation [Sto76,CKS81], the complexity class PSPACE can be characterized in terms of polynomial length-bounded alternation [CKS81], and many important classes have characterizations based on variants of alternation (see Chapter 19 of [Pap94]).

Unambiguity in nondeterministic computation is related to issues such as worst-case cryptography and the closure properties of $\#P$ (the class of functions that count the number of accepting paths of NP machines). The complexity class UP captures the notion of unambiguity in nondeterministic polynomial-time Turing machines. It is known that worst-case one-to-one one-way functions exist if and only if $P \neq UP$ [Ko85,GS88] and that UP equals probabilistic polynomial-time if and only if $\#P$ is closed under every polynomial-time computable operation [OH93]. Factoring, a natural problem with cryptographic applications, belongs to $UP \cap coUP$ and is not known to belong to a subclass of $UP \cap coUP$ nontrivially.

This paper studies the power of unambiguity in alternating computations. Niedermeier and Rossmanith [NR98] gave the following definition of unambiguity in alternating Turing machines: An alternating Turing machine is *unambiguous* if every accepting existential configuration has exactly one move to an accepting configuration and every rejecting universal configuration has exactly one move to a rejecting configuration. They introduced a natural analog UAP (unambiguous alternating polynomial-time) of UP for alternating Turing machines. Lange and Rossmanith [LR94] proposed three different approaches to define a hierarchy for unambiguous computations: The alternating unambiguous polynomial hierarchy AUPH, the unambiguous polynomial hierarchy UPH, and the promise unambiguous polynomial hierarchy UPH . Though it is known that $FEW \subseteq UAP \subseteq SPP$ [LR94,NR98] and $AUPH \subseteq UPH \subseteq UPH \subseteq UAP$ [LR94,CGRS04], a number of questions—such as, whether UAP is contained in the polynomial hierarchy, whether the unambiguity based hierarchies intertwine, whether these hierarchies are infinite, or whether some hierarchy is contained in a fixed level of the other hierarchy—related to these hierarchies have remained open [LR94]. Relatedly, Hemaspaandra and Rothe [HR97] showed that the existence of a sparse Turing complete set for UP has consequences on the structure of unambiguity based hierarchies. They proved that if UP has sparse Turing complete sets,

then for each $k \geq 3$, the k 'th level $\text{U}\Sigma_k^p$ of the unambiguous polynomial hierarchy (UPH) is contained in the $(k - 1)$ 'st level $\text{U}\Sigma_{k-1}^p$ of the promise unambiguous polynomial hierarchy.

Recently, Aida et al. [ACRW04] introduced “uniqueness” properties for two-player games of perfect information such as Checker, Chess, and Go. A two-person perfect information game has *global uniqueness* property if every winning position of player 1 has a unique move to win and every mis-step by player 1 is punishable by a unique winning reply by player 2 throughout the course of the game. Aida et al. [ACRW04] showed that the class of languages that reduce to globally-unique games, i.e., games with global uniqueness property, is the same as the class UAP. In another recent paper, Crâsmaru et al. [CGRS04] designed a protocol by which a series of globally-unique games can be combined into a single globally-unique game, even under the condition that the result of the new game is a non-monotone function of the results of the individual games that are unknown to the players. In complexity theoretic terms, they showed that the class UAP is self-low, i.e., $\text{UAP}^{\text{UAP}} = \text{UAP}$. They also observed that the graph isomorphism problem, whose membership in SPP was shown by Arvind and Kurur [AK02], in fact belongs to the subclass UAP of SPP.

In this paper, we investigate the power of unambiguity based alternating computation in three different settings. First, we study the relativized power of the unambiguity based hierarchies and the class UAP. We construct a relativized world in which the unambiguity based hierarchies—AUPH, UPH, and UPH —are infinite. We construct another relativized world where UAP is not contained in the polynomial hierarchy. This latter oracle result strengthens a result (relative to an oracle, UAP differs from the second level of UPH) of Crâsmaru et al. [CGRS04]. For each $k \geq 2$, we construct a relativized world where the unambiguity based hierarchies and the polynomial hierarchy have exactly k distinct levels and their k 'th levels collapse to PSPACE. Our results show that proving that any of the unambiguity based hierarchies is finite or that UAP is contained in the polynomial hierarchy, or that any of the unambiguity based hierarchies have at least k distinct levels, for any $k \geq 3$ (the case for $k = 2$ is trivial), is impossible by relativizable proof techniques. We mention that the structure of relativized hierarchies of classes has been investigated extensively in complexity theory (see, for instance [Yao85,Hås87,CGH⁺89,Ko89,Ko91]) and our investigation is a work in this direction.

Second, for every $k \geq 1$, we define the bounded-level unambiguous alternating solution class $\text{UAS}(k)$ as the class of all sets L for which there exists a polynomial-time alternating Turing machine N , which need not be unambiguous on every input, with at most k alternations such that $x \in L$ if and only if x is accepted unambiguously by N . A variant of this class (denoted by UAS in this paper), where the number of alternations is allowed to be unbounded, was studied by Wagner [Wag92] as the class ∇P of all sets that can be accepted by polynomial-time alternating Turing machines using partially defined AND and OR functions.¹ Beigel [Bei89] defined the class $\text{UP}_{\leq k(n)}$ as the class of sets in NP

¹The partial counterparts AND* and OR* differ from boolean functions AND and OR, respectively, as follows: AND* is undefined for input (0, 0) and OR* is undefined for input (1, 1). Thus, these partially defined boolean functions are the unambiguous counterparts of boolean AND and OR functions, respectively.

that are accepted by nondeterministic polynomial-time Turing machines with at most $k(n)$ accepting paths on each input of length n . Beigel [Bei89] constructed an oracle \mathcal{A} such that $\text{P}^{\mathcal{A}} \subset \text{UP}^{\mathcal{A}} \subset \text{UP}_{\leq k(n)}^{\mathcal{A}} \subset \text{UP}_{\leq k(n)+1}^{\mathcal{A}} \subset \text{FewP}^{\mathcal{A}} \subset \text{NP}^{\mathcal{A}}$, for every polynomial $k(n) \geq 2$. We show that there is a relativized world \mathcal{B} such that, for all $k \geq 1$, $\text{UP}_{\leq k}^{\mathcal{B}} \subset \text{UP}_{\leq k+1}^{\mathcal{B}}$, $\text{UAS}(k)^{\mathcal{B}} \subset \text{UAS}(k+1)^{\mathcal{B}}$, and relative to \mathcal{B} , the second level of \mathcal{UPH} is not contained in any level of AUPH .

Finally, we investigate the power of polynomial-time alternating Turing machines that preserve the bounded-level unambiguity property for every oracle. We show that a polynomial-time alternating Turing machine, which for every oracle has k alternating levels and is unambiguous, requires only weak oracle access in every relativized world. That is, for every oracle \mathcal{A} , the language of such a machine can be computed in $\text{P}^{\Sigma_k^p \oplus \mathcal{A}}$. This is a generalization of a result of Hartmanis and Hemachandra [HH90], which states that if a nondeterministic polynomial-time Turing machine is robustly categorical (i.e., for no oracle and for no input, the machine has more than one accepting path), then for every oracle \mathcal{A} , the machine accepts a language in $\text{P}^{\text{NP} \oplus \mathcal{A}}$.

2 Preliminaries

2.1 Notations

Let \mathbb{N} and \mathbb{N}^+ denote the set of nonnegative integers and positive integers, respectively. Our alphabet Σ is $\{0, 1\}$. For any deterministic or nondeterministic, or alternating Turing machine N , $A \subseteq \Sigma^*$, and $x \in \Sigma^*$, we use the shorthand $N^A(x)$ for “the computation of N with oracle A on input x .” The acronym NPTM stands for “nondeterministic polynomial-time Turing machine.” Let $\langle \cdot, \dots, \cdot \rangle$ denote a standard, fixed, easily computable, invertible, one-to-one, multiarity pairing function.

For every integer $m \in \mathbb{N}$ and variable y , let $(\exists^m y)$ be a shorthand for “ $(\exists y \in \Sigma^* : |y| \leq m)$ ” and $(\forall^m y)$ be a shorthand for “ $(\forall y \in \Sigma^* : |y| \leq m)$.” For every polynomial $p(\cdot)$ and for every predicate $R(x, y, z)$ of variables x, y, z , we use $(\exists^p! y)(\forall^p! z)R(x, y, z)$ to indicate that there exists a unique value y_1 for the y variable with $|y_1| \leq p(|x|)$, such that for all values z_1 for the z variable with $|z_1| \leq p(|x|)$, $R(x, y_1, z_1)$ is true, and for all values $y_2 \neq y_1$ for the y variable with $|y_2| \leq p(|x|)$, there exists a unique value $z(y_2)$ for the z variable with $|z(y_2)| \leq p(|x|)$ such that $\neg R(x, y_2, z(y_2))$ is true. We use $(\forall^p! y)(\exists^p! z)\neg R(x, y, z)$ to indicate that for all values y_1 for the y variable with $|y_1| \leq p(|x|)$, there exists a unique value $z(y_1)$ for the z variable with $|z(y_1)| \leq p(|x|)$ such that $\neg R(x, y_1, z(y_1))$ is true, and for all values $z_2 \neq z(y_1)$, $R(x, y_1, z_2)$ is true. In the same way, we interpret expressions, such as $(\exists^p! y_1)(\forall^p! y_2)(\exists^p! y_3) \dots R(x, y_1, y_2, y_3, \dots)$ and $(\forall^p! y_1)(\exists^p! y_2)(\forall^p! y_3) \dots \neg R(x, y_1, y_2, y_3, \dots)$, with bounded number of unambiguous alternations.

2.2 Alternating Computation

We assume that a *computation path* of an oracle alternating Turing machine (or, ATM in short) N encodes a complete valid computation of N relative to some oracle, i.e., is a

sequence of configurations including query strings and answers from the oracle. A *node* of an ATM N is defined by a configuration of N together with a valid computation path leading to this configuration. Hence, two nodes ν_1 and ν_2 of an oracle ATM are equal if and only if the configuration sequences, oracles queries, and oracles answers are the same for the computation paths leading to ν_1 and ν_2 . For any node ν of an oracle ATM N , let $Q_N(\nu)$ denote the set of queries along the path from the root to ν in $N^{(\cdot)}$, i.e., N with some oracle A .

We recursively assign levels in an ATM N as follows: (a) the root of N is at level 1, (b) if a node v is assigned a level i and if v is an existential node, then the first nonexistential (i.e., universal or leaf) node w reachable along some path from v to a leaf node of N is assigned level $i + 1$, (c) if a node v is assigned a level i and if v is a universal node, then the first nonuniversal (i.e., existential or leaf) node w reachable along some path from v to a leaf node of N is assigned level $i + 1$, and (d) for all other nodes of N , the concept of levels is insignificant to this work and so the levels are undefined. Without loss of generality, we assume that every leaf node of an ATM is at the same level. We term the nonleaf nodes for which levels are defined as the *salient* nodes of an ATM. If ϑ is a leaf node or a salient node, then we use $\text{level}(\vartheta)$ to denote the level of ϑ in the ATM. For any $k \in \mathbb{N}$, a k -level ATM is one for which, on any input, the maximum level assigned to a salient node is at most k . For the sake of generality, we can assume that a deterministic Turing machine is an ATM with no root and a nondeterministic Turing machine is an ATM with a single salient node, which is also the root of the ATM. Thus a deterministic Turing machine is a 0-level ATM and a nondeterministic Turing machine is a 1-level ATM.

Unless otherwise specified, the root of any ATM is assumed to be an existential node. We say that $N^A(x)$ is *unambiguous* if every accepting existential node in $N^A(x)$ has exactly one move to an accepting node and every rejecting universal node in $N^A(x)$ has exactly one move to a rejecting node. For every ATM N , $A \subseteq \Sigma^*$, and $x \in \Sigma^*$, we say that $N^A(x)$ accepts (rejects) with unambiguity if $N^A(x)$ accepts (respectively, rejects) and $N^A(x)$ is unambiguous. If $N^A(x)$ is unambiguous for every $x \in \Sigma^*$, then we say that N^A , i.e., N with oracle A , (or, simply N , if $A = \emptyset$) is unambiguous. An ATM N is called *robustly unambiguous* if $N^A(x)$ is unambiguous for every $x \in \Sigma^*$ and every oracle A .

2.3 Unambiguity in Alternating Computation

The complexity class UP captures the notion of unambiguity in nondeterministic polynomial-time computations. However, this notion of unambiguity becomes less clear when we focus our attention on alternating polynomial-time computations. In fact, Niedermeier and Rossmanith [NR98] observed that there might be three different approaches to define unambiguity based hierarchies, which are as follows.

Definition 2.1 (Unambiguity Based Hierarchies [LR94,NR98]) 1. *The alternating unambiguous polynomial hierarchy AUPH =_{df} $\bigcup_{k \geq 0} \text{AU}\Sigma_k^p$, where $\text{AU}\Sigma_0^p =_{df} \text{P}$ and for every $k \geq 1$, $\text{AU}\Sigma_k^p$ is the class of all sets $L \subseteq \Sigma^*$ for which there exist a polynomial $p(\cdot)$ and a polynomial-time computable predicate R such that,*

for all $x \in \Sigma^*$,

$$\begin{aligned} x \in L &\implies (\exists^{p!}y_1)(\forall^{p!}y_2) \dots (Q^{p!}y_k)R(x, y_1, y_2, \dots, y_k), \text{ and} \\ x \notin L &\implies (\forall^{p!}y_1)(\exists^{p!}y_2) \dots (\overline{Q}^{p!}y_k)\neg R(x, y_1, y_2, \dots, y_k), \end{aligned}$$

where $Q = \exists$ and $\overline{Q} = \forall$ if k is odd, and $Q = \forall$ and $\overline{Q} = \exists$ if k is even. For each $k \geq 0$, the class $\text{AUII}_k^p =_{df} \text{coAU}\Sigma_k^p$.

2. The unambiguous polynomial hierarchy is $\text{UPH} =_{df} \bigcup_{k \geq 0} \text{U}\Sigma_k^p$, where $\text{U}\Sigma_0^p =_{df} \text{P}$ and for every $k \geq 1$, $\text{U}\Sigma_k^p =_{df} \text{UP}^{\text{U}\Sigma_{k-1}^p}$. For each $k \geq 0$, the class $\text{UII}_k^p =_{df} \text{coU}\Sigma_k^p$.
3. The promise unambiguous polynomial hierarchy is $\text{UPH} =_{df} \bigcup_{k \geq 0} \mathcal{U}\Sigma_k^p$, where $\mathcal{U}\Sigma_0^p =_{df} \text{P}$, $\mathcal{U}\Sigma_1^p =_{df} \text{UP}$, and for every $k \geq 2$, $\mathcal{U}\Sigma_k^p$ is the class of all sets $L \in \Sigma_k^p$ such that for some oracle NPTMs N_1, N_2, \dots, N_k , $L = L(N_1^{L(N_2^{\dots^{L(N_k)})})$, and for every $x \in \Sigma^*$ and for every $1 \leq i \leq k-1$, $N_1^{L(N_2^{\dots^{L(N_k)})(x)}$ has at most one accepting path and if N_i asks a query w to its oracle $L(N_{i+1}^{\dots^{L(N_k)}(x)})$ during the computation of $N_1^{L(N_2^{\dots^{L(N_k)})(x)}$, then $N_{i+1}^{\dots^{L(N_k)}(w)}$ has at most one accepting path. For each $k \geq 0$, the class $\mathcal{UII}_k^p =_{df} \text{co}\mathcal{U}\Sigma_k^p$.

Niedermeier and Rossmanith [NR98] introduced the complexity class UAP as a natural analog of UP for alternating polynomial-time computations. UAP is known to lie in between the classes Few and SPP, i.e., $\text{Few} \subseteq \text{UAP} \subseteq \text{SPP}$ [LR94, NR98], and is known to contain a natural computational problem, namely the Graph Isomorphism problem [CGRS04]. Cr asmaru et al. [CGRS04] showed that UAP is self-low, i.e., $\text{UAP}^{\text{UAP}} = \text{UAP}$, and thus UAP is closed under all boolean operations and under polynomial-time Turing reducibility.

Definition 2.2 ([NR98]) *UAP is the class of sets accepted by unambiguous ATMs in polynomial time.*

The following theorem summarizes the known relationships among unambiguity based hierarchies, the class UAP, and other complexity classes.

Theorem 2.3 1. For all $k \geq 0$, $\text{AU}\Sigma_k^p \subseteq \text{U}\Sigma_k^p \subseteq \mathcal{U}\Sigma_k^p \subseteq \Sigma_k^p$ [LR94].

2. For all $k \geq 1$, $\text{UP}_{\leq k} \subseteq \text{AU}\Sigma_k^p \subseteq \text{U}\Sigma_k^p \subseteq \mathcal{U}\Sigma_k^p \subseteq \text{UAP}$ ([LR94] + [CGRS04]).

3. $\text{Few} \subseteq \text{UAP} \subseteq \text{SPP}$ ([LR94] + [NR98]).

The relativized versions of all these classes are defined in a standard way. The following facts follow easily from the definitions of the levels $\text{AU}\Sigma_k^p$ and AUII_k^p of the AUPH hierarchy.

Fact 2.4 1. $\text{AU}\Sigma_k^p = \text{AUII}_k^p \implies \text{AUPH} = \text{AU}\Sigma_k^p$.

2. $\text{AU}\Sigma_k^p = \text{AU}\Sigma_{k-1}^p \implies \text{AUPH} = \text{AU}\Sigma_{k-1}^p$.

3. $\text{AU}\Sigma_k^p \subseteq \Pi_k^p \implies \text{AU}\Sigma_{k+1}^p \subseteq \Sigma_k^p$.

Similar relations can be shown for the levels of UPH and $\mathcal{U}\mathcal{PH}$ (see also [HR97, NR98]).

3 Relativized Separations and Collapses of Unambiguity Based Hierarchies

In this section, we apply random restrictions of circuits for constructing oracles that separate or collapse the levels of unambiguity based hierarchies. Sheu and Long [SL96] constructed an oracle \mathcal{A} relative to which UP contains a language that is not in any level of the low hierarchy in NP. Formally, Sheu and Long [SL96] showed that there is an oracle \mathcal{A} such that for all $k \geq 1$, $\Sigma_k^{p, \text{UP}^{\mathcal{A}}} \not\subseteq \Sigma_k^{p, \mathcal{A}}$. In their proof, they introduced special kinds of random restrictions that were motivated by, but different from, the restrictions used by Håstad [Hås87]. Using the random restrictions of Sheu and Long [SL96], we construct a relativized world \mathcal{A} in which the unambiguity based hierarchies—AUPH, UPH, and UPH —are infinite. This extends the separation of the relativized polynomial hierarchy [Yao85, Hås87] to the separation of relativized unambiguity based hierarchies. We use the same restrictions to construct an oracle \mathcal{A} relative to which UAP is not contained in the polynomial hierarchy. Our separation results imply that proving that any of the unambiguity based hierarchies extends up to a finite level or proving that UAP is contained in the polynomial hierarchy is beyond the limits of relativizable proof techniques.

Finally, we apply random restrictions of Sheu and Long [SL96] to extend a result of Ko [Ko89]. Ko [Ko89] proved that for each $k \geq 1$, the relativized polynomial hierarchy collapses so that there are exactly k distinct levels in the hierarchy. We prove that for each $k \geq 2$, there is a relativized world where the unambiguity based hierarchies, AUPH, UPH, and UPH , and the polynomial hierarchy collapse so that each has exactly k distinct levels.²

3.1 Background and Notations

We now introduce certain notions that are prevalent in the theory of circuit lower bounds. A circuit is a directed acyclic graph where nonleaf nodes are associated with gates (ANDs/ORs) and leaf nodes are associated with variables and their complements, and boolean constants 0 and 1. In this paper, we consider only circuits whose underlying graphs are trees. Thus all circuits referred to in the paper are meant to be rooted trees. We represent the variables of a circuit by v_z , for some $z \in \Sigma^*$. The dual of a circuit C is obtained from C by replacing OR gates with ANDs, AND gates with ORs, variables x_i with \bar{x}_i , variables \bar{x}_j with x_j , and boolean constants, 0 and 1, with their complements, 1 and 0, respectively. A restriction ρ of a circuit C is a mapping from the variables of C to $\{0, 1, \star\}$. We say that a restriction ρ of a circuit C is an *assignment* if ρ assigns 0 or 1 to all the variables in C . Given a circuit C and a restriction ρ , $C[\rho]$ denotes the circuit obtained from C by substituting each variable x with $\rho(x)$ if $\rho(x) \neq \star$. A restriction ρ completely determines a circuit C , or in other words, $C[\rho]$ is completely determined, if $C[\rho]$ computes a constant function $\in \{0, 1\}$; in this case, we use the notation $C[\rho]$ to also denote

²This result—there is a relativized world where the unambiguity based hierarchies, AUPH, UPH, and UPH , and the polynomial hierarchy collapse so that each has exactly k distinct levels—holds for $k = 1$ as well, since $\text{UP}^{\text{PSPACE}} = \text{coNP}^{\text{PSPACE}} = \text{PSPACE}$.

the constant value computed by C on applying ρ (which sense is being used will be clear from the context). For every $A \subseteq \Sigma^*$, the restriction ρ_A on the variables v_z of a circuit C is $\rho_A(v_z) = 1$ if $z \in A$, and $\rho_A(v_z) = 0$ if $z \notin A$. The composition of two restrictions ρ_1 and ρ_2 , denoted by $\rho_1\rho_2$, is defined as follows: For every $x \in \Sigma^*$, $\rho_1\rho_2(x) = \rho_2(\rho_1(x))$. Thus if $\rho_1(x) \in \{0, 1\}$, then $\rho_1\rho_2(x) = \rho_1(x)$ and if $\rho_1(x) = \star$, then $\rho_1\rho_2(x) = \rho_2(x)$. A restriction ρ' extends ρ if the following holds:

1. domain of $\rho \subseteq$ domain of ρ' , and
2. for all variables v in the domain of ρ ,

$$\rho(v) = 0 \iff \rho'(v) = 0, \text{ and } \rho(v) = 1 \iff \rho'(v) = 1.$$

Furst, Saxe, and Sipser [FSS84] first showed the relationship between certain particular constant depth circuits, which were similar to those in Definition 3.1, and the relativized polynomial hierarchy. Since their work, variants of these constant depth circuits have been used in constructing relativized worlds involving Σ_k^p and Π_k^p classes. Below we define one such variant of constant depth circuits, namely $\Sigma_k(m)$ -circuits and $\Pi_k(m)$ -circuits, used for constructing relativized worlds involving Σ_k^p and Π_k^p classes.

Definition 3.1 ([FSS84]; see also [Ko91,SL94]) *For every $m \geq 1$ and $k \geq 1$, a $\Sigma_k(m)$ -circuit is a depth $k + 1$ circuit with alternating OR and AND gates such that*

1. the top gate, i.e., the gate at level 1, is an OR gate,
2. the total number of gates at levels 1 to $k - 1$ is bounded by 2^m ,
3. the fanins of gates at level k are unbounded.
4. the fanins of gates at level $k + 1$ are $\leq m$.

A $\Pi_k(m)$ -circuit is the dual circuit of a $\Sigma_k(m)$ -circuit.

For every $k \geq 1$, we say that $\sigma(\cdot; \cdot)$ is a $\Sigma_k^{P,(\cdot)}$ -predicate if there exist a predicate $R(A; x, y_1, \dots, y_k)$ over a set variable A and string variables x, y_1, y_2, \dots, y_k , and a polynomial $q(\cdot)$ such that the following hold: (i) $R(A; x, y_1, y_2, \dots, y_k)$ is computable in polynomial time by a deterministic oracle Turing machine that uses A as the oracle and $\langle x, y_1, \dots, y_k \rangle$ as the input and (ii) for every set A and string x , $\sigma(A; x)$ is true if and only if $(\exists^{q(|x|)} y_1)(\forall^{q(|x|)} y_2) \dots (Q_k^{q(|x|)} y_k) R(A; x, y_1, y_2, \dots, y_k)$ is true, where $Q_k = \exists$ if k is odd and $Q_k = \forall$ if k is even. We say that $\sigma(\cdot; \cdot)$ is a $\Pi_k^{P,(\cdot)}$ -predicate, where $k \geq 1$, if $\neg\sigma$ is a $\Sigma_k^{P,(\cdot)}$ -predicate.

The following proposition states the relationship between $\Sigma_k^{P,(\cdot)}$ -predicates ($\Pi_k^{P,(\cdot)}$ -predicates) and $\Sigma_k(m)$ -circuits (respectively, $\Pi_k(m)$ -circuits).

Proposition 3.2 ([FSS84]; see also [Ko91,SL94]) *Let $k \geq 1$. For every $\Sigma_k^{P,(\cdot)}$ -predicate ($\Pi_k^{P,(\cdot)}$ -predicate) σ , there is a polynomial $q(\cdot)$ such that, for all $x \in \Sigma^*$, there is a $\Sigma_k(q(|x|))$ -circuit (respectively, $\Pi_k(q(|x|))$ -circuit) $C_{\sigma,x}$ with the following properties:*

1. For every $A \subseteq \Sigma^*$, $C_{\sigma,x} \upharpoonright_{\rho_A} = 1$ if and only if $\sigma(A; x)$ is true, and

2. if v_z represents a variable in $C_{\sigma,x}$, then $|z| \leq q(|x|)$.

For every $h \geq 1$, we define a family of circuits \mathcal{F}_k^h . Ko [Ko91] defined a C_k^h circuit to be a depth k circuit in \mathcal{F}_k^h with an OR gate at the top and with fanins of gates at level k exactly equal to \sqrt{h} , and used these circuits to show that the relativized low and high hierarchies within NP are infinite. In [Ko89], Ko used a slightly different definition of C_k^h circuits to show that for every integer $k \geq 1$, the relativized polynomial hierarchy collapses so that it has exactly k levels. Sipser [Sip83] and Håstad [Hås87] earlier defined some other variants of these circuits.

We find it convenient to use the family of circuits \mathcal{F}_k^h , instead of C_k^h circuits, in our proofs for the following technical reasons: (i) We do not restrict ourselves to only those circuits which have an OR gate at the top or which have depth *exactly* k in the family \mathcal{F}_k^h of circuits (as is required in the proof of Lemma 3.19), and (ii) we no longer need to convert any circuit, obtained by applying a restriction, so that its bottom fanins are *exactly* the square root of its fanins at other levels.

\mathcal{F}_k^h circuits are described as follows.

Family \mathcal{F}_k^h of circuits, where $h \geq 1$: A circuit C of depth ℓ , where $1 \leq \ell \leq k$, is in \mathcal{F}_k^h if and only if the following holds:

1. C has alternating OR and AND gates,
2. the fanins of gates at levels 1 to $\ell - 1$ are exactly h ,
3. the fanins of gates at level ℓ are $\geq \sqrt{h}$,
4. every leaf of C is a unique positive variable, i.e., C has no negated variables and no constants as inputs, and no variable of C occurs more than once.

Let $\mathcal{B} = \{B_i\}_{i=1}^r$, where B_i 's are disjoint sets that cover the variables of C , and let q be a real number between 0 and 1. Sheu and Long [SL96] defined two probability spaces of restrictions, $\hat{R}_{q,\mathcal{B}}^+$ and $\hat{R}_{q,\mathcal{B}}^-$, and a probabilistic function g' that maps a restriction to a random restriction. A random restriction $\rho \in \hat{R}_{q,\mathcal{B}}^+$ ($\rho \in \hat{R}_{q,\mathcal{B}}^-$) is defined as follows: For each $1 \leq i \leq r$ and for each variable $x \in B_i$, let $\rho(x) = \star$ with probability q and let $\rho(x) = 1$ (respectively, $\rho(x) = 0$) with probability $1 - q$. We now define the probabilistic function $g'(\rho)$ for $\rho \in \hat{R}_{q,\mathcal{B}}^+$. For each $1 \leq i \leq r$, let $s_i = \star$ with probability q and let $s_i = 0$ with probability $1 - q$. Let $V_i \subseteq B_i$ be the set of variables x such that $\rho(x) = \star$. $g'(\rho)$ selects the variable v with the highest index in V_i , assigns value s_i to v , and assigns value 1 to all other variables in V_i . For $\rho \in \hat{R}_{q,\mathcal{B}}^-$, $g'(\rho)$ is defined in an analogous way by replacing 0 with 1 and 1 with 0 in the definition.

The switching lemma [Hås87] in its basic form says that if a random restriction chosen from an appropriately defined probability space is applied to an AND of ORs (OR of ANDs) with small bottom fanins, then with high probability the resulting circuit is equivalent to an OR of ANDs (respectively, AND of ORs) with small bottom fanin. In this paper, we need

the switching lemma given by Sheu and Long [SL96], which is an adaptation of Håstad's switching lemma [Hås87, Lemma 6.3] for Sheu and Long's random restrictions defined above.

Lemma 3.3 (Switching Lemma [SL96]) *Let C be a circuit consisting of an AND of ORs with bottom fanin $\leq t$. Let $\mathcal{B} = \{B_i\}_{i=1}^r$ be disjoint sets that cover the variables of C , and let q be a real number between 0 and 1. Then for a random restriction $\rho \in \hat{R}_{q,\mathcal{B}}^+$, $\text{Prob}[C \upharpoonright_{\rho g'(\rho)}$ is not equivalent to an OR of ANDs with bottom fanin $\leq s] \leq \alpha^s$, where $\alpha < 6qt$ and the probability is over the random choices done in defining ρ and $g'(\rho)$. The above probability holds also when $\hat{R}_{q,\mathcal{B}}^+$ is replaced by $\hat{R}_{q,\mathcal{B}}^-$, or when C is an OR of ANDs and is being converted to an AND of ORs.*

The application of this switching lemma is subsumed in the proof of Lemma 3.4. We do not require applying the switching lemma in this paper because Lemma 3.4 is sufficient for our purposes. However, we do require the particular random restrictions given by Sheu and Long [SL96], which are also used in the statement of Lemma 3.4.

Lemma 3.4 ([SL96]) *Let $\ell, t \in \mathbb{N}^+$. Let C_π be an arbitrary $\Sigma_{\ell+1}(t)$ -circuit ($\Pi_{\ell+1}(t)$ -circuit). Let $q \leq \frac{1}{12 \cdot t}$ and let $\mathcal{B} = \{B_i\}_{i=1}^r$ be an arbitrary partition of the variables of C_π . Then for a random restriction ρ , where $\rho \in \hat{R}_{q,\mathcal{B}}^+$ or $\rho \in \hat{R}_{q,\mathcal{B}}^-$, the following holds:*

$$\text{Prob}[C_\pi \upharpoonright_{\rho g'(\rho)} \text{ is equivalent to a } \Sigma_\ell(t)\text{-circuit (respectively, } \Pi_\ell(t)\text{-circuit)}] \geq \frac{2}{3},$$

where the probability is over the random choices done in defining ρ and $g'(\rho)$.

We call a circuit C constfree-positive if every leaf node of C is associated with a unique positive variable (i.e., C has no negated variables and no constants as inputs, and no variable of C occurs more than once). Sheu and Long [SL96] defined a notion called *U-condition* for restrictions of C_k^h . The same notion can be translated for any constfree-positive circuit C as follows. Let G_1, G_2, \dots, G_r denote the bottom gates of a constfree-positive circuit C . A restriction ρ is said to satisfy the U-condition for C if the following holds: For every $1 \leq i \leq r$, ρ assigns at most one variable of G_i to \star or 1 if the bottom gates are ORs and ρ assigns at most one variable of G_i to \star or 0 if the bottom gates are ANDs. We generalize the notion of U-condition to define a *global uniqueness condition (GU-condition)* for restrictions of any constfree-positive circuit C .

Definition 3.5 *We say that a restriction ρ satisfies the GU-condition for a constfree-positive circuit C if the computation of $C \upharpoonright_\rho$ has the following characteristics:*

1. *If an OR gate G_i of $C \upharpoonright_\rho$ has value 1, then there is exactly one input to G_i that has value 1 and all other inputs to G_i have value 0,*
2. *if an AND gate G_i of $C \upharpoonright_\rho$ has value 0, then there is exactly one input to G_i that has value 0 and all other inputs to G_i have value 1, and*
3. *if the output of any gate G_i of $C \upharpoonright_\rho$ is not completely determined, then no condition is imposed on inputs to G_i .*

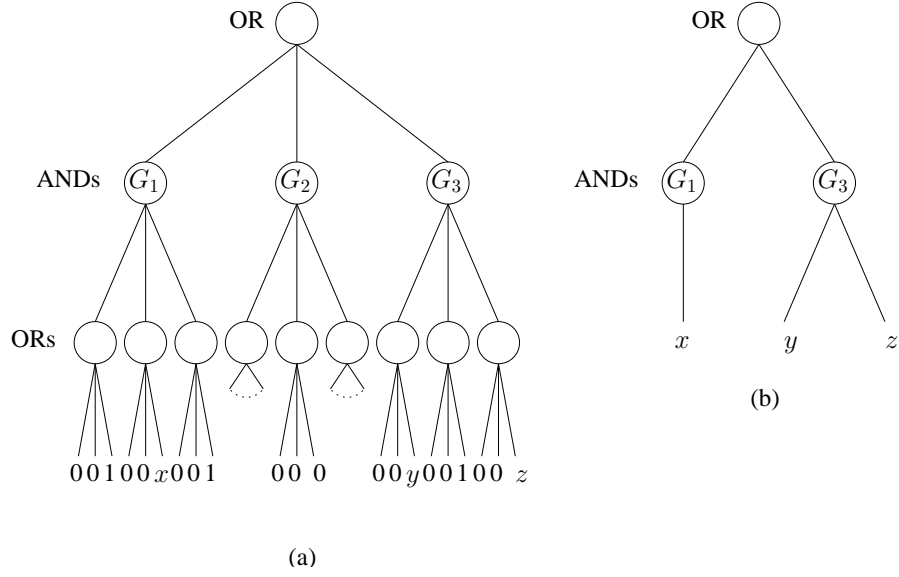


Figure 1: (a) A circuit $C[\rho]$ and (b) its max-subcircuit.

Thus in particular, a restriction ρ that maps all the variables of a constfree-positive circuit C to \star satisfies the GU-condition for the circuit since property (3) of Definition 3.5 is satisfied.

Let C be a constfree-positive circuit and let ρ be a restriction that satisfies the GU-condition for C . If $C[\rho]$ is not completely determined, then we define the *max-subcircuit* C' of $C[\rho]$ to be the following circuit.

- C' is equivalent to $C[\rho]$, i.e., C' and $C[\rho]$ compute the same boolean function.
- C' is obtained by simplifying $C[\rho]$ as follows: (i) First all constants are removed from $C[\rho]$, (ii) next if a gate is completely determined, then the entire subtree rooted at that gate is removed from $C[\rho]$, and (iii) finally if all the leftover bottom gates of $C[\rho]$ have fanins 1, then each leftover bottom gate of $C[\rho]$ is replaced by its child node.

We mention that if $C[\rho]$ is completely determined, then the max-subcircuit of $C[\rho]$ is undefined. (Since we will use the term max-subcircuit only when $C[\rho]$ is not completely determined, this does not cause any problems.)

Figure 1 shows a circuit $C[\rho]$, which is not completely determined, and its max-subcircuit.

3.2 Main Observations

Let C be a constfree-positive circuit with bottom gates G_1, G_2, \dots, G_r . Suppose we choose $\mathcal{B} = \{B_i\}_{i=1}^r$ such that B_i is the set of variables in the bottom gate G_i of the circuit C and choose a real number q between 0 and 1. Then the composition $\rho g'(\rho)$, where $\rho \in \hat{R}_{q,\mathcal{B}}^+$ if the bottom gates are ANDs and $\rho \in \hat{R}_{q,\mathcal{B}}^-$ if the bottom gates are ORs, and the function g' is as defined previously, satisfies the U-condition for C . This observation was crucial

in the proof by Sheu and Long [SL96] of the existence of a relativized world where UP is not in any level of the low hierarchy in NP. Our main observations, used in constructing relativized worlds separating or collapsing unambiguity based hierarchies, are summarized in Propositions 3.6, 3.7, and 3.8. (Since these propositions are easy to verify, we have omitted their proofs.)

Proposition 3.6 *Let ρ be a restriction that satisfies the U-condition for a constfree-positive circuit C of depth ≥ 2 . Let the circuit $C \upharpoonright_{\rho}$ be such that no gate at the second from last level of $C \upharpoonright_{\rho}$ is completely determined. Then ρ satisfies the GU-condition for C and the max-subcircuit of $C \upharpoonright_{\rho}$ is of depth one less than that of C .*

Proposition 3.7 *Let ρ be a restriction of a constfree-positive circuit C such that ρ satisfies the GU-condition for C and ρ does not completely determine C . Then there exist restrictions ρ_0 and ρ_1 such that both ρ_0 and ρ_1 satisfy the GU-condition for the max-subcircuit of $C \upharpoonright_{\rho}$, and moreover $C \upharpoonright_{\rho\rho_0} = 0$ and $C \upharpoonright_{\rho\rho_1} = 1$.*

Proposition 3.8 *Let ρ_1 be a restriction of a constfree-positive circuit C such that ρ_1 satisfies the GU-condition for C and ρ_1 does not completely determine C . If ρ_2 is a restriction that satisfies the GU-condition for the max-subcircuit of $C \upharpoonright_{\rho_1}$, then $\rho_1\rho_2$ satisfies the GU-condition for C .*

Sheu and Long [SL96] proved that applying a random restriction $\rho g'(\rho)$ satisfying the U-condition for the circuit C_{k+1}^h transforms the circuit to one containing a subcircuit computing the function computed by a C_k^h circuit with high probability. Lemma 3.9 generalizes this result of Sheu and Long [SL96] by showing that a similar transformation is possible, not just for a single but, for an exponential (in h) number of circuits in the family \mathcal{F}_{k+1}^h with high probability if a random restriction $\rho g'(\rho)$ satisfying the U-conditions for the circuits is applied. Moreover with high probability, the random restriction $\rho g'(\rho)$ satisfies the GU-condition for all the involved circuits, a property that is crucial for the feasibility of our oracle constructions.

The proof of Lemma 3.9 is similar to that of Lemma 6.8 of Håstad [Hås87] and Lemma A.2 of Ko [Ko89]. Ko's [Ko89] Lemma A.2 is basically a strengthening of Lemma 6.8 of Håstad [Hås87]. Lemma 3.9 differs from Lemma A.2 of Ko [Ko89] in two main respects: (i) Ko used random restrictions by Håstad [Hås87], whereas we require random restrictions by Sheu and Long [SL96], which are slightly different from that by Håstad [Hås87], and (ii) our lemma additionally guarantees that a random restriction satisfies the GU-condition for all the involved circuits with high probability.

Lemma 3.9 *Let $k \geq 2$, $m < 2^{h^{1/8}}$, and $h > h_0(k, m)$, for some constant $h_0(k, m)$ depending only on k and m . Let C_0, C_1, \dots, C_m be circuits in \mathcal{F}_{k+1}^h such that each C_i has depth ≥ 2 , the bottom gates of the C_i s are of the same type, and the variables of the C_i s are pairwise disjoint. Let G_1, G_2, \dots, G_r denote the bottom gates of the C_i s. Let $q = h^{-1/3}$ and let $\mathcal{B} = \{B_j\}_{j=1}^r$, where B_j is the set of variables of G_j . Then for a random restriction ρ , where $\rho \in \hat{R}_{q, \mathcal{B}}^+$ if the bottom gates G_j are ANDs and $\rho \in \hat{R}_{q, \mathcal{B}}^-$ if the bottom gates G_j are*

ORs, the following holds with probability $\geq 2/3$: For every $0 \leq i \leq m$, $\rho g'(\rho)$ satisfies the GU-condition for C_i , the max-subcircuit of $C_i \upharpoonright_{\rho g'(\rho)}$ is in \mathcal{F}_k^h , and the max-subcircuit has depth one less than that of C_i . Here the probability is over the random choices made in defining ρ and $g'(\rho)$.

Proof of Lemma 3.9. We assume that the bottom gates of C_i 's are ORs; a similar proof can be given when the bottom gates of C_i 's are ANDs. Let E_1 be the event that each bottom OR gate $G_j \upharpoonright_{\rho g'(\rho)}$ of the circuits $C_i \upharpoonright_{\rho g'(\rho)}$ takes the value $s_j \in \{\star, 1\}$ (the value assigned to the block B_j by ρ). We first show that $\Pr[E_1] \geq 5/6$ for all sufficiently large h .

To this end, let $G_j \upharpoonright_{\rho g'(\rho)}$ be a bottom OR gate. Note that $G_j \upharpoonright_{\rho g'(\rho)}$ does not take the value s_j if and only if each variable in G_j is assigned 0 by ρ . Thus the probability that $G_j \upharpoonright_{\rho g'(\rho)}$ does not take the value s_j is bounded by $(1-q)^{\sqrt{h}} \leq e^{-q\sqrt{h}}$. Since there are $m+1$ circuits C_i each containing at most h^k bottom OR gates, the probability that at least one of the bottom OR gates $G_j \upharpoonright_{\rho g'(\rho)}$ does not take the value s_j is $\leq (m+1) \cdot h^k \cdot e^{-q\sqrt{h}} \leq 1/6$, for all $h \geq h_1(k, m)$, where $h_1(k, m)$ is a constant depending only on k and m . It follows that $\Pr[E_1] \geq 5/6$ if $h \geq h_1(k, m)$.

Next we define E_2 to be the event that every AND gate at the second from last level of every $C_i \upharpoonright_{\rho g'(\rho)}$ has at least \sqrt{h} children nodes $G_j \upharpoonright_{\rho g'(\rho)}$ of OR gates having value $s_j = \star$. We show that $\Pr[E_2] \geq 5/6$ for all sufficiently large h .

To this end, let p_s denote the probability that an AND gate at the second from last level of $C_i \upharpoonright_{\rho g'(\rho)}$ has exactly s children nodes $G_j \upharpoonright_{\rho g'(\rho)}$ of OR gates having value $s_j = \star$. Then

$$p_s = \binom{h}{s} \cdot q^s \cdot (1-q)^{h-s},$$

since each OR gate $G_j \upharpoonright_{\rho g'(\rho)}$ takes value $s_j = \star$ independently with probability q . Thus the probability that an AND gate at the second from last level of $C_i \upharpoonright_{\rho g'(\rho)}$ has $< \sqrt{h}$ children nodes $G_j \upharpoonright_{\rho g'(\rho)}$ of ORs having value $s_j = \star$ is

$$\begin{aligned} &= \sum_{s=0}^{\sqrt{h}-1} p_s \\ &= \sum_{s=0}^{\sqrt{h}-1} \binom{h}{s} \cdot q^s \cdot (1-q)^{h-s}. \end{aligned}$$

It can be easily verified that, for all sufficiently large h and for every $1 \leq s \leq \sqrt{2h} - 1$, $\frac{p_s}{p_{s-1}} \geq 2$. Therefore,

$$\sum_{s=0}^{\sqrt{h}-1} p_s \leq p_{\sqrt{h}-1} \times \left(\sum_{s=0}^{\infty} 2^{-s} \right) \leq 2 \cdot p_{\sqrt{h}-1}.$$

Also, $p_{\sqrt{h}-1} \leq 2^{-(\sqrt{2h}-\sqrt{h})} \cdot p_{\sqrt{2h}-1} \leq 2^{-\sqrt{h}/3}$, since $p_{\sqrt{2h}-1} \leq 1$. It follows that the probability that there is an AND gate at the second from last level of some $C_i \upharpoonright_{\rho g'(\rho)}$ with

$< \sqrt{h}$ children nodes $G_j \upharpoonright_{\rho g'(\rho)}$ of OR gates having value $s_j = \star$ is $\leq \frac{2}{2\sqrt{h/3}} \cdot h^{k-1} \cdot (m+1) \leq \frac{1}{6}$, for all $h \geq h_2(k, m)$, where $h_2(k, m)$ is a constant depending only on k and m . Thus $\Pr[E_2] \geq 5/6$ if $h \geq h_2(k, m)$.

By the observation stated in the beginning of Section 3.2, $\rho g'(\rho)$ satisfies the U-condition for every C_i . Also, observe that if events E_1 and E_2 simultaneously occur, then none of the AND gates at the second from last level of every $C_i \upharpoonright_{\rho g'(\rho)}$ are completely determined. The lemma now follows from Proposition 3.6 and the fact that $\Pr[E_1 \wedge E_2] \geq 2/3$ if $h \geq \max\{h_1(k, m), h_2(k, m)\}$. \blacksquare (Lemma 3.9)

3.3 Relativized Unambiguity Based Hierarchies Being Infinite

Theorem 3.10 proves that there is a relativized world where each level $\text{AU}\Sigma_k^p$ of AUPH is not included in the corresponding Π_k^p level of PH. On the other hand, each level $\text{AU}\Sigma_k^p$ of AUPH is clearly contained in the Σ_k^p level of PH (see Theorem 2.3). Thus Theorem 3.10 shows a finer relationship between levels of the unambiguity based hierarchies and the polynomial hierarchy in a relativized setting.

Theorem 3.10 $(\exists \mathcal{A})(\forall k \geq 1)[\text{AU}\Sigma_k^{p, \mathcal{A}} \not\subseteq \Pi_k^{p, \mathcal{A}}]$.

Proof Our proof is inspired from that of Theorem 4.2 (relative to some oracle \mathcal{D} , for all $k \geq 1$, $\Sigma_k^{p, \text{UP}^{\mathcal{D}}} \not\subseteq \Sigma_k^{p, \mathcal{D}}$) by Sheu and Long [SL96]. For every $k \geq 1$, we define a test language $L_k(B)$ as follows: $L_k(B) \subseteq 0^*$ such that, for every $n \in \mathbb{N}^+$,

$$\begin{aligned} 0^n \in L_k(B) &\implies (\exists^n! y_1)(\forall^n! y_2) \dots (Q^n! y_k) \left[0^k 1 y_1 y_2 \dots y_k \in B \right], \text{ and} \\ 0^n \notin L_k(B) &\implies (\forall^n! y_1)(\exists^n! y_2) \dots (\overline{Q}^n! y_k) \left[0^k 1 y_1 y_2 \dots y_k \notin B \right], \end{aligned}$$

where $Q = \exists$ and $\overline{Q} = \forall$ if k is odd, and $Q = \forall$ and $\overline{Q} = \exists$ if k is even. We say that a set $B \subseteq \Sigma^*$ satisfies $\text{Valid}(B; n, k)$, where $n, k \in \mathbb{N}^+$, if the membership of 0^n in the test language $L_k(B)$ is well-defined. Clearly this test language $L_k(B)$ is defined only for particular sets B , which satisfy $\text{Valid}(B; n, k)$ for all $n \in \mathbb{N}^+$. We will construct an oracle \mathcal{A} such that $L_k(\mathcal{A})$ would be defined for all $k \geq 1$. This will also imply, by the definition of the test language $L_k(B)$, that for all $k \geq 1$, $L_k(\mathcal{A}) \in \text{AU}\Sigma_k^{p, \mathcal{A}}$.

Choose a minimal cardinality set $\mathcal{O} \subseteq \Sigma^*$ such that for every $k \geq 1$, $L_k(\mathcal{O}) = 0^*$. For every $k \geq 1$, let $\pi_{k,1}, \pi_{k,2}, \dots$ be an enumeration of $\Pi_k^{P, (\cdot)}$ -predicates. In stage $\langle k, i \rangle$, we diagonalize against $\pi_{k,i}$ and change \mathcal{O} at a certain length. Finally at the end of every stage, we set $\mathcal{A} := \mathcal{O}$. We now define the stages involved in the construction of the oracle.

Stage $\langle k, i \rangle$: Choose a very large integer n so that the construction in this stage does not spoil the constructions in previous stages. Also, n must be large enough to meet the requirements in the proof of Claim 1. Set $\mathcal{O} := \mathcal{O} - \Sigma^{k \cdot (n+1) + 1}$. Choose a set $B \subseteq 0^k 1 \Sigma^{k \cdot n}$ such that the following requirement is satisfied:

$$\text{Valid}(B; n, k) \text{ is true and } (0^n \in L_k(B) \iff \neg \pi_{k,i}(\mathcal{O} \cup B; 0^n)) \text{ is true.} \quad (3.a)$$

In Claim 1, we show that there is always a set $B \subseteq 0^k 1 \Sigma^{k \cdot n}$ satisfying Statement (3.a). Let $\mathcal{O} := \mathcal{O} \cup B$ and move to the next stage.

End of Stage

Clearly, the existence of a set B satisfying Statement (3.a) suffices to finish stage $\langle k, i \rangle$ successfully. Next, we prove that there is always such a set B .

Claim 1 *In every stage $\langle k, i \rangle$, there is a set $B \subseteq 0^k 1 \Sigma^{k \cdot n}$ satisfying Statement (3.a).*

Proof of Claim 1. We introduce a circuit $C(n, k)$ that encodes our test language in the following sense: For every $B \subseteq 0^k 1 \Sigma^{k \cdot n}$ such that ρ_B satisfies the GU-condition for $C(n, k)$, it holds that

$$\begin{aligned} C(n, k) \upharpoonright_{\rho_B} = 1 &\implies (\exists^n! y_1)(\forall^n! y_2) \dots (Q^n! y_k)[0^k 1 y_1 y_2 \dots y_k \in B], \\ &\text{and} \\ C(n, k) \upharpoonright_{\rho_B} = 0 &\implies (\forall^n! y_1)(\exists^n! y_2) \dots (\bar{Q}^n! y_k)[0^k 1 y_1 y_2 \dots y_k \notin B]. \end{aligned} \tag{3.b}$$

Statement (3.b) in turn implies, by the definition of our test language $L_k(B)$, that for every $B \subseteq 0^k 1 \Sigma^{k \cdot n}$ such that ρ_B satisfies the GU-condition for $C(n, k)$ it holds that

$$\begin{aligned} C(n, k) \upharpoonright_{\rho_B} = 1 &\implies 0^n \in L_k(B), \\ &\text{and} \\ C(n, k) \upharpoonright_{\rho_B} = 0 &\implies 0^n \notin L_k(B). \end{aligned} \tag{3.c}$$

The circuit $C(n, k)$ is defined as follows:

- The depth of $C(n, k)$ is k ,
- the top gate of $C(n, k)$ is an OR gate,
- the fanins of all the gates at levels 1 to k are exactly 2^n ,
- the variables of $C(n, k)$ are exactly those in $\{v_z \mid z \in 0^k 1 \Sigma^{k \cdot n}\}$, and
- the variables v_z occur in positive form in exactly one leaf of $C(n, k)$ in the lexicographic ordering of z .

Let $C_{\pi_{k,i}}$ be the $\Pi_k(p_i(n))$ -circuit corresponding to $\pi_{k,i}((\cdot); 0^n)$, for some polynomial $p_i(\cdot)$. By Statement (3.c), the proof of this claim is completed by showing that there is always a set $B \subseteq 0^k 1 \Sigma^{k \cdot n}$ such that

$$\rho_B \text{ satisfies the GU-condition for } C(n, k) \text{ and } C(n, k) \upharpoonright_{\rho_B} \neq C_{\pi_{k,i}} \upharpoonright_{\rho_{\mathcal{O} \cup B}}. \tag{3.d}$$

We define a restriction $\hat{\rho}_{\mathcal{O}}$ on $C_{\pi_{k,i}}$ as follows: For every variable v_z in $C_{\pi_{k,i}}$, if $z \in \mathcal{O}$ then let $\hat{\rho}_{\mathcal{O}}(v_z) = 1$, if $z \notin \mathcal{O} \cup 0^k 1 \Sigma^{k \cdot n}$ then let $\hat{\rho}_{\mathcal{O}}(v_z) = 0$, and if $z \in 0^k 1 \Sigma^{k \cdot n}$ then let $\hat{\rho}_{\mathcal{O}}(v_z) = \star$. Let $C_{\pi_{k,i}(\mathcal{O})} =_{df} C_{\pi_{k,i}} \upharpoonright_{\hat{\rho}_{\mathcal{O}}}$. Thus the only variables v_z appearing in $C_{\pi_{k,i}(\mathcal{O})}$ are the ones for which $z \in 0^k 1 \Sigma^{k \cdot n}$.

To get a contradiction, suppose that no set $B \subseteq 0^k 1 \Sigma^{k \cdot n}$ satisfying Statement (3.d) exists. Then the following holds: For every $B \subseteq 0^k 1 \Sigma^{k \cdot n}$,

$$\text{if } \rho_B \text{ satisfies the GU-condition for } C(n, k), \text{ then } C(n, k) \upharpoonright_{\rho_B} = C_{\pi_{k,i}(\mathcal{O})} \upharpoonright_{\rho_B}. \quad (3.e)$$

Since $C(n, k) \in \mathcal{F}_k^{2^n}$ is a depth k circuit with an OR gate at the top, $C_{\pi_{k,i}(\mathcal{O})}$ is a $\Pi_k(p_i(n))$ -circuit, and $p_i(n) \leq \frac{1}{12} \cdot 2^{n/3}$ for large n , we get a contradiction with Statement (3.e) and Lemma 3.11. This completes the proofs of Claim 1 and Theorem 3.10. \blacksquare (Claim 1 and Theorem 3.10)

Lemma 3.11 *Let $k \geq 1$ be an arbitrary integer. Let $C_0 \in \mathcal{F}_k^h$ be of depth k with an OR gate at the top. Let C_π be any $\Pi_k(\frac{1}{12} \cdot h^{1/3})$ -circuit. If h is sufficiently large (depending only on k), then there exists an assignment ρ of C_0 such that*

1. ρ satisfies the GU-condition for C_0 , and
2. $C_0 \upharpoonright_{\rho} \neq C_\pi \upharpoonright_{\rho}$.

Proof of Lemma 3.11. The proof is similar to that of Theorem 4.1 by Sheu and Long [SL96]. We prove the lemma by induction on k . For the base case $k = 1$, let C_0 be an arbitrary OR gate with $\geq \sqrt{h}$ variables. Let C_π be an arbitrary $\Pi_1(\frac{1}{12} \cdot h^{1/3})$ -circuit. Note that C_π is an AND of ORs with bottom fanin $\leq \frac{1}{12} \cdot h^{1/3}$. We show that there is an assignment ρ of C_0 such that ρ satisfies the GU-condition for C_0 and $C_0 \upharpoonright_{\rho} \neq C_\pi \upharpoonright_{\rho}$. Consider the following cases.

Case $C_\pi \upharpoonright_{\rho_0} = 0$: Then there is an OR gate G_i in C_π such that $G_i \upharpoonright_{\rho_0} = 0$. Since $\frac{1}{12} \cdot h^{1/3} < \sqrt{h}$, there is a variable v_z in C_0 that is not in G_i . Then $\rho_{\{z\}}$ satisfies the GU-condition for C_0 , $C_0 \upharpoonright_{\rho_{\{z\}}} = 1$, and $C_\pi \upharpoonright_{\rho_{\{z\}}} = 0$.

Case $C_\pi \upharpoonright_{\rho_0} = 1$: Then ρ_0 satisfies the GU-condition for C_0 , $C_0 \upharpoonright_{\rho_0} = 0$, and $C_\pi \upharpoonright_{\rho_0} = 1$.

We now assume that the lemma is correct for $k = \ell$. Let C_0 be an arbitrary depth $\ell + 1$ circuit in $\mathcal{F}_{\ell+1}^h$ with an OR gate at the top and let C_π be an arbitrary $\Pi_{\ell+1}(\frac{1}{12} \cdot h^{1/3})$ -circuit. Lemmas 3.9 and 3.4 imply that there is a restriction $\rho g'(\rho)$ such that (i) $\rho g'(\rho)$ satisfies the GU-condition for C_0 , (ii) the max-subcircuit C'_0 of $C_0 \upharpoonright_{\rho g'(\rho)}$ is a depth ℓ subcircuit in \mathcal{F}_ℓ^h with an OR gate at the top, and (iii) $C_\pi \upharpoonright_{\rho g'(\rho)}$ is equivalent to a $\Pi_\ell(\frac{1}{12} \cdot h^{1/3})$ -circuit.

By the induction hypothesis, there is an assignment ϖ such that ϖ satisfies the GU-condition for C'_0 and $C'_0 \upharpoonright_{\varpi} \neq C_\pi \upharpoonright_{\rho g'(\rho) \varpi}$. Since the max-subcircuit C'_0 and the circuit $C_0 \upharpoonright_{\rho g'(\rho)}$ compute the same function, it follows that $C_0 \upharpoonright_{\rho g'(\rho) \varpi} \neq C_\pi \upharpoonright_{\rho g'(\rho) \varpi}$.

It remains to show that $\rho g'(\rho) \varpi$ satisfies the GU-condition for C_0 . To this end, note that the restriction $\rho g'(\rho)$ satisfies the GU-condition for C_0 and ϖ satisfies the GU-condition for the max-subcircuit of $C_0 \upharpoonright_{\rho g'(\rho)}$. Apply Proposition 3.8. \blacksquare (Lemma 3.11)

The following corollaries are an easy consequence of Theorem 3.10.

Corollary 3.12 ([CGRS04]) *There is an oracle \mathcal{A} such that $\text{UP}^{\text{UP}^{\mathcal{A}}} \not\subseteq \text{P}^{\text{NP}^{\mathcal{A}}}$.*

Corollary 3.13 *There is an oracle \mathcal{A} relative to which the alternating unambiguous polynomial hierarchy AUPH, the unambiguous polynomial hierarchy UPH, the promise unambiguous polynomial hierarchy UP \mathcal{H} , and the polynomial hierarchy PH are infinite.*

We mention that Niedermeier and Rossmanith [NR98] cited an unpublished work by Rossmanith for the relativized separation of $\text{AU}\Sigma_k^p$ from $\text{U}\Sigma_k^p$, for each $k \geq 2$. However, this result does not seem to imply ours in any obvious way.

Note that Theorem 3.10 does not imply relativized separation of UAP from PH in any obvious way. We achieve this separation, using the proof techniques of Theorem 3.10, in Theorem 3.14.

Theorem 3.14 $(\exists \mathcal{A})[\text{UAP}^{\mathcal{A}} \not\subseteq \text{PH}^{\mathcal{A}}]$.

Proof The proof is almost the same as that of Theorem 3.10. We construct an oracle \mathcal{A} and a test language $L(\mathcal{A}) \in \text{UAP}^{\mathcal{A}}$ such that, for every $k \geq 1$, $L(\mathcal{A}) \notin \Pi_k^{p,\mathcal{A}}$. Clearly, this suffices to prove the theorem. We define our test language $L(B)$ as follows: $L(B) \subseteq 0^*$ such that for every $n \in \mathbb{N}^+$,

$$\begin{aligned} 0^n \in L(B) &\implies (\exists^n!y_1)(\forall^n!y_2)\dots(Q^n!y_n)[y_1y_2\dots y_n \in B], \text{ and} \\ 0^n \notin L(B) &\implies (\forall^n!y_1)(\exists^n!y_2)\dots(\overline{Q}^n!y_n)[y_1y_2\dots y_n \notin B], \end{aligned}$$

where $Q = \exists$ and $\overline{Q} = \forall$ if n is odd, and $Q = \forall$ and $\overline{Q} = \exists$ if n is even. We say that a set $B \subseteq \Sigma^*$ satisfies $\text{Valid}(B; n)$ if the membership of 0^n in the test language $L(B)$ is well-defined. Clearly, $L(B)$ is defined only for particular sets B , which satisfy $\text{Valid}(B; n)$ for all $n \in \mathbb{N}^+$. Our oracle \mathcal{A} will be constructed in a way that $L(\mathcal{A})$ would be defined. This will also imply that $L(\mathcal{A}) \in \text{UAP}^{\mathcal{A}}$.

Choose a minimal cardinality set $\mathcal{O} \subseteq \Sigma^*$ such that $L(\mathcal{O}) = 0^*$. For every $k \geq 1$, let $\pi_{k,1}, \pi_{k,2}, \dots$ denote an enumeration of $\Pi_k^{P,(\cdot)}$ -predicates. In stage $\langle k, i \rangle$, we diagonalize against $\pi_{k,i}$ and change \mathcal{O} at a certain length. Finally at the end of every stage, we set $\mathcal{A} := \mathcal{O}$.

Stage $\langle k, i \rangle$: Choose a very large integer n so that the construction in this stage does not affect the constructions in previous stages and the requirements in the proof of Claim 2 are met. Set $\mathcal{O} := \mathcal{O} - \Sigma^{n^2}$. Choose a set $B \subseteq \Sigma^{n^2}$ such that the following requirement is satisfied:

$$\text{Valid}(B; n) \text{ is true and } (0^n \in L(B) \iff \neg \pi_{k,i}(\mathcal{O} \cup B; 0^n)) \text{ is true.} \quad (3.f)$$

Claim 2 shows that there is always a set $B \subseteq \Sigma^{n^2}$ satisfying Statement (3.f). Let $\mathcal{O} := \mathcal{O} \cup B$ and move to the next stage.

End of Stage

Claim 2 *In every stage $\langle k, i \rangle$, there is a set $B \subseteq \Sigma^{n^2}$ satisfying Statement (3.f).*

Proof of Claim 2. Assume to the contrary that in some stage $\langle k, i \rangle$, no set $B \subseteq \Sigma^{n^2}$ satisfies Statement (3.f). Let $C(n)$ denote the following circuit: The depth of $C(n)$ is n , the top gate of $C(n)$ is an OR gate, the fanins of all the gates at levels 1 to n are 2^n , the variables of $C(n)$ are exactly those in $\{v_z \mid z \in \Sigma^{n^2}\}$, and the variables v_z occur in positive form in exactly one leaf of $C(n)$ in the lexicographic ordering of z . Thus C_n is a depth n circuit in $\mathcal{F}_n^{2^n}$. Let $C_{\pi_{k,i}}$ be the $\Pi_k(p_i(n))$ -circuit corresponding to $\pi_{k,i}(\cdot; 0^n)$.

Next, we define a restriction $\hat{\rho}_{\mathcal{O}}$ as follows: For every variable v_z of $C_{\pi_{k,i}}$, if $z \in \mathcal{O}$ then $\hat{\rho}_{\mathcal{O}}(v_z) = 1$, if $z \notin \mathcal{O} \cup \Sigma^{n^2}$ then $\hat{\rho}_{\mathcal{O}}(v_z) = 0$, and if $z \in \Sigma^{n^2}$ then $\hat{\rho}_{\mathcal{O}}(v_z) = \star$. Let $C_{\pi_{k,i}(\mathcal{O})} =_{df} C_{\pi_{k,i}} \upharpoonright_{\hat{\rho}_{\mathcal{O}}}$. The following statement follows from our assumptions: For every $B \subseteq \Sigma^{n^2}$,

$$\text{if } \rho_B \text{ satisfies the GU-condition for } C(n), \text{ then } C(n) \upharpoonright_{\rho_B} = C_{\pi_{k,i}(\mathcal{O})} \upharpoonright_{\rho_B}. \quad (3.g)$$

Since $C(n) \in \mathcal{F}_n^{2^n}$ is a depth n circuit with an OR gate at the top, $C_{\pi_{k,i}(\mathcal{O})}$ is a $\Pi_k(p_i(n))$ -circuit, and $p_i(n) \leq \frac{1}{12} \cdot 2^{n/3}$ for all large n , we get a contradiction with Statement (3.g) and Lemma 3.15. This completes the proofs of Claim 2 and Theorem 3.14. \blacksquare (Claim 2 and Theorem 3.14)

Lemma 3.15 *Let $k \geq 1$ be an arbitrary integer. Then the following is true for all $n \geq k$: Let $C_0 \in \mathcal{F}_n^h$ be of depth n with an OR gate at the top. Let C_π be any $\Pi_k(\frac{1}{12} \cdot h^{1/3})$ -circuit. If h is sufficiently large (depending only on k), then there exists an assignment ρ of C_0 such that*

1. ρ satisfies the GU-condition for C_0 , and
2. $C_0 \upharpoonright_{\rho} \neq C_\pi \upharpoonright_{\rho}$.

Proof of Lemma 3.15. Let C_0 be an arbitrary depth n circuit in \mathcal{F}_n^h with an OR gate at the top and let C_π be an arbitrary $\Pi_k(\frac{1}{12} \cdot h^{1/3})$ -circuit. Take an arbitrary depth k subcircuit $C'_0 \in \mathcal{F}_k^h$ of C_0 . Apply Lemma 3.11 to C'_0 and C_π and get the assignment ρ' of C'_0 . It is easy to see that ρ' can be completed to an assignment ρ of C_0 such that $C_0 \upharpoonright_{\rho} = C'_0 \upharpoonright_{\rho'}$ and moreover ρ satisfies the GU-condition for C_0 . Thus ρ satisfies the conditions of the lemma. \blacksquare (Lemma 3.15)

Crăsmaru et al. [CGRS04] showed that there is an oracle relative to which $\text{UAP} \neq \mathcal{US}_2^p$. Corollary 3.16 shows that in some relativized world, UAP is much more powerful than the promise unambiguous polynomial hierarchy UPH . Thus, Corollary 3.16 is a strengthening of their result.

Corollary 3.16 *There is an oracle relative to which $\text{UPH} \subset \text{UAP}$.*

Corollary 3.17 ([CGRS04]) *There is an oracle relative to which $\text{UAP} \neq \mathcal{US}_2^p$.*

3.4 Relativized Unambiguity Based Hierarchies Being Finite

We next prove in Theorem 3.18 that for each $k \geq 2$, there is a relativized world where the unambiguity based hierarchies and the polynomial hierarchy have exactly k distinct levels and all higher levels collapse to their k 'th levels. Earlier Ko [Ko89] proved a similar result for the relativized polynomial hierarchy: For each $k \geq 1$, there exists an oracle A such that the polynomial hierarchy has k distinct levels and the hierarchy collapses at the k 'th level. Thus Theorem 3.18 may be viewed as a strengthening of Ko's result from the polynomial hierarchy case to the case of unambiguity based hierarchies. The proof utilizes random restrictions of Sheu and Long [SL96] and some ideas of Ko [Ko89].

Theorem 3.18 $(\forall k \geq 1)(\exists \mathcal{A})[\text{AU}\Sigma_k^{p,\mathcal{A}} \not\subseteq \Pi_k^{p,\mathcal{A}}, \text{ but } \text{PH}^{\mathcal{A}} = \text{AU}\Sigma_{k+1}^{p,\mathcal{A}}].$

Proof Our oracle construction is inspired from Ko [Ko89], where he proved that for all $k \geq 1$, there is an oracle relative to which the polynomial hierarchy extends only to k levels. Fix a $k \geq 1$. We will construct an oracle \mathcal{A} such that

$$\text{AU}\Sigma_k^{p,\mathcal{A}} \not\subseteq \Pi_k^{p,\mathcal{A}}, \text{ and } \text{AU}\Sigma_{k+1}^{p,\mathcal{A}} = \Pi_{k+1}^{p,\mathcal{A}}.$$

Clearly, this suffices to prove the theorem. We define our test language $L(B)$ as follows: $L(B) \subseteq 0^*$ such that for every $n \in \mathbb{N}^+$,

$$\begin{aligned} 0^n \in L(B) &\implies (\exists^n!y_1)(\forall^n!y_2)\dots(Q^n!y_k)[1^{2^n}y_1y_2\dots y_k \in B], \text{ and} \\ 0^n \notin L(B) &\implies (\forall^n!y_1)(\exists^n!y_2)\dots(\overline{Q}^n!y_k)[1^{2^n}y_1y_2\dots y_k \notin B], \end{aligned}$$

where $Q = \exists$ and $\overline{Q} = \forall$ if k is odd, and $Q = \forall$ and $\overline{Q} = \exists$ if k is even. We will construct \mathcal{A} in a way that $L(\mathcal{A})$ would be defined, and thus $L(\mathcal{A})$ would be in $\text{AU}\Sigma_k^{p,\mathcal{A}}$. Let π_1, π_2, \dots be an enumeration of all $\Pi_k^{P,(\cdot)}$ -predicates.

Let $S_{k+1}(A)$ be a polynomial-time many-one complete set for $\Sigma_{k+1}^{p,A}$ with the property that the membership of any string x in $S_{k+1}(A)$ depends only on the set $\{y \in A \mid |y| < |x|\}$. Ko [Ko89] proved that for any $\ell \geq 1$ and for each set A , $\Sigma_\ell^{p,A}$ has such a complete set $S_\ell(A)$.³

We construct the oracle \mathcal{A} in stages. At every stage $s \in \mathbb{N}$, we maintain a set $\mathcal{A}(s)$ of strings that must be included and a set $\mathcal{A}'(s)$ of strings that must be forbidden in the oracle \mathcal{A} . The sets $\mathcal{A}(s)$ and $\mathcal{A}'(s)$ will always be disjoint, though not necessarily be complementary. The set $\mathcal{A}(s)$, for $s \geq 1$, will be constructed by adding some, possibly none, strings either to $\mathcal{A}(s-1)$ or to $\mathcal{A}(s-1) - \Sigma^s$. Likewise, we construct the set $\mathcal{A}'(s)$, for $s \geq 1$, by adding some, possibly none, strings either to $\mathcal{A}'(s-1)$ or to $\mathcal{A}'(s-1) - \Sigma^s$. We will ensure that at every stage s , no string of length $< s$ is included in $\mathcal{A}(s)$ or $\mathcal{A}'(s)$. Thus

³To give an idea about the polynomial-time many-one complete sets $S_\ell(A)$ for $\Sigma_\ell^{p,A}$, we give an inductive definition of $S_\ell(A)$ as given by Ko [Ko89]. $S_1(A)$ is the set $\{\langle i, z, 1^j \rangle \mid \text{the } i\text{'th nondeterministic oracle Turing machine } N_i \text{ accepts } z \text{ in } j \text{ moves with the oracle } A\}$. It is easy to show that $S_1(A)$ is polynomial-time many-one complete for $\Sigma_1^{p,A}$ and has the desired property—the membership of any string x in $S_1(A)$ depends only on the set $\{y \in A \mid |y| < |x|\}$. For $\ell > 1$, let $S_\ell(A) =_{df} S_1(S_{\ell-1}(A))$. It can be shown by induction that for any $\ell \geq 1$, $S_\ell(A)$ is polynomial-time many-one complete for $\Sigma_\ell^{p,A}$ and $S_\ell(A)$ has the desired property.

the memberships in the oracle \mathcal{A} of strings of length $< s$ will be fixed by the end of stage $s - 1$. This will be useful in arguing that the construction in stage s does not interfere with constructions in previous stages. Finally at the end of every stage, we will define \mathcal{A} as follows: $\mathcal{A} := \lim_{s \rightarrow \infty} \mathcal{A}(s)$.

In stage $s = (k + 2) \cdot n$, we will try to satisfy the following requirement $R_{1,i}$, where i is the least integer such that $R_{1,i}$ is not yet satisfied.

$R_{1,i}$: There exists $n_i \in \mathbb{N}^+$ such that

$$(0^{n_i} \in L(\mathcal{A}) \iff \neg \pi_i(\mathcal{A}; 0^{n_i})) \text{ is true.}$$

In stage $s = (k + 2) \cdot n + 1$, we will satisfy the following requirement.

$R_{2,n}$: For all strings u of length n ,

$$\begin{aligned} u \notin S_{k+1}(\mathcal{A}) &\implies (\exists^n! y_1)(\forall^n! y_2) \dots (Q^n! y_{k+1})[0uy_1y_2 \dots y_{k+1} \in \mathcal{A}], \text{ and} \\ u \in S_{k+1}(\mathcal{A}) &\implies (\forall^n! y_1)(\exists^n! y_2) \dots (\overline{Q}^n! y_{k+1})[0uy_1y_2 \dots y_{k+1} \notin \mathcal{A}], \end{aligned}$$

where $Q = \exists$ and $\overline{Q} = \forall$ if k is even, and $Q = \forall$ and $\overline{Q} = \exists$ if k is odd. As mentioned earlier, we will construct \mathcal{A} in a way that $L(\mathcal{A})$ would be in $\text{AU}\Sigma_k^{p,\mathcal{A}}$. The requirement $\bigwedge_i R_{1,i}$ ensures that $L(\mathcal{A}) \notin \Pi_k^{p,\mathcal{A}}$. The requirement $\bigwedge_n R_{2,n}$ ensures that the complement of the set $S_{k+1}(\mathcal{A})$ is in $\text{AU}\Sigma_{k+1}^{p,\mathcal{A}}$. Since $S_{k+1}(\mathcal{A})$ is a polynomial-time many-one complete set for $\Sigma_k^{p,\mathcal{A}}$, this would imply that $\Pi_k^{p,\mathcal{A}} = \text{AU}\Sigma_{k+1}^{p,\mathcal{A}}$. It is now clear that if a set \mathcal{A} satisfies $\bigwedge_i R_{1,i}$ and $\bigwedge_n R_{2,n}$, and if $L(\mathcal{A}) \in \text{AU}\Sigma_k^{p,\mathcal{A}}$, then $\text{AU}\Sigma_k^{p,\mathcal{A}} \not\subseteq \Pi_k^{p,\mathcal{A}}$, and $\text{AU}\Sigma_{k+1}^{p,\mathcal{A}} = \Pi_{k+1}^{p,\mathcal{A}}$.

We maintain a set T of indices of currently unsatisfied requirements $R_{1,i}$. Thus if $i \in T$ at some stage of oracle construction, then it implies that the requirement $R_{1,i}$ is not yet satisfied. If a requirement $R_{1,i}$ is satisfied at some stage s , then we delete the index i of the requirement $R_{1,i}$ from T . In every stage s , we also maintain an integer $\ell(s)$ that upper bounds the length of any string stored in $\mathcal{A}(s')$ or $\mathcal{A}'(s')$, for any $s' \leq s$. The role of the integer $\ell(s)$ is to avoid potential conflicts between requirements $R_{1,i}$ and $R_{1,j}$, for some $i \neq j$. Thus if $s > \ell(s - 1)$ for some stage s , then we may be assured that the construction in stage s will not affect the construction in previous stages.

Initially, choose a minimal cardinality set $\mathcal{A}(0) \subseteq \bigcup_{n \in \mathbb{N}^+} 1^{2n} \Sigma^{k \cdot n}$ such that $L(\mathcal{A}(0)) = 0^*$. Set $\mathcal{A}'(0) := \bigcup_{n \in \mathbb{N}^+} 1^{2n} \Sigma^{k \cdot n} - \mathcal{A}(0)$, $\ell(0) := 1$, and $T := \mathbb{N}^+$. We define stages $s \geq 1$ as follows.

Stage $s \notin \{(k + 2) \cdot n, (k + 2) \cdot n + 1\}$, for any $n \in \mathbb{N}^+$: Then move to the next stage with $\mathcal{A}(s) := \mathcal{A}(s - 1)$, $\mathcal{A}'(s) := \mathcal{A}'(s - 1)$, and $\ell(s) := \ell(s - 1)$.

End of Stage s

Stage $s = (k + 2) \cdot n$: If $s \leq \ell(s - 1)$ or if n is too small to meet the requirements in the proof of Claim 3, then move to the next stage with $\mathcal{A}(s) := \mathcal{A}(s - 1)$, $\mathcal{A}'(s) := \mathcal{A}'(s - 1)$, and $\ell(s) := \ell(s - 1)$.

Otherwise, if $s > \ell(s-1)$ and if n is large enough to meet the requirements in the proof of Claim 3, then do the following. Set $\mathcal{A}(s) := \mathcal{A}(s-1) - \Sigma^s$ and $\mathcal{A}'(s) := \mathcal{A}'(s-1) - \Sigma^s$. Let i be the minimum index in T and let C'_{π_i} be the $\Pi_k(p_i(n))$ -circuit corresponding to $\pi_i((\cdot); 0^n)$, for some polynomial $p_i(\cdot)$. Let C_{π_i} be the circuit C'_{π_i} with the following restrictions:

1. Variables v_z such that $|z| < s = (k+2) \cdot n$ are replaced by constants $\chi_{\mathcal{A}(s-1)}(z)$,
2. variables v_z such that $s < |z| \leq p_i(n)$ and $z \in 1^{2m}\Sigma^{k \cdot m}$, for some $m \in \mathbb{N}^+$, are replaced by constants $\chi_{\mathcal{A}(s-1)}(z)$,
3. variables v_z such that $s \leq |z| \leq p_i(n)$, $z \notin 1^{2n}\Sigma^{k \cdot n} \cup (\bigcup_m 0\Sigma^{(k+2) \cdot m})$ and z is not of the form as in restriction 2 above, are replaced by 0.

Restriction 1 makes sense because the memberships in \mathcal{A} of strings of length $< s$ will already be fixed by the end of stage $s-1$. Restrictions 2 and 3 make sense because (i) the variables v_z of C'_{π_i} satisfy $|z| \leq p_i(n)$, (ii) strings in $1^{2n}\Sigma^{k \cdot n}$ and those relevant to the satisfaction of requirements $R_{2,m}$, where $m \geq n$, are the only interesting ones for the construction at stage s , and (iii) strings z corresponding to the remaining variables of C'_{π_i} must confirm to the requirement that $L(\mathcal{A})$ is defined.

Thus the only variables v_z appearing in C_{π_i} are the ones for which $s \leq |z| \leq p_i(n)$ and $z \in 1^{2n}\Sigma^{k \cdot n} \cup (\bigcup_m 0\Sigma^{(k+2) \cdot m})$. Also for every $B \subseteq \{z \in \Sigma^* \mid v_z \text{ is a variable of } C_{\pi_i}\}$, it holds that

$$(C_{\pi_i} \upharpoonright_{\rho_B} = 1 \iff \pi_i((\mathcal{A}(s-1) - \Sigma^s) \cup B; 0^n)) \text{ is true.} \quad (3.h)$$

We must be careful in assigning boolean values to the variables v_z of C_{π_i} , i.e., in assigning memberships in \mathcal{A} of strings z , to satisfy the requirement $R_{1,i}$ because any arbitrary assignment to the variables of C_{π_i} that satisfy $R_{1,i}$ may conflict with the requirements $R_{2,m}$, for $m \geq n$. We actually need a partial assignment that guarantees the satisfaction of $R_{1,i}$ and leaves leeway for the other variables so that any requirement $R_{2,m}$, where $m \geq n$, may eventually be satisfied in some future stage $s' > s$. We show the existence of such a partial solution in Claim 3, which requires using Lemma 3.19.

We define circuits C_u for all strings u for which a potential conflict between the assignment of variables of C_{π_i} and the satisfaction of the requirement $R_{2,|u|}$ cannot be ignored. These circuits C_u are defined so that the following statement is satisfied: For every $B \subseteq \Sigma^*$ such that ρ_B satisfies the GU-condition for C_u , it holds that

$$\begin{aligned} C_u \upharpoonright_{\rho_B} = 1 &\implies (\exists^{|u|!} y_1)(\forall^{|u|!} y_2) \dots (Q^{|u|!} y_{k+1}) [0u y_1 y_2 \dots y_{k+1} \in B], \\ &\text{and} \\ C_u \upharpoonright_{\rho_B} = 0 &\implies (\forall^{|u|!} y_1)(\exists^{|u|!} y_2) \dots (\bar{Q}^{|u|!} y_{k+1}) [0u y_1 y_2 \dots y_{k+1} \notin B]. \end{aligned} \quad (3.i)$$

With the above goals in mind we define the circuits C_u , for every $u \in \Sigma^*$ such that $s \leq (k+2) \cdot |u| + 1 \leq p_i(n)$, as follows:

- The depth of C_u is $k+1$,

- the top gate of C_u is an OR gate,
- The fanins of all the gates at levels 1 to $k + 1$ are $2^{|u|}$, and
- the variables of C_u are exactly those in $\{v_z \mid z \in 0u\Sigma^{(k+1)\cdot|u|}\}$.
- the variables v_z occur in positive form in exactly one leaf of C_u in the lexicographic ordering of z .

Next we introduce a circuit $C(n, k)$ that encodes our test language in the following sense: For every $B \subseteq \Sigma^*$ such that ρ_B satisfies the GU-condition for $C(n, k)$, it holds that

$$\begin{aligned}
C(n, k) \upharpoonright_{\rho_B} = 1 &\implies (\exists^n!y_1)(\forall^n!y_2) \dots (Q^n!y_k)[1^{2^n}y_1y_2 \dots y_k \in B], \\
&\text{and} \\
C(n, k) \upharpoonright_{\rho_B} = 0 &\implies (\forall^n!y_1)(\exists^n!y_2) \dots (\overline{Q}^n!y_k)[1^{2^n}y_1y_2 \dots y_k \notin B].
\end{aligned} \tag{3.j}$$

By the definition of our test language $L(B)$, Statement (3.j) implies that for every $B \subseteq \Sigma^*$ such that ρ_B satisfies the GU-condition for $C(n, k)$, it holds that

$$\begin{aligned}
C(n, k) \upharpoonright_{\rho_B} = 1 &\implies 0^n \in L(B), \\
&\text{and} \\
C(n, k) \upharpoonright_{\rho_B} = 0 &\implies 0^n \notin L(B).
\end{aligned} \tag{3.k}$$

The circuit $C(n, k)$ is defined similarly to circuits C_u except that the depth of $C(n, k)$ is k , the fanins of all the gates at levels 1 to k are 2^n , and the variables of $C(n, k)$ are exactly those in $\{v_z \mid z \in 1^{2^n}\Sigma^{k \cdot n}\}$. It is easy to verify that $C(n, k) \in \mathcal{F}_{k+1}^{2^n}$ and for all the just defined circuits C_u holds that $C_u \in \mathcal{F}_{k+1}^{2^{|u|}}$.

The following claim is crucial for this stage.

Claim 3 *There exists a restriction ρ such that*

1. ρ completely determines $C(n, k)$,
2. ρ satisfies the GU-condition for $C(n, k)$ and for every C_u such that $s \leq (k+2)\cdot|u|+1 \leq p_i(n)$,
3. for any restriction ρ' extending ρ such that ρ' completely determines C_{π_i} and ρ' satisfies the GU-condition for every C_u , where $s \leq (k+2)\cdot|u|+1 \leq p_i(n)$, it holds that $C(n, k) \upharpoonright_{\rho'} \neq C_{\pi_i} \upharpoonright_{\rho'}$, and
4. ρ does not completely determine C_u , for every u such that $s \leq (k+2)\cdot|u|+1 \leq p_i(n)$.

Assuming the truth of the claim, set $\mathcal{A}(s) := \mathcal{A}(s) \cup \{z \mid \rho(z) = 1\}$, $\mathcal{A}'(s) := \mathcal{A}'(s) \cup \{z \mid \rho(z) = 0\}$, $\ell(s) := \max\{s, p_i(n)\}$, and $T := T - \{i\}$. Move to the next stage.

End of Stage $s = (k+2) \cdot n$

Stage $s = (k+2) \cdot n + 1$: For every $u \in \Sigma^n$, we first determine the membership of u in $S_{k+1}(\mathcal{A}(s-1))$. (We will show that for any $u \in \Sigma^n$, $u \in S_{k+1}(\mathcal{A}(s-1)) \iff u \in S_{k+1}(\mathcal{A})$.)

Thus it makes sense to determine the membership of every $u \in \Sigma^n$ in $S_{k+1}(\mathcal{A}(s-1))$. The following claim is crucial for this stage.

Claim 4 *For every $u \in \Sigma^n$, there exists a set $B(u) \subseteq \{z \in 0u\Sigma^{(k+1)\cdot|u|} \mid z \notin \mathcal{A}(s-1) \cup \mathcal{A}'(s-1)\}$ such that*

$$\begin{aligned} u \notin S_{k+1}(\mathcal{A}(s-1)) &\implies \\ &(\exists^{|u|!}y_1)(\forall^{|u|!}y_2) \dots (Q^{|u|!}y_{k+1})[0uy_1y_2 \dots y_{k+1} \in \mathcal{A}(s-1) \cup B(u)], \text{ and} \\ u \in S_{k+1}(\mathcal{A}(s-1)) &\implies \\ &(\forall^{|u|!}y_1)(\exists^{|u|!}y_2) \dots (\overline{Q}^{|u|!}y_{k+1})[0uy_1y_2 \dots y_{k+1} \notin \mathcal{A}(s-1) \cup B(u)], \end{aligned}$$

where $Q = \exists$ and $\overline{Q} = \forall$ if k is even, and $Q = \forall$ and $\overline{Q} = \exists$ if k is odd.

Assuming the truth of the claim, set $\mathcal{A}(s) := \mathcal{A}(s-1) \cup (\bigcup_{u \in \Sigma^n} B(u))$, $\mathcal{A}'(s) := \mathcal{A}'(s-1)$, and $\ell(s) := \max\{s, \ell(s-1)\}$. Move to the next stage.

End of Stage $s = (k+2) \cdot n + 1$

Observe that at no stage s' , we include any string of length $< s'$ in $\mathcal{A}(s')$ or in $\mathcal{A}'(s')$. The reason is as follows: In stage s' of the form $(k+2) \cdot m$, the only strings z we include in $\mathcal{A}(s')$ or in $\mathcal{A}'(s')$ are the ones for which $s' \leq |z| \leq p(m)$ for some polynomial $p(\cdot)$; in stage s' of the form $(k+2) \cdot m + 1$ we add strings z of length $|z| = s'$ in $\mathcal{A}(s')$; and if s' is not of the form $(k+2) \cdot m$ or $(k+2) \cdot m + 1$, then we do not include any string in $\mathcal{A}(s')$ or in $\mathcal{A}'(s')$.

We show that for every $i \in \mathbb{N}^+$, the requirement $R_{1,i}$ is eventually satisfied. The requirement $R_{1,i}$ will be considered in stage $s = (k+2) \cdot n + 1$, for some sufficiently large n . Assuming the truth of Claim 3, we assign strings to $\mathcal{A}(s)$ and to $\mathcal{A}'(s)$ at the end of stage s . This assignment of strings to $\mathcal{A}(s)$ and to $\mathcal{A}'(s)$ does not conflict with assignments made in any stage $s' < s$ because s is greater than $\ell(s-1)$, an upper bound on the maximum length string stored in $\mathcal{A}(s')$ or in $\mathcal{A}'(s')$, for any $s' \leq s-1$. Furthermore, this assignment of strings to $\mathcal{A}(s)$ and to $\mathcal{A}'(s)$ is never overridden in any later stage because $\ell(s) = \max\{s, p_i(n)\}$ and in no stage s' of the form $(k+2) \cdot m + 1$, we assign strings in $\mathcal{A}(s'-1) \cup \mathcal{A}'(s'-1)$ to $\mathcal{A}(s')$ or to $\mathcal{A}'(s')$.

By the end of stage $s' = p_i(n)$, all strings z , such that v_z is a variable in C_{π_i} , would have been assigned to $\mathcal{A}(s')$ or to $\mathcal{A}'(s')$. This also implies that the memberships in \mathcal{A} of all such strings would be fixed by the end of stage s' . Thus when we replace each variable v_z of $C(n, k)$ and C_{π_i} by $\rho_{\mathcal{A}}(v_z)$, then the following hold: These circuits become completely determined, and $\rho_{\mathcal{A}}$ satisfies the GU-condition for $C(n, k)$. Moreover, assuming the truth of Claim 4 and by the manner sets $B(u)$ are defined in Claim 4, $\rho_{\mathcal{A}}$ also satisfies the GU-condition for every C_u , where $s \leq (k+2) \cdot |u| + 1 \leq p_i(n)$. Thus property (3) of Claim 3 implies that $C(n, k) \upharpoonright_{\rho_{\mathcal{A}}} \neq C_{\pi_i} \upharpoonright_{\rho_{\mathcal{A}}}$. It follows from Statement (3.k) and Statement (3.h) that

$$(0^n \in L(\mathcal{A}) \iff \neg\pi_i(\mathcal{A}; 0^n)) \text{ is true.}$$

This completes the proof that $R_{1,i}$ is eventually satisfied.

We now show that for all $n \in \mathbb{N}^+$, $R_{2,n}$ is satisfied. The requirement $R_{2,n}$ is considered in stage $s = (k+2) \cdot n + 1$. Recall the aforementioned property of S_{k+1} because of which for any $u \in \Sigma^n$, the membership of u in $S_{k+1}(\mathcal{A}(s-1))$ depends only on the set $\{z \in \mathcal{A}(s-1) \mid |z| < |u|\}$. Since we never add any string of length $< s'$ to $\mathcal{A}(s')$ or to $\mathcal{A}'(s')$ in any stage s' , it follows that the membership of any string $u \in \Sigma^n$ in $S_{k+1}(\mathcal{A}(s-1))$ is preserved in $S_{k+1}(\mathcal{A}(s'))$, for any $s' \geq s-1$. Thus for every $u \in \Sigma^n$,

$$u \in S_{k+1}(\mathcal{A}(s-1)) \iff u \in S_{k+1}(\mathcal{A}). \quad (3.1)$$

Let us first assume that Claim 4 is true. From Claim 4, it follows that for every $u \in \Sigma^n$, we can find a set $B(u) \subseteq 0u\Sigma^{(k+1) \cdot |u|}$ satisfying the claim. At the end of stage s , we include strings in $\bigcup_{u \in \Sigma^n} B(u)$ to $\mathcal{A}(s)$. This assignment of strings to $\mathcal{A}(s)$ does not conflict with assignments made in any stage $s' < s$ because no string $z \in \bigcup_{u \in \Sigma^n} B(u)$ belongs to $\mathcal{A}(s-1) \cup \mathcal{A}'(s-1)$. Furthermore, this assignment of strings to $\mathcal{A}(s)$ is never overridden because strings in $\bigcup_{u \in \Sigma^n} B(u)$ are of length s and at no later stage $s' > s$ we assign a string a length $< s'$ to $\mathcal{A}(s')$ or to $\mathcal{A}'(s')$. It then follows from Claim 4 and Statement (3.1) that for any $u \in \Sigma^n$,

$$\begin{aligned} u \notin S_{k+1}(\mathcal{A}) &\implies (\exists^{|u|!}y_1)(\forall^{|u|!}y_2) \dots (Q^{|u|!}y_{k+1})[0uy_1y_2 \dots y_{k+1} \in \mathcal{A}], \text{ and} \\ u \in S_{k+1}(\mathcal{A}) &\implies (\forall^{|u|!}y_1)(\exists^{|u|!}y_2) \dots (\overline{Q}^{|u|!}y_{k+1})[0uy_1y_2 \dots y_{k+1} \notin \mathcal{A}], \end{aligned}$$

where $Q = \exists$ and $\overline{Q} = \forall$ if k is even, and $Q = \forall$ and $\overline{Q} = \exists$ if k is odd. This completes the proof that $R_{2,n}$ is satisfied.

It only remains to prove Claim 3 and Claim 4. We first show that Claim 4 is true, assuming the truth of Claim 3. After proving Claim 4, we give a proof for Claim 3.

Proof of Claim 4. Assume that Claim 3 is true. Fix a $u \in \Sigma^n$. If no string in $0u\Sigma^{(k+1) \cdot |u|}$ has been assigned to $\mathcal{A}(s-1)$ or to $\mathcal{A}'(s-1)$, then we obviously have a set $B(u)$ satisfying the claim by Proposition 3.7. Otherwise, some string in $0u\Sigma^{(k+1) \cdot |u|}$ has previously been assigned to $\mathcal{A}(s-1)$ or to $\mathcal{A}'(s-1)$. This assignment must have been made in at most one stage $s' = (k+2) \cdot m$, for some $m \leq n$, by the manner $\ell(s')$ is defined. In that stage, we would have chosen a restriction ρ satisfying Claim 3 to set $\mathcal{A}(s')$ and $\mathcal{A}'(s')$. By the properties (2) and (4) of ρ (see Claim 3), ρ satisfies the GU-condition for C_u and ρ does not completely determine C_u . It follows by Proposition 3.7 that there exist restrictions ρ' and ρ'' on the variables of $C_u \upharpoonright_\rho$ such that (a) both ρ' and ρ'' satisfy the GU-condition for the max-subcircuit of $C_u \upharpoonright_\rho$, and (b) $C_u \upharpoonright_{\rho\rho'} = 0$ and $C_u \upharpoonright_{\rho\rho''} = 1$. Define $B_0(u) := \{z \in 0u\Sigma^{(k+1) \cdot |u|} \mid \rho(v_z) = * \text{ and } \rho'(v_z) = 1\}$ and $B_1(u) := \{z \in 0u\Sigma^{(k+1) \cdot |u|} \mid \rho(v_z) = * \text{ and } \rho''(v_z) = 1\}$. Then both $B_0(u)$ and $B_1(u)$ are disjoint from $\mathcal{A}(s-1) \cup \mathcal{A}'(s-1)$, and the following hold by Proposition 3.8:

$$\begin{aligned} &(\exists^{|u|!}y_1)(\forall^{|u|!}y_2) \dots (Q^{|u|!}y_{k+1})[0uy_1y_2 \dots y_{k+1} \in \mathcal{A}(s-1) \cup B_1(u)], \text{ and} \\ &(\forall^{|u|!}y_1)(\exists^{|u|!}y_2) \dots (\overline{Q}^{|u|!}y_{k+1})[0uy_1y_2 \dots y_{k+1} \notin \mathcal{A}(s-1) \cup B_0(u)], \end{aligned}$$

where $Q = \exists$ and $\overline{Q} = \forall$ if k is even, and $Q = \forall$ and $\overline{Q} = \exists$ if k is odd. We can now choose $B(u)$ as either $B_1(u)$ or $B_0(u)$ depending on whether $u \notin S_{k+1}(\mathcal{A}(s-1))$ or

$u \in S_{k+1}(\mathcal{A}(s-1))$. Thus Claim 4 is proved. ■ (Claim 4)

Proof of Claim 3. Notice that $C(n, k)$ is in $\mathcal{F}_{k+1}^{2^n}$, whereas for every $u \in \Sigma^*$ such that $s \leq (k+2) \cdot |u| + 1 \leq p_i(n)$, the circuit C_u is in $\mathcal{F}_{k+1}^{2^{|u|}}$. So first choose a deterministic restriction ρ' on the variables of the C_u 's such that for all C_u 's, it holds that $C_u \upharpoonright_{\rho'} \in \mathcal{F}_{k+1}^{2^n}$. Such a restriction can be guaranteed to exist by using Proposition 3.7. Since $p_i(n) < \frac{1}{12} \cdot 2^{n/3}$ and the number of circuits C_u is $\leq 2^{p_i(n)} < 2^{2^{n/8}}$, for all sufficiently large n , we can obtain a restriction ρ satisfying the conditions of Lemma 3.19. The restriction $\rho' \rho$ thus satisfies the conditions of Claim 3. ■ (Claim 3)

This completes the proof of Theorem 3.18. ■ (Theorem 3.18)

Lemma 3.19 *Let $k \geq 1$, $m < 2^{h^{1/8}}$, and $h > h_0(k, m)$, for some constant $h_0(k, m)$ depending only on k and m . Let C_0, C_1, \dots, C_m be $m+1$ circuits in \mathcal{F}_{k+1}^h such that C_0 is of depth k , C_1, \dots, C_m are of depth $k+1$, the top gates of C_0, C_1, \dots, C_m are all ORs, and the variables of C_0, C_1, \dots, C_m are pairwise disjoint. Let C_π be any $\Pi_k(\frac{1}{12} \cdot h^{1/3})$ -circuit with the same variables as those of C_0, C_1, \dots, C_m . Then there exists a restriction ρ on the variables of the C_i s, where $0 \leq i \leq m$, such that*

1. ρ completely determines C_0 .
2. ρ satisfies the GU-condition for C_0, C_1, \dots, C_m .
3. for any restriction ρ' extending ρ such that ρ' completely determines C_π and ρ' satisfies the GU-condition for C_1, C_2, \dots, C_m , it holds that $C_0 \upharpoonright_{\rho'} \neq C_\pi \upharpoonright_{\rho'}$.
4. ρ does not completely determine C_1, C_2, \dots, C_m .

Proof of Lemma 3.19. We prove the lemma by induction on k . For the base case, i.e., when $k = 1$, C_0 is an OR gate with $\geq \sqrt{h}$ variables, and C_1, C_2, \dots, C_m are ORs of ANDs with top fanins h and bottom fanins $\geq \sqrt{h}$. The circuit C_π is a $\Pi_1(\frac{1}{12} \cdot h^{1/3})$ -circuit. We consider the following cases.

Case-I: There is a restriction ρ such that

- (a) $\rho(v_z) = 0$ for all variables v_z of C_0 ,
- (b) ρ satisfies the GU-condition for each C_i , where $1 \leq i \leq m$, and
- (c) $C_\pi \upharpoonright_{\rho} = 0$.

Then there is an OR gate G in C_π such that $G \upharpoonright_{\rho} = 0$. Since $\frac{1}{12} \cdot h^{1/3} < \sqrt{h}$, there is a variable v_{z_0} in C_0 but not in G . Define a restriction $\hat{\rho}$ as follows:

- $\hat{\rho}(v_z) = 0$ for all variables $v_z \neq v_{z_0}$ of C_0 ,
- $\hat{\rho}(v_{z_0}) = 1$,
- $\hat{\rho}(v_z) = \rho(v_z)$ if v_z is a variable of G , and

- $\hat{\rho}(v_z) = \star$ if v_z is not a variable of C_0 and of G .

It easily follows that $\hat{\rho}$ completely determines C_0 and C_π , and $C_0 \upharpoonright_{\hat{\rho}} \neq C_\pi \upharpoonright_{\hat{\rho}}$. Since $\hat{\rho}$ assigns exactly one variable of C_0 to 1 and assigns 0 to the remaining variables of C_0 , $\hat{\rho}$ satisfies the GU-condition for C_0 . Also, since ρ satisfies the GU-condition for each C_i , where $1 \leq i \leq m$, and since the variables of C_0 are disjoint from those of C_1, C_2, \dots, C_m , it follows that $\hat{\rho}$ satisfies the GU-condition for each C_i , where $1 \leq i \leq m$. Moreover, for each C_i , where $1 \leq i \leq m$, since the bottom and top fanins of C_i are $\geq \sqrt{h} > \frac{1}{12} \cdot h^{1/3}$, every AND gate of C_i has at least one variable not occurring in G and there is an AND gate G_i of C_i such that no variables of G_i occur in G . $\hat{\rho}$ assigns all these variables, i.e., variables of C_i not occurring in G , to \star . It is now clear that $\hat{\rho}$ does not completely determine C_i , for all $1 \leq i \leq m$. Thus $\hat{\rho}$ satisfies the conditions of Lemma 3.19.

Case-II: For all restrictions ρ such that

- $\rho(v_z) = 0$ for all variables v_z of C_0 ,
- ρ satisfies the GU-condition for each C_i , where $1 \leq i \leq m$, and
- ρ completely determines C_π ,

it holds that $C_\pi \upharpoonright_{\rho} = 1$.

Define a restriction $\hat{\rho}$ as follows:

- $\hat{\rho}(v_z) = 0$ for all variables v_z of C_0 , and
- $\hat{\rho}(v_z) = \star$ if v_z is not a variable of C_0 .

It easily follows that $C_0 \upharpoonright_{\hat{\rho}} = 0$, $\hat{\rho}$ does not completely determine C_1, C_2, \dots, C_m , and $\hat{\rho}$ satisfies the GU-condition for C_0, C_1, \dots, C_m . Also by our assumption in this case, for all restrictions ρ' extending $\hat{\rho}$ such that (i) ρ' satisfies the GU-condition for C_1, C_2, \dots, C_m , and (ii) ρ' completely determines C_π , it holds that $C_\pi \upharpoonright_{\rho'} = 1 \neq 0 = C_0 \upharpoonright_{\rho'}$. Thus $\hat{\rho}$ satisfies the conditions of Lemma 3.19.

Induction Hypothesis: Assume that the lemma is true for $k - 1$, for some $k \geq 2$.

Induction Step: Let C_0, C_1, \dots, C_m be arbitrary circuits in \mathcal{F}_{k+1}^h such that C_0 has depth k , C_1, C_2, \dots, C_m have depth $k + 1$, the top gates of C_0, C_1, \dots, C_m are all ORs, and the variables of C_0, C_1, \dots, C_m are pairwise disjoint. Let C_π be an arbitrary $\Pi_k(\frac{1}{12} \cdot h^{1/3})$ -circuit with the same variables as those of C_0, C_1, \dots, C_m .

We prove the induction step for even k ; the proof for odd k is symmetric. Since k is even, the bottom gates of C_0 are ANDs, and the bottom gates of C_1, C_2, \dots, C_m are ORs. Because of a technical reason⁴ in applying the switching lemma (see Lemma 3.3), we need to make these bottom gates all of the same type. Therefore, we transform circuit C_0 into a

⁴The technical reason for making the bottom gates of the involved circuits all of the same type is explained as follows. As observed in the beginning of Section 3.2, a restriction $\rho g'(\rho)$ satisfies the U-condition for a circuit C if $\rho \in \hat{R}_{q, \mathcal{B}}^+$ when the bottom gates are ANDs, or if $\rho \in \hat{R}_{q, \mathcal{B}}^-$ when the bottom gates are ORs. (Here q is a real number between 0 and 1, and $\mathcal{B} = \{B_i\}_{i=1}^r$ is such that B_i is the set of variables of the i 'th bottom

circuit C'_0 as follows: First obtain the dual of C_0 , and then replace each variable \bar{x}_j of the dual by a new variable y_j of C'_0 . We change the variables of C_π accordingly. That is, we replace every occurrence of x_j in C_π by \bar{y}_j and replace every occurrence of \bar{x}_j in C_π by y_j , for each variable x_j of C_0 . Thus the variables of C'_0 are disjoint from those of C_1, C_2, \dots, C_m , and the variables of C_π are the same as those of C'_0, C_1, \dots, C_m .

Lemma 3.4 and Lemma 3.9 imply that there is a restriction $\rho g'(\rho)$ with the following properties: (a) $\rho g'(\rho)$ satisfies the GU-condition for C'_0 and for every C_i , where $1 \leq i \leq m$, (b) $C_\pi \upharpoonright_{\rho g'(\rho)}$ is equivalent to a $\Pi_{k-1}(\frac{1}{12} \cdot h^{1/3})$ -circuit D_π , (c) the max-subcircuit D'_0 of $C'_0 \upharpoonright_{\rho g'(\rho)}$ is in \mathcal{F}_k^h , and (d) for every $1 \leq i \leq m$, the max-subcircuit D_i of $C_i \upharpoonright_{\rho g'(\rho)}$ is in \mathcal{F}_k^h . Also note that (a) D'_0 has depth $k-1$, (b) D_1, D_2, \dots, D_m have depth k , (c) D'_0 contains a subset of the variables of C'_0 , and (d) for every $1 \leq i \leq m$, D_i contains a subset of the variables of C_i . Next we transform D'_0 into a circuit $D_0 \in \mathcal{F}_k^h$ of the same depth, where the variables of D_0 form a subset of the variables of C_0 , as follows: First obtain the dual of D'_0 , and then replace each variable \bar{y}_j of the dual by the variable x_j of C_0 . The variables of D_π are changed accordingly. It now follows by the induction hypothesis that there is a restriction ϖ on D_π such that

1. ϖ completely determines D_0 ,
2. ϖ satisfies the GU-condition for D_0, D_1, \dots, D_m ,
3. for any restriction ϖ' extending ϖ such that ϖ' completely determines D_π and ϖ' satisfies the GU-condition for D_1, D_2, \dots, D_m , it holds that $D_0 \upharpoonright_{\varpi'} \neq D_\pi \upharpoonright_{\varpi'}$.
4. ϖ does not completely determine D_1, D_2, \dots, D_m .

Define a restriction ρ' as follows: ρ' is the same as $\rho g'(\rho)$ on the variables of C_1, C_2, \dots, C_m , but for every variable x_j of C_0 ,

$$\rho'(x_j) = \begin{cases} 1 - \rho g'(\rho)(y_j) & \text{if } \rho g'(\rho)(y_j) \in \{0, 1\}, \text{ and} \\ \star & \text{if } \rho g'(\rho)(y_j) = \star, \end{cases}$$

where y_j is the variable of C'_0 corresponding to the variable x_j of C_0 . Note that ρ' satisfies the GU-condition for each C_i , where $0 \leq i \leq m$. Also, note that each D_i is the max-subcircuit of $C_i \upharpoonright_{\rho'}$. Therefore by Proposition 3.8, $\rho' \varpi$ satisfies the GU-condition for each C_i . It is easy to verify that $\rho' \varpi$ also satisfies the remaining conditions of Lemma 3.19. This completes the proof of Lemma 3.19. ■ (Lemma 3.19)

The following corollary follows easily from Theorem 3.18, Theorem 2.3 and Fact 2.4.

Corollary 3.20 *For all $k \geq 2$, there is a relativized world where*

1. *AUPH collapses so that it has exactly k levels.*

gate of the circuit C .) A random restriction ρ has relevance with the switching lemma (Lemma 3.3) when ρ is either from the probability space $\hat{R}_{q,\mathcal{B}}^+$ or from the probability space $\hat{R}_{q,\mathcal{B}}^-$. Thus in order for a random restriction ρ to satisfy the U-condition for a collection of circuits with pairwise disjoint sets of variables and to have relevance with the switching lemma, we require that either all the bottom gates are ANDs (so that ρ can be chosen from $\hat{R}_{q,\mathcal{B}}^+$) or all the bottom gates are ORs (so that ρ can be chosen from $\hat{R}_{q,\mathcal{B}}^-$).

2. UPH collapses so that it has exactly k levels.
3. \mathcal{UPH} collapses so that it has exactly k levels.
4. PH collapses so that it has exactly k levels.
5. each level $\text{AU}\Sigma_\ell^p$ of AUPH is not contained in the corresponding level Π_ℓ^p of PH, for $1 \leq \ell \leq k - 1$.
6. $\text{PH} = \text{AUPH} = \text{UPH} = \mathcal{UPH} = \text{AU}\Sigma_k^p$.

We strengthen Theorem 3.18 by showing in Theorem 3.21 that for each $k \geq 2$, there is a relativized world where the first k levels of the unambiguity based hierarchies separate and their k 'th levels collapse not just to PH, but to PSPACE.

Theorem 3.21 $(\forall k \geq 1)(\exists \mathcal{A})[\text{AU}\Sigma_k^{p,\mathcal{A}} \not\subseteq \Pi_k^{p,\mathcal{A}}, \text{ but } \text{PSPACE}^{\mathcal{A}} = \text{AU}\Sigma_{k+1}^{p,\mathcal{A}}]$.

Proof The proof is essentially the same as that of Theorem 3.18. Ko [Ko89] proved that for each oracle A , the set $Q(A) =_{df} \{\langle i, z, 1^j \rangle \mid \text{the } i\text{'th deterministic oracle Turing machine } M_i \text{ with oracle } A \text{ accepts } z \text{ using at most } j \text{ cells}\}$ is complete for PSPACE^A and has the following desired property: The membership of a string x in $Q(A)$ depends only on the set $\{y \in A \mid |y| < |x|\}$. It is easy to see that using the set $Q(A)$ in place of the set $S_{k+1}(A)$ in the proof of Theorem 3.18 suffices to prove the theorem. \blacksquare (Theorem 3.21)

4 Complexity of Unambiguous Alternating Solution

Wagner studied the class ∇P , denoted by UAS in this paper, of all sets that are accepted by polynomial-time alternating Turing machines with partially defined AND and OR functions. UAS is a natural class with complete sets and is related to UAP in the same way as US [BG82] is related to UP. We define a variant of UAS, denoted by $\text{UAS}(k)$, where the number of alternations allowed is bounded by some constant $k \geq 1$, instead of the unbounded number of alternations in the definition of UAS. (Thus $\text{UAS}(1)$ is the same as the unique solution class US.)

Definition 4.1 ([Wag92]) *The class UAS, denoted by ∇P in [Wag92], is the class of all sets $L \subseteq \Sigma^*$ for which there exist polynomials $p(\cdot)$ and $q(\cdot)$, and a polynomial-time computable predicate R such that, for all $x \in \Sigma^*$,*

$$x \in L \iff (\exists^{p!} y_1)(\forall^{p!} y_2) \dots (Q^{p!} y_q) R(x, y_1, y_2, \dots, y_q),$$

where $Q = \exists$ if $q(|x|)$ is odd and $Q = \forall$ if $q(|x|)$ is even.

The class $\text{UAS}(k)$, for every $k \geq 1$, consists of all sets for which strings in the set are accepted unambiguously by some polynomial-time alternating Turing machine N with at most k alternations, while strings not in the set either are rejected by N or are accepted with ambiguity by N . A formal definition is as follows.

Definition 4.2 *The class $\text{UAS}(k)$, for $k \geq 1$, is the class of all sets $L \subseteq \Sigma^*$ for which there exist a polynomial $p(\cdot)$ and a polynomial-time computable predicate R such that, for all $x \in \Sigma^*$,*

$$x \in L \iff (\exists^{p!}y_1)(\forall^{p!}y_2) \dots (Q^{p!}y_k)R(x, y_1, y_2, \dots, y_k),$$

where $Q = \exists$ if k is odd and $Q = \forall$ if k is even.

The following results either are well-established or follow easily from the definitions of concerned complexity classes.

Theorem 4.3 1. $\text{US} \subseteq \text{UAS} \subseteq \text{C}=\text{P}$ and $\text{UAS} \subseteq \forall\oplus\text{P}$ [Wag92].

2. For every $k \geq 1$, $\text{UP} \subseteq \text{US} \subseteq \text{UAS}(k) \subseteq \text{UAS}(k+1) \subseteq \text{UAS}$.

3. For every $k \geq 1$, $\text{AU}\Sigma_k^p \subseteq \text{UAS}(k) \subseteq \text{P}^{\Sigma_k^p}$.

We can define a variant of the class $\text{UAS}(k)$, denoted by $\text{UAS}_\forall(k)$, to be the class of all sets L accepted by some (not necessarily on every input unambiguous) polynomial-time alternating Turing machine N in which the number of alternations is bounded by some constant $k \geq 1$, the root is a universal node, and $x \in L$ if and only if x is accepted unambiguously by N . Note that because a $\text{UAS}(k)$ machine is not promised to be unambiguous when the input does not belong to the set accepted by the machine, $\text{coUAS}(k)$ is possibly not the same as $\text{UAS}_\forall(k)$. For instance, it is easy to show that $\text{UP}_{\leq k}$ (and in fact NP) is contained in coUS ($= \text{coUAS}(1)$). On the other hand, we show in Theorem 4.5 a relativized world where $\text{UP}_{\leq k}$ is not even contained in $\text{UAS}_\forall(k)$. Since $\text{UAS}(k) \subseteq \text{UAS}_\forall(k+1)$ in every relativized world, we obtain as a corollary (see Corollary 4.6) an oracle \mathcal{A} with $\text{UP}_{\leq k+1}^{\mathcal{A}} \not\subseteq \text{UAS}(k)^{\mathcal{A}}$.

Theorem 4.5 implies that relative to an oracle \mathcal{A} , for all $k \geq 1$, $\text{UP}_{\leq k+1}^{\mathcal{A}}$ is not contained in $\text{UAS}(k)^{\mathcal{A}}$. Thus relative to the same oracle, bounded ambiguity classes $\text{UP}_{\leq k}$ and bounded-level unambiguous alternating solution classes $\text{UAS}(k)$ form infinite hierarchies. Theorem 4.5 also implies that there is a relativized world where for all $k \geq 1$, $\text{UP}_{\leq k+1}$ is not contained in $\text{AU}\Sigma_k^p$. In contrast, Lange and Rossmanith [LR94] proved that $\text{FewP} \subseteq \mathcal{U}\Sigma_2^p$ in every relativized world. It follows that relative to the oracle of Theorem 4.5, for all $k \geq 1$, $\mathcal{U}\Sigma_2^{p,\mathcal{A}} \not\subseteq \text{AU}\Sigma_k^{p,\mathcal{A}}$.

In the proofs of this section, we utilize the notions of Σ_k - and Π_k -machines, which we define as follows. The Σ_k - and Π_k -machines are oracle ATMs having at most k levels for any oracle. A Σ_k -machine has an existential root node if the number of levels in the machine is at least one. Similarly, a Π_k -machine has a universal root node if it has at least one level. If no input is specified for an ATM N with oracle A , then we assume that N^A starts with some arbitrary initial configuration. Let ν be any node in $N^{(\cdot)}$. Depending on the oracle B , ν may or may not appear in N^B ; if ν appears in N^B , then ν may either accept in N^B or reject in N^B .

The proof of Theorem 4.5 uses Lemma 4.4. Informally, Lemma 4.4 shows limitations of bounded-level oracle ATMs that preserve unambiguity with small extensions of oracles.

Lemma 4.4 *Let $\mathcal{O}, U \subseteq \Sigma^*$ with $\mathcal{O} \cap U = \emptyset$, and $k, m \in \mathbb{N}$. Let N be an arbitrary Π_k -machine (Σ_k -machine) with some fixed initial configuration, satisfying the following properties:*

1. *On each path, N makes no more than m queries.*
2. *For every $A \subseteq U$ with $\|A\| \leq k$, $N^{\mathcal{O} \cup A}$ retains unambiguity.*
3. *$N^{\mathcal{O}}$ rejects (respectively, accepts).*

Let

$$C = \{\alpha \in U \mid N^{\mathcal{O} \cup \{\alpha\}} \text{ accepts (respectively, rejects)}\}.$$

Then $\|C\| \leq 8^k \cdot m$.

Proof We prove this lemma by induction over k . Let N be a Π_0 -machine satisfying the conditions of the lemma. Machine N is a deterministic Turing machine that queries no more than m strings, and $N^{\mathcal{O}}$ rejects. Hence, $N^{\mathcal{O} \cup \{\alpha\}}$ accepts for no more than m strings $\alpha \in U$. Therefore, $\|C\| \leq m$. Thus, the lemma holds for $k = 0$. Next, let N be a Π_1 -machine satisfying the conditions of the lemma. We may assume that N has exactly one level, which has a universal node at the root. Because $N^{\mathcal{O}}$ rejects with unambiguity, there is a unique leaf node t in $N^{(\cdot)}$ that rejects in $N^{\mathcal{O}}$. On the path to t , N queries no more than m strings. Hence, node t rejects also in $N^{\mathcal{O} \cup \{\alpha\}}$ for all but m strings $\alpha \in U$. Therefore, $\|C\| \leq m$, and so the lemma holds for $k = 1$. The cases of Σ_0 - and Σ_1 -machines are treated analogously.

We now assume that Lemma 4.4 is correct for all $k = 0, 1, 2, \dots, \ell - 1$, where $\ell \geq 2$. Let N be a Π_ℓ -machine satisfying the conditions of the lemma. To get a contradiction, assume that $\|C\| > 8^\ell \cdot m$. We know that $N^{\mathcal{O}}$ rejects with unambiguity. Hence, there is a unique existential salient node t on the second level of $N^{(\cdot)}$ that rejects in $N^{\mathcal{O}}$. Let $C' := C - Q_N(t)$. (Recall from Section 2.2 that $Q_N(t)$ denotes the set of queries along the path from the root to the node t in $N^{(\cdot)}$.) We have $\|C'\| > (8^\ell - 1)m$. For every $\alpha \in C'$, t accepts in $N^{\mathcal{O} \cup \{\alpha\}}$ by the definition of the set C . For every $\alpha \in C'$, denote by $s(\alpha)$ the unique node on the third level of $N^{(\cdot)}$ reachable from t in $N^{\mathcal{O} \cup \{\alpha\}}$ such that $s(\alpha)$ accepts in $N^{\mathcal{O} \cup \{\alpha\}}$.

Define an equivalence relation ρ on C' as follows: For all $\alpha_1, \alpha_2 \in C'$,

$$\alpha_1 \rho \alpha_2 \iff s(\alpha_1) = s(\alpha_2).$$

Let $[\alpha] = \{\alpha' \in C' \mid \alpha' \rho \alpha\}$. We consider two cases:

Case 1: There is an equivalence class of ρ of size $\geq \|C'\|/2$. Let $[\alpha]$ be such an equivalence class. Clearly, $\|[\alpha]\| \geq (8^\ell - 1) \cdot m/2$. The node $s(\alpha)$ appears in $N^{\mathcal{O} \cup \{\beta\}}$ for every $\beta \in [\alpha]$. Hence, node $s(\alpha)$ also appears in $N^{\mathcal{O}}$ (because $\|[\alpha]\| \geq (8^\ell - 1) \cdot m/2 > m$ and no more than m strings are queried on each path). However, $s(\alpha)$ rejects in $N^{\mathcal{O}}$ because t rejects in $N^{\mathcal{O}}$.

Let \widehat{N} be the $\Pi_{\ell-2}$ -machine that starts with node $s(\alpha)$. We know that $\widehat{N}^{\mathcal{O}}$ rejects. On the other hand, $\widehat{N}^{\mathcal{O} \cup \{\beta\}}$ accepts for every $\beta \in [\alpha]$. Apply Lemma 4.4 to \widehat{N} and get $\|[\alpha]\| \leq 8^{\ell-2} \cdot m$. A contradiction.

Case 2: The size of every equivalence class of ρ is $\leq \|C'\|/2$. It is easy to see that there exists $J \subseteq C'$ such that

$$\|C'\|/4 \leq \left\| \bigcup_{\alpha \in J} [\alpha] \right\| \leq \|C'\|/2.$$

Let

$$C_1 = \bigcup_{\alpha \in J} [\alpha] \quad \text{and} \quad C_2 = C' - C_1.$$

For each $\alpha_1 \in C_1$, let N_1 be the $\Pi_{\ell-2}$ -machine that starts with node $s(\alpha_1)$. Note that $N_1^{\mathcal{O} \cup \{\alpha_1\}}$ accepts. Let

$$\text{conflicting}(\alpha_1) = \{\beta_2 \in C_2 \mid N_1^{\mathcal{O} \cup \{\alpha_1, \beta_2\}} \text{ rejects or } \beta_2 \in Q_N(s(\alpha_1))\}.$$

Clearly, N_1 is a fortiori also a $\Sigma_{\ell-1}$ -machine. With N_1 for N , $\mathcal{O} \cup \{\alpha_1\}$ for \mathcal{O} , and C_2 for U , the conditions of Lemma 4.4 are satisfied. Hence, $|\text{conflicting}(\alpha_1)| \leq 8^{\ell-1} \cdot m + \|Q_N(s(\alpha_1))\| \leq (8^{\ell-1} + 1) \cdot m$. Analogously, for each $\alpha_2 \in C_2$, let N_2 be the $\Pi_{\ell-2}$ -machine that starts with node $s(\alpha_2)$. Let

$$\text{conflicting}(\alpha_2) = \{\beta_1 \in C_1 \mid N_2^{\mathcal{O} \cup \{\alpha_2, \beta_1\}} \text{ rejects or } \beta_1 \in Q_N(s(\alpha_2))\}.$$

Here, we also obtain $|\text{conflicting}(\alpha_2)| \leq (8^{\ell-1} + 1) \cdot m$.

Claim 5 *We can choose $\alpha_1 \in C_1$ and $\alpha_2 \in C_2$ such that $\alpha_1 \notin \text{conflicting}(\alpha_2)$ and $\alpha_2 \notin \text{conflicting}(\alpha_1)$.*

Let us assume that the claim is true. Take two such strings α_1 and α_2 . Then both $N_1^{\mathcal{O} \cup \{\alpha_1, \alpha_2\}}$ (starting with $s(\alpha_1)$) and $N_2^{\mathcal{O} \cup \{\alpha_2, \alpha_1\}}$ (starting with $s(\alpha_2)$) are accepting. Node $s(\alpha_1)$ appears in $N^{\mathcal{O} \cup \{\alpha_1\}}$. String α_2 is not queried on the path from the root to $s(\alpha_1)$ in $N^{\mathcal{O} \cup \{\alpha_1\}}$. Hence $s(\alpha_1)$ appears also in $N^{\mathcal{O} \cup \{\alpha_1, \alpha_2\}}$. Analogously, node $s(\alpha_2)$ appears in $N^{\mathcal{O} \cup \{\alpha_1, \alpha_2\}}$. Hence, $s(\alpha_1)$ and $s(\alpha_2)$ accept in $N^{\mathcal{O} \cup \{\alpha_1, \alpha_2\}}$. Since nodes $s(\alpha_1)$ and $s(\alpha_2)$ are different nodes on the third level of $N^{(\cdot)}$ reachable from t in $N^{\mathcal{O} \cup \{\alpha_1, \alpha_2\}}$, we conclude that $N^{\mathcal{O} \cup \{\alpha_1, \alpha_2\}}$ loses unambiguity. A contradiction. This completes the proof of Lemma 4.4. ■ (Lemma 4.4)

Proof of Claim 5 We have

$$\|C_1\| \geq \|C'\|/4 > (8^\ell - 1) \cdot m/4$$

and

$$\|C_2\| \geq \|C'\|/2 \geq (8^\ell - 1) \cdot m/2.$$

On the other hand for every $\alpha_1 \in C_1$,

$$|\text{conflicting}(\alpha_1)| \leq (8^{\ell-1} + 1) \cdot m,$$

and for every $\alpha_2 \in C_2$,

$$\|\text{conflicting}(\alpha_2)\| \leq (8^{\ell-1} + 1) \cdot m.$$

A simple counting argument shows that there is pair $(\alpha_1, \alpha_2) \in C_1 \times C_2$ such that $\alpha_2 \notin \text{conflicting}(\alpha_1)$ and $\alpha_1 \notin \text{conflicting}(\alpha_2)$. \blacksquare (Claim 5)

We now prove Theorem 4.5.

Theorem 4.5 $(\exists \mathcal{A})(\forall k \geq 1)[\text{UP}_{\leq k}^{\mathcal{A}} \not\subseteq \text{UAS}_{\forall(k)}^{\mathcal{A}}]$.

Proof For every $k \in \mathbb{N}^+$, we define our test language $L_k(B)$ as follows:

$$L_k(B) = \{0^k 10^n \mid B \cap 0^k 1\Sigma^n \neq \emptyset\}.$$

We will construct an oracle \mathcal{A} such that $\mathcal{A} \subseteq 0\{0\}^*1\{0,1\}^*$ and for every $k, n \in \mathbb{N}^+$, $\|\mathcal{A} \cap 0^k 1\Sigma^n\| \leq k$. This will guarantee that, for every $k \in \mathbb{N}^+$, $L_k(\mathcal{A})$ is in $\text{UP}_{\leq k}^{\mathcal{A}}$. For every $k \in \mathbb{N}^+$, let $N_{k,1}, N_{k,2}, N_{k,3}, \dots$ be an enumeration of polynomial-time bounded Π_k -machines such that, for every $i \in \mathbb{N}^+$, the computation time of $N_{k,i}$ is $p_i(n) =_{df} n^i + i$. Let $\mathcal{A} := \emptyset$. In stage $\langle k, i \rangle$, we diagonalize against $N_{k,i}$ and change \mathcal{A} at certain length.

Stage $\langle k, i \rangle$: Choose n large enough such that (a) no string of length n or more is queried by machines considered in previous stages and (b) $2^n > 3 \cdot 8^k \cdot p_i(n)$. We consider two cases.

Case 1: $N_{k,i}^{\mathcal{A} \cup S}(0^n)$ retains unambiguity for every $S \subseteq 0^k 1\Sigma^n$ with $\|S\| \leq k$.

Case 1.a: $N_{k,i}^{\mathcal{A}}(0^n)$ accepts. Move to the next stage.

Case 1.b: $N_{k,i}^{\mathcal{A}}(0^n)$ rejects. Apply Lemma 4.4 with $N := N_{k,i}(0^n)$, $\mathcal{O} := \mathcal{A}$, $U := 0^k 1\Sigma^n$, and $m := p_i(n)$. We get $\|C\| \leq 8^k \cdot p_i(n) < 2^n$. Hence there is an $\alpha \in 0^k 1\Sigma^n$ such that $N_{k,i}^{\mathcal{A} \cup \{\alpha\}}(0^n)$ rejects. Set $\mathcal{A} := \mathcal{A} \cup \{\alpha\}$ and move to the next stage.

Case 2: $N_{k,i}^{\mathcal{A} \cup S}(0^n)$ loses unambiguity for some $S \subseteq 0^k 1\Sigma^n$ with $\|S\| \leq k$.

Case 2.a: $N_{k,i}^{\mathcal{A} \cup S}(0^n)$ loses unambiguity for some $S \subseteq 0^k 1\Sigma^n$ with $1 \leq \|S\| \leq k$. Set $\mathcal{A} := \mathcal{A} \cup S$ and move to the next stage.

Case 2.b: $N_{k,i}^{\mathcal{A}}(0^n)$ loses unambiguity, but $N_{k,i}^{\mathcal{A} \cup S}(0^n)$ retains unambiguity for every $S \subseteq 0^k 1\Sigma^n$ with $1 \leq \|S\| \leq k$. Then there appears a node t in $N_{k,i}^{\mathcal{A}}(0^n)$ such that one of the following is true:

- (1) t is an existential node that leads to two nodes t_1 and t_2 at the next level that are accepting in $N_{k,i}^{\mathcal{A}}(0^n)$ with unambiguity.
- (2) t is a universal node that leads to two nodes t_1 and t_2 at the next level that are rejecting in $N_{k,i}^{\mathcal{A}}(0^n)$ with unambiguity.

Without loss of generality, assume that (1) is true. Let N_1 and N_2 be the $\Pi_{k'}$ -machines that start with node t_1 and t_2 , respectively. Note that $k' < k$, and $N_1^{\mathcal{A} \cup S}$ and $N_2^{\mathcal{A} \cup S}$ retain unambiguity for every $S \subseteq 0^k 1 \Sigma^n - (Q_{N_{k,i}}(t_1) \cup Q_{N_{k,i}}(t_2))$ with $\|S\| \leq k$. A fortiori, N_1 and N_2 are also $\Sigma_{k''}$ -machines for some $k'' \leq k$. Applying Lemma 4.4, we obtain

$$\|\{\alpha \in S \mid N_j^{\mathcal{A} \cup \{\alpha\}} \text{ rejects}\}\| \leq 8^k \cdot p_i(n)$$

for $j \in \{1, 2\}$. Hence there are no more than $3 \cdot 8^k \cdot p_i(n) < 2^n$ strings $\alpha \in 0^k 1 \Sigma^n$ such that anyone of (i), (ii), and (iii) holds, where (i) t_1 or t_2 do not appear in $N_{k,i}^{\mathcal{A} \cup \{\alpha\}}(0^n)$, (ii) $N_1^{\mathcal{A} \cup \{\alpha\}}$ rejects, and (iii) $N_2^{\mathcal{A} \cup \{\alpha\}}$ rejects. Therefore, there exists an $\alpha \in 0^k 1 \Sigma^n$ such that both t_1 and t_2 appear in $N_{k,i}^{\mathcal{A} \cup \{\alpha\}}(0^n)$, and, moreover, both $N_1^{\mathcal{A} \cup \{\alpha\}}$ and $N_2^{\mathcal{A} \cup \{\alpha\}}$ accept. Hence $N_{k,i}^{\mathcal{A} \cup \{\alpha\}}(0^n)$ loses unambiguity at node t . Set $\mathcal{A} := \mathcal{A} \cup \{\alpha\}$ and move to the next stage.

This completes the proof of Theorem 4.5. ■ (Theorem 4.5)

Corollary 4.6 $(\exists \mathcal{A})(\forall k \geq 1)[\text{UP}_{\leq k+1}^{\mathcal{A}} \not\subseteq \text{UAS}(k)^{\mathcal{A}}]$.

Corollary 4.7 *There is an oracle \mathcal{A} such that, for every $k \geq 1$, $\text{UP}_{\leq k}^{\mathcal{A}} \subset \text{UP}_{\leq k+1}^{\mathcal{A}}$, $\text{AU}\Sigma_k^{p,\mathcal{A}} \subset \text{AU}\Sigma_{k+1}^{p,\mathcal{A}}$, $\text{UAS}(k)^{\mathcal{A}} \subset \text{UAS}(k+1)^{\mathcal{A}}$, and $\text{U}\Sigma_2^{p,\mathcal{A}} \not\subseteq \text{AU}\Sigma_k^{p,\mathcal{A}}$.*

5 Power of Robustly Unambiguous Alternating Machines

Hartmanis and Hemachandra [HH90] showed that robustly categorical nondeterministic polynomial-time Turing machines (i.e., NPTMs that for no oracle and no input have more than one accepting path) accept simple languages in the sense that, for every oracle A , the languages accepted by such machines are in $\text{P}^{\text{NP} \oplus A}$. Thus if $\text{P} = \text{NP}$, then robustly categorical NPTMs cannot separate P^A from NP^A , for any oracle A . Theorem 5.1 generalizes this result of Hartmanis and Hemachandra [HH90] and shows that, for every oracle A , robustly k -level unambiguous polynomial-time alternating Turing machines accept languages that are in $\text{P}^{\Sigma_k^p \oplus A}$. That is, we show that if a polynomial-time ATM N preserves k -level alternation unambiguously in every oracle world, then for each oracle A , it holds that $L(N^A) \in \text{P}^{\Sigma_k^p \oplus A}$. Thus similar to the case of robustly categorical NPTMs, if $\text{P} = \text{NP}$, then robustly k -level unambiguous polynomial-time alternating Turing machines cannot separate P^A from $\Sigma_k^{p,A}$, and consequently cannot separate P^A from NP^A .

Theorem 5.1 *For every $k \in \mathbb{N}^+$, the following holds:*

$$(\forall \mathcal{A})[N^{\mathcal{A}} \text{ is a } k\text{-level unambiguous polynomial-time ATM}] \implies (\forall \mathcal{A})[L(N^{\mathcal{A}}) \in \text{P}^{\Sigma_k^p \oplus \mathcal{A}}].$$

Proof The proof is by induction on k . The base case, $k = 1$, holds by [HH90, Theorem 2.1], i.e., $(\forall \mathcal{A})[N^{\mathcal{A}} \text{ is a categorical NPTM}] \implies (\forall \mathcal{A})[L(N^{\mathcal{A}}) \in \text{P}^{\text{NP} \oplus \mathcal{A}}]$.

Our induction hypothesis is the following: For every $j \leq k - 1$, it holds that

$$(\forall \mathcal{A})[N^{\mathcal{A}} \text{ is a } j\text{-level unambiguous polynomial-time ATM}] \implies (\forall \mathcal{A})[L(N^{\mathcal{A}}) \in \mathsf{P}^{\Sigma_j^p \oplus \mathcal{A}}].$$

Let \mathcal{A} be an oracle and let N be a robustly k -level unambiguous polynomial-time ATM. We define an oracle NPTM \widehat{N} with access to oracle $\Sigma_{k-1}^p \oplus \mathcal{A}$ as follows. On any input x , $\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}}$ guesses an existential computation path from the root (i.e., the level one node) to a universal node ϑ at level two in the computation tree of $N^{\mathcal{A}}(x)$. Upon reaching the node ϑ on this guessed path, $\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}}$ simulates the computation subtree of $N^{\mathcal{A}}(x)$ rooted at the node ϑ . Since the computation subtree of $N^{\mathcal{A}}(x)$ rooted at the node ϑ is robustly $(k-1)$ -level unambiguous, by induction hypothesis this simulation can be done in $\mathsf{P}^{\Sigma_{k-1}^p \oplus \mathcal{A}}$. Since this works for every \mathcal{A} , and since N is robustly k -level unambiguous polynomial-time ATM, the following are true:

(a) For every \mathcal{A} , $L(\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}}) = L(N^{\mathcal{A}})$.

(b) For every \mathcal{A} , $\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}}$ is categorical.

We now show that $L(\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}}) \in \mathsf{P}^{\Sigma_k^p \oplus \mathcal{A}}$. The proof of this part is similar to the proof by Hartmanis and Hemachandra [HH90, Theorem 2.1]. Here, we give a sketch of the proof for the sake of completeness. Let $p(\cdot)$ be the running-time of \widehat{N} with any oracle. We define a deterministic polynomial-time computable procedure $M^{\Sigma_k^p \oplus \mathcal{A}}$ accepting $L(\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}})$.

On input x , $M^{\Sigma_k^p \oplus \mathcal{A}}(x)$ does the following:

1. Initialize database $S := \emptyset$.
2. Repeat the following for $p(|x|)$ iterations:

Find an accepting path ρ in the computation tree of $\widehat{N}^{\Sigma_{k-1}^p \oplus \star}(x)$ consistent with S . (This step can be done in $\mathsf{P}^{\Sigma_k^p}$ since $\|S\|$ is of polynomial size.) If no such ρ exists, then halt and reject. Otherwise, i.e., if ρ exists, then query \mathcal{A} about the membership of strings queried along ρ and update S with this information. If the answers of the queries along ρ are consistent with \mathcal{A} , then halt and accept.

3. Accept if there is an accepting path in the computation tree of $\widehat{N}^{\Sigma_{k-1}^p \oplus \star}(x)$ consistent with S that queries only strings in S , and reject if no such path exists.

By the definition of M , $M^{\Sigma_k^p \oplus \mathcal{A}}$ is computable in polynomial time. We now show that $M^{\Sigma_k^p \oplus \mathcal{A}}$ accepts $L(\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}})$.

It is easy to see that it is sufficient to show that $x \in L(\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}})$ implies that $M^{\Sigma_k^p \oplus \mathcal{A}}(x)$ accepts. Suppose that $\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}}(x)$ accepts. Let T be the set of strings queried to \mathcal{A} along the unique accepting computation ρ_T of $\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}}(x)$. If $M^{\Sigma_k^p \oplus \mathcal{A}}(x)$ accepts in some iteration

of step 2, then we are done. So assume that $M^{\Sigma_k^p \oplus \mathcal{A}}(x)$ does not accept in any of the $p(|x|)$ iterations of step 2. This also implies that $M^{\Sigma_k^p \oplus \mathcal{A}}(x)$ does not reject in any iteration of step 2, since the accepting path ρ_T has not been considered so far. Let S_i be the set of strings queried to \mathcal{A} in the i 'th iteration of step 2 and let ρ_{S_i} be the path found in that iteration. Note that ρ_{S_i} and ρ_T are different. The crucial observation is:

There must be a query q_i in $S_i \cap T$ that is answered in a conflicting way in ρ_{S_i} and ρ_T .

This can be seen as follows. If there is no such string q_j , then there will be an oracle \mathcal{O} that is consistent with the way the strings queried along ρ_{S_i} and ρ_T are answered. Then relative to $\Sigma_{k-1}^p \oplus \mathcal{O}$, $\widehat{N}(x)$ will have at least two accepting paths, which will give a contradiction with our assumption that $(\forall \mathcal{A})[\widehat{N}^{\Sigma_{k-1}^p \oplus \mathcal{A}}$ is categorical].

This query q_i must be different from q_j , for any $1 \leq j < i$, because the database S in the i th iteration of step 2 is consistent with \mathcal{A} in the membership of any string queried in previous iterations. Thus in each iteration of step 2, the membership in \mathcal{A} of a new query from T is found. So, after $p(|x|)$ iterations of step 2, the membership of all the strings queried along ρ_T is known. It follows that $M^{\Sigma_k^p \oplus \mathcal{A}}(x)$ will accept on the execution of step 3. ■

Corollary 5.2 *For all $k \in \mathbb{N}^+$, if $P = NP$ and $(\forall \mathcal{A})[N^{\mathcal{A}}$ is a k -level unambiguous polynomial-time ATM], then $(\forall \mathcal{A})[L(N^{\mathcal{A}}) \in P^{\mathcal{A}}]$.*

Crescenzi and Silvestri [CS98] showed that languages accepted by robustly complementary and categorical oracle NPTMs are in $P^{(UP \cup \text{co}UP) \oplus \mathcal{A}}$. In fact, their proof actually shows that the languages of such machines are computable in $P^{(UP \cap \text{co}UP) \oplus \mathcal{A}}$. Theorem 5.3 is a generalization of this result of Crescenzi and Silvestri [CS98] for robustly bounded-level unambiguous polynomial-time alternating Turing machines.

Theorem 5.3 *For all $k_i, k_j \in \mathbb{N}^+$, the following holds: If for all oracles \mathcal{A} , $N_i^{\mathcal{A}}$ and $N_j^{\mathcal{A}}$ are, respectively, k_i -level and k_j -level unambiguous polynomial-time ATMs and $L(N_i^{\mathcal{A}}) = \overline{L(N_j^{\mathcal{A}})}$, then for all oracles \mathcal{A} , $L(N_i^{\mathcal{A}}) \in P^{(UP^{\Sigma_{k-1}^p} \cap \text{co}UP^{\Sigma_{k-1}^p}) \oplus \mathcal{A}}$, where $k = \max\{k_i, k_j\}$.*

Proof Let \mathcal{A} be an oracle and let N_i, N_j be ATMs as in the statement of the theorem. Define oracle NPTMs \widehat{N}_i and \widehat{N}_j corresponding to N_i and N_j , respectively, in the manner \widehat{N} is defined from ATM N in Theorem 5.1. Let $k =_{df} \max\{k_i, k_j\}$. Thus, the following hold for $\ell \in \{i, j\}$:

- (a) For every \mathcal{A} , $L(\widehat{N}_\ell^{\Sigma_{k-1}^p \oplus \mathcal{A}}) = L(N_\ell^{\mathcal{A}})$.
- (b) For every \mathcal{A} , $\widehat{N}_\ell^{\Sigma_{k-1}^p \oplus \mathcal{A}}$ is categorical.
- (c) For every \mathcal{A} , $L(\widehat{N}_i^{\Sigma_{k-1}^p \oplus \mathcal{A}}) = \overline{L(\widehat{N}_j^{\Sigma_{k-1}^p \oplus \mathcal{A}})}$.

It remains to show that $L(\widehat{N}_i^{\Sigma_{k-1}^p \oplus \mathcal{A}}) \in \mathsf{P}(\mathsf{UP}^{\Sigma_{k-1}^p} \cap \mathsf{coUP}^{\Sigma_{k-1}^p} \oplus \mathcal{A})$. The proof of this part is omitted as it is identical to the proof by Crescenzi and Silvestri [CS98, Theorem 8] (if N_0 and N_1 are two robustly complementary and categorical oracle NPTMs, then for all oracles \mathcal{A} , $L(N_0^{\mathcal{A}}) \in \mathsf{P}(\mathsf{UP} \cap \mathsf{coUP}) \oplus \mathcal{A}$) and Hartmanis and Hemachandra [HH90, Theorem 2.1]. ■

6 Open Questions

We now mention some open questions and directions for further research. Theorem 3.10 implies that there is a relativized world where the unambiguity based hierarchies are infinite. On the other hand, Theorem 3.18 implies that for each $k \geq 2$, there is a relativized world where these hierarchies have exactly k distinct levels and all their higher levels collapse to their k 'th levels. In spite of these results, a number of questions related to the relativized structure of unambiguity based hierarchies remain open. For instance, is there a relativized world where AUPH is finite, but UPH and \mathcal{UPH} are infinite? Is there a relativized world where the polynomial hierarchy is infinite, but AUPH and UPH collapse?

Hemaspaandra and Rothe [HR97] showed that if UP has sparse Turing-complete sets, then for every $k \geq 3$, $\mathsf{U}\Sigma_k^p \subseteq \mathcal{U}\Sigma_{k-1}^p$. Are there other complexity-theoretic assumptions that can help in concluding about the structure of unambiguity based hierarchies?

Fortnow [For99] showed that $\mathsf{PH} \subset \mathsf{SPP}$ relative to a random oracle. Theorem 3.14 shows that there is a relativized world where $\mathsf{UAP} \not\subseteq \mathsf{PH}$. Can we extend the oracle separation of UAP from PH to a random oracle separation?

Aida et al. [ACRW04] and Crâsmaru et al. [CGRS04] discussed whether UAP equals SPP. In fact, Crâsmaru et al. [CGRS04] pointed out their difficulty in building an oracle \mathcal{A} such that $\mathsf{UAP}^{\mathcal{A}} \neq \mathsf{SPP}^{\mathcal{A}}$. Can the ideas involved in oracle constructions in this paper be used to attack this problem?

Finally, is it the case that similar to robustly bounded-level unambiguous polynomial-time ATMs, robustly unbounded-level unambiguous polynomial-time ATMs require weak oracle access in every relativized world?

Acknowledgment We thank Lane Hemaspaandra and Jörg Rothe for their helpful advice, guidance, and support.

References

- [ACRW04] S. Aida, M. Crâsmaru, K. Regan, and O. Watanabe. Games with uniqueness properties. *Theory of Computing Systems*, 37(1):29–47, 2004.
- [AK02] V. Arvind and P. Kurur. Graph isomorphism is in SPP. In *Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science*, pages 743–750, Los Alamitos, November 2002. IEEE Computer Society Press.

- [Bei89] R. Beigel. On the relativized power of additional accepting paths. In *Proceedings of the 4th Structure in Complexity Theory Conference*, pages 216–224. IEEE Computer Society Press, June 1989.
- [BG82] A. Blass and Y. Gurevich. On the unique satisfiability problem. *Information and Control*, 55(1–3):80–88, 1982.
- [CGH⁺89] J. Cai, T. Gundermann, J. Hartmanis, L. Hemachandra, V. Sewelson, K. Wagner, and G. Wechsung. The boolean hierarchy II: Applications. *SIAM Journal on Computing*, 18(1):95–111, 1989.
- [CGRS04] M. Crâșmaru, C. Glaßer, K. Regan, and S. Sengupta. A protocol for serializing unique strategies. In *Proceedings of the 29th International Symposium on Mathematical Foundations of Computer Science*, pages 660–672. Springer-Verlag *Lecture Notes in Computer Science #3153*, August 2004.
- [CKS81] A. Chandra, D. Kozen, and L. Stockmeyer. Alternation. *Journal of ACM*, 26(1):114–133, 1981.
- [CS98] P. Crescenzi and R. Silvestri. Sperner’s lemma and robust machines. *Computational Complexity*, 7:163–173, 1998.
- [For99] L. Fortnow. Relativized worlds with an infinite hierarchy. *Information Processing Letters*, 69(6):309–313, 1999.
- [FSS84] M. Furst, J. Saxe, and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17:13–27, 1984.
- [GS88] J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.
- [Hås87] J. Håstad. *Computational Limitations of Small-Depth Circuits*. MIT Press, 1987.
- [HH90] J. Hartmanis and L. Hemachandra. Robust machines accept easy sets. *Theoretical Computer Science*, 74(2):217–225, 1990.
- [HR97] L. Hemaspaandra and J. Rothe. Unambiguous computation: Boolean hierarchies and sparse Turing-complete sets. *SIAM Journal on Computing*, 26(3):634–653, 1997.
- [Ko85] K. Ko. On some natural complete operators. *Theoretical Computer Science*, 37(1):1–30, 1985.
- [Ko89] K. Ko. Relativized polynomial-time hierarchies having exactly k levels. *SIAM Journal on Computing*, 18(2):392–408, 1989.
- [Ko91] K. Ko. Separating the low and high hierarchies by oracles. *Information and Computation*, 90(2):156–177, 1991.

- [LR94] K.-J. Lange and P. Rossmanith. Unambiguous polynomial hierarchies and exponential size. In *Proceedings of the 9th Structure in Complexity Theory Conference*, pages 106–115. IEEE Computer Society Press, June/July 1994.
- [NR98] R. Niedermeier and P. Rossmanith. Unambiguous computations and locally definable acceptance types. *Theoretical Computer Science*, 194(1–2):137–161, 1998.
- [OH93] M. Ogiwara and L. Hemachandra. A complexity theory for feasible closure properties. *Journal of Computer and System Sciences*, 46(3):295–325, 1993.
- [Pap94] C. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.
- [Sip83] M. Sipser. Borel sets and circuit complexity. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, pages 61–69. ACM Press, 1983.
- [SL94] M. Sheu and T. Long. The extended low hierarchy is an infinite hierarchy. *SIAM Journal on Computing*, 23(3):488–509, 1994.
- [SL96] M. Sheu and T. Long. UP and the low and high hierarchies: A relativized separation. *Mathematical Systems Theory*, 29(5):423–449, 1996.
- [ST05] H. Spakowski and R. Tripathi. On the power of unambiguity in alternating machines. In *Proceedings of the 15th International Symposium on Fundamentals of Computation Theory*, pages 125–136. Springer-Verlag *Lecture Notes in Computer Science #3623*, August 2005. Accepted subject to minor revision, *Theory of Computing Systems*.
- [Sto76] L. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1–22, 1976.
- [Wag92] K. Wagner. Alternating machines using partially defined “AND” and “OR”. Technical Report 39, Institut für Informatik, Universität Würzburg, January 1992.
- [Yao85] A. Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science*, pages 1–10, 1985.