

Complexity of the r -query Tautologies in the Presence of a Generic Oracle

Toshio Suzuki

Osaka Prefecture University
Sakai, Osaka 599-8531, Japan
suzuki@mi.cias.osakafu-u.ac.jp

To appear in:

Notre Dame Journal of Formal Logic 41 (2000)

Printed in 2002, by the delay of the publisher.

This is a preprint version of the above paper.

©2000 University of Notre Dame

Publisher's site: <http://projecteuclid.org/>

Complexity of the r -query Tautologies in the Presence of a Generic Oracle

Toshio Suzuki

Department of Mathematics and Information Sciences
Osaka Prefecture University, Sakai, Osaka 599-8531, Japan
suzuki@mi.cias.osakafu-u.ac.jp

May 18, 1997; revised August 20, 1998

Abstract

Extending techniques in Dowd (*Information and Computation* vol. 96 (1992)) and those in Poizat (*J. Symbolic Logic* vol. 51 (1986)), we study computational complexity of $rTAUT[A]$ in the case when A is a generic oracle, where r is a positive integer and $rTAUT[A]$ denotes the collection of all r -query tautologies with respect to an oracle A . We introduce the notion of ceiling-generic oracles, as a generalization of Dowd's notion of t -generic oracles to arbitrary finitely testable arithmetical predicates. We study how existence of ceiling-generic oracles affects behavior of a generic oracle, by which we show that $\{X : coNP[X] \text{ is not a subset of } NP[rTAUT[X]]\}$ is comeager in the Cantor space. Moreover, using ceiling-generic oracles, we present an alternative proof of the fact (Dowd) that the class of all t -generic oracles has Lebesgue measure zero.

Keywords: Computational complexity, Generic oracle, Random oracle, t -generic oracle.

Mathematics Subject Classification: Primary 68Q15; Secondary 03D15.

1 Introduction

Arithmetical forcing was introduced by Feferman [12] soon after Cohen's independence proofs in set theory [8, 9]. Since Hinman's work [13], arithmetical forcing has been studied in recursion theory. For example, see Jockusch [14] or Odifreddi [17]. Later, arithmetical forcing and its variations were used as tools to study $P = ?NP$ question by some people. Typical examples are Dowd [10, 11], Ambos-Spies et al. [1], Poizat [18] and Blum and Impagliazzo [6]. Among them, Dowd investigated the relationship between uniform machines and $NP = ?coNP$ question. For this purpose, he studied the relativized propositional calculus by introducing the notion of t -generic oracles. Extending techniques in [11] and those in [18], we study computational complexity of

$rTAUT[A]$, the collection of all r -query tautologies with respect to an oracle A . In particular, we investigate the case where A is a Cohen-Feferman generic oracle. Although we shall present precise definitions in the next section, let us review the definition of $rTAUT[A]$ in an informal manner. The relativized propositional calculus is an extension of the propositional calculus. We get the former by adding a countable set $\{\xi^n(q_1, \dots, q_n) : n \geq 1\}$ of connectives to the latter. Roughly speaking, $\xi^n(q_1, \dots, q_n)$ asserts that a certain binary sequence, of length less than n , associated to the given bit string $q_1 \cdots q_n$ belongs to the oracle that we are considering. Suppose that r is a positive integer. A relativized formula is called an r -query formula if it has just r -many occurrences of additional connectives. For each oracle A , $rTAUT[A]$ denotes the collection of all (binary representations of) r -query formulas that are tautologies with respect to A .

An oracle G is called *t-generic* [11] if every relativized tautology with respect to G is forced by a polynomial sized portion of G . More formally, G is t-generic if there exists a polynomial p such that for each formula F of the relativized propositional calculus such that F is a tautology with respect to G , there exists a function S that satisfies the following three requirements.

- (1) $\text{dom}(S) \subseteq \text{dom}(G)$, $\text{ran}(S) \subseteq \{0, 1\}$ and $S(u) = G(u)$ for all $u \in \text{dom}(S)$, where we identify an oracle with its characteristic function: we denote this statement by “ $S \sqsubseteq G$.”
- (2) $\text{Card}(\text{dom}(S)) \leq p(|F|)$, where $\text{Card}(X)$ denotes the cardinality of X and $|F|$ denotes the length of (the binary representation of) F .
- (3) For any oracle A such that $S \sqsubseteq A$, F is a tautology with respect to A : we denote this statement by “ S forces $F \in TAUT[X]$.”

The above requirement (2) asserts nothing about the length of the elements of $\text{dom}(S)$, but the length of these elements are clearly bounded by the number of variables appearing in F .

According to [11, Lemma 7], t-generic oracles do not exist. Thus, in particular, we have the following.

Fact 1 (A corollary of [11, Lemma 7]) *The class of all t-generic oracles has Lebesgue measure zero in the Cantor space.* \square

Dowd proved his Lemma 7 of [11] by using the following lemma. His expression M^X is, in our notation, $M[X]$. Similarly, \mathcal{N} is $\{0, 1\}^*$: we denote the collection of all bit strings of finite length by $\{0, 1\}^*$, as in the textbook on computational complexity by Balcázar et al. [4]. (On the other hand, Kunen’s textbook on set theory [15] denotes this collection by ${}^{<\omega}2$.) For each natural number n , $\{0, 1\}^n (= {}^n2)$ and $\{0, 1\}^{\leq n} (= {}^{\leq n}2)$ are similarly defined. It is easily verified that the cardinality of $\{0, 1\}^{\leq n}$ is $2^{n+1} - 1$ for each natural number n . Recall that a language A is called *sparse* if there exists a polynomial p such that for each natural number n , $\text{Card}(A \cap \{0, 1\}^{\leq n}) \leq p(n)$.

Citation [11, Lemma 6]

Lemma *If a deterministic polynomial time oracle machine M^X accepts all its inputs with respect to a t -generic oracle G , then it is forced to do so by a sparse set of queries. That is, there is a partial function Y from \mathcal{N} to $\{0,1\}$ satisfying $Y \sqsubseteq G$ whose domain is sparse, which forces $\forall x M^X(x)$.*

Proof. The relativized formula asserting that “on all inputs of length $\leq n$ the machine M accepts” is a tautology with respect to the oracle G for every n , and its length is bounded by a polynomial in n . Therefore the n th is forced by a set W_n of queries to G of size polynomial in n . Let $W = \bigcup\{W_n : n \text{ is a power of } 2\}$. Then W is sparse, and forces the statement. \square

Careful readers may hesitate, because the following assertion is false, by a counter example below.

Assertion 1(false) Suppose that p is a polynomial, and that for each positive integer n , D_n is a subset of $\{0,1\}^{\leq p(n)}$ such that $\text{Card}(D_n) \leq p(n)$. Let $D = \bigcup\{D_n : n \text{ is a power of } 2\}$. Then D is sparse. \square

Example 1 For each natural number $n \geq 2$, let $k(n)$ be the largest natural number k such that $2^{k+1} - 1 \leq n$. For each n , let $D_n = \{0,1\}^{\leq k(n)}$. Let $D = \bigcup\{D_n : n \text{ is a power of } 2\}$. Then, for each $n \geq 2$, D_n is a subset of $\{0,1\}^{\leq n}$ and $\text{Card}(D_n)$ is at most n . However, we have $D = \{0,1\}^*$. \square

Nevertheless, **Fact 1** is right. In section 3, we shall present a direct alternative proof of **Fact 1**, by introducing the notion of ceiling-generic oracles (c-generic oracles, for short).

Next, we shall investigate how existence of c-generic oracles affects behavior of a Cohen-Feferman generic oracle. By using **Fact 1** and the method of Baker et al. [2], we shall strengthen the well-known result (Mehlhorn [16], [18] and [11]) that the following class of oracles is comeager: $\{X : P[X] \neq NP[X]\}$. More precisely, in section 4, we shall show that the following is comeager, where r is an arbitrary positive integer: $\{X : coNP[X] \not\subseteq NP[rTAUT[X]]\}$.

By the way, Dowd also introduced weak versions of the notion of t -generic oracles. Suppose that r is a positive integer. An oracle G is called an r -generic oracle (in Dowd’s sense), if it satisfies the definition of a t -generic oracle with r -query tautology in place of tautology.

Fact 2 (section 4 of [11]) *The class of all r -generic oracles (in Dowd’s sense) is meager, and has Lebesgue measure one in the Cantor space. Further, this class is closed under finite changes i.e. if A is r -generic and $B(u) = A(u)$ for all but finitely many bit strings u then B is also r -generic.* \square

Extending Dowd’s work about r -generic oracles, the following was shown in Suzuki [20].

Fact 3 *The following two assertions are equivalent.*

- (1) The class of all A such that $1TAUT[A] \notin P[A]$ has Lebesgue measure one.
- (2) The unrelativized classes R and NP are not identical. \square

Recall that $P \subseteq R \subseteq NP$. For the definition of the computational complexity class R , see [4].

2 Notation and definitions

The set of all natural numbers is denoted by $\mathbb{N} = \{0, 1, 2, \dots\}$. For a function f and a set $D \subseteq \text{dom}(f)$, $f \upharpoonright D$ denotes the restriction of f to D . A subset of $\{0, 1\}^*$ is called an *oracle* or a *language*, according to the context. We identify an oracle with its characteristic function; thus, an oracle is a function from $\{0, 1\}^*$ to $\{0, 1\}$. Suppose that A and B are oracles. $A \oplus B$ denotes the join of A and B . The only one important property of the join is that its polynomial time many-one degree is a supremum of those of A and B . According to the textbook of complexity theory [4], we adopt the language $\{u0 : u \in A\} \cup \{v1 : v \in B\}$ as a formal definition of the join; of course, there are different ways to define the join (see e.g. Rogers [19]). $P[A]$ denotes the set of all oracles which are polynomial time Turing reducible to A . “ $A \equiv_T^P B$ ” means that A and B are polynomial time Turing equivalent. “ $A \equiv B \text{ (mod. finite)}$ ” means that the following set is finite: $\{x \in \{0, 1\}^* : A(x) \neq B(x)\}$. Suppose that $M[X]$ is an oracle Turing machine and that A is an oracle. Then, $\text{Lang}(M[A])$ denotes the language accepted by the machine $M[X]$ with the oracle A . For each oracle A , Book [7] introduced the computational complexity class $NPQUERY[A]$ as follows. A language B belongs to $NPQUERY[A]$ if $B = \text{Lang}(M[A])$ for some nondeterministic oracle machine $M[X]$ such that $M[X]$ uses a polynomial amount of work space and make a polynomial number of queries to associated oracle in each computation. It was shown in Balcázar et al. [3] that for any oracle A , $NPQUERY[A] = NP[QBF \oplus A]$, where QBF is a well-known $PSPACE$ -complete set.

By adding a countable set $\{\xi^n(q_1, \dots, q_n) : n \geq 1\}$ of connectives to the propositional calculus, we get *the relativized propositional calculus*. If A is an oracle and n is a positive integer, we define an n -ary Boolean function A^n as follows, and we interpret the connective ξ^n as the Boolean function A^n . Let λ be the empty string. We order all bit strings in lexicographic order: $\lambda (= z(0)), 0 (= z(1)), 1 (= z(2)), 00 (= z(3)), 01 (= z(4)), \dots$ etc. Now, suppose that u is a bit string whose length is n . Say, $u = z(2^n - 1 + j)$, where $j \leq 2^n - 1$. Then we set $A^n(u_1, u_2, \dots, u_n)$ to be equal to $A(z(j))$. That is, $A^n(0, \dots, 0, 0) = A(\lambda)$, $A^n(0, \dots, 0, 1) = A(0)$, $A^n(0, \dots, 1, 0) = A(1), \dots$, and $A^n(1, \dots, 1, 1) = A(0^n)$. This rather obscure definition of A^n is forced on us in place of the more direct $A^n(u_1, \dots, u_n) = A(u)$, because we want that the information contained in A^n be preserved in A^{n+1} , and also because a predicate in a tautology must have a definite number of arguments. In fact, $A^n(u_1, \dots, u_n)$ denotes membership to A of the string corresponding to u by the bijection between $\{0, 1\}^n$ and $\{0, 1\}^{\leq n-1} \cup \{0^n\}$ which respects the lexicographic order. The corresponding string $z(j)$ is very simply obtained from u : if u is 0^n then

$z(j) = \lambda$; otherwise, first, delete from u the first 1 from the left and all the 0's at its left, then the resulting string is $z(j - 1)$, and $z(j)$ is easily obtained.

$TAUT[A]$ denotes the set of all (binary representations of) relativized formulas which are tautologies with respect to the oracle A . Suppose that r is a positive integer. We consider a relativized formula with r occurrences of additional connectives; at the expense of adding dummy variables, it can be put in the form:

$$\left((a^{(1)} \Leftrightarrow \xi^{i_1}(q_1^{(1)}, \dots, q_{i_1}^{(1)})) \wedge \dots \wedge (a^{(r)} \Leftrightarrow \xi^{i_r}(q_1^{(r)}, \dots, q_{i_r}^{(r)})) \right) \Rightarrow H,$$

where H is a query free formula. According to the terminology of [11], we call a relativized formula of the above form an r -query formula. Note that it is only the number r of queries which is relevant to this definition, not their length i_1, \dots, i_r . A relativized formula F is called an r -query tautology with respect to A if F is an r -query formula and F is a tautology with respect to A . $rTAUT[A]$ denotes the set of all (binary representations of) r -query tautologies with respect to A . Moreover, by $TAUT$, we denote the collection of all (binary representations of) tautologies of usual propositional calculus. Let X be a unary predicate symbol denoting membership to a given oracle and y be a variable for a bit string. Membership to the set $TAUT[X]$ is expressed by an arithmetical predicate, that we denote $TAUT(X)(y)$. For each r , a predicate $rTAUT(X)(y)$ is similarly defined. As is well-known, $TAUT[X]$ is uniformly $coNP[X]$ -complete [11, p.68]: that is, for any polynomial time-bounded nondeterministic oracle Turing machine $M[X]$, there exists a function f such that f is polynomial time computable (without an oracle) and for any oracle A and for any bit string u , $M[A]$ rejects u if and only if $f(u)$ belongs to $TAUT[A]$.

A function S is called a *forcing condition* (condition, for short) if $\text{dom}(S)$ is a finite subset of $\{0, 1\}^*$ and $\text{ran}(S) \subseteq \{0, 1\}$. A collection D of conditions is called *dense* if for every condition S , there exists a condition $T \in D$ such that $S \sqsubseteq T$. An oracle G is called a *Cohen-Feferman generic oracle* (or, a generic oracle) if for any collection D of conditions such that D is arithmetical and dense, there exists a condition S such that $S \in D$ and $S \sqsubseteq G$. Such definitions of dense sets and generic oracles appear e.g. in Definition 1.1 of [6]. It is well-known that the collection of all Cohen-Feferman generic oracles form a comeager set in the Cantor space [13, 10]. Note that 1-generic oracles in Dowd's sense and Feferman's generic oracles are completely different concepts. In fact, any Cohen-Feferman generic oracle is not 1-generic in Dowd's sense [11, Theorem 12].

3 Ceiling-generic oracles

We begin by presenting an alternative proof of **Fact 1**.

Definition 1 *Suppose that $\varphi(X)(y)$ is an arithmetical predicate, where X is a unary symbol denoting membership to a given oracle, and y is a variable for a bit string.*

1. ([18]. See also Tanaka and Kudoh [21]) $\varphi(X)(y)$ is finitely testable (or, test fini) if there exists a function $f : \mathbb{N} \rightarrow \mathbb{N}$ such that for every oracle A and every bit string u , $\varphi(A)(u)$ holds if and only if $\varphi(A \upharpoonright (\{0, 1\}^{\leq f(|u|)}))(u)$ holds, where we identify a condition $A \upharpoonright (\{0, 1\}^{\leq n})$ with an oracle B defined as follows: $A \upharpoonright (\{0, 1\}^{\leq n}) \sqsubseteq B$, and $B(u) = 0$ for all u such that $|u| > n$. Moreover, for each oracle A , $\varphi[A]$ denotes the set $\{u \in \{0, 1\}^* : \varphi(A)(u)\}$.
2. We say “a condition S forces $\varphi(X)(u)$,” where u is a given bit string, if $\varphi(A)(u)$ holds for any oracle A such that $S \sqsubseteq A$.
3. Suppose that $\varphi(X)(y)$ is finitely testable, G is an oracle, and f is a function from \mathbb{N} to \mathbb{N} . G is f -ceiling-generic for $\varphi(X)(y)$ (f - c -generic for $\varphi(X)(y)$, for short), if for any bit string u for which $\varphi(G)(u)$ holds, there exists a condition $S \sqsubseteq G$ such that $\text{Card}(\text{dom}(S)) \leq f(|u|)$ and S forces $\varphi(X)(u)$. G is ceiling-generic for $\varphi(X)(y)$ (c -generic for $\varphi(X)(y)$, for short), if there exists a polynomial p such that G is p - c -generic for $\varphi(X)(y)$. \square

Alternative Proof of Fact 1.

The oracle-dependent language $CORANGE[X]$ is well-known among the reader of Bennet and Gill [5]. We express membership to this language by a predicate $CORANGE(X)(y)$. More precisely, $CORANGE(X)(y)$ denotes the following assertion:

$$\neg \exists u \text{ such that } y = X(u1)X(u10)X(u100) \cdots X(u10^{|u|-1}).$$

Note that y and u in the above assertion have the same length, and hence the above assertion is finitely testable. Recall that $TAUT[X]$ is uniformly $coNP[X]$ -complete. Thus, there exists a function f such that f is computable (without an oracle) in polynomial time, and for any oracle A and any bit string w , $CORANGE(A)(w)$ holds if and only if we have $f(w) \in TAUT[A]$. Therefore, if A is t -generic, then A is c -generic for $CORANGE(X)(y)$. Hence $CORANGE[A]$ is a finite set; indeed, letting p be a polynomial for which A is p - c -generic, whenever 2^n is sufficiently larger than $p(n)$, $CORANGE[A]$ does not contain any y of length n , since a condition of size $p(n)$ cannot force all the u 's of size n so that $y \neq X(u1)X(u10)X(u100) \cdots X(u10^{|u|-1})$. Thus, all t -generic oracles belong to the following class: $\{X : CORANGE[X] \in NP[X]\}$. However, by [5], this class has Lebesgue measure zero.

4 Application of ceiling-generic oracles

In this section, we study how existence of ceiling-generic oracles affects behavior of a generic oracle, and strengthen the well-known result that the following class of oracles is comeager: $\{X : P[X] \neq NP[X]\}$.

Theorem 1 *Suppose that $\varphi(X)(y)$ and $\psi(X)(y)$ are finitely testable arithmetical predicates, G_1 is an oracle, and suppose that the following three hypothesisises hold for every oracle A such that $A \equiv G_1$ (mod. finite).*

(H. 1) *A is c -generic for $\varphi(X)(y)$.*

(H. 2) *A is c -generic for $\neg\varphi(X)(y)$.*

(H. 3) *A is not c -generic for $\psi(X)(y)$.*

Then, for every Cohen-Feferman generic oracle G_2 , we have

$$\psi[G_2] \notin NP[\varphi[G_2]].$$

Proof: Suppose that $M[X]$ is a polynomial time-bounded nondeterministic oracle Turing machine, and suppose that S_0 is an arbitrary condition. We shall show existence of a condition T such that T is an extension of S_0 , and T forces $\psi[X] \neq \text{Lang}(M[\varphi[X]])$. Let A be an oracle such that $A \equiv G_1$ (mod. finite) and A is an extension of S_0 (i.e. $S_0 \sqsubseteq A$). Assume that p is a polynomial such that A is p - c -generic for $\varphi(X)(y)$ and A is p - c -generic for $\neg\varphi(X)(y)$. By the hypothesisises (H. 1) and (H. 2), such a p surely exists. Let t be a polynomial that is a time-bounding function of $M[X]$. We may assume $n \leq t(n) < t(n+1)$, for all natural numbers n , and may assume that the same thing holds with p in place of t . Let us define a polynomial q as follows.

$$q(x) = t(x) \cdot p(t(x)) + \text{Card}(\text{dom}(S_0)).$$

By the hypothesis (H.3), A is not q - c -generic for $\psi(X)(y)$. Moreover, the predicate $\psi(X)(y)$ is finitely testable. Hence, there exists a bit string u for which the following holds: “ $\psi(A)(u)$ is true, and for each condition S such that $S \sqsubseteq A$ and $\text{Card}(\text{dom}(S)) \leq q(|u|)$, there exists a condition T such that $S \sqsubseteq T$ and T forces $\neg\psi(X)(u)$.” We fix such a u .

In the case where $M[\varphi[A]]$ accepts u . We consider a fixed accepting computation of M . Since in course of the computation M asks at most $t(|u|)$ questions of size at most $t(|u|)$ to the oracle, there exists a condition S_1 such that $S_1 \sqsubseteq A$, $\text{Card}(\text{dom}(S_1)) \leq t(|u|) \cdot p(t(|u|))$ and S_1 forces that $M[\varphi[X]]$ accepts the bit string u . Since S_0 and S_1 are compatible, there exists a condition S_2 such that S_2 is a common extension of them (i.e. $S_0 \sqsubseteq S_2$ and $S_1 \sqsubseteq S_2$) and $\text{Card}(\text{dom}(S_2)) \leq q(|u|)$. Hence, by our choice of the bit string u , there exists a condition T such that $S_2 \sqsubseteq T$ and T forces $\neg\psi(X)(u)$. We fix such a T .

Otherwise. We consider the arithmetical predicate $\psi_0(X)(y)$ defined by the following assertion: “ $\psi(X)(y)$ is true, and $M[\varphi[X]]$ rejects y .” Since the predicate $\psi_0(X)(y)$ is finitely testable and $\psi_0(A)(u)$ is true, there exists a condition $S_3 \sqsubseteq A$ such that S_3 forces $\psi_0(X)(u)$. Let T be a common extension of S_0 and S_3 .

In either case, $S_0 \sqsubseteq T$, and T forces $\psi[X] \neq \text{Lang}(M[\varphi[X]])$. \square

Corollary 2 *Suppose that r is a positive integer. Then, the following class of oracles is comeager:*

$$\{X : \text{coNP}[X] \not\subseteq NP[rTAUT[X]]\}.$$

Proof: Note that one counter-example is sufficient to refute a tautology. Thus, *any* oracle is p -c-generic for $\neg rTAUT(X)(y)$ with $p(n) =_{\text{def.}} r$ (for each $n \in \mathbb{N}$). Let G_1 be an r -generic oracle in Dowd's sense such that G_1 is not t -generic. By **Fact 1** and **Fact 2**, we know that such a G_1 surely exists, and that the following triple satisfies the three hypothesis (H. 1), (H. 2) and (H. 3):

$$(rTAUT(X)(y), TAUT(X)(y), G_1).$$

Hence, by **Theorem 1**, for each Cohen-Feferman generic oracle G_2 , we have $TAUT[G_2] \notin NP[rTAUT[G_2]]$. \square

Remark: Since $NPQUERY[A] = NP[QBF \oplus A]$ for any oracle A , it is easily seen that the statements of **Theorem 1** and **Corollary 2** hold with $NPQUERY[]$ in place of $NP[]$. \square

Let $L_{BGS}[X]$ be the oracle-dependent tally set defined as follows.

$$L_{BGS}[X] = \{0^n : \neg \exists y \in A(|y| = n)\}.$$

It is well-known that Baker et al. used (the complement of) the above tally set in [2] to show existence of an oracle A such that $P[A] \neq NP[A]$. Later, some people interpreted the method of Baker et al. as a forcing method, and they showed that $P[G_2] \neq NP[G_2]$ for every Cohen-Feferman generic oracle G_2 (e.g. [10, 11], [6]). However, the polynomial time many-one degree of the tally set $L_{BGS}[X]$ is so low that $L_{BGS}[X]$ is useless to separate $TAUT[X]$ from $rTAUT[X]$ i.e. useless to show **Corollary 2**. To see this, let us prove an example by using $L_{BGS}[X]$. Suppose that G_2 is a Cohen-Feferman generic oracle. Then, the following holds:

$$(4.1) \quad 1TAUT[G_2] \notin NP[QBF \oplus G_2].$$

Moreover, as a special case of (4.1), we have the following:

$$(4.2) \quad 1TAUT[G_2] \notin P[TAUT \oplus G_2].$$

A proof of (4.1) by using $L_{BGS}[X]$ is as follows. Suppose that $M[X]$ is a polynomial time-bounded nondeterministic oracle Turing machine. Let D_M be the set of all conditions that force the following assertion (4.3).

$$(4.3) \quad L_{BGS}[X] \neq \text{Lang}(M[QBF \oplus X])$$

By the method of the proofs of Theorem 3 and 4 of [2], it is verified that D_M is dense, and hence every Cohen-Feferman generic oracle X satisfies (4.3). Therefore, for each Cohen-Feferman generic oracle G_2 , we have $L_{BGS}[G_2] \notin NP[QBF \oplus G_2]$. Since the above tally set $L_{BGS}[A]$ is polynomial time many-one reducible to $1TAUT[A]$ for each oracle A , we have (4.1).

Of course, we can show (4.1) without using $L_{BGS}[X]$. First, note the following.

Claim Suppose $\psi(X)(y)$ is a finitely testable arithmetical predicate and G_1 is an oracle. And, suppose that the hypothesis (H. 3) holds for every oracle A such that $A \equiv G_1 \pmod{\text{finite}}$. Then, for every Cohen-Feferman generic oracle G_2 , we have

$$\psi[G_2] \notin NP[QBF \oplus G_2].$$

Proof: We consider the predicate $\varphi(X)(y)$ defined by “ $y \in X$.” Clearly, any oracle is c -generic for $\varphi(X)(y)$ and c -generic for $\neg\varphi(X)(y)$. And, for any oracle A , the language $\varphi[A]$ is just A itself. Hence, by **Theorem 1** and **Remark** after the proof of **Corollary 2**, we get **Claim**. \square

Let \mathcal{F} be the class of all oracles which are *not* 1-generic in Dowd’s sense. By **Fact 2**, \mathcal{F} is comeager in the Cantor space, and is closed under finite changes; indeed, \mathcal{F} contains all Cohen-Feferman generic oracles [11, Theorem 12]. Take an oracle $G_1 \in \mathcal{F}$, and let $\psi(X)(y)$ be the predicate $1TAUT(X)(y)$. Then, we get (4.1) by **Claim**.

By the way, in the statement of **Theorem 1**, it is essential that the three hypothesises (H. 1), (H. 2) and (H. 3) hold not only for $A = G_1$ but also for any A such that $A \equiv G_1 \pmod{\text{finite}}$. Compare the above **Claim** with the following **Example**.

Example 2 There exists a pair $(\psi_0(X)(y), G_1)$ that satisfies all of the following three requirements.

1. $\psi_0(X)(y)$ is a finitely testable arithmetical predicate and G_1 is an oracle.
2. G_1 is not c -generic for $\psi_0(X)(y)$.
3. For each Cohen-Feferman generic oracle G_2 , we have $\psi_0[G_2] \in P[G_2]$.

Proof: For each positive integer i and for each query free formula H , we denote the following 1-query formula by $\natural\langle 1, i, H \rangle$:

$$(a \Leftrightarrow \xi^i(q_1, \dots, q_i)) \Rightarrow H.$$

Let G_1 be a 1-generic oracle in Dowd’s sense with respect to a polynomial p . We may assume $n \leq p(n) \leq p(n+1)$, for all natural numbers n . We consider the arithmetical predicate $\psi_0(X)(y)$ defined by the following assertion: “for some $n \in \mathbb{N}$, $y = 0^n$, and for each $i \leq n$ and for each query free formula H , if $\natural\langle 1, i, H \rangle$ is a tautology with respect to X then there exists a condition $S \sqsubseteq X$ such that $\text{Card}(\text{dom}(S))$ is at most $p(|\natural\langle 1, i, H \rangle|)$ and S forces $\natural\langle 1, i, H \rangle \in TAUT[X]$.”

We show that G_1 is not c -generic for $\psi_0(X)(y)$. Assume for a contradiction that G_1 is q - c -generic for $\psi_0(X)(y)$, where q is a polynomial. We may assume $n \leq q(n) \leq q(n+1)$, for all natural numbers n . Let c be a sufficiently large natural number and let m be a natural number satisfying the following inequality:

$$(4.4) \quad c \cdot p(c \cdot q(m)^c + c) < 2^m - 1.$$

Since G_1 is 1-generic in Dowd's sense with respect to the polynomial p , we have $\psi_0(G_1)(0^m)$. Therefore, by our assumption for a contradiction, there exists a condition $S \sqsubseteq G_1$ such that $\text{Card}(\text{dom}(S))$ is at most $q(m)$ and S forces $\psi_0(X)(0^m)$. Let $\{v^{(1)}, \dots, v^{(d)}\}$ be an enumeration of all bit strings v such that $v \in \text{dom}(S)$ and $S(v) = 1$. Of course, we have the following:

$$d \leq q(m).$$

Let H_0 be a query free formula such that for each oracle X , the 1-query formula $\natural\langle 1, m, H_0 \rangle$ is a tautology with respect to X if and only if the following assertion holds:

$$(4.5) \quad (\forall u \in X \cap \{0, 1\}^{\leq m-1}) (u = v^{(1)} \text{ or } \dots \text{ or } u = v^{(d)}).$$

We choose H_0 so that its length $|H_0|$ would be as short as possible. We define an oracle A as follows: $S \sqsubseteq A$, and $A(u) = 0$ for all $u \notin \text{dom}(S)$. Then, we have $\natural\langle 1, m, H_0 \rangle \in 1TAUT[A]$. On the other hand, $\psi_0(A)(0^m)$ holds, since this predicate is forced by S . Hence, by our definition of $\psi_0(X)(y)$, there exists a condition $T \sqsubseteq A$ such that $\text{Card}(\text{dom}(T))$ is at most $p(|\natural\langle 1, m, H_0 \rangle|)$ and T forces $\natural\langle 1, m, H_0 \rangle \in TAUT[X]$. Thus, T forces the assertion (4.5). However, by the inequality (4.4) and by our choice of the formula H_0 , we may assume $\text{Card}(\text{dom}(T)) < (2^m - 1)/c$. Recall that the cardinality of $\{0, 1\}^{\leq m-1}$ is $2^m - 1$. Hence, there exists an oracle X such that the assertion (4.5) fails but $T \sqsubseteq X$, a contradiction.

Finally, let G_2 be a Cohen-Feferman generic oracle; let us show $\psi_0[G_2] \in P[G_2]$. Then, G_2 is not a 1-generic oracle in Dowd's sense [11, Theorem 12]. Therefore, $\psi_0[G_2]$ is a finite set. \square

Acknowledgement

I wish to thank Professor Hisao Tanaka for his encouragement and useful discussions. I thank the anonymous referee for his/her kind advice.

This research was partially supported by Grant-in-Aid for Scientific Research (No. 09440072), Ministry of Education, Science, Sports and Culture of Japan.

References

- [1] Ambos-Spies, K., H. Fleischhack, and H. Huwig, “ P -generic sets,” pp. 58-68 in *ICALP 84*, Lect. Notes Comput. Sci. vol. 172, edited by J. Paredaens, Springer, Berlin, 1984.
- [2] Baker, T., J. Gill, and R. Solovay, “Relativizations of the $P = ?NP$ question,” *SIAM J. Comput.*, vol. 4 (1975), pp. 431-442.
- [3] Balcázar, J. L., R. V. Book, and U. Schöning, “On bounded query machines,” *Theoret. Comput. Sci.*, vol. 40 (1985), pp. 237-243.
- [4] Balcázar, J. L., J. Díaz, and J. Gabarró, *Structural complexity I*, Springer, Berlin, 1988.
- [5] Bennett, C. H. and J. Gill, “Relative to a random oracle A , $P^A \neq NP^A \neq co-NP^A$ with probability 1,” *SIAM J. Comput.*, vol. 10 (1981), pp. 96-113.
- [6] Blum, M. and R. Impagliazzo, “Generic oracles and oracle classes,” pp. 118-126 in *28th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, 1987.
- [7] Book, R. V., “Bounded query machines: on NP and $PSPACE$,” *Theoret. Comput. Sci.*, vol. 15 (1981), pp. 27-39.
- [8] Cohen, P. J., “The independence of the continuum hypothesis I,” *Proc. Nat. Acad. Sci. USA*, vol. 50 (1963), pp. 1143-1148.
- [9] Cohen, P. J., “The independence of the continuum hypothesis II,” *Proc. Nat. Acad. Sci. USA*, vol. 51 (1964), pp. 105-110.
- [10] Dowd, M., “Forcing and the P -hierarchy,” Laboratory for Computer Science Research, Rutgers University, Technical Report No. **LCSR-TR-35**, 1982.
- [11] Dowd, M., “Generic oracles, uniform machines, and codes,” *Information and Computation*, vol. 96 (1992), pp. 65-76.
- [12] Feferman, S., “Some applications of the notions of forcing and generic sets,” *Fund. Math.*, vol. 56 (1965), pp. 325-345.
- [13] Hinman, P. G., “Some applications of forcing to hierarchy problems in arithmetic,” *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, vol. 15 (1969), pp. 341-352.
- [14] Jockusch, C. G. Jr., “Degrees of generic sets,” pp. 110-139 in *Recursion theory: its generalizations and applications*, London Math. Soc. Lect. Note Series vol. 45, edited by F.R. Drake and S.S. Wainer, Cambridge University Press, Cambridge, 1980.
- [15] Kunen, K., *Set theory*, North-Holland, Amsterdam, 1980.

- [16] Mehlhorn, K., "On the size of sets of computable functions," pp. 190-196 in *14th Annual Symposium on Switching & Automata Theory*, IEEE Computer Society Press, Los Alamitos, 1973.
- [17] Odifreddi, P., "Forcing and reducibilities," *J. Symbolic Logic*, vol. 48 (1983), pp. 288-310.
- [18] Poizat, B., " $Q = NQ ?$," *J. Symbolic Logic*, vol. 51 (1986), pp. 22-32.
- [19] Rogers, H. Jr., *Theory of recursive functions and effective computability*, MacGraw-Hill, New York, 1967.
- [20] Suzuki, T., "Random oracles, and tautology with one query," Department of Mathematics and Information Sciences, Osaka Prefecture University, Research Report No. **DMIS-RR-96-2**, 1996.
- [21] Tanaka, H. and M. Kudoh, "On relativized probabilistic polynomial time algorithms," *Journal of the Mathematical Society of Japan*, vol. 49 (1997), pp. 15-30.