Logarithmic truth-table reductions and minimum sizes of forcing conditions (preliminary draft)

Masahiro Kumabe\textsuperscript{1)}, Toshio Suzuki\textsuperscript{2)*}, Takeshi Yamazaki\textsuperscript{3)}

\textsuperscript{1)}: University of the Air, 31-1, Ōoka, Minami-ku, Yokohama 232-0061, Japan kumabe@u-air.ac.jp
\textsuperscript{2),3)}: Department of Mathematics and Information Sciences Osaka Prefecture University, Sakai, Osaka 599-8531, Japan toshios@acm.org, yamazaki@mi.s.osakafu-u.ac.jp

April 5, 2005

Abstract

In our former works, for a given concept of reduction, we study the following hypothesis: "For a random oracle $A$, with probability one, the degree of the one-query tautologies with respect to $A$ is strictly higher than the degree of $A."$ In our former works, the following three results are shown: (1) the hypothesis for polynomial-time Turing reduction is equivalent to the assertion that the probabilistic complexity class $R$ is not equal to $NP$, (2) the hypothesis for polynomial-time truth-table reduction implies that $P$ is not $NP$, (3) (to appear in Arch. Math. Logic) the hypothesis holds for polynomial-time bounded-truth-table reduction. In this note, we show that the hypothesis holds for $(\log n)^{O(1)}$-question truth-table-reduction (without polynomial-time bound). As applications of this result, we show a lower bound and an upper bound of forcing complexity (i.e., the minimum size of forcing condition that forces a given formula) of the one-query tautologies with respect to a random oracle. We show that if $A$ is a random oracle then with probability one, the forcing complexity of the one-query tautology with respect to $A$ is greater than polynomial of $\log |F|$, and it is at most $O(|F|^2)$, where $|F|$ denotes the length of a formula.

\textsuperscript{*}The author was partially supported by Grant-in-Aid for Scientific Research (No. 14740082), Japan Society for the Promotion of Science.
1 Preface

In our former works [Su98, Su99, Su00, Su01, Su02, Su05], by extending the work of Ambos-Spies [Am86] and related works, we consider the relationships with the canonical product measure of Cantor space and complexity of one-query tautologies. A formula $F$ of the relativized propositional calculus is called a one-query formula if $F$ has exactly one occurrence of a query symbol. For example,

$$(q_0 \leftrightarrow \xi^3(q_1, q_2, q_3)) \Rightarrow (q_1 \Rightarrow q_0)$$

is a one-query formula, where $q_0, q_1, q_2, q_3$ are usual propositional variables. We assume that each propositional variable takes the value 0 or 1 (0 denotes false and 1 denotes true). And, $\xi^3$ in the above formula is a query symbol. For a given oracle $A$, a function $A^3$ is defined as follows, where $\lambda$ is the empty string, and the query symbol $\xi^3$ is interpreted as the function $A^3$.

$$A^3(000) = A(\lambda), \quad A^3(001) = A(0), \quad A^3(010) = A(1), \quad A^3(011) = A(00),$$

$$A^3(100) = A(01), \quad A^3(101) = A(10), \quad A^3(110) = A(11), \quad A^3(111) = A(00).$$

Thus, more informally, the following holds for each $j = 0, 1, \ldots, 2^3 - 1$, where the order of strings is defined as the canonical length-lexicographic order.

$$A^3(\text{the } (j + 1)\text{st } 3\text{-bit string}) = A(\text{the } (j + 1)\text{st } 3\text{-bit string}).$$

For each $n$, an $n$-ary Boolean function $A^n$ is defined in the same way, and an interpretation of the query symbol $\xi^n$ is defined in the same way. For an oracle $A$, the concept of a tautology with respect to $A$ is defined in a natural way. If a one-query formula $F$ is a tautology with respect to $A$, then we say $F$ is a one-query tautology with respect to $A$. The set of all one-query tautologies with respect to $A$ is denoted by $\text{1TAUT}^A$.

In [Su02], for a given concept $\leq_{\alpha}$ of reduction, we study the following hypothesis, where $\text{1TAUT}^X$ denotes the set of all one-query tautologies with respect to an oracle $X$.

One-query-jump hypothesis for $\leq_{\alpha}$: The class $\{X : 1\text{TAUT}^X \leq_{\alpha} X\}$ has measure zero.

For a given reduction $\leq_{\alpha}$, we denote the corresponding one-query-jump hypothesis by $[\leq_{\alpha}]$.

In [Su98], it is shown that the one query-jump hypothesis for $p$-T reduction is equivalent to "$R \neq \text{NP}$." And, in [Su02], it is shown that the one query-jump hypothesis for $p$-tt reduction implies "$P \neq \text{NP}$."

In [Su05], we show that the one query-jump hypothesis for $p$-btt reduction holds, where $p$-btt denotes polynomial-time bounded-truth-table reduction. The
anonymous referee of [Su05] noticed that the one query-jump hypothesis holds for bounded-truth-table reduction without polynomial-time bound, and Kumabe independently noticed the same result. The referee's proof, which may be found in [Su05], uses some concepts of resource-bounded generic oracles in [AM97]. Kumabe's proof is more simple.

In §3 of this note, we introduce Kumabe's proof of the above result. In §4, we extend the result, and show that the one query-jump hypothesis holds for $(\log n)^{O(1)}$-question tt-reduction (without polynomial-time bound). In §5, as applications of the result in §4, we show a lower bound and an upper bound of forcing complexity (i.e., the minimum size of forcing condition that forces a given formula) of the one-query tautologies with respect to a random oracle. We show that if $A$ is a random oracle then with probability one, the forcing complexity of the one-query tautologies with respect to $A$ is greater than $(\log |F|)^{O(1)}$, and it is at most $O(|F|^2)$.

The three of authors had a meeting at July 22, 2004, at the office of T.S. in Osaka Prefecture University. This note is a research memo on the meeting, and is an extension of [Su05].

2 Notation

Most of our notation is the same as that of [Su02] and [Su05], and almost all undefined notions may be found in these papers. An article by Kawanishi and Suzuki [KS05] in this volume of Surikaisekikenkyusho Kōkyūroku contains basic definitions on the relativized propositional calculus and Dowd-type generic oracles. The journal version of [Su02] may be purchased at Science Direct.

http://www.sciencedirect.com/science/journals

ω stands for $\{0, 1, 2, 3 \cdots\}$, while N stands for $\{1, 2, 3 \cdots\}$. In some textbooks, the complexity class R is denoted by RP. For the detail of the class R, see for example [BDG88].

The definition of polynomial-time truth-table reduction and its variant may be found in [LLS75].

3 Bounded truth table reduction

In this section, we show the following.

Proposition 1 The Lebesgue measure of the set

$$\{X : \text{ITAUT}^X \leq_{\text{btt}} X\}$$

is zero. In other words, one-query jump hypothesis [Su02, Su05] for btt-reduction (without polynomial-time bound) holds.
Sketch of proof (due to Kumabe):

For each oracle $X$, let $L^X := \bigcup_n \{(u, v, w) \in \{0, 1\}^n : |u| = |v| = |w| = n \text{ and } X^n(u) = X^n(v) = X^n(w)\}$. It is easy to see that $L^X \leq_{\text{m}}^{\text{p}} 1\text{TAUT}^X$.

Suppose that $f$ is a recursive function such that for each string $x$, it holds that $f(x)$ is of the form $(\varphi_x, s_{x,1}, s_{x,2})$, where $\varphi_x$ is a function from $\{0, 1\}^2$ to $\{0, 1\}$, and $s_{x,1}, s_{x,2}$ are strings.

It is easy to show the following class has measure zero.

$$\{X : L^X \text{ is } 2\text{tt}-\text{reducible to } X \text{ via } f\}$$

For each forcing condition $S$, there exists strings $x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}, x^{(6)}$ and a forcing condition $T$ such that

(1) $\text{dom} T = \text{dom} S \cup \{x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}, x^{(6)}\}$, and

(2) for any oracle $X$ extending $T$, it holds that $L^X$ is not 2tt-reducible to $X$ via $f$.

Therefore, the class $\{X : L^X \text{ is } 2\text{tt}-\text{reducible to } X \text{ via } f\}$ has measure zero. $\square$

4 \text{ (log } n)^{O(1)\text{-question}} \text{ tt-reduction}

Theorem 2 The Lebesgue measure of the following set is zero.

$$\{X : 1\text{TAUT}^X \leq_{(\log n)^{O(1)}}^{\text{tt}} X\}$$

In other words, one-query jump hypothesis for $\text{(log } n)^{O(1)\text{-tt-reduction}}$ (without polynomial-time bound) holds.

5 \text{ Lower and upper bounds to forcing complexity}

Theorem 3 Let $D_{\text{log}}$ be the class of all oracles $D$ such that there exists a positive integer $c$ (c may depend on D) of the following property. For any $F \in 1\text{TAUT}^D$, there exists a forcing condition $S \subseteq D$ such that $S$ forces $F$ to be a tautology and

$$|\text{dom } S| \leq (\log |F|)^c.$$ 

Then $D_{\text{log}}$ has measure zero.

Question: Is $D_{\text{log}}$ empty?

Theorem 4 Let $D_{\text{quad}}$ be the class of all oracles $D$ such that there exists a positive integer $c$ (c may depend on $D$) of the following property. For any $F \in 1\text{TAUT}^D$, there exists a forcing condition $S \subseteq D$ such that $S$ forces $F$ to be a tautology and

$$|\text{dom } S| \leq c|F|^2 + c,$$

where $|F|$ denotes the length of the binary code of $F$.

Then $D_{\text{quad}}$ has measure one.
**Question:** Let $D_{\text{linear}}$ be the class defined similarly to $D_{\text{quad}}$ by using a linear formula $c|F| + c$ instead of a quadratic $c|F|^2 + c$. Then, is $D_{\text{linear}}$ empty? If non-empty, does it have positive measure?

**References**


