数理解析研究所講究録 1442 巻 2005 年 42-47

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

Masahiro Kumabe[1)], Toshio Suzuki[2)*], Takeshi Yamazaki[3)]
1): University of the Air,
31-1, Ōoka, Minami-ku, Yokohama 232-0061, Japan
kumabe@u-air.ac.jp
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

放送大学 隈部正博, 大阪府立大学 理学部 鈴木登志雄, 山崎 武

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.

*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 forumla* 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, ξ^3 in the above formula is a query symbol. For a given oracle A, a function A^3 is defined as follows, where λ is the empty string, and the query symbol ξ^3 is interpreted as the function A^3.

$$\begin{array}{llll} A^3(000) = A(\lambda), & A^3(001) = A(0), & A^3(010) = A(1), & A^3(011) = A(00), \\ A^3(100) = A(01), & A^3(101) = A(10), & A^3(110) = A(11), & A^3(111) = A(000). \end{array}$$

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

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

For each n, an n-ary Boolean function A^n is defined in the same way, and an interpretation of the query symbol ξ^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 $1\mathrm{TAUT}^A$.

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

One-query-jump hypothesis for $\leq_\alpha$: The class $\{X : 1\mathrm{TAUT}^X \leq_\alpha X\}$ 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 $\neq$ NP."

And, in [Su02], it is shown that the one query-jump hypothesis for p-tt reduction implies "P $\neq$ 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 23, 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 *Sūrikaisekikenkyūsho 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 $\mathbb{N}$ 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*

$$\{X : 1\mathrm{TAUT}^X \leq_{\mathrm{btt}} X\}$$

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 $L^X \leq_m^p 1\mathrm{TAUT}^X$.

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 φ_x is a function from $\{0,1\}^2$ to $\{0,1\}$, and $s_{x,1}, s_{x,2}$ are strings.

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

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

For each forcing condition S, there exists strings $x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}, x^{(5)}$ and a forcing condition T such that

(1) $\operatorname{dom} T = \operatorname{dom} S \cup \{x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}, x^{(5)}\}$, and

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

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

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

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

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

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

5 Lower and upper bounds to forcing complexity

Theorem 3 *Let $\mathcal{D}_{\log}$ 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 $F \in 1\mathrm{TAUT}^D$, there exists a forcing condition $S \sqsubseteq D$ such that S forces F to be a tautology and*

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

Then $\mathcal{D}_{\log}$ has measure zero.

Question: Is $\mathcal{D}_{\log}$ empty ?

Theorem 4 *Let $\mathcal{D}_{\mathrm{quad}}$ 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 $F \in 1\mathrm{TAUT}^D$, there exists a forcing condition $S \sqsubseteq D$ such that S forces F to be a tautology and*

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

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

Then $\mathcal{D}_{\mathrm{quad}}$ has measure one.

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

References

[Am86] Ambos-Spies, K.: Randomness, relativizations, and polynomial reducibilities. In: *Structure in Complexity Theory*, Lect. Notes Comput. Sci. **223** (A. L. Selman, Eds.), pp.23-34, Springer, Berlin, 1986.

[AM97] Ambos-Spies, K., Mayordomo, E.: Resource-bounded measure and randomness. In: *Complexity, logic, and recursion theory*, Lecture Notes in Pure and Applied Mathematics **187** (A. Sorbi, Eds.), pp.1-47, Marcel Dekker, New York, 1997.

[BDG88] Balcázar, J. L., Díaz, J., Gabarró, J.: *Structural complexity I.* Springer, Berlin, 1988.

[BG81] Bennett, C. H., Gill, J.: Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq$ co-NP^A with probability 1. *SIAM J. Comput.*, **10** (1981), pp. 96-113.

[Do92] Dowd, M.: Generic oracles, uniform machines, and codes. *Information and Computation*, **96** (1992), pp. 65-76.

[KS05] Kawanishi, A. and Suzuki, T.: Random extraction from hand-drawing curves and its semantics (in Japanese). *Sūrikaisekikenkyūsho Kōkyūroku*, this volume.

[LLS75] Ladner, R. E., Lynch, N. A., Selman, A. L.: A comparison of polynomial time reducibilities. *Theoret. Comput. Sci.*, **1** (1975), pp.103-123.

[Su98] Suzuki, T.: Recognizing tautology by a deterministic algorithm whose while-loop's execution time is bounded by forcing. *Kobe Journal of Mathematics*, **15** (1998), pp. 91-102.

[Su99] Suzuki, T.: Computational complexity of Boolean formulas with query symbols. Doctoral dissertation (1999), Institute of Mathematics, University of Tsukuba, Tsukuba-City, Japan.

[Su00] Suzuki, T.: Complexity of the r-query tautologies in the presence of a generic oracle. *Notre Dame J. Formal Logic*, **41** (2000), pp. 142-151.

[Su01] Suzuki, T.: Forcing complexity: minimum sizes of forcing conditions. *Notre Dame J. Formal Logic*, **42** (2001), pp. 117-120.

[Su02] Suzuki, T.: Degrees of Dowd-type generic oracles. *Inform. and Comput.*, **176** (2002), pp. 66-87.

[Su05] Suzuki, T.: Bounded truth table does not reduce the one-query tautologies to a random oracle. *Archive for Mathematical Logic*, to appear.