Computational Complexity of Boolean Formulas with Query Symbols

(クエリー記号付きブール式の計算複雑さ)

論文概要

Toshio SUZUKI

(鈴木 登志雄)

An abstract of
a dissertation submitted to the Doctoral Program
in Mathematics, the University of Tsukuba
in partial fulfillment of the requirements for the
degree of Doctor of Philosophy (Science)

January, 1999

各種の数学的対象に対する計算複雑さの尺度は、これまで様々な研究者によって提唱されてきた。例えば、多項式時間 Turing 次数、Kolmogorov 計算量、回路計算量など。にもかかわらず、計算複雑さについて、いまだに性質がよく知られていない数学的対象は、数多い。

Cohen が強制法（forcing）によって連続体仮説の独立性証明をした直後、Feferman [5] は算術的強制法を導入した。Hinman [6] の後を受けて、1970 年代以降、算術的強制法は帰納的関数論において発展。更に 1980 年代以降、算術的強制法とその変種は $P =?NP$ 問題の研究に応用されるに至った。代表例は Ambos-Spies et al. [1]、Poizat [8]、Blum and Impagliazzo [3]、Dowd [4] などである。

本論文では、Dowd [4] と Poizat [8] の generic oracles の手法を発展させ、フォーシング計算量の概念を導入する。フォーシング計算量とは、与えられた算術的述語を強制する強制条件の最小サイズを表す。そして、本論文ではフォーシング計算量の概念を用いて、A が「多数派」のオラクルである場合に対して $coNP[A]$ の内部構造を調べる。特に、$TAUT[A]$ と $rTAUT[A]$ の計算複雑さを研究する：これらはクエリー記号付きブール式の集合である。「多数派」の数学的な定式化としては、確率的な定式化（Cantor 空間において、ルベーグ測度 1 の集合を「多数派」とみなす）と位相的な定式化（comeager な集合を「多数派」とみなす）の二つの立場がある。なお、本論文は、後述する参考文献のうち、特に [9]、[10]、[11] に補足を加え、再構成したものである。

• 基本的な概念 •

オラクル・テューリング機械（oracle Turing machine）とは、外部情報を利用できるアルゴリズムのことであり、おおまかに言うと、プログラマーに以下のような形の制御文の使用を許すことによって得られるものである。

---

if u belongs to the oracle /* ⇐ この行は「クエリー」と呼ばれる。 */
　　then ... ; **else** ... ;
end-if　　/* u はビット列。 */

オラクル・テューリング機械の計算に先立って、ビット列の集合が固定される。この集合をオラクル（oracle）と呼ぶ。ビット列全体の集合を $\{0,1\}^*$ で表す。オラクルをその特性関数と同一視して $\{0,1\}^*$ から $\{0,1\}$ への関数をオラクルと言うことにする。テューリング機械が recursive functions を計算するのと同様に、オラクル・テューリング機械は、与えられたオラクル A に関して recursive な functions を計算する。さて、[4] に従って、n 個（$n \geq 1$）の命題変数に対する演算子としてξ^n というクエリー記号を導入しよう。$\xi^n(q_1, \ldots, q_n)$ のおおまかな意味は、「ビット列 $q_1 \cdots q_n$ がオラクルに属す」ということである。定義をもう少し詳しく述べよう。各オラクル A に対し、n-変数ブール関数 A^n を導入する。話を簡単にするため、ここでは A^3 の意味を説明しよう。まず、長さ 3 のビット列全体の集合 $\{0,1\}^3$ と $\{0,1\}^*$ に、（短さ優先の）辞書式順序を導入する。ここで λ は長さゼロのビット列を表す。

$$\{0,1\}^3 : \quad 000, \quad 001, \quad 010, \quad 011, \quad 100, \quad 101, \quad 110, \quad 111.$$
$$\{0,1\}^* : \quad \lambda, \quad 0, \quad 1, \quad 00, \quad 01, \quad 10, \quad 11, \quad 000, \quad \ldots$$

いま、$\{0,1\}^*$ の最初の $2^3=8$ 個の元の集合 $\{\lambda,\ldots,000\}$ を $\mathrm{Str}(3)$ で表そう。以下の図式が可換となるように関数 A^3 を定める。但し、$\simeq$ は辞書式順序に関する順序同型を表す。

$$\begin{array}{ccc} & & A^3 \\ \{0,1\}^3 & \longrightarrow & \{0,1\} \\ \simeq \big\downarrow & & \nearrow A \restriction \mathrm{Str}(3) \\ \mathrm{Str}(3) & & \end{array}$$

オラクル A が与えられたとき、$\xi^3(q_1,q_2,q_3)$ を $A^3(q_1q_2q_3)$ として解釈する。この一見遠回りな定義をする理由は、(1) こう定義すると、$\xi^n(q_1,\ldots,q_n)=\xi^{n+1}(0,q_1,\ldots,q_n)$ となって ξ^n の情報が ξ^{n+1} に引き継がれること、(2) 命題論理の演算子の引数は、ある特定の値でなければならないこと、の 2 点にある。そして、通常の命題論理にクエリー記号の集合 $\{\xi^n : n=1,2,3,\ldots\}$ を付け加えた論理体系を、the relativized propositional calculus と言う。この論理体系において、オラクル A に関する恒真式全体の集合を、$TAUT[A]$ で表す。また、クエリー記号をちょうど r個持つ式を r-query formula と言う（r は自然数）。$TAUT[A]$ の元で、しかも r-query formula になっているもの全体の集合を $rTAUT[A]$ で表し、この集合の元を A に関する r-query tautologies と言う。

• 方法論上の特色 •

(1) フォーシング計算量（forcing complexity）：算術的述語の情報圧縮可能性の尺度。

あるオラクルの定義域を、ビット列のある有限集合に制限して得られる関数を、強制条件（forcing condition）という。いま、$X(\sim)$ はオラクルへの所属を表す一項述語記号、y はビット列を表す変数、そして$\varphi(X)(y)$ は finitely testable （= test fini、[8] を参照）な算術的述語とする。ビット列 u に対し、「S が $\varphi(X)(u)$ を強制（force）する」とは、S を部分関数とする任意のオラクル A に対して、$\varphi(A)(u)$ が成り立つこと、と定義する。さて、A をオラクル、$f:\mathbb{N}\to\mathbb{N}$ を関数とする。任意の自然数 n に対し、$f(n)$ が以下の条件を満たす自然数 k の最小値に等しいとき、f を「φ の A に関するフォーシング計算量（forcing complexity）」と呼んで、自然数 n に対して $f(n)$ の値を

$$\mathrm{FC}(\varphi(X)(y),A,n)$$

で表す：「長さが n のビット列 u で、$\varphi(A)(u)$ が成り立つ任意のものに対し、A（の特性関数）の部分関数 S で（定義域の）サイズが高々 k のものが存在して、S が $\varphi(X)(u)$ を強制する。」本論文では、フォーシング計算量をテューリング機械の計算複雑さの研究に応用して、後に述べる結果 (a) と (b) を証明する。

(2) 強制法の決定性アルゴリズムへの応用。

Dowd [4, Theorem 11] は強制法を非決定性テューリング機械の制御に応用してみせた。本論文では更に一歩踏み込んで、強制法を決定性テューリング機械の while-loop の実行回数

の制御に応用して、後に述べる結果 (c) を証明し、r-query tautology が、計算量理論の根本問題とどのように関係しているのかを明らかにする。

• 主要な結果 •

(a) 先行する結果に対する明快な別証明。

以下の性質を持つ coNP[X]-述語 $\varphi(X)(y)$ の一例を具体的に構成する。任意のオラクル A と任意の自然数 n に対して、フォーシング計算量の下界が以下のように与えられる：

$$\mathrm{FC}(\varphi(X)(y), A, n) \geq \frac{2^{n-1} - n + 1}{n}.$$

この例を用い、t-generic oracle の非存在という Dowd の結果 [4, Theorem 7] に対し簡潔な新しい証明を提示する。また、フォーシング計算量に関するオラクルの階層を考察することで、(Dowd の意味での) r-generic oracles 全体の集合がルベーグ測度 1 だという Dowd の結果 [4, Theorem 10] に対し明快な証明を与える。

(b) Cohen-Feferman generic oracles についての結果。

オラクルの集合 $\{X : P[X] \neq NP[X]\}$ が comeager であることは、古典的な結果である (Mehlhorn [7]、および既述の [8]、[3]、[4])。本論文では、与えられた算術的述語に関して小さな（高々 n の多項式の）フォーシング計算量を持つオラクルの存在が Cohen-Feferman generic oracles の振る舞いにどのような影響を与えるかを考察することにより、上記の古典的結果を改良し、以下のオラクルの集合が comeager であることを示す。但し、ここで r は任意の正の整数である。

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

(c) 強制法による while-loop の制御。

オラクルの集合 $\{X : TAUT[X] \notin P[X]\}$ がルベーグ測度 1 であることも、よく知られている (Bennet and Gill [2])。では、$TAUT[X]$ を $rTAUT[X]$ で置き換えても同様なことが言えるだろうか？但し、r は正の整数である。本論文では、while-loop の実行回数が強制法によって制御されるような決定性アルゴリズムを構成することにより、A が Dowd の意味での r-generic oracle であるとき、以下の関係式が成り立つことを示す。

$$rTAUT[A] \equiv_T^P TAUT \oplus A.$$

その結果、以下の二つの主張が同値であることを証明する（R は「$P \subseteq R \subseteq NP$」となる、よく知られた計算量クラス)。

(1) $\{X : rTAUT[X] \notin P[X]\}$ がルベーグ測度 1 である。

(2) $R \neq NP$.

参考文献

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

[3] 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.

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

[5] Feferman, S., "Some applications of the notions of forcing and generic sets," *Fund. Math.*, vol. 56 (1965), pp. 325-345.

[6] 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.

[7] 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.

[8] Poizat, B., "$Q = NQ$?," *J. Symbolic Logic*, vol. 51 (1986), pp. 22-32.

[9] Suzuki, T., "Complexity of the r-query tautologies: in presence of a generic oracle," *Notre Dame J. Formal Logic*, *to appear.*

[10] Suzuki, T., "Recognizing tautology by a deterministic algorithm whose while-loop's execution time is bounded by forcing," *Kobe Journal of Mathematics*, *to appear.*

[11] Suzuki, T., ' Forcing complexity: supplement to "complexity of the r-query tautologies," ' *preprint.*