日本数学会 1999 年度 秋季総合分科会 於 広島大学 ・数学基礎論分科会 特別講演

クエリー記号付きブール式のフォーシング計算量

鈴木 登志雄・阪府大 総合科

(Toshio Suzuki, Dept. of Math. and Info. Sci., Osaka Prefecture Univ.)

suzuki@mi.cias.osakafu-u.ac.jp

1999 年 9 月

概要: M. Dowd は 1992 年の論文で, クエリー記号付きブール式の計算複雑さと強制条件の最小サイズについて先駆的な研究を行なった. 本稿では Dowd の論文のデバッグと拡張についての, 筆者の最近４年間の研究を紹介する. 特に, 以下の話題をとりあげる. (1) Dowd 型ジェネリック・オラクルの存在に関する議論のデバッグ; (2) ジェネリック・オラクルとランダム・オラクルに対する coNP$[A]$ の内部構造; (3) 算術的述語を媒介にした, 強制条件の最小サイズと pT-degree との間の密接な関係; (4) オラクルにクエリー数限定恒真式の集合を対応させる作用素の基本性質; (5) 帰納的集合の階層における Dowd 型ジェネリック・オラクルの分布.

Mathematics Subject Classification: 68Q15; 03D15.

1 序

クエリー記号付きブール式の体系を the Relativized Propositional Calculus と呼ぶ. 本稿ではこれを RPC と呼ぶことにする. RPC の計算複雑さについての本格的な研究は Dowd [Do 92] の section 3 と 4 に始まる. 与えられた RPC の式を強制する強制条件の最小サイズについての法則性に着眼することによって, 本格的な研究が始まったのである. [Do 92] は決して読みやすいとは言えず, 誤りもある. 最初の本格的論文が誤りを含んでいたことは, RPC の研究にとって厄介なことだった.

算術的強制法の計算量理論への応用は数多いが, その中で [Do 92] は (少なくとも現時点では) 異彩を放つ文献である. 算術的強制法そのもの, あるいは, Ambos-Spies 式の資源限定強制法 (resource-bounded genericity) を使う研究の方が長い歴史を持ち, 多くの文献で論じられている. なかでも Blum and Impagliazzo [BI 87] は, ジェネリック・オラクルで相対化された計算量クラスの分離問題と, 相対化されない計算量クラスの分離問題との密接な関係を指摘した. なお, **本稿でジェネリック・オラクルと言えば, 算術的強制法の本来のジェネリック・オラクルを指す**. n-generic oracle **についても同様である. 誤解を避けるため**, Dowd **の** t-generic oracle **と** r-generic oracle **は, それぞれ** tautology-generic oracle, r-Dowd oracle **と呼ぶことにする**. さて, 算術的強制法そのものを使う諸文献の中でも, 特に Poizat [Po86] は, 相対化された計算量クラスを (2 階の) 算術的述語と結び付けるやりかたの巧みさで知られる. その主定理は, ふたつの相対化された計算量クラスがひとつのオラクルに関して分離できれば, (ある条件の下で) それらは任意のジェネリック・オラクルに関して分離できるというものである. Cook et al. [CIY 97] は, [Po86] をいっそう洗練された理論へと拡張

した. [CIY 97] の主定理は, (ある条件をみたす) ふたつの 2 階の計算量クラスが分離できる必要十分条件は, 対応する相対化された計算量クラスがジェネリック・オラクルに関して分離できることだというものである.

筆者は 1996 年以降, Dowd の先駆的なアイデアを体系的な研究として育てあげることを目指して, RPC の研究を実行している. 特に, [Do 92] と [Po 86] の議論を融合し, 与えられた (2 階の) 算術的述語を強制する強制条件の最小サイズを計算コストの問題として考察した. この最小サイズを, フォーシング計算量 (forcing complexity) と呼ぶ. その結果, [Do 92] のデバッグと拡張が同時並行的に進んだのである. 結果的に, [Po 86] を, [CIY 97] とは違った方向へ発展させることにもなり, また, [Am 96] とは違うタイプの資源限定強制法について研究を進めることにもなった.

以下, 本稿の概略を述べる. § 2 では定義と用語の説明をする. 特に基本的で重要な概念については, 今, ここであらましを述べておこう. まず, 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する. $\xi^{\mathsf{n}}(q_1, \ldots, q_{\mathsf{n}})$ のおおまかな意味は, 「ビット列 $q_1 \cdots q_{\mathsf{n}}$ がオラクルに属す」ということである. RPC は, 通常の命題論理にクエリー記号の集合 $\{\xi^{\mathsf{n}} : n \in \mathsf{N}\}$ を加えたものである. 通常の恒真式全体の集合を TAUT で表し, 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, ちょうどひとつのクエリー記号を持つ式を one-query formula と呼ぶ. One-query formula であって, なおかつ TAUT$[A]$ の元になっているものは A に関する one-query tautology と呼ばれる. A に関する one-query tautology 全体の集合を 1TAUT$[A]$ で表す. 同様にして, 自然数 r に対して r-query formula, オラクル A に関する r-query tautology, rTAUT$[A]$ の概念を導入する. オラクル A が tautology-generic oracle であるとは, ある多項式 p があって, 任意の $F \in$ TAUT$[A]$ に対し, A の (特性関数の) 有限部分 S があって, 以下の条件が成り立つことを言う: 「まず, S は F が恒真式であることを強制し, なおかつ, S の (定義域の) サイズは高々 $p(|F|)$ である」. また, 自然数 r に対し, オラクル A が r-Dowd oracle であるとは, tautology-generic oracle の定義で TAUT$[A]$ のところを rTAUT$[A]$ で置き換えた条件が成り立つことを言う.

本稿 § 3 では「tautology-generic oracle の非存在」に関するデバッグについて述べる. Dowd が tautology-generic oracle の非存在を証明するにあたって暗に仮定している前提に対し, 筆者は [Su 99b] において反例を与えた. 更に [Su 99c] において (2 階の) 算術的述語のフォーシング計算量を用いて, Dowd とは異なるやりかたで tautology-generic oracle の非存在を証明した.

次に, 「r-Dowd oracle の存在」に関するデバッグについて (本稿 § 4). Dowd 自身による r-Dowd oracle の存在証明は, 最小強制条件の存在の一意性に全面的に依存している. ここで最小強制条件というのは, 与えられたブール式を強制する強制条件でサイズ最小なもののことである. [Su 99c] で筆者は, $r \geq 2$ の場合には最小強制条件の存在の一意性が破れることに注意した. そして, 同じ論文の中で筆者は, フォーシング計算量に関するオラクルの階層の崩壊の例を示した. この階層の崩壊の例によって Dowd の議論を修正・補強し, 「r-Dowd oracle 全体のクラスが Cator 空間においてルベーグ測度 1 を持つ」という Dowd の結果を正当化した.

次に, [Do 92] の拡張について述べる. まず, coNP$[A]$ の内部構造について. rTAUT$[A]$ の計算量の研究は, coNP$[A]$ の内部構造の研究に他ならない. 1996 年から 1998 年にかけて, 筆者は A が「多数

派」のオラクルである場合に対して TAUT$[A]$ と rTAUT$[A]$ の計算量についての研究を進めた. より詳しくは, 以下のとおり. 「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) のふたつの立場がある. まず, 任意のオラクル A に対して以下の自明な関係が成り立つことに注意されたい.

Diagram 1. (coNP$[A]$ の内部構造)

$$\mathrm{TAUT} \oplus A \leq^{\mathsf{P}}_{\mathsf{T}} 1\mathrm{TAUT}[A] \leq^{\mathsf{P}}_{\mathsf{T}} 2\mathrm{TAUT}[A] \leq^{\mathsf{P}}_{\mathsf{T}} r\mathrm{TAUT}[A] \leq^{\mathsf{P}}_{\mathsf{T}} \mathrm{TAUT}[A]$$

では, A がジェネリック・オラクルのときと A がランダム・オラクルのとき, それぞれの場合, Diagram 1 がどのようになるか？言い換えると, どこが真の不等号になり, どこが同値関係になるか？この問題について, Dowd 自身は [Do 92] で特に言及していない. 但し, G がジェネリック・オラクルのとき $G <^{\mathsf{P}}_{\mathsf{T}}$ TAUT$[G]$ となることは, よく知られている ([Po 86], [Do 92], [BI 87]. Mehlehorn [Me 73] も参照されたし). また, ランダム・オラクル A に対して確率 1 を以って $A <^{\mathsf{P}}_{\mathsf{T}}$ TAUT$[A]$ が成り立つことも古典的な結果である (Bennet and Gill [BG 81]).

A がジェネリック・オラクルの場合の Diagram 1 の研究においては, [Su 99b] の主定理が鍵となる. その定理は, 算術的述語を媒介にしたフォーシング計算量と pT-degree との間の関係を示すものであり, [Po 86] と [Do 92] の手法を融合したものである. その内容をおおまかに言えば, 以下のとおり:

「いま, 次のような関係が成り立つとする.

$$\{A : A \text{ はオラクルで, 述語 } \varphi(A)(y) \text{ に関するフォーシング計算量が小さい }\}$$
$$\% \ \{A : A \text{ はオラクルで, 述語 } \psi(A)(y) \text{ に関するフォーシング計算量が小さい }\}$$

但し, ここで『小さい』というのは『ビット列 y の長さ (桁数) の高々多項式』という意味である. このとき, (ある条件の下で) 任意のジェネリック・オラクル G に対して

$$\{u \in \{0,1\}^* : \varphi(G)(u)\} \ <^{\mathsf{P}}_{\mathsf{T}} \ \{u \in \{0,1\}^* : \psi(G)(u)\}$$

という関係が成り立つ. すなわち, % に対しては, 向きが反対の $<^{\mathsf{P}}_{\mathsf{T}}$ が対応する.」

上記定理の詳しい内容は後で述べる. Diagram 1 で A がジェネリック・オラクルである場合については現在も研究を続行中であるが, 上記の定理を用い, [Su 99b], [Su 99c], [Su 99d] において, かなりの程度明らかにすることができた (本稿 § 5).

また, 筆者は [Su 98] において, 最小強制条件を生成する決定性アルゴリズムの while-loop の実行回数を吟味した. その結果, A がランダム・オラクルである場合には Diagram 1 が崩壊することを示した. すなわち, 一番右の TAUT$[A]$ を除き, これらの言語は皆, 同じ pT-degree を持つ (本稿 § 6). また, その証明の過程で, Dowd 型ジェネリック・オラクル (one-Dowd oracle) に対して one-query operator が果たす役割と, one-generic oracle に対して jump-operator が果たす役割との間にある種の類似性があることを見出した. ここで one-query operator とは, オラクル A に言語 1TAUT[A] を対応させる作用素のことである. One-query operator と jump-operator の間に更なる類似性があるか？を追求した結果, ランダム・オラクルに対する 1TAUT[A] のふるまいと, 相対化されない計算量クラスとの間のいくつかの関係を [Su 98] および [Su 99d] において示した (本稿 § 7).

筆者は 1999 年に入ってからも RPC とフォーシング計算量についての研究を続行しており, [Do 92] の新たなデバッグも行なった. 特に, 算術的階層および帰納的集合の階層における one-Dowd oracle の分布状況についての研究を行なった. 計算機科学にとっては, 帰納的集合はジェネリック・オラクル以上に興味深い対象である. Dowd は one-Dowd oracle は帰納的可算ではありえない, と述べている. しかし, これは誤りである. 筆者は [Su 99d] において, 原始帰納的な one-Dowd oracle の実例を構成した. 更に, テューリング次数については, 「任意のテューリング次数は one-Dowd oracle を含む」という optimal な結果を示した (本稿 § 8).

◇ ◇ ◇

歴史的背景と文献案内: 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 [Fe 65] は算術的強制法を導入した. Hinman [Hi 69] 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. Jockusch [Jo 80] は算術的強制法全般に関する基本文献である.

ジェネリック・オラクルが計算コストに関係するのには必然的な背景がある. Baker et al. [BGS 75] における $\mathrm{P}[A] \neq \mathrm{NP}[A]$ となるオラクル A の構成の要点は, finite extension method (injury のない, priority argument の最も初等的な形) である. そして, ある性質を持つ集合を finite extension method で作れるならば, それと大体同じ性質を持つジェネリック・オラクルが存在する. このあたりの事情についての解説は, [Am 96] の序章に見られる. ジェネリック・オラクルと計算量理論の関係全般についての総合報告としては, [田中 96] がある. なお, [Po 86] の主定理の相対化については Tanaka and Kudoh [TK 97] を参照.

[Am 96] で扱われる各種の資源限定ジェネリック・オラクルは, finite extension starategy の時間計算量に制約を設け, それに対応する資源限定版の dense sets を考察することによって導入される. 他方, tautology-generic oracle および r-Dowd oracle は, すでに見たとおり, 強制条件の最小サイズに関する空間的制約によって定義される.

なお, 筆者の学位論文 [Su 99a] は, 主に [Su 98], [Su 99b], [Su 99c] の内容に基づく. 本稿の § 7 までの内容は**定理 3** (Fragility of 2-Dowd property) を除き, [Su 99a] で述べた事柄である.

2 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 /* $\Leftarrow$ 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. また, 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.

さて, 先ほど導入したクエリー記号 ξ^n の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.

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

いま, $\{0,1\}^*$ の最初の 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.

$$
\begin{tikzcd}
\{0,1\}^3 \arrow[r, "A^3"] \arrow[d, "\simeq"'] & \{0,1\} \\
\mathrm{Str}(3) \arrow[ur, "A \restriction \mathrm{Str}(3)"'] &
\end{tikzcd}
$$

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.

なお, 辞書式順序で $(k+1)$ 番目のビット列を $z(k)$ で表すことがある. たとえば, $\lambda = z(0)$ となる. ここで自然数 k の n ビット 2 進表記と k 自身とを同一視すれば, 上記の A^n の定義を以下のごとく簡潔に言い表すことができる. もっとも, これは少々粗雑な記法であるが.

$$A^n(k) = A(z(k)).$$

3 Tautology-generic oracle の非存在

NP $=?$ coNP 問題に関する以下の定理は, [Do 92] の主定理である.

Dowd の Theorem 8 [Do 92, Theorem 8] Suppose that $M[\sim]$ is a nondeterministic oracle machine such that for every oracle A, we have $\mathrm{Lang}(M[A]) = \mathrm{TAUT}[A]$. Then for no A, the language TAUT$[A]$ is accepted in polynomial time. ¤

この定理を示すため, Dowd は以下の補題を用いた.

Dowd の Lemma 7 [Do 92, Lemma 7] Tautology-generic oracles do not exist. ¤

そして, Dowd の Lemma 7 自体は以下の補題を用いて証明されたことになっている. 彼の表現 M^X は我々の表記で言えば $M[X]$ のことである. 同様に, $\mathcal{N}$ は $\{0,1\}^*$ のことである. オラクル A が sparse であるとは, ある多項式 p があって, 各自然数 n に対し, $\mathrm{Card}(A \cap \{0,1\}^{\le n}) \le p(n)$ となることを言う.

引用 1 [Do 92, 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 $\le n$ 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 nth 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. ¤

注意深い読者はとまどうかもしれない. なぜなら, 以下の主張は間違いだからである. その理由は, すぐ次に掲げた反例による.

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

例 1 [Su 99b] For each natural number $n \ge 2$, let $k(n)$ be the largest natural number k such that $2^{k+1} - 1 \le n$. For each n, let $D_n = \{0,1\}^{\le k(n)}$. Let $D = \bigcup\{D_n : n \text{ is a power of } 2\}$. Then, for each $n \ge 2$, D_n is a subset of $\{0,1\}^{\le n}$ and $\mathrm{Card}(D_n)$ is at most n. However, we have $D = \{0,1\}^*$. ¤

筆者は [Su 99b] で展開した議論を改良して, [Su 99c] において, 以下のごとく Dowd の Lemma 7 の証明を与えた. いま, y はビット列を表す変数, X は与えられたオラクルへの所属を表す 1 項述語

記号とする. $\varphi(X)(y)$ を算術的述語とする. 更に, $\varphi(X)(y)$ は finitely testable (= test fini, [Po 86] を参照) だとする. 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, $f : \mathsf{N} \to \mathsf{N}$ 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 の有限部分 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. 」

定理 1 [Su 99c] There exists a finitely testable arithemtical predicate $\varphi(X)(y)$ such that the following two requirements are satisfied.

1. $\varphi(X)(y)$ is uniformly coNP$[X]$. In other words, there exists a polynomial-time computable function f such that for every oracle A and for every bit string u, we have $\varphi(A)(u)$ if and only if $f(u) \in \mathrm{TAUT}[A]$.
2. For every oracle A and for every positive integer n, a lower bound for the forcing complexity is given as follows.
$$\mathrm{FC}(\varphi(X)(y), A, n) \geq \frac{2^{\mathsf{n}-1} - n + 1}{n}.$$

¤

Dowd **の** Lemma 7 は, **定理** 1 からただちに導かれる.

4 r-Dowd oracle **の存在**

Dowd の以下の結果は, 彼の Theorem 8 と一対をなす.

Dowd の Theorem 11 [Do 92, Theorem 11] If NP = coNP then there exists a nondeterministic oracle machine $M[\sim]$ which satisfies the following two requirements.

1. For every oracle A, we have $\mathrm{Lang}(M[A]) = \mathrm{TAUT}[A]$.
2. For every positive integer r and for every r-Dowd oracle D, $M[D]$ accepts every member of $r\mathrm{TAUT}[D]$ in polynomial time. ¤

Dowd **の** Theorem 11 に関連した結果として, 彼は以下のことを示している.

Dowd の Theorem 10 [Do 92, Theorem 10] For any integer r, the class of all r-Dowd oracles has Lebesgue measure one in Cantor space. ¤

上記定理の Dowd による証明の要点は, RPC の式のうちある条件を満たすものの総数を数えることにある．その総数を数える際, 最小強制条件の存在の一意性が重要な役割を果たす．しかし, $r \geq 2$ の場合には, かかる一意性は破れてしまうのである．たとえば, 以下の 2-query formula を考えてみよう．

$$\xi^3(0,0,1) \Leftrightarrow \xi^3(1,0,0)$$

A を任意のオラクルとする． A に関して上記の式が恒真式となる必要十分条件は $A^3(001)$ と $A^3(100)$ が同じ値を持つことである．言い換えると, $A(0) = A(01)$ ということである．その共通の値が 0 でもよいし 1 でもよい．ゆえに, 上記の式を強制する最小強制条件はふたつある．一方は $S_0 := \{(0,0),(01,0)\}$, 他方は $S_1 := \{(0,1),(01,1)\}$ である．

筆者は [Su 99c] において, Dowd の Theorem 10 の証明を補強して水漏れのないものにした．それは, この定理の背後にある階層構造を調べることによって行なった．フォーシング計算量に関するオラクルの階層構造である．但し, この議論は, やや込み入った計算を要する．議論のあらましを以下に述べよう．まず, r-Dowd oracle 全体のクラスを, $r\mathrm{DO}_3$ で表すことにする．さて, $F \in r\mathrm{TAUT}[X]$ という主張を表す算術的述語を $r\mathrm{TAUT}(X)(F)$ で表そう．$r\mathrm{DO}_3$ とは, 述語 $r\mathrm{TAUT}(X)(F)$ の A に関するフォーシング計算量が高々多項式になっているようなオラクル A 全体の集合に他ならない．[Su 99c] では, $r \geq 2$ の場合に対して, disentangled r-query formula というものを導入した．これらは, r-query formula のうち, 扱いやすい特殊な形をしたものとして定義される．そこで, $r\mathrm{TAUT}(X)(F)$ の代わりに, 「F がオラクル X に関する disentangled r-query tautology である」という主張を表す算術的述語を考える．この述語に関するフォーシング計算量が高々多項式になるオラクル全体のクラスを $r\mathrm{DO}_2$ で表すことにする．さらに, $r\mathrm{DO}_2$ の定義において, 「フォーシング計算量が小さい」というところを「フォーシング計算量が小さいかどうかはともかく, 部分的フォーシング計算量が小さい」という, いっそう緩やかな条件に置き換えて得られるオラクルのクラスを, $r\mathrm{DO}_1$ で表すことにする．これらの間の自明な関係は, Diagram 2 によって与えられる．

Diagram 2. (フォーシング計算量に関する階層)

$$\begin{array}{ccccccc}
 & & 2\mathrm{DO}_1 & \supseteq & 3\mathrm{DO}_1 & \supseteq \cdots \\
 & & \text{\rotatebox{90}{$\subseteq$}} & & \text{\rotatebox{90}{$\subseteq$}} & \\
 & & 2\mathrm{DO}_2 & \supseteq & 3\mathrm{DO}_2 & \supseteq \cdots \\
 & & \text{\rotatebox{90}{$\subseteq$}} & & \text{\rotatebox{90}{$\subseteq$}} & \\
1\mathrm{DO}_3 & \supseteq & 2\mathrm{DO}_3 & \supseteq & 3\mathrm{DO}_3 & \supseteq \cdots
\end{array}$$

しかるべき条件を満たす disentangled r-query formula の数え上げを行ない, さらに RPC の式の interpolation を考察して帰納法を進めると, 以下の**定理 2** を得る．ここで interpolation の考察というのは [Do 92] に見られる議論であり, $Q \Rightarrow H$ という形の tautology のフォーシング計算量が小さ

いことを示すために, RPC の式 I をうまく選んで, $Q \Rightarrow I$ と $I \Rightarrow H$ のいずれも小さいフォーシング計算量を持つことを示すという論法を指す.

定理 2 [Su 99c] In Diagram 2, each vertical hierarchy collapses. Thus, we get Diagram 3.

Diagram 3. (フォーシング計算量に関する階層の崩壊)

$$
\begin{array}{ccccccc}
 & & 2\mathrm{DO}_1 & & 3\mathrm{DO}_1 & & \\
 & & \| & & \| & & \\
 & & 2\mathrm{DO}_2 & & 3\mathrm{DO}_2 & & \\
 & & \| & & \| & & \\
1\mathrm{DO}_3 & \supseteq & 2\mathrm{DO}_3 & \supseteq & 3\mathrm{DO}_3 & \supseteq \cdots &
\end{array}
$$

¤

ところで, disentangled r-query tautology (であることを表す算術的述語) の部分的フォーシング計算量を考える場合には, 最小強制条件 (もどき) の存在の一意性が成り立つのである. その結果, Dowd による one-Dowd oracle の存在証明とほとんど同じ議論によって, 各々の $r \geq 2$ に対し, $r\mathrm{DO}_1$ がルベーグ測度 1 であることがわかる. したがって, Dowd の Theorem 10 が成り立つことがわかる.

以下, 参考までに, disentangled r-query formula の定義と例と基本的な性質, および $r\mathrm{DO}_1$ の定義を掲げておく.

定義 1 [Su 99c] Suppose that r and n are positive integers such that we have $r \geq 2$. A triple $\delta = (t, B, f)$ is called an (r,n)-**disentangled matrix** if the following three requirements are satisfied. The set of all (r,n)-disentangled matrices is denoted by $\mathrm{DEM}(r,n)$.

1. t is a positive integer such that $\log_2 r \leq t \leq \min\{n, r(r-1)/2\}$.
2. B is a matrix of type (r,t) such that each element is 0 or 1 and such that rows are pairwise different.
3. $f : \{1, \cdots, t\} \to \{1, \ldots, n\}$ is an order preserving mapping; we shall often denote f by the sequence $\langle f(1), \ldots, f(t) \rangle$. ¤

定義 2 [Su 99c] Suppose that r is a positive integer such that $r \geq 2$.

1. Suppose n is a positive integer and $\delta = (t, B, f)$ is an (r,n)-disentangled matrix. For $i = 1, \ldots, r$, we define a set $\mathrm{Str}(n, \delta, i)$ as follows. $\mathrm{Str}(n, \delta, i)$ is the collection of all bit strings $z(m)$ such that we have $z(2^{\mathsf{n}} - 1 + m) \in \{0,1\}^{\mathsf{n}}$ and such that, letting $z(2^{\mathsf{n}} - 1 + m) = u_1 \cdots u_{\mathsf{n}}$, the bit string $u_{\mathsf{f}(1)} u_{\mathsf{f}(2)} \cdots u_{\mathsf{f}(t)}$ is identical with the ith row of the matrix B. For a given query free formula H, we define $\delta\langle r, n, H \rangle$ as follows. First, we temporarily introduce a formula F

as follows.

$$F \equiv_{\mathrm{def.}} \text{“}\Big(\bigwedge_{i=1}^{r} (a^{(i)} \Leftrightarrow \xi^{n}(q_1^{(i)}, \ldots, q_n^{(i)})) \Big) \Rightarrow H.\text{”}$$

We define $\delta\langle r, n, H\rangle$ by the following substitution, where each $b_j^{(i)}$ denotes the (i, j)-component of the matrix B.

$$\begin{aligned} \delta\langle r, n, H\rangle \equiv_{\mathrm{def.}} F[b_1^{(1)}/q_{f(1)}^{(1)}] \cdots [b_t^{(1)}/q_{f(t)}^{(1)}] \\ \cdots [b_j^{(i)}/q_{f(j)}^{(i)}] \cdots \\ [b_1^{(r)}/q_{f(1)}^{(r)}] \cdots [b_t^{(r)}/q_{f(t)}^{(r)}]. \end{aligned}$$

2. Assume that F is a relativized formula. We call F a **disentangled r-query formula** if F is of the form $\delta\langle r, n, H\rangle$, where n is a natural number, δ is an (r, n)-disentangled matrix and H is a query free formula. If F is a disentangled r-query formula and F is a tautology with respect to an oracle A, then we call F a **disentangled r-query tautology with respect to A.** ¤

例 2 (disentangled 3-query formula の例) We consieder the case where $r = 3$ and $n = 4$. Suppose H is a query free formula. Let $\delta = (t, B, f)$, where $t = 2$, $f = \langle 2, 3\rangle$ and B is the following matrix.

$$B := \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Then, $\delta\langle r, n, H\rangle$ is given as follows.

$$\begin{aligned} \Big((a^{(1)} \Leftrightarrow \xi^4(q_1^{(1)}, 1, 0, q_4^{(1)})) \wedge \\ (a^{(2)} \Leftrightarrow \xi^4(q_1^{(2)}, 0, 1, q_4^{(2)})) \wedge \\ (a^{(3)} \Leftrightarrow \xi^4(q_1^{(3)}, 1, 1, q_4^{(3)}))\Big) \Rightarrow H. \end{aligned}$$

¤

例 2 についての注: f の役割は行列 B を埋め込む列の番号を指定することにある. また, $\{0,1\}^4$ から $\{z(0), \ldots, z(2^4 - 1)\}$ への標準的な順序同型 (つまり, 自然数 k の 4 ビット 2 進表記を $z(k)$ に対応させる対応) による $\{a10d : a, d \in \{0,1\}\}$ の像が $\mathrm{Str}(4, \delta, 1)$ である. 同様に, $*01*$ たちの像が $\mathrm{Str}(4, \delta, 2)$, $*11*$ たちの像が $\mathrm{Str}(4, \delta, 3)$ である. $\delta\langle r, n, H\rangle$ においては, みっつのクエリーのそれぞれが「データ領域の相異なるパーティション ($\mathrm{Str}(4, \delta, 1)$, $\mathrm{Str}(4, \delta, 2)$, $\mathrm{Str}(4, \delta, 3)$) へアクセスすることが保証されている」のがポイントである. ¤

さきほど, disentangled r-query tautology (であることを表す算術的述語) の部分的フォーシング計算量を考える場合には, 最小強制条件 (もどき) の存在の一意性が成り立つと述べた. それは, 以下の事実を指す.

修正版 Dowd の Lemma 9 [Su 99c] (see also [Do 92, Lemma 9]) Suppose that r and n are positive integers such that $r \geq 2$. Suppose $\delta \in \mathrm{DEM}(r,n)$ and suppose that H is a query free formula and E is a set of bit strings satisfying the following inclusion.

$$\mathrm{Str}(n,\delta,2)+\cdots+\mathrm{Str}(n,\delta,r) \subseteq E \subseteq \mathrm{Str}(n) \setminus \mathrm{Str}(n,\delta,1).$$

Let A_0 be a forcing condition whose domain is E. Assume that $F \equiv_{\mathrm{def.}} \delta\langle r,n,H\rangle$ is a disentangled r-query tautology with respect to some oracle extending A_0. Then, there exists a forcing condition S_1 such that $\mathrm{dom}(S_1) \subseteq \mathrm{Str}(n,\delta,1)$ and such that for any forcing condition T_1 whose domain is a subset of $\mathrm{Str}(n,\delta,1)$, the following two assertions are equivalent.

1. $S_1 \sqsubseteq T_1$.
2. $T_1 + A_0$ forces F.

Such a forcing condition S_1 is uniquely determined only by the disentangled r-query formula F and the forcing condition A_0. And, for any oracle A extending A_0, if F is a tautology with respect to A then A is an extension of S_1. (Because, letting $T_1 \equiv_{\mathrm{def.}} A \upharpoonright \mathrm{Str}(n,\delta,1)$, $T_1 + A_0$ forces F.) $\square$

「オラクル A が $r\mathrm{DO}_1$ に属す」とは, 以下の条件が成り立つこと, と定める: A に関する disentangled r-query tautology であるような任意の $F :\equiv \delta\langle r,n,H\rangle$ と上の補題に言う条件を満たす任意の集合 E に対して, 上の補題における S_1 で (F の長さの) 多項式サイズのものが存在する; 但し, ここで A_0 としては $A \upharpoonright E$ をとるものとする.

5 coNP[G] の内部構造: G がジェネリック・オラクルの場合

再び Diagram 3 について考えよう. さきほどは縦の階層が崩壊することを見た. 残るは横の階層のみである. もはや, 右下添え字を省略して, 各レベルを $r\mathrm{DO}$ ($r = 1,2,3\ldots$) と書くことにする. また, tautology-generic oracle 全体の集合を $t\,\mathrm{DO}$ と書き, $\mathcal{C}$ で Cantor 空間を表そう. Dowd の Lemma 7 と Dowd の Theorem 10 により, 任意の自然数 r に対して $\mathcal{C} \supsetneq r\mathrm{DO} \supsetneq t\,\mathrm{DO} = \emptyset$ という関係が成り立つ. Diagram 3 の第 1 レベルと第 2 レベルに関連して, 以下の結果がある.

定理 3 [Su99d] (Fragility of 2-Dowd property) For every one-Dowd oracle D, there exists a one-Dowd oracle E such that E is polynomial-time one-one equivalent to D and E is not 2-Dowd. $\square$

すなわち, p-time one-one degree と one-Dowd という性質を保ったまま, 2-Dowd という性質だけを壊すことができるのである. そこで, r を 3 以上の任意の自然数とすると, 以下を得る.

Diagram 4. (フォーシング計算量に関する階層の分離)

$$\mathcal{C} \supsetneq 1\mathrm{DO} \supsetneq 2\mathrm{DO} \supseteq r\mathrm{DO} \supsetneq t\,\mathrm{DO} = \emptyset$$

Diagram 4 は, Diagram 1 のオラクル A をジェネエリック・オラクル G で置き換えた場合と深く関わっている. 結論としては, 次のようになる.

定理 4 ([Su 99b] および [Su99d]) For every generic oracle G, we have Diagram 5, where r is an arbitrary natural number such that $r \geq 3$.

Diagram 5. (coNP[G] の内部構造; 但し G はジェネリック・オラクル)

$$\mathrm{TAUT} \oplus G \ <^{\mathsf{P}}_{\mathsf{T}} \ 1\mathrm{TAUT}[G] \ <^{\mathsf{P}}_{\mathsf{T}} \ 2\mathrm{TAUT}[G] \leq^{\mathsf{P}}_{\mathsf{T}} r\mathrm{TAUT}[G] \ <^{\mathsf{P}}_{\mathsf{T}} \mathrm{TAUT}[G]$$

¤

充填論法 (padding argument, [BDG 95] 参照) と [BGS 75] の finite extension method を組み合わせることによって, 以下の**定理 5** を得る. **定理 4** は, Diagram 4 と**定理 5** の組み合わせによって導かれる. ここで, 言葉の説明をしておく. A をオラクル, $\varphi(X)(y)$ を finitely testable な算術的述語だとする. $\varphi(A)(u)$ が成り立つようなビット列 u 全体の集合を, $\varphi[A]$ で表す.

$$\varphi[A] := \{u \in \{0,1\}^* : \varphi(A)(u)\}.$$

また, A が celing-generic oracle であるとは, A に関する φ のフォーシング計算量が高々多項式になることを言う.

定理 5 [Su 99b] Suppose that $\varphi(X)(y)$ and $\psi(X)(y)$ are finitely testable arithmetical predicates and G_1 is an oracle. Suppose that for every oracle A, if $A(u) = G_1(u)$ for all but finitely many bit strings u, then the following three hypothesisses hold.

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

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

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

Then, for every generic oracle G_2, we have the following.

$$\psi[G_2] \notin \mathrm{NP}[\varphi[G_2]].$$

¤

たとえば, $F \in 1\mathrm{TAUT}[X]$ という主張を表す述語を$\varphi(X)(F)$ とすると, 任意のオラクル A に対し, $\varphi[A] = 1\mathrm{TAUT}[A]$ となる. また, 述語 $\varphi(X)(F)$ に関する ceiling-generic oracle とは one-Dowd oracle に他ならず, $\varphi(X)(F)$ に関する ceiling-generic oracle 全体のクラスとは 1DO のことである. このように, 算術的述語を媒介にして, Diagram 4 の各レベルと Diagram 5 の各レベルが対応している. そして**定理 5** により, Diagram 4 で % になっているところには, Diagram 5 では向きがひっくり返って $<^{\mathsf{P}}_{\mathsf{T}}$ が対応するのである.

6 coNP[A] の内部構造: A がランダム・オラクルの場合

Diagram 1 は, ランダム・オラクルに関してはジェネリック・オラクルと対照的な結果になる.

定理 6 [Su 98] Suppose that r is a positive integer and D is an r-Dowd oracle. Then, we have $\mathrm{TAUT} \oplus D \equiv^{\mathrm{P}}_{\mathrm{T}} r\mathrm{TAUT}[D]$. ¤

証明のあらすじは以下のとおり. まず, one-query formula を入力とし, 最小強制条件がもし存在するならそれを生成する, という決定性アルゴリズムを考え, その while-loop の実行回数を考察する. かくして, $r = 1$ の場合の証明を得る. $r \geq 2$ の場合の証明は, RPC の式について, 式の長さとクエリー記号の数の trade-off を考察することによってなされる.

定理 6 と Dowd **の** Theorem 10 および Kurtz の結果 [Kur 83] により, ランダム・オラクル A に対し, 確率 1 を以って Diagram 6 が成り立つ. ただし, ここで r は 3 以上の任意の自然数である.

Diagram 6. (coNP[A] の内部構造; 但し A はランダム・オラクル)

$$\mathrm{TAUT} \oplus A \equiv^{\mathrm{P}}_{\mathrm{T}} 1\mathrm{TAUT}[A] \equiv^{\mathrm{P}}_{\mathrm{T}} 2\mathrm{TAUT}[A] \equiv^{\mathrm{P}}_{\mathrm{T}} r\mathrm{TAUT}[A] <^{\mathrm{P}}_{\mathrm{T}} \mathrm{TAUT}[A]$$

さて, Dowd **の** Theorem 11 の対偶をとると, 次の事がわかる: 「もし, ある one-Dowd oracle D で $1\mathrm{TAUT}[D] \notin \mathrm{NP}[D]$ となるものがあれば, $\mathrm{NP} \neq \mathrm{coNP}$ (unrelativized) となる」. ここで, 仮定をはるかに弱いものと取り替えても, 興味ある結論が得られる. **定理** 6 とその証明を応用することにより, Dowd **の** Theorem 11 の拡張版を示すことができる. 以下の定理に出てくる R はよく知られた計算量クラスであり, 確率テューリング機械を使って定義される. $\mathrm{P} \subseteq \mathrm{R} \subseteq \mathrm{NP}$ という位置にある. R に属する集合の代表例は, 素数の 2 進表記全体の集合 PRIMES である ([BDG 95] 参照).

定理 7 [Su 98] Suppose r is a positive integer. Then, the following two assertions are equivalent.

- The following class has Lebesgue measure one:

  $\{X : \text{The pT-degree of } r\mathrm{TAUT}[X] \text{ is strictly higher than that of } X\}$

- $\mathrm{R} \neq \mathrm{NP}$ (unrelativized). ¤

定理 8 [Su 99d] If there exists a one-Dowd oracle D such that the p-tt-degree of $1\mathrm{TAUT}[D]$ is strictly higher than that of D, then we have $\mathrm{P} \neq \mathrm{NP}$. ¤

7 One-query-jump hypothesis

さて, G が one-generic oracle のとき, 以下が成り立つことはよく知られている [Jo 80].

$$\emptyset' \oplus G \equiv_{\mathrm{T}} G'.$$

定理 6 で $r=1$ として得られる関係

$$1\mathrm{TAUT}[\emptyset]\oplus D \equiv^{\mathsf{P}}_{\mathsf{T}} 1\mathrm{TAUT}[D]$$

は, この事実の類似物と言える.

そこで, jump-operator と one-query operator (すなわち, $\lambda X.\ 1TAUT[X]$) の間に更なる類似があるかどうか検討してみる. いま, $\leq_{\mathsf{X}}$ を $\leq^{\mathsf{P}}_{\mathsf{T}}$ あるいは $\leq^{\mathsf{P}}_{\mathsf{tt}}$ のような還元 (concept of reducibility) だとする. 以下の主張を**還元 $\leq_{\mathsf{X}}$ に関する** one-query-jump hypothesis と呼び, その基本的な性質を考察することにしよう.

One-query-jump hypothesis for $\leq_{\mathsf{X}}$. "The class of all oracles A of the following property has Lebesgue measure one: the X-degree of $1TAUT[A]$ is strictly higher than the X-degree of A."

Diagram 7 は各種の還元の間の自明な関係を示す. それぞれの記号の意味は以下のとおり:

$\leq^{\mathsf{P}}_{1}$ は多項式時間 1 対 1 還元 (p-time one-one reducibility) ,

$\leq^{\mathsf{P}}_{\mathsf{m}}$ は多項式時間多対 1 還元 (p-time many-one reducibility) ,

$\leq^{\mathsf{P}}_{\mathsf{d}}$ は多項式時間選言還元 (p-time disjunctive reducibility) ,

$\leq^{\mathsf{P}}_{\mathsf{c}}$ は多項式時間連言還元 (p-time conjunctive reducibility) ,

$\leq^{\mathsf{P}}_{1-\mathsf{tt}}$ は多項式時間 1 真理値表還元 (p-time one-truth-table reducibility) ,

$\leq^{\mathsf{P}}_{\mathsf{tt}}$ は多項式時間真理値表還元 (p-time truth-table reducibility)

を, それぞれ表す. これらの還元の詳しい定義については, [LLS 75] を参照されたい. ここで $\leq_{\mathsf{X}} \to \leq_{\mathsf{Y}}$ は任意のオラクル A と B に対し, $A \leq_{\mathsf{X}} B$ ならば $A \leq_{\mathsf{Y}} B$ であることを表す.

Diagram 7. (Reducibilities)

$$\begin{array}{ccccccccc}
 & & & & \leq^{\mathsf{P}}_{\mathsf{d}} & & & & \\
 & & & \nearrow & & \searrow & & & \\
\leq^{\mathsf{P}}_{1} & \to & \leq^{\mathsf{P}}_{\mathsf{m}} & \to & \leq^{\mathsf{P}}_{\mathsf{c}} & \to & \leq^{\mathsf{P}}_{\mathsf{tt}} & \to & \leq^{\mathsf{P}}_{\mathsf{T}} \\
 & & & \searrow & & \nearrow & & & \\
 & & & & \leq^{\mathsf{P}}_{1-\mathsf{tt}} & & & &
\end{array}$$

Diagram 8 はこれらの還元に対する one-query jump hypothesisses が, 相対化されない計算量クラスに関する有名な未解決問題とどう関わっているかを示す. 暫定的に, $[\leq_{\mathsf{X}}]$ と [Prime] という記号を導入する. これらの意味は以下のとおり. それぞれの還元 $\leq_{\mathsf{X}}$ に対し, $[\leq_{\mathsf{X}}]$ は対応する one-query-jump hypothesis を表す. [Prime] は「PRIMES が NP 完全ではない」という主張を表す. 矢印は「ならば」を示し, 両側矢印は「同値」を示す.

Diagram 8. (one-query-jump hypothesisses)

$$
\begin{array}{ccccccccc}
 & & & & [\leq^{\mathsf{P}}_{\mathsf{d}}] & & & & \\
 & & & \swarrow & & \nwarrow & & & \\
[\leq^{\mathsf{P}}_{1}] & \leftarrow & [\leq^{\mathsf{P}}_{\mathsf{m}}] & \leftarrow & [\leq^{\mathsf{P}}_{\mathsf{c}}] & \leftarrow & [\leq^{\mathsf{P}}_{\mathsf{tt}}] & \leftarrow & [\leq^{\mathsf{P}}_{\mathsf{T}}] \\
 & & & \nwarrow & & \swarrow & \downarrow_{(1)} & & \updownarrow_{(2)} \\
 & & & & [\leq^{\mathsf{P}}_{1-\mathsf{tt}}] & & \mathrm{P} \neq \mathrm{NP} & & \mathrm{R} \neq \mathrm{NP} \\
 & & & & & & & \nwarrow^{(4)} & \downarrow_{(3)} \\
 & & & & & & & & [\mathrm{Prime}]
\end{array}
$$

矢印 (1) と (2) は**定理 7** と**定理 8** によって成り立つ. 矢印 (3) と (4) は以前からよく知られていた話である ([BDG 95, § 6.1] の Rabin の素数判定アルゴリズムを参照).

Diagram 8 に現れる主張のいくつかは, 確かに ZFC 集合論の定理になっていることに注意しておく.

定理 9 [Su 99d] One-query-jump hypothesis for p-time disjunctive reducibility is a theorem of ZFC. One-query-jump hypothesis for p-time one-truth-table reducibility is a theorem of ZFC, too. Thus, we have Diagram 9, where $\vdash [\leq_{\mathsf{X}}]$ denotes that the one-query-jump hypothesis for $\leq_{\mathsf{X}}$ is a theorem of ZFC.

Diagram 9. (one-query-jump hypothesisses)

$$
\begin{array}{ccccccccc}
 & & & & \vdash [\leq^{\mathsf{P}}_{\mathsf{d}}] & & & & \\
 & & & & & & & & \\
\vdash [\leq^{\mathsf{P}}_{1}] & & \vdash [\leq^{\mathsf{P}}_{\mathsf{m}}] & & [\leq^{\mathsf{P}}_{\mathsf{c}}] & \leftarrow & [\leq^{\mathsf{P}}_{\mathsf{tt}}] & \leftarrow & [\leq^{\mathsf{P}}_{\mathsf{T}}] \\
 & & & & & & \downarrow & & \updownarrow \\
 & & & & \vdash [\leq^{\mathsf{P}}_{1-\mathsf{tt}}] & & \mathrm{P} \neq \mathrm{NP} & & \mathrm{R} \neq \mathrm{NP} \\
 & & & & & & & \nwarrow & \downarrow \\
 & & & & & & & & [\mathrm{Prime}]
\end{array}
$$

¤

8 帰納的集合の階層における one-Dowd oracle の分布

ジェネリック・オラクルとランダム・オラクルは Cantor 空間において「多数派」を占める. 一方, 算術的階層に属するオラクルは「選び抜かれた少数派」と言える. 本稿の締めくくりとして, 算術的階層, 特に帰納的集合の階層における one-Dowd oracle の分布状況についての筆者の研究を報告する.

さて, Δ^0_2 は one-generic oracle を含むが, Σ^0_1 は one-generic oracle を含まない. すなわち, one-generic oracle は帰納的可算ではありえない: これはよく知られた事実である. Dowd は, 同様な理由

より one-Dowd oracle は帰納的可算ではありえない, と述べている. しかし, これは誤りである. 筆者は以下を示した.

定理 10 [Su 99d] There exists a one-Dowd oracle D such that D is primitive recursive. ¤

更に, テューリング次数については, 以下の optimal な結果を得た.

定理 11 [Su 99d] (Ubiquity of one-Dowd oracles) Every Turing degree contains a one-Dowd oracle. ¤

定理 10 の証明のあらすじはは以下のとおり.

Construction: よく知られているように, Cantor 空間における辞書式順序は整列順序ではない. しかしながら, 1DO の部分クラス $\mathcal{K}$ で, 辞書式順序に関して最小元を持つものがある. これを示すため, 十分大きい自然数 k と c を固定し, 多項式 $p(x) = x^{\mathsf{k}} + c$ に関して one-Dowd となるオラクル全体のクラスを $\mathcal{K}$ とおく. 次に, one-query formlas 全体の集合 (それを仮に Form で表そう) を可算個の (無限) 部分集合に分割する. 各自然数 n に対して, 次元 (ξ^{m} の m) が n である one-query formula 全体の集合を $\mathrm{Form}_{\mathsf{n}}$ で表そう.

$$\mathrm{Form} = \bigcup_{\mathsf{n} \in \mathsf{N}} \mathrm{Form}_{\mathsf{n}}.$$

各自然数 n に対して, オラクルの有限先頭部分についての requirement R_{n} を導入する.

R_{n}: 「与えられた先頭部分 S は $\{z(0), \ldots, z(2^{\mathsf{n}-1})\}(= \mathrm{Str}(n))$ を定義域とする強制条件である. さらに, $F \in 1\mathrm{TAUT}[X] \cap \mathrm{Form}_{\mathsf{n}}$ という主張を表す述語を $\varphi_{\mathsf{n}}(X)(F)$ とすると, S は『オラクルの φ_{n} についてのフォーシング計算量が高々 $p(|F|)$ である』という主張を強制する.」

A がオラクルのとき, もし任意の自然数 n に対して先頭部分 A ¹ $\mathrm{Str}(n)$ が requirement R_{n} を満たすならば, $A \in \mathcal{K}$ が成り立つ.

さて, 強制条件 S が requirement R_{n} をみたし, なおかつ S のしかるべき先頭部分たちがそれぞれ $R_1, \ldots, R_{\mathsf{n}-1}$ をみたすとき, 「S survives at n」と言うことにする. そこで, あらためて, R_{n} より強い requirement として以下の R_{n}^{θ} を考える.

R_{n}^{θ}: 「与えられた先頭部分 S は n における survivors のうち, 辞書式順序に関して最小のもの (以下, 『n における最小 survivor』 と呼ぶ) である.」

各 n に対して requirement R_{n}^{θ} を満たしながら, オラクルを先頭部分から順次構成していくことを考える. この構成で, injury は起きない: つまり, $m < n$ のとき, ステージ n における最小 survivor は, 必ずステージ m における最小 survivor の子孫である. その理由は, 任意の強制条件 S と任意の自然数 n に対し, もし S survives at n ならば, S の拡張 T であって, T survives at $n+1$ となるものが存在するからである: この事実は, [Do 92] における Dowd **の** Theorem 10 の証明の前半部分を吟味するとわかる. また, n が小さいときは, S survives at n となる S が確かに存在することもわかる. かくして, この構成法により, 辞書式順序に関する $\mathcal{K}$ の最小元を得る. その最小元を D とおく.

Verification:　明らかに D は one-Dowd である．後は, D が原始帰納的であることを示せばよい．ここで, コンパクト性定理と似たようなことを考える．各 n に対し, $\mathrm{Form}_{\mathrm{n}}$ は無限集合だが, 実際は $\mathrm{Form}_{\mathrm{n}}$ の有限部分集合で requirement R_{n} を決定できる．そこで requirement R_{n} の定義を吟味すると, R_{n} が原始帰納的だとわかる．ゆえに, 与えられた n に対して n における最小 survivor を生成する原始帰納的なアルゴリズムがある．したがって, D は原始帰納的である．以上が, **定理** 10 の証明のあらすじである．

定理 11 の証明のあらすじは以下のとおり．1DO は非可算な Borel 集合であるから, perfect subset を持つのは明らかである．しかし, **定理** 10 の証明をよく吟味すると, survivor 全体の集合自体が perfect tree であることがわかる (perfect set と perfect tree については [Je 78] 参照)．したがって, 任意のオラクル A を "survivor tree" の branch でコードできる．この branch は one-Dowd oracle である．しかも, "survivor tree" (の node の集合) は原始帰納的であるから, このコーディングにおいて Turing-degree は不変に保たれる (このようなコーディングのやりかたについては, [Ta 73] も参照)．以上が, **定理** 11 の証明のあらすじである．

かくして, Σ^0_1 は one-Dowd oracle を含むことがわかった．しかし, Σ^{P}_1 $(=\mathrm{NP})$ はどうか？この問題については, 以下の事実がある．ここで P/poly は多項式サイズのサーキットを持つ集合全体のクラスを表す．

命題 12　[Su 99d]　None of the following complexity classes contains a one-Dowd oracle: P, NP, coNP, BPP, P/poly. ¤

Diagram 10, 11, 12 は, Δ^0_2 内部における one-Dowd oracle の分布状況を示す．これらの図で, $C_1 \to C_2$ は $C_1 \subseteq C_2$ を表す．そして, $C_1 \to_{\neq} C_2$ は $C_1 \,\$\, C_2$ を表す．記号 $C+$ (と $C-$ の, それぞれ) はクラス C が one-Dowd oracle を含む (one-Dowd oracle を含まない) ことを表す．他方, C¢ (と C^{-} の, それぞれ) はクラス C が one-generic oracle を含む (one-generic oracle を含まない) ことを表す．PH は多項式時間階層を表し, PrRec は原始帰納的な集合全体のクラスを表す．

Diagram 10. (Higher levels)

$$
\begin{array}{ccccccc}
 & & & & \Sigma^{0\,-}_1 & & \\
 & & & \nearrow_{\neq} & & \searrow_{\neq} & \\
\mathrm{PrRec}+ & \to_{\neq} & \Sigma^0_0+ & & & & \Delta^0_2\text{¢} \\
 & & & \searrow_{\neq} & & \nearrow_{\neq} & \\
 & & & & \Pi^{0\,-}_1 & &
\end{array}
$$

Diagram 11. (Middle levels)

$$
\begin{array}{ccccccccc}
\Delta_2^{\mathsf{P}} & \rightarrow & \Sigma_2^{\mathsf{P}} \cap \Pi_2^{\mathsf{P}} & \rightarrow & \mathrm{PH} & \rightarrow & \mathrm{PSPACE} & \rightarrow_{\neq} & \mathrm{PrRec}+ \\
 & \nearrow & & & & & & & \\
\mathrm{BPP}- & \rightarrow_{\neq} & \mathrm{P/poly} -^{-} & & & & & &
\end{array}
$$

Diagram 12. (Lower levels)

$$
\begin{array}{ccccccc}
 & & \mathrm{R}- & \rightarrow & \mathrm{NP}- & & \\
 & \nearrow & & \searrow & & \searrow & \\
\mathrm{P}- & & & & \mathrm{BPP}- & & \Delta_2^{\mathsf{P}} \\
 & \searrow & & \nearrow & & \nearrow & \\
 & & \mathrm{coR}- & \rightarrow & \mathrm{coNP}- & &
\end{array}
$$

• 結語と謝辞 •

RPC とフォーシング計算量の研究を発展させ, ジェネリック・オラクル, ランダム・オラクル, 相対化されない階層の 3 者を結ぶ秩序を更に追及していきたい. 学位論文に関してお世話になった田中尚夫, 本橋信義, 江田勝哉, 加茂静夫の各先生に謹んで感謝の気持ちを申し上げる. なお, 本研究は文部省科学研究費 (No. 09440072, 09440078, 11740073) によって部分的に援助を受けた.

参考文献

[Am 96] Ambos-Spies, K., Resource-bounded genericity, in "Computability, enumerability, unsolvability directions in recursion theory," London Math. Soc. Lect. Note Series vol. 224 (S. B. Cooper, T. A. Slaman and S. S. Wainer, Eds.), pp. 1-59, Cambridge University Press, Cambridge, 1996.

[BGS 75] Baker, T., J. Gill and R. Solovay, Relativizations of $P = ?NP$ question, SIAM J. Comput. vol. 4 (1975) 431-442.

[BDG 95] Balcázar, J. L., J. Díaz, and J. Gabarró, "Structural complexity I, second edition," Springer, Berlin, 1995.

[BG 81] Bennett, C. H. and J. Gill, "Relative to a random oracle A, $P^{\mathsf{A}} \neq NP^{\mathsf{A}} \neq co\text{-}NP^{\mathsf{A}}$ with probability 1," SIAM J. Comput., vol. 10 (1981), pp. 96-113.

[BI 87] 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.

[CIY 97] Cook, S., R. Impagliazzo and T. Yamakami, "A tight relationship between generic oracles and type-2 complexity theory," *Information and Computation*, vol. 137 (1997), pp. 159-170.

[Do 92] Dowd, M., "Generic oracles, uniform machines, and codes," *Information and Computation*, vol. 96 (1992), pp. 65-76.

[Fe 65] Feferman, S., "Some applications of the notions of forcing and generic sets," *Fund. Math.*, vol. 56 (1965), pp. 325-345.

[Hi 69] 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.

[Je 78] Jech, T., "Set theory," Academic Press, San Diego, 1978.

[Jo 80] Jockusch, C. G. Jr., Degrees of generic sets, *in* "Recursion theory: its generalizations and applications," London Math. Soc. Lect. Note Series vol. 45 (F.R. Drake and S.S. Wainer, Eds.), pp. 110-139, Cambridge University Press, Cambridge, 1980.

[Ko 82] Ko, Ker-I., Some observations on the probabilistic algorithms and NP-hard problems, *Inform. Process. Lett.* vol. 14 (1982), 39-43.

[Kum 96] Kumabe, M., Degrees of generic sets, *in* "Computability, enumerability, unsolvability directions in recursion theory," London Math. Soc. Lect. Note Series vol. 224 (S. B. Cooper, T. A. Slaman and S. S. Wainer, Eds.), pp. 167-183, Cambridge University Press, Cambridge, 1996.

[Kur 83] Kurtz, S. A., "On the random oracle hypothesis," *Inform. Control*, vol. 57 (1983), pp. 40-47.

[LLS 75] Ladner, R. E., N. A. Lynch, and A. L. Selman, "A comparison of polynomial time reducibilities," *Theoret. Comput. Sci.*, vol. 1 (1975), pp. 103-123.

[Me 73] 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.

[Od 89] Odifreddi, P., "Classical recursion theory," North-Holland, Amsterdam, 1989.

[Po 86] Poizat, B., "$Q = NQ$?," *J. Symbolic Logic*, vol. 51 (1986), pp. 22-32.

[Su 98] Suzuki, T., "Recognizing tautology by a deterministic algorithm whose while-loop's execution time is bounded by forcing," Kobe Journal of Mathematics, vol.15 (1998), pp. 91-102.

[Su 99a] Suzuki, T., "Computational complexity of Boolean formulas with query symbols," Doctoral dissertation, Institute of Mathematics, University of Tsukuba, Tsukuba-City, Japan, 1999.

[Su 99b] Suzuki, T., "Complexity of the r-query tautologies: in presence of a generic oracle," Notre Dame J. Formal Logic, to appear.

[Su 99c] Suzuki, T., ' Forcing complexity: supplement to "complexity of the r-query tautologies," ' preprint.

[Su 99d] Suzuki, T., "Degrees of Dowd-type generic oracles," preprint.

[Ta 73] Tanaka, H., "Π^1_1 sets of sets, hyperdegrees and related problems," Journal of the Mathematical Society of Japan, vol. 25 (1973), pp. 609-621.

[TK 97] Tanaka, H. and M. Kudoh, "On relativized probabilistic polynomial time algorithms," Journal of the Mathematical Society of Japan, vol. 49 (1997), pp. 15-30.

[田中 96] 田中尚夫, "数学基礎論的手法の計算量理論への応用," 数学, vol. 48 (1996), pp. 372-384.