アルゴリズム 63－9
（1998．7．22）

数え上げ計算モデルの計算能力について

戸田誠之助
日本大学文理学部応用数学科
〒156 東京都世田谷区桜上水 3-25-40
toda@am.chs.nihon-u.ac.jp

概要 本稿では，数え上げ問題に内在する計算構造が強力な計算能力を持っていることを述べる．このことを端的に示す事実として，適当な論理回路 C と適当な多項式 $p(n)$ ならびに存在記号と全称記号の有限回の組み合わせを用いて，

$$\varphi(\vec{x}) \equiv \exists_p \vec{y}_1 \forall_p \vec{y}_2 \cdots \exists_p \vec{y}_{k-1} \forall_p \vec{y}_k C(\vec{x}, \vec{y}_1, \vec{y}_2, \cdots, \vec{y}_{k-1}, \vec{y}_k)$$

（ここで，$\exists_p \vec{y}$ は $\exists \vec{y} \in \{0,1\}^{p(|\vec{x}|)}$ を略記したものである；$\forall_p \vec{y}$ も同様.）

といった形式で定義できる任意の論理関数 φ が，$(s(C)+p(|\vec{x}|))^{O(1)}$ サイズ（$s(C)$ は論理回路 C のサイズ）の積和標準形（和積標準形でもよい）のブール式 ψ と適当な多項式 $q(n)$ を用いて，

$$\varphi(\vec{x}) \equiv |\{\, \vec{y} \in \{0,1\}^{q(|\vec{x}|)} : \psi(\vec{x}, \vec{y}) = 1 \,\}| \bmod 2$$

と表現できることを示す．本稿では，このような結果をオペレータを基盤にした枠組みに基づいて議論する．

キーワード 計算量理論，数え上げ問題，偶奇性判定問題，多項式時間階層，論理回路

On the power of computation structures involved in counting problmes

Seinosuke TODA
Department of Applied Mathmatics
College of Humanities and Sciences
Nihon University
Sakurajyousui 3-25-40, Setagaya-ku, Tokyo 156

Abstract In this paper, we give a brief survey on the power of computation structures involved in counting problems. We demonstrate that those structures are powerful enough to represent a finite number of compositions of exsistential and universal computations. As a typical fact, we show that for any boolean function φ which can be represented by the form

$$\varphi(\vec{x}) \equiv \exists_p \vec{y}_1 \forall_p \vec{y}_2 \cdots \exists_p \vec{y}_{k-1} \forall_p \vec{y}_k C(\vec{x}, \vec{y}_1, \vec{y}_2, \cdots, \vec{y}_{k-1}, \vec{y}_k)$$

where C is a boolean circuit, $p(n)$ is a polynomial, and $\exists_p \vec{y}$ and $\forall_p \vec{y}$ are abbreviations of $\exists \vec{y} \in \{0,1\}^{p(|\vec{x}|)}$ and $\forall \vec{y} \in \{0,1\}^{p(|\vec{x}|)}$ respectively, it can be represented by

$$\varphi(\vec{x}) \equiv |\{\, \vec{y} \in \{0,1\}^{q(|\vec{x}|)} : \psi(\vec{x}, \vec{y}) = 1 \,\}| \bmod 2$$

using a polynomial $q(n)$ and a conjunctive normal form formula ψ of size $(s(C)+p(|\vec{x}|))^{O(1)}$ where $s(C)$ denotes the size of C. We discuss this sort of facts in terms of an operator-based theory.

Keywords computational complexity theory, counting problem, parity, polynomial-time hierarchy, boolean circuit

1 準備

この節では以後の議論に必要な基本的な定義を示す.

定義 1.1 ブール値からなる集合 $\{0,1\}$ を以下では $\mathcal{B}$ で表す. また, ブール値の有限列 —以後, **ビット列**と呼ぶ— すべてからなる集合を $\mathcal{B}^*$ で表す. また更に, 任意の自然数 m に対して, 長さ (ビット数) m のビット列全体を $\mathcal{B}^m$ で表す. $\mathcal{B}^*$ に属する任意のビット列をベクトル記号を援用して $\vec{x}$ と表すことにする. また, $\vec{x}$ の長さを $|\vec{x}|$ で表す. ■

本稿では, 論理回路に基づいて計算量クラスを定義する. なお, 論理回路の一様性 (回路図を効率よく出力できるかどうか) については議論せず, 非一様な論理回路を扱う. このため, 本稿で扱う計算量クラスはすべて非一様なものである. また, 以下では定義の内容を簡略化しているので, 詳しくは [Miy93] を参照されたい.

定義 1.2 **論理回路** —以後単に, **回路**という— とは, 定数ゲート, 入力ゲート, AND ゲート, OR ゲート, および, NOT ゲート (と呼ばれる頂点) からなる有向閉路を持たない有向グラフである. ただし, この有向グラフは次の条件を満たさなければならない.

- 任意の定数ゲートと任意の入力ゲートの入次数は 0 である. また, 各定数ゲートにはブール値を表す 0 または 1 が割り付けられており, 各入力ゲートには, 入力変数 (の名前) が割り付けられている.
- 任意の AND ゲートおよび OR ゲートの入次数は 2 であり, 任意の NOT ゲートの入次数は (当然) 1 である.

入力変数の個数 (注 : 入力ゲートの個数ではない) が n の回路を **n 入力回路**という. 回路内のゲート数を**サイズ**と呼ぶ. また, 回路内の最長有向道の長さ (有向辺の本数) をその回路の**段数**という. ■

注意 本稿では, 還元可能性を計算する回路を除いて, (多入力) 1 出力の回路を扱う. ■

定義 1.3 回路の可算無限列 $C_1, C_2, \ldots$ ——以後, $\{C_n\}$ で表す——を**回路族**と言う. ただし, 各 $n \geq 1$ に対して, C_n は n 入力回路でなければならない. 同様に, 論理関数の可算無限列 $\varphi_1, \varphi_2, \ldots$ —以後, $\{\varphi_n\}$ で表す—を**論理関数族**と言う. ただし, 各 $n \geq 1$ に対して, φ_n は n 変数論理関数である. $\{C_n\}$ が $\{\varphi_n\}$ を計算するとは, 各 C_n が φ_n を計算するときを言う.

回路族 $\{C_n\}$ が**多項式サイズ限定**であるとは, 適当な多項式 $p(n)$ が存在して, 各 C_n のサイズが $p(n)$ 以下であるときを言う. 多項式サイズ限定の回路族によって計算できる論理関数族すべてからなるクラスを PSIZE で表す. ■

定義 1.4 積和標準形 (disjunctive normal form) の形をした回路を **DNF 回路**と呼ぶことにする. 多項式サイズ限定の DNF 回路族によって計算できる論理回路族すべてからなるクラスを DNF で表すことにする. 同様に, 和積標準形 (conjunctive normal form) の形をした回路を **CNF 回路**と呼ぶことにする. 多項式サイズ限定の CNF 回路族によって計算できる論理関数族すべてからなるクラスを CNF で表すことにする. また更に, DNF∩CNF を BNF で表す. ■

定義 1.5 $Q(y)$ を任意の (記号論理学で言うところの) 述語とし, Δ を変数 y が取り得る値からなる有限集合とする. このとき, **偶奇限量記号** $\oplus$ を次で定める :

$$\oplus y \in \Delta\,[Q(y)] \leftrightarrow |\{y \in \Delta : Q(y)\}| \equiv 1 \pmod 2 \quad ■$$

2 計算量クラスについて

次節以降では, PSIZE や CNF といった特定のクラスについて議論する前に, 任意のクラスについて議論を行い, そこで得られた結果を特定のクラスに適用していく. しかしながら, 次節以降の一部の結果は, ある特殊なクラスについては成立しない. この点を本節で議論しておく.

定義 2.1 論理関数族 $\{\psi_n\}$ が**入力長に関して自明** —以後単に, **自明**と呼ぶ— であるとは, 各 ψ_n が定値関数であるときを言う. なお, 入力長毎に出力値が変化してもよいことに注意されたい. 簡単な具体例としては, 奇数長の入力に対しては 1 を出力し, 偶数長の入力に対しては 0 を出力する論理関数族などがある. 以後, すべての入力に対して 0 を出力する n 変数定値関数を $\mathbf{0}_n$ で表し, 1 を出力する n 変数定値関数を $\mathbf{1}_n$ で表す. ■

上のような論理関数族を「自明」と呼ぶ理由は, 論理ゲートを一切使用しない回路族 —定数ゲートの値をそのまま出力する回路族— によって計算できてしまうことによる. 逆の観点から言うと, 回路族 (のような非一様な計算モデル) では自明な論理関数族の計算量を全く議論できないことが分かる. この点は非一様な計算モデルの弱点ではあるが, 我々が自然に遭遇する計算問題 (例えば, NP 完全問題など) について議論する際, この点が何かの障害になることはまずあり得ないと思う. *

自明な論理関数族だけからなるクラスについては, 次節以降で述べる一部の議論が適用できない. 一部の証明の中では, どうしても非自明な論理関数族が必要になる. そこで次のよ

*実際, NP 完全問題については, 非一様な計算モデルに基づいても計算困難と結論できるであろうと予想されており, より具体的には, 次のような予想が存在する.

[予想] NP $\subseteq$ PSIZE $\Rightarrow$ P=NP.

なお, この逆は自明である. 上記の NP を PSPACE や EXPTIME に置き換えたものもいまだ予想の域を脱していない. 特に, EXPTIME$\not\subseteq$PSIZE が証明できていないことは特筆に値すると思う (対角線論法は使えない).

うな定義を行う．

定義 2.2 $\mathcal{C}$ を任意のクラスとする．このとき，クラス $\tilde{\mathcal{C}}$ を次のように定義する．$\mathcal{C}$ が非自明な論理関数族を含んでいるならば，$\tilde{\mathcal{C}} = \mathcal{C}$ とする．一方，$\mathcal{C}$ が非自明な論理関数族を含んでいないならば，非自明な論理関数族 $\{\eta_n\}$ を任意に選んで，$\tilde{\mathcal{C}} = \mathcal{C} \cup \{\{\eta_n\}\}$ とする．$\{\eta_n\}$ としてはどのようなものでもよいが，例えば，

$$\eta_1(0) = 0,\ \eta_1(1) = 1,\ \eta_n = \mathbf{0}_n \quad (n \geq 2)$$

で定義されるものなどを使用すればよい． ■

本稿では以上の定義に基づいて議論を進めるが，何かの目的のために恣意的な定義を行わない限り，すべてのクラスは非自明な論理関数族を含んでいると考えてよい．従って，以下で扱うすべてのクラスは非自明な論理関数族を必ず含むものと仮定し，更に $\tilde{\mathcal{C}}$ は $\mathcal{C}$ のことだと考えても，一般性を大きく損ねるということはない．

3 オペレータ

本節では，既存の計算量クラス（例えば，PSIZE や CNF など）から新たな計算量クラスを生成するためのオペレータを幾つか定義する．また，それらの基本的な性質を述べる．

定義 3.1 $\mathcal{C}$ を論理関数族からなる任意のクラスとする．このとき，新たなクラス $\exists\cdot\mathcal{C}$，$\forall\cdot\mathcal{C}$，$\mathrm{co}\cdot\mathcal{C}$，および，$\oplus\cdot\mathcal{C}$ を次のように定める．任意の論理関数族 $\{\varphi_n\}$ に対して:

(1) $\{\varphi_n\} \in \exists\cdot\mathcal{C} \Leftrightarrow$ 論理関数族 $\{\psi_n\} \in \mathcal{C}$ と多項式 $p(n)$ が存在して，任意の $\vec{x} \in \mathcal{B}^*$ に対して，

$$\varphi_n(\vec{x}) = 1 \leftrightarrow \exists \vec{y} \in \mathcal{B}^{p(n)}[\psi_{n+p(n)}(\vec{x}, \vec{y}) = 1]$$

が成り立つ．ここで，n は $\vec{x}$ の長さを表す．

(2) $\{\varphi_n\} \in \forall\cdot\mathcal{C} \Leftrightarrow \{\psi_n\} \in \mathcal{C}$ と多項式 $p(n)$ が存在して，任意の $\vec{x}$ に対して，

$$\varphi_n(\vec{x}) = 1 \leftrightarrow \forall \vec{y} \in \mathcal{B}^{p(n)}[\psi_{n+p(n)}(\vec{x}, \vec{y}) = 1]$$

が成り立つ．ここで，n は $\vec{x}$ の長さを表す．

(3) $\{\varphi_n\} \in \mathrm{co}\cdot\mathcal{C} \Leftrightarrow$ 論理関数族 $\{\neg\varphi_n\}$ が $\mathcal{C}$ に属する．ここで，"¬" は論理否定を表す．

(4) $\{\varphi_n\} \in \oplus\cdot\mathcal{C} \Leftrightarrow$ 論理関数族 $\{\psi_n\} \in \mathcal{C}$ と多項式 $p(n)$ が存在して，任意の $\vec{x} \in \mathcal{B}^*$ に対して，

$$\varphi_n(\vec{x}) = 1 \leftrightarrow \oplus \vec{y} \in \mathcal{B}^{p(n)}[\psi_{n+p(n)}(\vec{x}, \vec{y}) = 1]$$

が成り立つ．ここで，n は $\vec{x}$ の長さを表す． ■

次に，還元可能性（変換可能性とも言う）をいくつか定義する．なお，本稿では，還元可能性もオペレータの一種と見なしている点に注意されたい．

定義 3.2 $\{\varphi_n\}$ と $\{\psi_n\}$ を任意の論理関数族とする．

(1) $\{\varphi_n\}$ が $\{\psi_n\}$ に **$\leq_{\mathrm{m}}$-還元可能**であるとは，次の条件を満たす多項式サイズ限定の回路族 $\{D_n\}$ が存在するときをいう．任意の $\vec{x} \in \mathcal{B}^*$ に対して：

- D_n はビット列 $\vec{y}$ を出力する多入力多出力の回路である．ここで，n は $\vec{x}$ の長さを表す．
- $\varphi_n(\vec{x}) = \psi_m(\vec{y})$．ここで，$m$ は $\vec{y}$ の長さを表す．

(2) $\{\varphi_n\}$ が $\{\psi_n\}$ に **$\leq_{\mathrm{d}}$-還元可能**であるとは，次の条件を満たす多項式サイズ限定の回路族 $\{D_n\}$ が存在するときをいう．任意の $\vec{x} \in \mathcal{B}^*$ に対して：

- D_n はビット列のリスト $\vec{y}_1, \vec{y}_2, \ldots, \vec{y}_k$ $(k \geq 1)$ を出力する多入力多出力の回路である．ここで，n は $\vec{x}$ の長さを表す．
- $\varphi_n(\vec{x}) = \psi_{m_1}(\vec{y}_1) \vee \psi_{m_2}(\vec{y}_2) \vee \cdots \vee \psi_{m_k}(\vec{y}_k)$．ここで，各 m_i は $\vec{y}_i$ の長さを表す．

(3) $\{\varphi_n\}$ が $\{\psi_n\}$ に **$\leq_{\mathrm{c}}$-還元可能**であるとは，次の条件を満たす多項式サイズ限定の回路族 $\{D_n\}$ が存在するときをいう．任意の $\vec{x} \in \mathcal{B}^*$ に対して：

- D_n はビット列のリスト $\vec{y}_1, \vec{y}_2, \ldots, \vec{y}_k$ を出力する多入力多出力の回路である．ここで，n は $\vec{x}$ の長さを表す．
- $\varphi_n(\vec{x}) = \psi_{m_1}(\vec{y}_1) \wedge \psi_{m_2}(\vec{y}_2) \wedge \cdots \wedge \psi_{m_k}(\vec{y}_k)$．ここで，各 m_i は $\vec{y}_i$ の長さを表す．

$\leq_{\mathrm{x}}$ を上で定めた任意の還元可能性を表す記号とする．このとき，論理関数族 $\{\varphi_n\}$ が論理関数族 $\{\psi_n\}$ に $\leq_{\mathrm{x}}$-還元可能であることを，$\{\varphi_n\} \leq_{\mathrm{x}} \{\psi_n\}$ で表す．

$\mathcal{C}$ を任意のクラスとするとき，$\leq_{\mathrm{x}}\cdot\mathcal{C}$ を

$$\leq_{\mathrm{x}}\cdot\mathcal{C} = \{\{\varphi_n\} : \exists\{\psi_n\} \in \mathcal{C}[\{\varphi_n\} \leq_{\mathrm{x}} \{\psi_n\}]\}$$

で定める． ■

以下に上で定めたオペレータの基本的な性質を示す．

命題 3.3 任意のクラス $\mathcal{C}$ に対して次が成り立つ．なお，以下の記述の中で，$\leq_{\mathrm{x}}$ は定義 3.2 で定めた任意の還元可能性を表し，$\mathcal{O}$ は定義 3.1 の中で定めた任意のオペレータ（ただし，co を除く）を表している．

(1) $\mathcal{C} \subseteq \leq_{\mathrm{m}}\cdot\mathcal{C} \subseteq \leq_{\mathrm{d}}\cdot\mathcal{C} \cap \leq_{\mathrm{c}}\cdot\mathcal{C}$.

(2) $\leq_{\mathrm{x}}\cdot\leq_{\mathrm{x}}\cdot\mathcal{C} = \leq_{\mathrm{x}}\cdot\mathcal{C}$，かつ，$\leq_{\mathrm{m}}\cdot\leq_{\mathrm{x}}\cdot\mathcal{C} = \leq_{\mathrm{x}}\cdot\leq_{\mathrm{m}}\cdot\mathcal{C} = \leq_{\mathrm{x}}\cdot\mathcal{C}$.

(3) $\mathcal{O}\cdot\mathcal{O}\cdot\mathcal{C} = \mathcal{O}\cdot\mathcal{C}$.

(4) $\leq_{\mathrm{x}}\cdot\mathcal{O}\cdot\mathcal{C} \subseteq \mathcal{O}\cdot\leq_{\mathrm{x}}\cdot\mathcal{C}$.

(5) $\mathrm{co}\cdot\leq_{\mathrm{m}}\cdot\mathcal{C} = \leq_{\mathrm{m}}\cdot\mathrm{co}\cdot\mathcal{C}$，$\mathrm{co}\cdot\leq_{\mathrm{d}}\cdot\mathcal{C} = \leq_{\mathrm{c}}\cdot\mathrm{co}\cdot\mathcal{C}$，かつ，$\mathrm{co}\cdot\leq_{\mathrm{c}}\cdot\mathcal{C} = \leq_{\mathrm{d}}\cdot\mathrm{co}\cdot\mathcal{C}$.

(6) $\mathrm{co}\cdot\mathrm{co}\cdot\mathcal{C} = \mathcal{C}$.

(7) $\mathrm{co}\cdot\exists\cdot\mathcal{C} = \forall\cdot\mathrm{co}\cdot\mathcal{C}$，かつ，$\mathrm{co}\cdot\forall\cdot\mathcal{C} = \exists\cdot\mathrm{co}\cdot\mathcal{C}$.

(8) $\oplus\cdot\mathcal{C} = \oplus\cdot\mathrm{co}\cdot\mathcal{C}$.

(9) $\mathrm{co}\cdot\oplus\cdot\mathcal{C} \subseteq \oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$.

(10) $\mathcal{C} \subseteq \mathcal{O}\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$.

(略証) (1) から (7) まではほとんど明らかなので詳細は読者に任せる．

(8) 任意の正整数 m に対して，$\mathcal{B}^m$ の要素数が偶数であることに注意すると，任意の論理関数族 $\{\psi_n\}$，任意の正整数 n，任意の多項式 $p(n)$，ならびに，任意の $\vec{x} \in \mathcal{B}^n$ に対して，

$$\oplus\vec{y} \in \mathcal{B}^{p(n)}\,[\psi(\vec{x},\vec{y}) = 1] \leftrightarrow \oplus\vec{y} \in \mathcal{B}^{p(n)}\,[\neg\psi(\vec{x},\vec{y}) = 1]$$

が成り立つ．これより，(8) の主張が得られる．†

(9) $\{\varphi_n\}$ を $\mathrm{co}\cdot\oplus\cdot\mathcal{C}$ に属する任意の論理関数族とする．このとき，論理関数族 $\{\psi_n\}$ と多項式 $p(n)$ が存在して，任意の $\vec{x} \in \mathcal{B}^*$ に対して，

$$\varphi_n(\vec{x}) = 1 \leftrightarrow \neg \oplus \vec{y} \in \mathcal{B}^{p(n)}[\psi_{n+p(n)}(\vec{x},\vec{y}) = 1]$$

が成り立つ．ここで，n は $\vec{x}$ の長さを表す．以下では，$\{\psi_n\}$ が自明な場合と非自明な場合に分けて議論する．

場合 1 $\{\psi_n\}$ が自明であるとき．この場合，$\{\varphi_n\} = \{1_n\}$ が成り立つ．そこで，$\{\eta_n\}$ を $\vec{\mathcal{C}}$ に属する非自明な論理関数族とし，$\eta_\ell(\vec{f}) = 0$ かつ $\eta_\ell(\vec{t}) = 1$ を満たす入力長 ℓ とビット列 $\vec{f}$，$\vec{t} \in \mathcal{B}^\ell$ を適当に選択する．また更に，論理関数 τ_{n+1} $(n \geq 1)$ を次で定める．任意の入力 $\vec{x} \in \mathcal{B}^{n+1}$ に対して：

- $x_{n+1} = 0$ のとき，$\tau_{n+1}(\vec{x}) = \eta_\ell(\vec{f})$ と定める．
- $x_{n+1} = 1$ のとき，$\tau_{n+1}(\vec{x}) = \eta_\ell(\vec{t})$ と定める．

なお，τ_1 については，$\tau_1 = \eta_1$ と定めておく．

以上で定義された論理関数族 $\{\tau_n\}$ に関して，$\{\tau_n\} \leq_{\mathrm{m}} \{\eta_n\}$ となることは明らかであろう．従って，$\{\tau_n\} \in \leq_{\mathrm{m}}\cdot\mathcal{C}$ が成り立つ．また更に，任意の $\vec{x} \in \mathcal{B}^*$ に対して，

$$\varphi_n(\vec{x}) = 1 \leftrightarrow \oplus\vec{y} \in \mathcal{B}^1[\tau_{n+1}(\vec{x},\vec{y}) = 1]$$

が成り立つことも明らかであろう．よって，この場合には，$\{\varphi_n\} \in \oplus\cdot\leq_{\mathrm{m}}\cdot\mathcal{C}$ が成り立つ．

場合 2 $\{\psi_n\}$ が非自明であるとき．この場合，まず $\psi_\ell(\vec{f}) = 0$ かつ $\psi_\ell(\vec{t}) = 1$ を満たす入力長 ℓ とビット列 $\vec{f}$，$\vec{t} \in \mathcal{B}^\ell$ を適当に選択する．そこで，論理関数 $\tau_{n+p(n)+1}$ $(n \geq 1)$ を次のように定義する．任意の $\vec{x} \in \mathcal{B}^n$ と任意の $\vec{y}z$ $\mathcal{B}^{p(n)+1}$ （ただし，$\vec{y} \in \mathcal{B}^{p(n)}$ かつ $z \in \mathcal{B}$）に対して：

(1) $\psi_{n+p(n)}=\mathbf{0}_{n+p(n)}$ または $\psi_{n+p(n)}=\mathbf{1}_{n+p(n)}$ のとき：
- $\vec{y}z = 1^{p(n)+1}$ ならば $\tau_{n+p(n)+1}(\vec{x},\vec{y}z) = \psi_\ell(\vec{t})$.
- $\vec{y}z \neq 1^{p(n)+1}$ ならば $\tau_{n+p(n)+1}(\vec{x},\vec{y}z) = \psi_\ell(\vec{f})$.

(2) $\psi_{n+p(n)} \neq \mathbf{0}_{n+p(n)}$ かつ $\psi_{n+p(n)} \neq \mathbf{1}_{n+p(n)}$ のとき：
まず，$\psi_{n+p(n)}(\vec{t}_x,\vec{t}_y) = 1$ および $\psi_{n+p(n)}(\vec{f}_x,\vec{f}_y) = 0$ を満たす $\vec{t}_x$, $\vec{t}_y \in \mathcal{B}^n$ と $\vec{f}_x$, $\vec{f}_y \in \mathcal{B}^{p(n)}$ を適当に選択する．そこで：
- $z = 1$ かつ $\vec{y} = 1^{p(n)}$ ならば $\tau_{n+p(n)+1}(\vec{x},\vec{y}z) = \psi_{n+p(n)}(\vec{t}_x,\vec{t}_y)$ とする．
- $z = 1$ かつ $\vec{y} \neq 1^{p(n)}$ ならば $\tau_{n+p(n)+1}(\vec{x},\vec{y}z) = \psi_{n+p(n)}(\vec{f}_x,\vec{f}_y)$ とする．
- $z = 0$ ならば $\tau_{n+p(n)+1}(\vec{x},\vec{y}z) = \psi_{n+p(n)}(\vec{x},\vec{y})$ とする．

また更に，$n + p(n) + 1$ の形で表すことができない任意の入力長 m に対して，τ_m を $\tau_m = \psi_m$ と定めておく．

以上で定義される論理関数族 $\{\tau_n\}$ に関して，$\{\tau_n\} \leq_{\mathrm{m}} \{\psi_n\}$ が成り立つことは明らかであろう．よって，$\{\tau_n\} \in \leq_{\mathrm{m}}\cdot\mathcal{C}$ が成り立つ．また更に，$\tau_{n+p(n)+1}$ の定義より，任意の正整数 n と任意の $\vec{x} \in \mathcal{B}^n$ に対して，

$$\oplus\vec{y}z \in \mathcal{B}^{p(n)+1}\,[\tau_{n+p(n)+1}(\vec{x},\vec{y}z) = 1] \leftrightarrow \neg \oplus \vec{y} \in \mathcal{B}^{p(n)}\,[\psi_{n+p(n)}(\vec{x},\vec{y}) = 1]$$

が成り立つことも明らかであろう．よって，$\{\varphi_n\} \in \oplus\cdot\leq_{\mathrm{m}}\cdot\mathcal{C}$ が成り立つ．

(10) (9) と同様の論法で（しかも，もっと簡単に）証明できるので，読者に任せる． ■

4 Isolation Lemmas

次節では，$\exists$-オペレータや $\forall$-オペレータが $\oplus$-オペレータに置き換えられることを示す．これを示すために，現在では Isolation lemma と呼ばれている Valiant&Varizani[VV86] によって示された組み合わせ論的な結果と，その結果から得られる補題をまずは述べる．

定義 4.1‡ m を任意の正整数とし，$\vec{h}$ と $\vec{y}$ を $\mathcal{B}^m$ に属する任意のビット列とする．このとき，$\vec{h}\cdot\vec{y}$ を次で定める．

$$\vec{h}\cdot\vec{y} = (h_1 \wedge y_1) \oplus (h_2 \wedge y_2) \oplus \cdots \oplus (h_m \wedge y_m)$$

ここで，各 h_i, y_i は $\vec{h},\vec{y}$ の i 番目のブール値を表し，$\oplus$ は排他的論理和を表す．

G をブール値からなる任意の $r \times m$ 行列とし，この行列の第 i 番目の行ベクトルを $\vec{g}_i$ で表す．このとき，$\vec{g}_1\cdot\vec{y}$, $\vec{g}_2\cdot\vec{y}$, …, $\vec{g}_r\cdot\vec{y}$ をこの順で並べて得られる $\mathcal{B}^r$ の要素を $G\cdot\vec{y}$ で表す．

S を $\mathcal{B}^m$ の任意の部分集合とする．このとき，$G * S$ を

$$G * S = \{\vec{y} \in S : G\cdot\vec{y} = 0^r\}$$

で定める．ここで，0^r は 0 を r 個並べた列を表す． ■

定義 4.2 p, q を任意の正整数とする．ブール値を要素とする $p \times q$ 行列すべてからなる集合を $\mathcal{H}_{p,q}$ で表す．また，任意の $H \in \mathcal{H}_{p,q}$ と任意の整数 r $(1 \leq r \leq p)$ に対して，第 $r+1$ 行目から第 p 行目までを H から除いて得られる H の部分行列を $H^{(r)}$ で表すことにする． ■

次は Isolatin lemma として知られているもの（の一つ）である．

補題 4.3§ [VV86] m を任意の正整数とし，S を $\mathcal{B}^m$ の任意

†符号化の基礎となる記号の集合を（例えば）3 進数にした場合には，この証明の中で述べた議論は成立しない．しかしながら，この場合でも，次のような結果を示すことができる．

$$\leq_{\mathrm{m}}\cdot\oplus\cdot\mathcal{C} = \leq_{\mathrm{m}}\cdot\oplus\cdot\mathrm{co}\cdot\mathcal{C}.$$

このことから，$\oplus$-オペレータを付加したとき，どのようなクラスであっても補集合演算を吸収してしまうと考えてよい．

‡参考：この定義の中で述べている $\vec{h}\cdot\vec{y}$ は線形空間 $\mathrm{GF}(2)^m$ の内積を表し，$G\cdot\vec{y}$ は $\mathrm{GF}(2)^m$ から $\mathrm{GF}(2)^r$ への線形写像を表している．また，$G * S$ は G によって表される線形写像の核と S との共通部分を表している．

の空でない部分集合とする．このとき，

$$\Pr\left[H \in \mathcal{H}_{2m,m} : \exists k\left[|H^{(k)} * S| = 1\right]\right] \geq 1/2$$

が成り立つ．■

以下は，Isolation lemma の非一様版である．次節ではこの補題を使用する．

補題 4.4 m を任意の正整数とする．このとき，$H_{1,m}, H_{2,m}, \ldots, H_{m,m} \in \mathcal{H}_{2m,m}$ が存在して，

$$\forall S \subseteq \mathcal{B}^m\left[S \neq \emptyset \rightarrow \exists i, r\left[|H^{(r)}_{i,m} * S| = 1\right]\right]$$

が成り立つ．なお，各行列に付けた 2 番目の添え字はこれらの行列が m に依存して定まることを明記するために使用している．

（証明）$(2^m-1)\times 2^{2m^2}$ の 2 次元の表 $T^{(0)}$ を次のように定める．T の各行は $\mathcal{B}^m$ の各部分集合（空集合は除く）に対応させ，$T^{(0)}$ の各列は $\mathcal{H}_{2m,m}$ に属する各行列に対応させる．そこで，$T^{(0)}$ の第 i 行に対応する $\mathcal{B}^m$ の部分集合を S_i で表し，T の第 j 列に対応する行列を G_j で表すとき，T の第 (i,j) 成分 $T^{(0)}_{i,j}$ を

$$T^{(0)}_{i,j} = \begin{cases} 1 & \text{if } \exists r\left[|G_j^{(r)} * S_i| = 1\right] \\ 0 & \text{otherwise} \end{cases}$$

と定める．

補題 4.3 より，$T^{(0)}$ の各行はその成分の半分以上が 1 になっている．従って，$T^{(0)}$ 全体で見ても半分以上の成分が 1 であることが分かる．このことより，$T^{(0)}$ のある列はその成分の半分以上が 1 になっているはずである．そこで，そのような $T^{(0)}$ の列を選択し，その列に対応する行列を $H_{1,m}$ とおく．更に，その列の中で成分 1 を含む行すべてを $T^{(0)}$ から削除することによって，新たな表 $T^{(1)}$ を作成する．$T^{(1)}$ についても表全体で見るとその成分の半分以上が 1 になっている．従って，$T^{(0)}$ の場合と同様に，半分以上の成分が 1 になっているような列を見つけることができる．そこで，この列に対応する行列を $H_{2,m}$ とおく．また更に，$T^{(0)}$ から $T^{(1)}$ を作ったときと同じ方法を用いて $T^{(1)}$ から $T^{(2)}$ を作る．

以上の操作を繰り返すことによって，いつかは表の中の行がすべて削除されることは明らかであろう．また更に，新たな表を作る際には，その直前の表の半分以上の行が削除されるので，上記の操作を高々 m 回実行することによってすべての行が削除されることも分かる．

以上の操作をちょうど m 回実行してすべての行を削除できたときには，この操作で得られた行列を所望の $H_{1,m}, \ldots, H_{m,m}$ とおけばよい．一方，m 回未満の操作によってすべての行を削除できたときには，まだ定義されていない残りの行列を適当に設定すればよい．

表 $T^{(0)}$ の定義の仕方より，以上で得られる行列が補題の条件を満たすことは明らかであろう．■

§[VV86] では，

$$\Pr\left[H \in \mathcal{H}_{m,m} : \exists k\left[|H^{(k)} * S| = 1\right]\right] \geq 1/4$$

となることが示されているが，この結果からここで述べている補題が直ちに得られる．

5 $\exists$,$\forall$ versus $\oplus$

本節では，$\exists$-オペレータや $\forall$-オペレータが $\oplus$-オペレータに置き換え可能であることを示す．

定理 5.1 任意のクラス $\mathcal{C}$ に対して，$\exists\cdot\mathcal{C} \subseteq \leq_{\mathrm{d}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$.

（証明）$\{\varphi_n\}$ を $\exists\cdot\mathcal{C}$ に属する任意の論理関数族とする．このとき，$\exists\cdot\mathcal{C}$ の定義より，論理関数族 $\{\psi_n\} \in \mathcal{C}$ と多項式 $p(n)$ が存在して，任意の $\vec{x} \in \mathcal{B}^*$ に対して，

$$\varphi_n(\vec{x}) = 1 \leftrightarrow \exists \vec{y} \in \mathcal{B}^{=p(n)}[\psi_{n+p(n)}(\vec{x},\vec{y}) = 1]$$

が成り立っている（ここで，$n = |\vec{x}|$）．以下では，$\{\psi_n\}$ が自明である場合と非自明である場合に分けて議論する．

場合 1 $\{\psi_n\}$ が自明であるとき．この場合，明らかに $\{\varphi_n\}$ も自明である．そこで，$\{\eta_n\}$ を $\tilde{\mathcal{C}}$ に属する非自明な論理関数族とし，$\eta_\ell(\vec{f}) = 0$ かつ $\eta_\ell(\vec{t}) = 1$ を満たす入力長 ℓ とビット列 $\vec{f}$, $\vec{t} \in \mathcal{B}^\ell$ を適当に選択する．また更に，論理関数 τ_{n+1} $(n \geq 1)$ を次で定める．任意の入力 $\vec{x} \in \mathcal{B}^{n+1}$ に対して：

- $\varphi_n = \mathbf{0}_n$ のとき，$\tau_{n+1}(\vec{x}) = \eta_\ell(\vec{f})$.
- $\varphi_n = \mathbf{1}_n$ かつ $x_{n+1} = 0$ のとき，$\tau_{n+1}(\vec{x}) = \eta_\ell(\vec{f})$.
- $\varphi_n = \mathbf{1}_n$ かつ $x_{n+1} = 1$ のとき，$\tau_{n+1}(\vec{x}) = \eta_\ell(\vec{t})$.

なお，τ_1 については，$\tau_1 = \eta_1$ と定めておく．

この $\{\tau_n\}$ の定義より，

(a) $\{\tau_n\} \leq_{\mathrm{m}} \{\eta_n\}$ が成り立つこと，従ってまた，$\{\tau_n\} \in \leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$ が成り立つこと，および，

(b) 任意の $\vec{x} \in \mathcal{B}^*$ に対して，

$$\varphi_n(\vec{x}) = 1 \leftrightarrow \oplus\vec{y} \in \mathcal{B}^1[\tau_{n+1}(\vec{x},\vec{y}) = 1]$$

が成り立つこと（ここで，$n = |\vec{x}|$），

は明らかであろう．以上より，$\{\varphi_n\} \in \oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$ が成り立つ．また，このことと命題 3.3(1) より，$\{\varphi_n\} \in \leq_{\mathrm{d}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$ が成り立つ．

場合 2 $\{\psi_n\}$ が非自明であるとき．この場合，まず $\psi_\ell(\vec{f}) = 0$ かつ $\psi_\ell(\vec{t}) = 1$ を満たす入力長 ℓ とビット列 $\vec{f}, \vec{t} \in \mathcal{B}^\ell$ を適当に選択する．ψ は非自明なので，このような $\ell, \vec{f}, \vec{t}$ が必ず存在することに注意されたい．次に，各正整数 m に対して，補題 4.4 で述べた行列 $H_{1,m}, H_{2,m}, \ldots, H_{m,m} \in \mathcal{H}_{2m,m}$ を適当に選択する．

● **$\{\tau_n\}$ の定義．** 以上の材料を用いて，各正整数 n, r（ただし，$1 \leq r \leq 2p(n)$）に対して論理関数 $\tau_{2(n+rp(n))}$ を次のように定義する．任意の $\vec{x} \in \mathcal{B}^n$, $H \in \mathcal{H}_{r,p(n)}$，および，$\vec{y}\vec{z} \in \mathcal{B}^{n+rp(n)}$（ただし，$\vec{y} \in \mathcal{B}^{p(n)}$ かつ $\vec{z} \in \mathcal{B}^{n+(r-1)p(n)}$）に対して：

(1) $\psi_{n+p(n)} = \mathbf{1}_{n+p(n)}$ のとき：

- $\vec{y}\vec{z} = 1^{n+rp(n)}$ ならば

$$\tau_{2(n+rp(n))}(\vec{x},H,\vec{y}\vec{z})=\psi_\ell(\vec{t})$$

とし，

- $\vec{y}\vec{z}\neq 1^{n+rp(n)}$ ならば

$$\tau_{2(n+rp(n))}(\vec{x},H,\vec{y}\vec{z})=\psi_\ell(\vec{f})$$

とする．

(2) $\psi_{n+p(n)}\neq 1_{n+p(n)}$ のとき：まず，$\psi_{n+p(n)}(\vec{f}_x,\vec{f}_y)=0$ を満たす $\vec{f}_x\in\mathcal{B}^n$ と $\vec{f}_y\in\mathcal{B}^{p(n)}$ を適当に選択する．

そこで：

- $H\cdot\vec{y}=0^r$ かつ $\vec{z}=0^{n+(r-1)p(n)}$ ならば

$$\tau_{2(n+rp(n))}(\vec{x},H,\vec{y}\vec{z})=\psi_{n+p(n)}(\vec{x},\vec{y})$$

とし，

- $H\cdot\vec{y}\neq 0^r$ または $\vec{z}\neq 0^{n+(r-1)p(n)}$ ならば

$$\tau_{2(n+rp(n))}(\vec{x},H,\vec{y}\vec{z})=\psi_{n+p(n)}(\vec{f}_x,\vec{f}_y)$$

とする．

また更に，$2(n+rp(n))$ (ただし，$1\leq r\leq 2p(n)$) という形で表すことができない任意の入力長 $m\geq 1$ に対して，$\tau_m=\psi_m$ と定めておく．

● $\{\tau_n\}\in\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$. 以上で定義される論理関数族 $\{\tau_n\}$ が $\{\psi_n\}$ に $\leq_{\mathrm{m}}$-還元可能であることは明らかである．この還元可能性を実現する回路族を明示的に定義したければ，任意の入力長 $m\geq 1$ に対して，これまでに述べた τ_m の定義における「$\tau_m(\vec{u})=\psi_\clubsuit(\vec{v})$ とする」(なお，$\clubsuit$ はそれぞれの文脈に応じた ψ の入力長を表す) という下りを「還元可能性を実現する回路 D_m は入力 $\vec{u}$ に対して $\vec{v}$ を出力する」と読み替えればよい．以上より，$\{\tau_n\}\in\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$ が成り立つ．

● $\{\mu_m\}$ の定義 & $\{\mu_m\}\in\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$. 次に，任意の正整数 m に対して，論理関数 μ_m を次のように定める．任意の $\vec{u}\in\mathcal{B}^m$ に対して：

$$\mu_m(\vec{u})=1\leftrightarrow\oplus\vec{v}\in\mathcal{B}^m[\tau_{2m}(\vec{u},\vec{v})].$$

以上で定義される論理関数族 $\{\mu_m\}$ が $\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$ に属することは明らかであろう．以下では，任意の正整数 n と任意の $\vec{x}\in\mathcal{B}^n$ に対して，

$$\varphi_n(\vec{x})=\bigvee_{i,r}\mu_{n+rp(n)}(\vec{x},H^{(r)}_{i,p(n)}) \qquad \cdots(*)$$

が成り立つことを示す．

● (*) の証明. まず，$\varphi_n(\vec{x})=0$ であった場合を考える．この場合，この証明の最初で述べた φ_n と $\psi_{n+p(n)}$ の関係より，任意の $\vec{y}\in\mathcal{B}^{p(n)}$ に対して，$\psi_{n+p(n)}(\vec{x},\vec{y})=0$ が成り立つ．従って，$\tau_{2(n+rp(n))}$ の定義の (2) より，任意の i,r と任意の $\vec{v}\in\mathcal{B}^{n+rp(n)}$ に対して，$\tau_{2(n+rp(n))}(\vec{x},H^{(r)}_{i,p(n)},\vec{v})=0$ が成り立つ．従ってまた，μ の定義より，任意の i,r に対して，$\mu_{n+rp(n)}(\vec{x},H^{(r)}_{i,p(n)})=0$ が成り立つ．以上より，$\varphi_n(\vec{x}=0$ であった場合には (*) が成り立つ．

次に，$\varphi_n(\vec{x})=1$ であった場合を考えていく．この場合，更に，二つの場合に分けて議論する．

まず，$\psi_{n+p(n)}=1_{n+p(n)}$ であった場合を考える．この場合，$\tau_{2(n+p(n))}$ ―ここで，$r=1$ としている点に注意― の定義の (1) より，任意の $\vec{v}\in\mathcal{B}^{n+p(n)}$ に対して，

$\vec{v}=1^{n+p(n)}$ ならば $\tau_{2(n+rp(n))}(\vec{x},H^{(r)}_{i,p(n)},\vec{v})=1$，かつ，

$\vec{v}\neq 1^{n+p(n)}$ ならば $\tau_{2(n+rp(n))}(\vec{x},H^{(r)}_{i,p(n)},\vec{v})=0$

が成り立つ．よって，この場合には ($H^{(r)}_{i,p(n)}$ とは無関係に)，$\mu_{n+rp(n)}(\vec{x},H^{(r)}_{i,p(n)})=1$ が成り立つ．従って，この場合にも (*) が成り立つ．

次に，$\psi_{n+p(n)}\neq 1_{n+p(n)}$ であった場合を考える．そこで，集合 $S_{\vec{x}}\subseteq\mathcal{B}^{p(n)}$ を

$$S_{\vec{x}}=\{\vec{y}\in\mathcal{B}^{p(n)}:\psi(\vec{x},\vec{y})=1\}$$

と定める．ここで，$\varphi(\vec{x})=1$ であることと $\{\varphi_n\}$ と $\{\psi_n\}$ との関係より，$S_{\vec{x}}\neq\emptyset$ であることに注意されたい．このとき，補題 4.4 より，ある i,r が存在して，

$$|H^{(r)}_{i,p(n)}*S_{\vec{x}}|=1$$

が成り立つ．いま，$H^{(r)}_{i,p(n)}*S_{\vec{x}}$ に属する唯一のビット列を $\vec{y}$ とおくことにする．このとき，$\tau_{2(n+rp(n))}$ の定義の (2) より，任意の $\vec{v}\in\mathcal{B}^{n+rp(n)}$ に対して，

$\vec{v}=\vec{y}0^{n+(r-1)p(n)}$ ならば $\tau_{2(n+rp(n))}(\vec{x},H^{(r)}_{i,p(n)},\vec{v})=1$，かつ，

$\vec{v}\neq\vec{y}0^{n+(r-1)p(n)}$ ならば $\tau_{2(n+rp(n))}(\vec{x},H^{(r)}_{i,p(n)},\vec{v})=0$

が成り立つ．従って，$\mu_{n+rp(n)}$ の定義より，

$$\mu_{n+rp(n)}(\vec{x},H^{(r)}_{i,p(n)})=1$$

が成り立つ．よって，この場合にも (*) が成り立つ．

以上より，上記の (*) が成立する．また，この (*) より，$\{\varphi_n\}\leq_{\mathrm{d}}\{\mu_n\}$ となることは明らかだろう．よって，$\{\varphi_n\}$ は $\leq_{\mathrm{d}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$ に属する． ■

命題 3.3 および定理 5.1 を用いることによって計算量クラス (というより，オペレータ) の間の非自明な関係が簡単に得られる．以下では，そのような非自明な関係の幾つかを示していく．

注意 以下の証明の中で，「3.3(n)」は命題 3.3 の (n) 番を表しており，「5.1」は定理 5.1 を表している．なお，自明と思われるものには命題や定理の番号を示さないこともある． ■

系 5.2 任意のクラス $\mathcal{C}$ に対して次が成り立つ．

$$\exists\cdot\mathcal{C}\cup\forall\cdot\mathcal{C}\subseteq\leq_{\mathrm{d}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}\cap\leq_{\mathrm{c}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}.$$

(証明) まず初めに，$\forall\cdot\mathcal{C}\subseteq\leq_{\mathrm{c}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$ を示す．

$$\begin{aligned}
\forall\cdot\mathcal{C} &= \mathrm{co}\cdot\mathrm{co}\cdot\forall\mathcal{C}\\
&= \mathrm{co}\cdot\exists\cdot\mathrm{co}\cdot\mathcal{C}\\
&\subseteq \mathrm{co}\cdot\leq_{\mathrm{d}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\mathrm{co}\cdot\tilde{\mathcal{C}} && (5.1)\\
&= \leq_{\mathrm{c}}\cdot\mathrm{co}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}} && (3.3(5)(8))\\
&\subseteq \leq_{\mathrm{c}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}} && (3.3(9))\\
&= \leq_{\mathrm{c}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}} && (3.3(2))
\end{aligned}$$

次に，$\exists\cdot\mathcal{C}\subseteq\leq_{\mathrm{c}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$ を示す．

$$
\begin{aligned}
\exists\cdot\mathcal{C} &= \mathrm{co}\cdot\mathrm{co}\cdot\exists\cdot\mathcal{C} \\
&= \mathrm{co}\cdot\forall\cdot\mathrm{co}\cdot\mathcal{C} \\
&\subseteq \mathrm{co}\cdot\leq_{\mathrm{c}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\mathrm{co}\cdot\tilde{\mathcal{C}} && \text{(前述の結果)} \\
&= \mathrm{co}\cdot\leq_{\mathrm{c}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}} && \text{(3.3(5)(8))} \\
&= \leq_{\mathrm{d}}\cdot\mathrm{co}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}} && \text{(3.3(5))} \\
&\subseteq \leq_{\mathrm{d}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}} && \text{(3.3(9)(2))}
\end{aligned}
$$

同様の方法を用いて，$\forall\cdot\mathcal{C}\subseteq\leq_{\mathrm{d}}\cdot\oplus\cdot\leq_{\mathrm{m}}\cdot\tilde{\mathcal{C}}$ も示すことができる．その詳細は読者に任せる． ■

系 5.3 任意のクラス $\mathcal{C}$ に対して次が成り立つ．

$$\exists\cdot\mathcal{C}\cup\forall\cdot\mathcal{C}\subseteq\oplus\cdot\leq_{\mathrm{d}}\cdot\tilde{\mathcal{C}}\cap\oplus\cdot\leq_{\mathrm{c}}\cdot\tilde{\mathcal{C}}.$$

（証明）上記の系と命題 3.3(2)(4) より明らか． ■

定義 5.4 各整数 $k\geq 0$ に対して，$\exists\forall^{k}\cdot\mathcal{C}$，$\forall\exists^{k}\cdot\mathcal{C}$，$\exists\forall^{*}\cdot\mathcal{C}$ を次で定める．

(1) $\exists\forall^{0}\cdot\mathcal{C}=\forall\exists^{0}\cdot\mathcal{C}=\mathcal{C}$,
(2) $\exists\forall^{k+1}\cdot\mathcal{C}=\exists\cdot\forall\exists^{k}\cdot\mathcal{C}$，$\forall\exists^{k+1}\cdot\mathcal{C}=\forall\cdot\exists\forall^{k}\cdot\mathcal{C}$,
(3) $\exists\forall^{*}\cdot\mathcal{C}=\bigcup_{k\geq 0}\exists\forall^{k}\cdot\mathcal{C}$. ■

定理 5.5 任意のクラス $\mathcal{C}$ に対して次が成り立つ．

$$\exists\forall^{*}\cdot\mathcal{C}\subseteq\oplus\cdot\leq_{\mathrm{d}}\cdot\tilde{\mathcal{C}}\cap\oplus\cdot\leq_{\mathrm{c}}\cdot\tilde{\mathcal{C}}.$$

（証明）k に関する帰納法を用いて，

$$\exists\forall^{k}\cdot\mathcal{C}\cup\forall\exists^{k}\cdot\mathcal{C}\subseteq\oplus\cdot\leq_{\mathrm{d}}\cdot\tilde{\mathcal{C}}\cap\oplus\cdot\leq_{\mathrm{c}}\cdot\tilde{\mathcal{C}}.$$

を証明すればよい．$k=0$ の場合は，命題 3.3(1)(10) より直ちに得られる．そこで，適当な k に関して，上記の包含関係が成り立っていたと仮定する．このとき：

$$
\begin{aligned}
&\exists\forall^{k+1}\cdot\mathcal{C}\cup\forall\exists^{k+1}\cdot\mathcal{C} \\
&\quad\subseteq \exists\forall^{k+1}\cdot\tilde{\mathcal{C}}\cup\forall\exists^{k+1}\cdot\tilde{\mathcal{C}} \\
&\quad= \exists\cdot\forall\exists^{k}\cdot\tilde{\mathcal{C}}\cup\forall\cdot\exists\forall^{k}\cdot\tilde{\mathcal{C}} \\
&\quad\subseteq \exists\cdot\oplus\cdot\leq_{\mathrm{d}}\cdot\tilde{\mathcal{C}}\cup\forall\cdot\oplus\cdot\leq_{\mathrm{d}}\cdot\tilde{\mathcal{C}} && \text{(帰納法の仮定)} \\
&\quad\subseteq \oplus\cdot\leq_{\mathrm{d}}\cdot\oplus\cdot\leq_{\mathrm{d}}\cdot\tilde{\mathcal{C}} && \text{(系 5.3)} \\
&\quad\subseteq \oplus\cdot\leq_{\mathrm{d}}\cdot\tilde{\mathcal{C}} && \text{(3.3(2)(3)(4))}
\end{aligned}
$$

同様の方法によって，$\exists\forall^{k+1}\cdot\mathcal{C}\cup\forall\exists^{k+1}\cdot\mathcal{C}\subseteq\oplus\cdot\leq_{\mathrm{c}}\cdot\tilde{\mathcal{C}}$ も証明できる． ■

最後に，これまでの結果を PSIZE に適用したものを示す．

系 5.6 $\exists\forall^{*}\cdot\mathrm{PSIZE}\subseteq\oplus\cdot\mathrm{PSIZE}$.

（証明）PSIZE が非自明な論理関数族を含むこと，ならびに，$\leq_{\mathrm{d}}\cdot\mathrm{PSIZE}=\leq_{\mathrm{c}}\cdot\mathrm{PSIZE}=\mathrm{PSIZE}$ が成り立つことは明らか．よって，上記の定理より，この系が直ちに得られる． ■

補題 5.7 $\mathrm{PSIZE}\subseteq\oplus\cdot\mathrm{BNF}$.

（略証） Cook の定理（CNF-SAT の NP 完全性）の証明を変形することによって，$\mathrm{PSIZE}\subseteq\oplus\cdot\mathrm{BNF}$ が簡単に示せる．詳細は読者に任せる． ■

系 5.8 $\exists\forall^{*}\cdot\mathrm{PSIZE}\subseteq\oplus\cdot\mathrm{BNF}$. ■

謝辞

今回の講演が皆さんに何らかの刺激を与えるものとはとうてい思えませんが，数え上げ問題は計算量理論とアルゴリズム論の両面から見て面白い対象だと思います．Permanent に代表されるような奇妙な性質を持った問題の分析，存在性判定問題や探索問題などとの関連性の探求，近似アルゴリズムの可能性の探求，多項式時間アルゴリズムの設計などに関して，まだ多くの課題が残されているように思います．参考文献には，特に基本的と思われる論文と最近の解説を掲載しました．少しでも興味を持たれた方々は，何か研究されてみることをお勧めしたいと思います．

最後になりますが，今回の講演の機会を与えて下さいましたアルゴリズム研究会ならびにコンピュテーション研究会の皆様に感謝致します．

参考文献

[For97] L.Fortnow: Counting Complexity, Complexity Theory Retrospective II(L.Hamaspaandra and A.Selman eds.), Chapter 4, 1997.

[SJ89] A.Sinclare and M.Jerrum: Approximation counting, uniform generating and rapidly mixing Markov chains, Info.Comp., Vol.82, 93–133, 1989.

[KLM89] R.Karp, M.Luby and N.Madras: Monte-Carlo approximation algorithms for enumeration problems, J. Algorithms, Vo.10, 429–448, 1989.

[KST93] J.Köbler, U.Schöning and J.Torán: The Graph Isomorphism Problem, Birkhäuser, 1993.

[Miy93] 宮野悟：並列アルゴリズム—理論と設計—，近代科学社，1993.

[Va79a] L.Valiant: The complexity of computing the permanent, Theoret. Comput. Sci., Vol.8, 189–201, 1979.

[Va79b] L.Valiant: The complexity of reliability and enumeration problems, SIAM J. Computing, Vol.8, 401–421, 1979.

[VV86] L.Valiant and V.Vazirani: NP is as easy as detecting unique solutions, Theoret. Comput. Sci., Vol.47, 85–93, 1986.

[Wel93] D.J.Welsh: Complexity: Knots, Colourings and Counting, London Math. Soc. Lecture Notes Series 186, 1993.