２００６年数学基礎論サマースクール
限定算術の新展開

黒田覚（群馬県立女子大学）

2006/8/31–9/2

目 次

1　イントロダクション

この講義では，計算量理論と弱い算術体系の理論の関わりについて，入門的な解説を行う．この２つの分野の関係が明確な形で表されたのは，S.Buss の学位論文 [1] においてである．Buss はその中で，本質的にペアノ算術の弱い部分体系となるような算術体系の階層

を定義し，それが多項式時間階層と対応することを示した．これがきっかけとなって算術体系を用いて様々な計算量クラスを表し，またそれらの性質が多くの研究者によって調べられており，この分野は証明論における主要な一分野として，今日まで発展を遂げてきた．

当初は，Buss 流の体系が研究の主流であったが，近年では Buss の提出した体系とは別の形のものも提案されてきており，中でも，２進列に直接言及するような体系は，その扱いやすさも手伝って，多くの結果が得られている．

そこでここでは，Buss の提出した体系と，Cook らによって研究が進められているいわゆる２種 (two-sort) の体系について、その計算量理論との関わりを中心に解説する．

2　計算量理論

今日では，計算量理論はその興味が多岐に分かれてきており，ひとことでそれをいいあらわすことは，極めて難しいであろうと思われる．しかしながら誤解を恐れずに言えば，そこにおける重要な問題は，$P = NP$ 問題に代表される計算量クラスの分離問題，ということになるであろう．この講義で扱う限定算術の理論も，この『分離問題』の解決のために提案されたアプローチであり，様々な計算量クラスに対応する算術体系を構成するということが，その出発点になる．そこで，この節では，計算量クラスの概説を目標とする．

計算量の概念は Hartimanis and Sterns [9] において，初めて明確な形で提出されている．この論文をきっかけにして，その基本的な性質が調べられたが，１９７０年代に入って S.A.Cook と R.M.Karp が独立に NP 完全問題の存在を発見し，これが特に２つの計算量クラス P と NP に対する興味を引き起こした．また Cook は [4] において，今日，$NP = co\text{-}NP$ 問題として知られているものと同等の問題を，命題論理における証明の複雑さとして述べ，この論文は，限定算術の理論の構築にも重要な役割をはたしている．

この後，いわゆる『計算量クラスの分離問題』とともに様々な計算量クラスが考案され，今日では１００を超える計算量クラスが提案され，その強さが調べられるに至っている．

以下では，限定算術の理論との関連が深い計算量クラスの基本概念と主要な結果について述べることにする．計算量理論全体の概観については Papadimitriou [18] などを参照のこと．

2.1　基本概念など

通常，コンピュータや回路などによる計算においては，データは２進数で表されることが多い．いま，２進数の１ビットを表す記号 $\Sigma = \{0, 1\}$ をアルファベットとよぶ．データは有限２進列で与えられ，それら全体の集合を

$$\Sigma^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots\}$$

で表すことにする．ここで，ε は空の列とする．この節では Σ^* の要素 x の長さを $|x|$ で表すことにする．ただし $|\varepsilon| = 0$ とする．

$A \subseteq \Sigma^*$ について，入力 $x \in \Sigma^*$ が A に属するかどうかを問う問題を決定問題という．以下では集合 $A \subseteq \Sigma^*$ をその決定問題と同一視して，単に決定問題 A という．A につい

ての決定問題を計算するアルゴリズムが存在するとき，A は決定可能，あるいは計算可能であるという．

以下に述べる O-記法は，計算量の定義に際して有用である．

定義 1 (O-記法) 自然数上の関数 $f(n)$ と $g(n)$ に対して，ある定数 c が存在して，十分大きな n について，$f(n) < c \cdot g(n)$ となるとき，$f(n) = O(g(n))$ と表す．

また本稿を通じて，対数の底は 2 とする．

2.2 チューリング機械と計算量

さて，まずチューリング機械モデルでの計算量について見てみよう．以下では，計算モデルはチューリング機械とする[1]．

決定問題 $A \subseteq \Sigma^*$ の時間計算量が $t(n)$ であるとは，A を決定するチューリング機械 M で，すべての入力 $x \in \Sigma^*$ に対して，M は $t(|x|)$ ステップ以内で計算を終了するものが存在するときをいう．また，A の領域計算量が $s(n)$ であるとは，A を決定するチューリング機械 M で，すべての入力 x に対して，M が x の下で使用する作業テープのセルの数が $s(|x|)$ で押さえられるときをいう．

これらの計算量の定義は，非決定性アルゴリズムに対して自然に拡張することが可能である．また，領域計算量の場合には，使用した入力テープの領域は考慮に入れられないことに注意する．

これらの定義から以下の計算量クラスが考えられる．

$$\begin{aligned}
\mathbf{P} &= \{A \subseteq \Sigma^* : A \text{ は } n^{O(1)}\text{時間計算可能 }\} \\
\mathbf{NP} &= \{A \subseteq \Sigma^* : A \text{ は 非決定性 } n^{O(1)}\text{時間計算可能 }\} \\
\mathbf{L} &= \{A \subseteq \Sigma^* : A \text{ は } O(\log(n)) \text{ 領域計算可能 }\} \\
\mathbf{NL} &= \{A \subseteq \Sigma^* : A \text{ は 非決定性 } O(\log(n)) \text{ 領域計算可能 }\}
\end{aligned}$$

定義から明らかに，

$$\mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{P} \subseteq \mathbf{NP}$$

であるが，これらの包含関係が proper かどうかはわかっていない．

決定性チューリング機械については，関数のクラスも自然に定義することができる．

関数 $f : \Sigma^* \to \Sigma^*$ が多項式時間計算可能であるとは，入力 $x \in \Sigma^*$ に対して，$f(x)$ を出力テープに書き出して，多項式時間で停止するチューリング機械が存在するときをいう．多項式時間計算可能な関数のクラスを **FP** で表す．

P や **NP** をオラクル付きチューリング機械によって一般化したものが，多項式時間階層である．

定義 2 $i \geq 0$ に対して，Δ_i^p，Σ_i^p および Π_i^p を次で定義する．

$$\begin{aligned}
&\Delta_0^p = \Sigma_0^p = \Pi_0^p = \mathbf{P} \\
&\Delta_{i+1}^p = \{A \subseteq \Sigma^* : A \text{ は } \Sigma_i^p \text{ の集合をオラクルとして } \mathbf{P} \text{ で決定可能 }\} \\
&\Sigma_{i+1}^p = \{A \subseteq \Sigma^* : A \text{ は } \Sigma_i^p \text{ の集合をオラクルとして } \mathbf{NP} \text{ で決定可能 }\} \\
&\Pi_i^p = \{A \subseteq \Sigma^* : \Sigma^* \setminus A \in \Sigma_{i+1}^p\}
\end{aligned}$$

[1] チューリング機械についての定義はここでは省略する．[18] などを参照されたい．

$\mathbf{PH} = \bigcup_{i \geq 0} \Sigma_i^p$ を多項式時間階層 *(polynomial hierarchy)* という．

これに対応する関数のクラスも定義しておく．

定義 **3** $i \geq 0$ に対して $\square_i^p = \mathbf{FP}^{\Sigma_i^b}$.

2.3 ブール値回路と計算量

チューリング機械に続いてよく使われる計算モデルに，ブール値回路 **(Boolean circuit)** がある．このモデルは，とくに **P** より弱い計算量クラスを定義するのに有効である．

ブール値回路は有向グラフを使って定義されるので，まずグラフに関するいくつかの定義を述べることにしよう．ある頂点に対して入る辺の数をその頂点の *fan-in*，頂点から出て行く辺の数を *fan-out* という．有向グラフがサイクルなしであるとは，そのすべての頂点について，自分自身に戻る路が存在しないときをいう．ブール値回路を考えるときには，頂点をゲートとよぶことにする．

入力数 n のブール値回路（以下，単に回路という）とは，以下の条件を満たすサイクルなしのラベル付き有向グラフ (labelled directed acyclic graph) のことである．

- あるゲートの fan-in が 0 のとき，そのゲートを入力ゲートといい，0 から $n-1$ までのいずれかの数字がラベルされている．
- あるゲートの fan-in が 1 のとき，そのゲートのラベルは $\wedge$, $\vee$, $\neg$ のいずれかである．
- あるゲートの fan-in が 2 以上のとき，そのゲートのラベルは $\wedge$, $\vee$, のいずれかである．

Fan-out が 0 のゲートを出力ゲートという．出力ゲートが 1 つの回路を単出力 **(single-output)** 回路といい，2 つ以上の回路を多出力 **(multi-output)** 回路という．

入力数 n の回路は，n ビットの入力が与えられると，その i ビット目をラベル i の入力ゲートに割りあてて，他のゲートの値をそのラベルの真理表にしたがって計算していく．そして，出力ゲートの値を回路の出力とする．

回路の場合，それぞれの回路が受け取る入力は，ビット数がある値に限られるため，Σ^0 上の問題を回路によって計算するためには，入力のビット数ごとに 1 つずつの回路を用意する必要がある．このことを以下のように定義する．

定義 **4** $A \subseteq \Sigma^*$ は以下を満たすとき，回路族 $\{C_n\}_{n \in \omega}$ によって受理されるという．

- すべての n に対して，C_n は入力数 n の単出力回路である．
- すべての n と $x \in \Sigma^n$ に対して，

$$x \in A \Leftrightarrow C_n \text{ は } x \text{ を受理する．}$$

以下では回路族 $\{C_n\}_{n \in \omega}$ を考えるとき，C_n の入力数は n であるとする．

さて，回路による計算量を定義しよう．いま C を回路とするとき，C のサイズ **(size)** を

$$size(C) = C \text{ に含まれるゲートの数}$$

C の深さ **(depth)** を

$$depth(C) = \max\{l : l \text{ は } C \text{ のある入力ゲートから出力ゲートまでの路の長さ }\}$$

とする．また，C の fan-in とは，C に含まれるゲートの fan-in の最大値とする．

この定義から次のような計算量クラスが考えられる．

定義 5 ある $i \geq 0$ に対して，$\mathbf{AC}^i$ はサイズ $n^{O(1)}$，深さ $O((\log n)^i)$ で，*fan-in* が無制限の回路族で計算される問題のクラスとする．また，$\mathbf{NC}^i$ はサイズ $n^{O(1)}$，深さ $O((\log n)^i)$ で，*fan-in* が *2* の回路族で計算される問題のクラスとする．

これらのクラスについて，次の包含関係が成り立つことは容易にわかる．

命題 1 すべての $i \geq 0$ について，$\mathbf{NC}^i \subseteq \mathbf{AC}^i \subseteq \mathbf{NC}^{i+1}$.

関数のクラスについては，出力の長さが多項式のものに限ることにする．関数 $f : \Sigma^* \to \Sigma^*$ が多項式増加 **(polynomial growth)** であるとは，ある多項式 $p(n)$ が存在して，すべての $x \in \Sigma^*$ に対して，$|f(x)| \leq p(|x|)$ であるときをいう．このとき，$\mathbf{FAC}^i$ はサイズ $n^{O(1)}$，深さ $O((\log n)^i)$ で，fan-in が無制限の多出力回路族で計算される，多項式増加関数のクラスとする．

さて，ここでひとつ問題がある．このようにして定義された計算量クラスは，このままでは不十分である．なぜなら、$\mathbf{NC}^0$ は極めて弱い計算量クラスであるにもかかわらず，計算不能集合を計算する $\mathbf{NC}^0$ の回路族が存在してしまうのである．これは次のように見ることができる．いま，$A \subseteq \mathbb{N}$ を計算不能集合とする．このとき，回路族 $\{C_n\}_{n\in\omega}$ を

$$C_n = \begin{cases} 1 & n \in A \text{ のとき} \\ 0 & n \notin A \text{ のとき} \end{cases}$$

とすると，この回路族は計算不能集合を計算し，サイズ，深さともに定数である．このような事態を避けるために，回路族を考えるときは，つぎの一様性を条件としてあたえることにする．

定義 6 関数族 $\{C_n\}_{n\in\omega}$ の *direct connection language(DCL)* とは，組 $(a, b, l, 0^n)$ で，

- a, b は C_n のゲートで, a は b から入力を受け取る．
- l はゲート a のラベルである．

となるものの集合とする．関数族が U_{E^*}**-一様 (uniform)** とは，その *DCL* が *DLOGTIME* のチューリング機械で決定可能であることをいう．

以下では，回路計算量クラスはすべて U_{E^*}-一様であると仮定する．

チューリング機械のクラスと，回路計算量のクラスには次のような関係がある．

命題 2 多項式時間計算可能なクラス $\mathbf{P}$ は多項式サイズの U_{E^*}-一様回路族で計算可能なクラスに一致する．

命題 3 $\mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{AC}^1$.

次の定理は回路計算量の下界性証明において，極めて重要である．

定理 1 (Yao [20], Håstad [10]) 入力ビットにおける 1 の数の偶奇性を計算する関数 $Parity$ は，$\mathbf{AC}^0$ に属さない．

この定理の証明に用いられた手法は**スイッチング補題 (switching lemma)** と呼ばれ，回路計算量や証明の複雑さに関する下界証明に極めて重要な手法を与えている．

これらをまとめると，上記の計算量クラスの間には以下のような関係がある．

$$\mathbf{NC}^0 \subsetneq \mathbf{AC}^0 \subsetneq \mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{AC}^1 \subseteq \cdots \subseteq \mathbf{P} \subseteq \mathbf{NP}.$$

2.4 完全問題

ほとんどの自然な計算量クラスには，**完全問題 (complete problem)** が存在することが知られている．完全問題は，その計算量クラスを代表する問題と考えることができるため，与えられたクラスの任意の問題を考えるよりは，完全問題を扱った方が議論がしやすいことも多い．

定義 7 $A, B \subseteq \Sigma^*$ に対して，A は B に多項式時間還元可能であるとは，$f \in \mathbf{FP}$ が存在して，任意の $x \in \Sigma^*$ に対して，

$$x \in A \Leftrightarrow f(x) \in B$$

が成り立つときをいう．このとき $A \leq_m^p B$ と書く．

L や **NL** は多項式時間計算可能性より弱いクラスなので，多項式時間還元可能性は意味がない．そこで，より弱い計算に関する還元可能性を考える．

定義 8 $A, B \subseteq \Sigma^*$ に対して，A は B に $\mathbf{AC}^0$-還元可能であるとは，$f \in \mathbf{FAC}^0$ が存在して，任意の $x \in \Sigma^*$ に対して，

$$x \in A \Leftrightarrow f(x) \in B$$

が成り立つときをいう．このとき $A \leq_m^0 B$ と書く．

定義 9 $\mathcal{C}$ を計算量クラスとし，$A \subseteq \Sigma^*$ とする．このとき，A が 多項式時間還元可能性（$\mathbf{AC}^0$-還元可能性）について $\mathcal{C}$-完全であるとは

1. $A \in \mathcal{C}$,
2. すべての $B \in \mathcal{C}$ に対して，$B \leq_m^p A$（$B \leq_m^0 A$）

が成り立つときをいう．

以下では混乱のおそれがない限り，還元可能性は省略して単に $\mathcal{C}$-完全という．

いくつかの計算量クラスについて，知られている完全問題を以下にあげておく．

Satisfiability： 充足可能性問題

$$SAT = \{P : P \text{ は充足可能な命題論理式 }\}$$

は **NP**-完全である.

Three coloring： 頂点 3 彩色問題

$$3COLOR = \{G : G \text{ は頂点を 3 色で塗り分けられるグラフ }\}$$

は **NP**-完全である.

Circuit value： 回路値問題

$$CVP = \{(C, x) : \text{回路 } C \text{ は入力 } x \text{ の下で 1 を出力する }\}$$

は **P**-完全である.

Satisfiability of Horn formulae: Horn 論理式に関する充足可能性問題

Horn 論理式とは conjunctive normal form で，それぞれのクローズには negative なリテラルが高々 1 つしか含まれないものとする．このとき

$$Horn\text{-}SAT = \{P : P \text{ は充足可能な Horn 論理式 }\}$$

は **P**-完全である.

st-Connectivity： 到達可能性問題.

$$st\text{-}Conn = \{(G, s, t) : \text{有向グラフ } G \text{ には頂点 } s \text{ から頂点 } t \text{ まで路が存在する }\}$$

は **NL**-完全である.

Deterministic st-Connectivity： 有向 forest に関する到達可能性問題

$$st\text{-}DConn = \{(G, s, t) : \text{有向 forest } G \text{ には頂点 } s \text{ から頂点 } t \text{ まで路が存在する }\}$$

は **L**-完全である.

Satisfiability for 2CNF： 2CNF に関する充足可能性問題

$2CNF$ は conjunctive normal form で，すべてのクローズは高々 2 つのリテラルしか含まない命題論理式とするとき,

$$2SAT = \{P : P \text{ は充足可能な } 2CNF\}$$

は **NL**-完全である.

2.5 記述計算量

記述計算量 (descriptive complexity) の理論は，有限モデル理論の一分野で，その応用は計算量理論に限らず，データベース理論や定理証明系など多岐にわたるが，計算量理論に限って考えると，決定問題の論理式による表現と，その計算量との間の関連を調べるのが主たる目的の一つである．

まず，はじめにおおまかなアイディアを与えた後に，基本概念と主要な結果を述べる．記述計算量および有限モデル理論については，Immerman [12] や Libkin [17] がよい入門書である．

いま，領域の大きさが有限の構造が与えられたとし，その領域を $\{0,1,\ldots,n-1\}$ とする．この構造が何を表すかは，その言語に含まれる述語記号によって決定される．例えば，2変数述語 $E(x,y)$ が含まれるような構造

$$\mathcal{A}_G = (\{0,1,\ldots,n-1\}, E^{\mathcal{A}_G})$$

は E を辺の接続関係と見なすことにより，頂点数 n の有向グラフを表している．また，自然な線形順序 $\leq$ と，1変数述語 P を持つ構造

$$\mathcal{A}_S = (\{0,1,\ldots,n-1\}, \leq^{\mathcal{A}_S}, P^{\mathcal{A}_S})$$

は，長さ n の2進列と見ることができる．このように，有限構造によって様々な対象を表現することが可能である．

ところで，いま無向グラフを表すような構造 $\mathcal{A}$ を考えたとき，この構造が「3彩色可能なグラフである」ということをこの言語上の論理式で書いたものを，φ_{3color} としよう．このとき，充足関係 $\mathcal{A} \models \varphi_{3color}$ は $\mathcal{A}$ が3彩色可能であるとき，そのときに限り成り立つことがわかる．2.4 で見たように，この問題は **NP**-完全であるから，φ_{3color} の論理式としての複雑さが，**NP** という計算量クラスを表していると予想するのは，極めて自然であろう．

これが，記述計算量と計算量クラスを結びつける基本的なアイディアであり，実際，多くの計算量クラスは論理式の自然なクラスに対応することが知られている．

では，上に述べたことをより厳密に表してみよう．まず基本的な概念を与える．定数記号と述語記号の集合

$$\tau = \{R_1^{a_1}, \ldots, R_r^{a_r}, c_1, \ldots, c_s\}$$

を**語彙 (vocabulary)** という．ここで，$R_i^{a_i}$ は a_i-変数述語記号，c_i は定数記号とする．一般の場合は関数記号も含めるが，ここでは入れないことにする．語彙 τ 上の（有限）構造とは組

$$\mathcal{A} = \langle \{0,1,\ldots,n-1\}, R_1^{\mathcal{A}}, \ldots, R_r^{\mathcal{A}}, c_1^{\mathcal{A}}, \ldots, c_s^{\mathcal{A}} \rangle$$

のことをいう．

例 **1**　*1.* E を2変数述語記号とするとき，$\tau = \{E\}$ 上の構造は有限グラフを与える．

2. min, max を定数記号，$\leq$ を2変数述語記号とし，$\tau = \{\leq, \min, \max\}$ とする．このとき τ 上の構造は $\leq$ を通常の大小関係，$\min = 0$, $\max = n-1$ と解釈することにより，全順序の入った構造と見なすことができる．これを**順序構造 (ordered structure)** という．

3. 2．に加えてさらに，3変数述語記号 $+, \times$ を考える．いま，$\tau = \{\leq, +, \times, \min, \max\}$ とするとき，τ 上の構造 $\mathcal{A}$ において，

$$\mathcal{A} \models +(x, y, z) \Leftrightarrow x + y = z$$
$$\mathcal{A} \models \times(x, y, z) \Leftrightarrow x \cdot y = z$$

と解釈すると，$\mathcal{A}$ は算術の構造となる．これを**算術構造 (arithmetical structure)** という．

語彙 τ 上の**ロジック (logic)** とは，τ 上の論理式の集合のことをいう．

例 **2** 1. **FO** は1階論理式，すなわち1階の量化子のみを含む論理式全体のロジックとする．

2. **SO** は2階論理式全体のロジックとする．

3. **SO∃** は1階論理式 φ に対して，$(\exists X_1) \cdots (\exists X_1)\varphi$ の形の論理式で構成されるロジックとする．

計算量クラスとロジックの関係は，次の定義によって与えられる．

定義 10 ロジック Φ が計算量クラス $\mathcal{C}$ を語彙 τ 上で**とらえる (capture)** とは，

1. すべての $\varphi \in \Phi$ と τ 上の構造 $\mathcal{A}$ に対して，関係 $\mathcal{A} \models \varphi$ は $\mathcal{C}$ のアルゴリズムで決定可能であり，

2. $C \in \mathcal{C}$ を τ 上の構造についての問題とする．このとき $\varphi \in \Phi$ が存在して，すべての $\mathcal{A} \in C$ に対して，

$$\mathcal{A} \in C \Leftrightarrow \mathcal{A} \models \varphi$$

が成り立つことをいう．

この関係が初めて知られたのは，次についてである．

定理 2 (Fagin [5]) **SO∃** はすべての語彙上で，**NP** をとらえる．

実は，この定理がユニークなのは,「すべての語彙上で」というところにある．というのは，**P** やその部分クラスに対しては，すべての語彙上でそのクラスをとらえるロジックは，知られていないからである．これに対して，例えば，**FO** については次が知られている．

定理 3 **FO** は順序を含む語彙上で，$\mathbf{AC}^0$ をとらえる．

では，$\mathbf{AC}^0$ と **NP** の間のクラスをとらえるロジックはどんなものだろうか？これについてはいくつかのアプローチがあるが，そのいずれも，それぞれのクラスに対する完全問題が重要な役割を果たす．

まず，2階論理式を使うものについてみてみよう．

定義 11 論理式が制限された **(restricted)SO∃** であるとは，それが量化子を含まない論理式 φ に対して，

$$(\exists X_1) \cdots (\exists X_k)(\forall y_1) \cdots (\forall y_l)\varphi(X_1, \ldots, X_k, y_1, \ldots, y_l)$$

の形で表されるときをいう．

この制限された **SO**∃ の部分クラスによって，**P** や **NL** などがとらえられることが，Grädel [7] によって示されている．

定義 12 量化子を含まない論理式 $\varphi(X_1,\ldots,X_k,y_1,\ldots,y_l)$ が $X_1,\ldots,X_k$ について *Horn* であるとは，φ が *CNF* であり，$X_1,\ldots,X_k$ を命題変数と見なしたとき，*Horn* 論理式であることをいう．同様に，$X_1,\ldots,X_k$ について *Krom* であるとは，$X_1,\ldots,X_k$ について *2CNF* であることをいう．

SO∃-$Horn$ は，制限された **SO**∃ で量化子のない部分 $\varphi(X_1,\ldots,X_k,y_1,\ldots,y_l)$ が $X_1,\ldots,X_k$ について *Horn* であるような論理式全体のロジックとする．同様に，**SO**∃-$Krom$ は，制限された **SO**∃ で量化子のない部分 $\varphi(X_1,\ldots,X_k,y_1,\ldots,y_l)$ が $X_1,\ldots,X_k$ について *Krom* であるような論理式全体のロジックとする．

定理 4 (Grädel [7]) *1.* **SO**∃-$Horn$ は順序を含む語彙上で，**P** をとらえる．

2. **SO**∃-$Krom$ は順序を含む語彙上で，**NL** をとらえる．

これらの証明には，Horn 論理式と 2CNF についての充足可能性がそれぞれ **P**-完全，**NL**-完全であることが用いられる．

3 限定算術

限定算術 (bounded arithmetic) は通常，指数関数が定義できないような，弱い算術体系のことを指す．このような体系が研究されるようになったのは，おそらく Paris と Wilkie による $I\Delta_0$ とその周辺の体系についての一連の研究が，きっかけとなったと思われる．

限定算術が計算量理論との関係で注目されるようになったのは，S. Buss による学位論文 [1] によるところが大きい．Buss はこの論文で，多項式階層に対応するような弱い算術システムの体系を提案し，それらに関する理論の基礎を築いた．これ以来，Buss による体系の研究が限定算術の理論の中心となり，多くの体系が提案され，それらについて多くの性質が知られるようになっている．

この節では，この Buss による体系が，どのような形で計算量クラスと結びついているかについて紹介する．

3.1 基本的な定義

まず限定算術の言語を定義する．限定算術の理論は，ペアノ算術などよりはるかに弱い帰納法公理しか持たないので，定義可能な関数はかなり弱いものになる．ところが，これらの体系において，ある種の計算のコード化などを行うためには，いくつかの関数が必要になるため，あらかじめ言語に基本的な関数を入れておく必要がある．したがって限定算術の言語，$\mathcal{L}_{BA}$ を次の記号を含むものとする．

- 変数：$x_0, x_1, \ldots$
- 定数記号：0, 1

- 関数記号：$S(x) = x + 1$, $x + y$, $x \cdot y$, $\lfloor \frac{x}{2} \rfloor$, $|x| = \lfloor \log_2(x + 1) \rfloor$, $x \# y = 2^{|x| \cdot |y|}$
- 述語記号：$x \leq y$, $x = y$

$\mathcal{L}_{BA}$ の項や論理式は，通常通り定義する．

有界量化子 **(bounded quantifier)** とは，$(\forall x \leq t)$, $(\exists x \leq t)$ の形のものをいう．ここで，t は x を含まない項とする．シャープな有界量化子 **(sharply bounded quantifier)** とは，上と同様の t について，$(\forall x \leq |t|)$, $(\exists x \leq |t|)$ のものをいう．量化子がすべて有界量化子であるような論理式を有界論理式 **(bounded formula)** という．

定義 13 $i \geq 0$ に対して，$\mathcal{L}_{BA}$-論理式の集合 Σ_i^b, Π_i^b を以下を満たす最小の集合として定義する．

- $\Sigma_0^b = \Pi_0^b$ は，量化子がすべてシャープな有界量化子であるような論理式の集合とする．
- Σ_i^b と Π_i^b は $\wedge$, $\vee$ とシャープな有界量化子について閉じている．
- $\varphi \in \Sigma_{i+1}^b$（または Π_{i+1}^b），$\psi \in \Pi_{i+1}^b$（または Σ_{i+1}^b）のとき，$\varphi \to \psi, \neg\psi \in \Sigma_{i+1}^b$（または Π_{i+1}^b）
- $\varphi(x) \in \Sigma_{i+1}^b$ のとき，$(\exists x < t)\varphi(x) \in \Sigma_{i+1}^b$ かつ $(\forall x < t)\varphi(x) \in \Pi_{i+2}^b$
- $\varphi(x) \in \Pi_{i+1}^b$ のとき，$(\exists x < t)\varphi(x) \in \Pi_{i+1}^b$ かつ $(\forall x < t)\varphi(x) \in \Sigma_{i+2}^b$

3.2 Buss の体系

さて，Buss による S_2^i と T_2^i の定義を述べることにする．これらの体系は，帰納法の公理によって公理化されるが，それらは次のようなものである．

BASIC は $\mathcal{L}_{BA}$ の記号を定義するような有限個の公理の集合とする．具体的な定義については，[1] などを参照のこと．

定義 14 Φ を論理式の集合とするとき，Φ-*IND*，Φ-*PIND*，Φ-*LIND* をそれぞれ次の公理図式とする．

- Φ-*IND* : $\varphi(0) \wedge (\forall x)(\varphi(x) \to \varphi(x + 1)) \to (\forall x)\varphi(x)$
- Φ-*PIND* : $\varphi(0) \wedge (\forall x)(\varphi(\lfloor \frac{x}{2} \rfloor) \to \varphi(x)) \to (\forall x)\varphi(x)$
- Φ-*LIND* : $\varphi(0) \wedge (\forall x)(\varphi(x) \to \varphi(x + 1)) \to (\forall x)\varphi(|x|)$

ここで，$\varphi \in \Phi$ とする．

定義 15 $i \geq 0$ とするとき，S_2^i は次の公理で公理化される，$\mathcal{L}_{BA}$-体系とする．

- *BASIC*
- Σ_i^b-*PIND*

T_2^i は S_2^i の Σ_i^b-*PIND* を Σ_i^b-*IND* で置き換えたものとする．

これらの体系について，次の関係が成り立つ．

命題 4 $i \geq 1$ のとき，$S_2^i \vdash \Sigma_i^b$-*LIND* かつ $BASIC + \Sigma_i^b$-*LIND* $\vdash \Sigma_i^b$-*PIND*.

命題 5 $i \geq 1$ に対して，$S_2^i \vdash \Pi_i^b$-*PIND* かつ $T_2^i \vdash \Pi_i^b$-*IND*.

命題 6 $i \geq 0$ に対して，$S_2^i \subseteq T_2^i \subseteq S_2^{i+1}$.

(証明) $S_2^i \subseteq T_2^i$ は $T_2^i \vdash \Sigma_i^b$-LIND と命題4から明らか．$T_2^i \subseteq S_2^{i+1}$ を示すには，$\varphi(x) \in \Sigma_i^b$ に対して，

$$S_2^{i+1} \vdash \varphi(0) \wedge (\forall x)(\varphi(x) \to \varphi(x+1)) \wedge \neg\varphi(a)$$

とする．このとき $\psi(x) \equiv (\forall y \leq a)(\psi(y) \to \psi(x+y))$ とおくと，

$$S_2^{i+1} \vdash \psi(0) \wedge (\forall x)(\psi(x) \to \psi(x+1))$$

であり，$\psi \in \Pi_{i+1}^b$ だから命題5により $\psi(a)$ となるが，$\psi(a) \to \varphi(a)$ だから仮定に矛盾する． □

限定算術の体系において，チューリング機械などの計算を定義するのには，文字列をコード化するような関数や，その性質についての述語などが必要になる．ところが，これらの関数や述語は言語には含まれていないので，あらためて用意する必要がある．このときに役に立つのが次の結果である．

定義 16 T を $\mathcal{L}_{BA}$-理論とし，Φ を $\mathcal{L}_{BA}$-論理式の集合とする．関数 f が T で Φ-定義可能であるとは，ある $\varphi \in \Phi$ に対して，

- $T \vdash (\forall \bar{x})(\exists! y)\varphi(\bar{x}, y)$ かつ，
- $\mathbb{N} \models (\forall \bar{x})(\exists y)\varphi(\bar{x}, f(\bar{x}))$

が成り立つことをいう．

定理 5 関数 $f(\bar{x})$ が S_2^1 で Σ_1^b-定義可能であるとする．このとき 関数記号 f とその定義式を S_2^1 につけくわえた体系 $S_2^1(f)$ は S_2^1 の保存拡大である．

述語についても同様にして，S_2^1 につけ加えることができる．

定義 17 述語 $R(\bar{x})$ が体系 T において Δ_i^b-定義可能であるとは，$\varphi, \psi \in \Sigma_i^b$ が存在して，

- $T \vdash (\forall \bar{x})(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$ かつ
- $\mathbb{N} \models (\forall \bar{x})(R(\bar{x}) \leftrightarrow \varphi(\bar{x}))$

が成り立つことをいう．

定理 6 R を S_2^1 で Δ_1^b-定義可能な述語とするとき，S_2^1 に記号 R とその定義式をつけ加えた体系 $S_2^1(R)$ は S_2^1 の保存拡大である．

次の定理は，限定算術においてもっとも基本的なものである．

定理 7 (Parikh の定理) T を S_2^i または T_2^i のいずれかとし，

$$T \vdash (\forall \bar{x})(\exists y)\varphi(\bar{x}, y)$$

とするとき，$\bar{x}$ のみを変数として含む $\mathcal{L}_{BA}$ の項 $t(\bar{x})$ が存在して，

$$T \vdash (\forall \bar{x})(\exists y \leq t(\bar{x}))\varphi(\bar{x}, y)$$

が成り立つ．

(証明) 証明論的な証明と，モデルを使った証明の両方が知られているが，ここでは簡明なモデルによる証明を紹介する．

今，x のみを変数とする項すべてを並べて, $t_1(x), t_2(x), \ldots$ とする．このとき，すべての $t_i(x)$ に対して，$T\neg\vdash (\forall x)(\exists \leq t_i(x))\varphi(x, y)$ であるとする．このとき

$$T + (\forall y \leq t_i(c))\neg\varphi(c, y)$$

は無矛盾であるから，コンパクト性定理により

$$T + (\forall y \leq t_1(c))\neg\varphi(c, y) + (\forall y \leq t_2(c))\neg\varphi(c, y) + \cdots$$

も無矛盾であり，この理論のモデル M が存在する．このとき，

$$K = \{a \in M : \text{ある } c \text{ に対して } M \models a \leq t_i(c)\}$$

とすると，$K \models T + (\forall y)\neg\varphi(c, y)$ となり，仮定に矛盾する． □

3.3 Cook の体系 PV

Cook は Buss より先に，多項式時間計算に対応する証明体系 PV を定義している．これはもともと，命題論理証明の複雑さをはかる道具として考えられたものであるが，のちに Buss の S_2^i や T_2^i とも深い関係があり，限定算術の理論において多くの応用があることがわかってきた．

Cook はこの体系を等式についての形式的体系 (equational system) として定義したが，ここではそれを 1 階述語論理に拡張したものを考える．この体系を定義するにはまず，計算量クラスの帰納数論的な特徴付けが必要となる．

定義 18 関数 f が g,h_0,h_1,k から *bounded recursion on notation (BRN)* によって定義されるとは，

$$\begin{aligned} &f(0, \bar{x}) = g(\bar{x}), \\ &f(2n, \bar{x}) = h_0(n, \bar{x}, f(n, \bar{x})) \quad n \neq 0 \text{ のとき}, \\ &f(2n+1, \bar{x}) = h_1(n, \bar{x}, f(n, \bar{x})) \end{aligned}$$

かつ，すべての n,$\bar{x}$ について $f(n, \bar{x}) \leq k(n, \bar{x})$ が成り立つときをいう．

これによって **FP** は次のように特徴づけられる．

定理 8 (Cobham [3]) **FP** は関数 $Z(x)=0$,$S_0(x)=2x$,$S_1(x)=2x+1$, $P_n^i(x_1,\ldots,x_n)=x_i$,$x\#y=2^{|x|\cdot|y|}$ を含み，合成と *BRN* について閉じている最小のクラスである．

これによって PV_1 を定義する．

定義 19 PV_1 を次で定義される体系とする．

- PV_1 の言語は，$\mathcal{L}_{BA}$ に定理 *8* によって与えられる関数を表す記号すべてを加えたものである．
- PV_1 の公理は，定理 *8* によって与えられる関数の定義式に，量化子のない論理式についての *PIND* 図式を加えたものである．

この体系は多項式時間階層に拡張される．

定義 20 $i\geq 1$ のとき PV_{i+1} を次で定義される体系とする．**FP** の帰納関数論的な定義に初期関数として，Σ_i^b 述語の特徴関数をつけ加えたものを $\mathbf{FP}_i$ とする．このとき

- PV_{i+1} の言語は，$\mathcal{L}_{BA}$ に $\mathbf{FP}_i$ の関数を表す記号をすべて付け加えたものである．
- PV_1 の公理は，$\mathbf{FP}_i$ の関数の定義式に，量化子のない論理式についての *PIND* 図式を加えたものである．

PV_i に対して，次のことが成り立つ．

定理 *9* $i\geq 1$ について PV_i は Π_1^0 公理化可能である．

このことと，*Herbrand* の定理により，PV_i で定義される関数は $\Box_i^p$ に一致することがわかる．また *Buss* の体系との関係については次のことが知られている．

定理 *10* $i\geq 1$ のとき，PV_i は T_2^i の保存拡大である．

このように，計算量クラスの帰納関数論的な定義は，算術体系を与えるのに有用であるが，Ferreira [6] や Kuroda [16] 等においても同様な体系が与えられている．計算量クラスの帰納関数論的な定義については，Clote-Kranakis [2] に詳細な解説がある．

3.4 Witnessing 定理

Buss は上述の体系について，そこで定義される関数や述語のクラスがある計算量クラスと一致することを示した．つまり S_2^i と T_2^i の階層は多項式時間階層に対応する体系である．このことを示すのに Buss は witnessing 法と呼ばれる手法を開発した．ここではこのしゅほうについて解説し，Buss の主定理を示す．

Witnessing 法のおおまかなアイディアは以下のとおりである．例えば S_2^1 を sequent calculus 上で形式化したものを考えることにして，Σ_0^b 論理式 $\varphi(a,x)$, $\psi(b,y)$ に対して，

$$(\exists x)\varphi(a,x)\longrightarrow(\exists y)\psi(a,y)$$

が S_2^1 で証明されるとする．S_2^1 についてカット除去定理が成り立つので，この sequent の証明で Σ_1^b 論理式のみを含むものが存在する．このときこの証明において $\varphi(a,f(a))$ を満

たすような多項式時間関数 f が存在するとき，$\psi(a, g(a))$ を満たすような多項式時間関数 g が存在することを，証明における推論規則の数についての帰納法により証明することができる．

では，このアイディアを形式的に遂行しよう．まず，S^i_2 を LK 上で形式化する．

定義 21 *LKB* は *LK* に以下の規則を加えた体系とする．

$$\frac{\varphi(t), \Gamma \longrightarrow \Delta}{t \leq s, (\forall x \leq s)\varphi(x), \Gamma \longrightarrow \Delta}\ (\forall \leq : left) \quad \frac{a \leq t, \Gamma \longrightarrow \Delta, \varphi(a)}{\Gamma \longrightarrow \Delta, (\forall x \leq t)\varphi(x)}\ (\forall \leq : right)$$

$$\frac{a \leq t, \varphi(a), \Gamma \longrightarrow \Delta}{(\exists x \leq t)\varphi(x), \Gamma \longrightarrow \Delta}\ (\exists \leq : left) \quad \frac{\Gamma \longrightarrow \Delta, \varphi(t)}{t \leq s, \Gamma \longrightarrow \Delta, (\exists x \leq s)\varphi(x)}\ (\exists \leq : right)$$

ここで，*(∀ ≤:right)* と *(∃ ≤:left)* の変数 a は下式にはあらわれないとする．

定義 22 *IND*，*PIND*，*LIND* をそれぞれ次の推論規則とする．

$$\frac{\Gamma, \varphi(a) \longrightarrow \varphi(a+1), \Delta}{\Gamma, \varphi(0) \longrightarrow \varphi(t), \Delta}\ (IND)$$

$$\frac{\Gamma, \varphi(\lfloor \frac{a}{2} \rfloor) \longrightarrow \varphi(a), \Delta}{\Gamma, \varphi(0) \longrightarrow \varphi(t), \Delta}\ (PIND)$$

$$\frac{\Gamma, \varphi(a) \longrightarrow \varphi(a+1), \Delta}{\Gamma, \varphi(0) \longrightarrow \varphi(|t|), \Delta}\ (LIND)$$

ここで φ をこれらの規則の主論理式 **(principal formula)** という．

このとき，S^i_2 は BASIC を初式に加えて，LKB に Σ^b_i 論理式についての PIND（または LIND) 規則を加えたものとして形式化できる．また，T^i_2 は同様に IND 規則を加えたものとなる．

このように形式化したとき，それぞれの体系についてカット除去定理が成り立つ．以下では，定理の主張のみを述べる．詳細については例えば Krajíček[15] などを参照のこと．

定理 11 $i \geq 1$ とし，S^i_2 で $\Gamma \longrightarrow \Delta$ が証明可能であるとする．このとき $\Gamma \longrightarrow \Delta$ の S^i_2 での証明で，どのカット論理式も *free* でないものが存在する．

これから次が得られる．

系 1 $i \geq 1$ とし，S^i_2 で $\Gamma \longrightarrow \Delta$ が証明可能であるとし，Γ および Δ に現れる論理式はすべて Σ^b_i または Π^b_i であるとする．このとき $\Gamma \longrightarrow \Delta$ の S^i_2 での証明で，そこに現れる論理式はすべて Σ^b_i または Π^b_i であるようなものが存在する．

以上で基礎的な準備が整ったので，証明の本質的な部分を述べることにしよう．以下では，

$$Seq(w) \Leftrightarrow w \text{ は文字の列のコードである．}$$

$$(w)_i = \text{列 } w \text{ の } i \text{ 番目の項目}$$

とする．これらはそれぞれ Δ^b_1-定義可能な述語と，Σ^b_1 定義可能な関数であるから，S^1_2 の中で自由に使うことができる．

定義 23 $i \geq 1$ とし，$\varphi \in \Sigma_i^b$ に対して，$\bar{a}$ をそれに含まれる自由変数とする．このとき論理式

$$Witness_{\varphi}^{i,\bar{a}}(w, \bar{a})$$

を次のように定義する．

1. $\varphi \in \Sigma_{i-1}^b \cup \Pi_{i-1}^b$ のとき，$Witness_{\varphi}^{i,\bar{a}}(w, \bar{a}) \equiv \varphi(\bar{a})$.
2. $\varphi \equiv \varphi_1 \wedge \varphi_2$ のとき，

$$Witness_{\varphi}^{i,\bar{a}}(w, \bar{a}) \equiv Seq(w) \wedge Witness_{\varphi_1}^{i,\bar{a}}((w)_1, \bar{a}) \wedge Witness_{\varphi_2}^{i,\bar{a}}((w)_2, \bar{a})$$

3. $\varphi \equiv \varphi_1 \vee \varphi_2$ のとき，

$$Witness_{\varphi}^{i,\bar{a}}(w, \bar{a}) \equiv Seq(w) \wedge (Witness_{\varphi_1}^{i,\bar{a}}((w)_1, \bar{a}) \vee Witness_{\varphi_2}^{i,\bar{a}}((w)_2, \bar{a}))$$

4. $\varphi(\bar{a}) \equiv (\forall x \leq |s(\bar{a})|)\varphi_0(x, \bar{a})$ で $\varphi \notin \Sigma_{i-1}^b \cup \Pi_{i-1}^b$ のとき，

$$Witness_{\varphi}^{i,\bar{a}}(w, \bar{a}) \equiv Seq(w) \wedge (\forall x \leq |s(\bar{a})|)Witness_{\varphi_0}^{i,x,\bar{a}}((w)_{x+1}, \bar{a})$$

5. $\varphi(\bar{a}) \equiv (\exists x \leq s(\bar{a}))\varphi_0(x, \bar{a})$ で $\varphi \notin \Sigma_{i-1}^b \cup \Pi_{i-1}^b$ のとき，

$$Witness_{\varphi}^{i,\bar{a}}(w, \bar{a}) \equiv Seq(w) \wedge (w)_2 \leq s(\bar{a}) \wedge Witness_{\varphi_0}^{i,x,\bar{a}}((w)_1, \bar{a}, (w)_2)$$

6. $\varphi \equiv \neg\varphi_0$ で $\varphi \notin \Sigma_{i-1}^b \cup \Pi_{i-1}^b$ のときは，$\neg$ を Σ_{i-1}^b 部分論理式まで押し込んでから，上のいずれかの規則を適用する．

補題 1 $i \geq 1$ とし，$\varphi \in \Sigma_i^b$ とするとき

1. $Witness_{\varphi}^{i,\bar{a}}(w, \bar{a})$ は S_2^i で Δ_i^b 定義可能である．
2. $PV_1 \vdash Witness_{\varphi}^{i,\bar{a}}(w, \bar{a}) \rightarrow \varphi(\bar{a})$.
3. $S_2^1 + BB\Sigma_i^b \vdash \varphi(\bar{a}) \rightarrow (\exists w)Witness_{\varphi}^{i,\bar{a}}(w, \bar{a})$.

さて，以上の準備により Buss の Witnessing 定理を述べることができる．

定理 12 (Witnessing 定理 [1]) $i \geq 1$ とし，$\varphi, \psi \in \Sigma_i^b$ に対して，

$$S_2^i \vdash \varphi(\bar{a}) \longrightarrow \psi(\bar{a})$$

とする．ここで $\bar{a}$ はこの *sequent* の自由変数すべてを含むとする．このとき PV_i の関数記号 $f(w, \bar{a})$ が存在して

- $f \in \Box_i^p$ かつ S_2^i で Σ_i^b 定義可能であり，
- $PV_i \vdash Witness_{\varphi}^{i,\bar{a}}(w, \bar{a}) \longrightarrow Witness_{\psi}^{i,\bar{a}}(f(w, \bar{a}), \bar{a})$

が成り立つ．

(証明) 定理の条件が成り立つとすると，系 1 により $A(\bar{a}) \longrightarrow B(\bar{a})$ の S_2^i における証明 π で，$\Sigma_i^b \cup \Pi_i^b$ の論理式のみを含むものが存在する．この π における式は

$$C_1, \ldots, C_k, D_1, \ldots, D_l \longrightarrow E_1, \ldots, E_u, F_1, \ldots, F_v$$

で，$C_j, E_j \in \Sigma_i^b$ $D_j, F_j \in \Pi_i^b$ の形をしていると仮定してよい．ここで

$$G = C_1 \wedge \cdots \wedge C_k \wedge \neg F_1 \wedge \cdots \wedge \neg F_v$$
$$H = E_1 \wedge \cdots \wedge E_u \wedge \neg D_1 \wedge \cdots \wedge \neg D_l$$

とおくとき，

$$PV_i \vdash Witness_G^{i,\bar{b}}(w, \bar{b}) \longrightarrow Witness_H^{i,\bar{b}}(g(w, \bar{b}), \bar{b})$$

となる $g \in \square_i^p$ が存在することを示せばよい．以下，π における推論規則の個数についての帰納法により証明するが，最後の推論規則が $(\exists \leq$:right)，カットと Σ_i^b-PIND のときのみを示し，それ以外は読者にゆだねる．

($\exists \leq$:right)

$$\frac{\Gamma \quad \longrightarrow \quad \Delta\varphi(t, \bar{a})}{t \leq s, \Gamma \quad \longrightarrow \quad \Delta, (\exists x \leq s)\varphi(x, \bar{a})}$$

の上式に対する witness を $g_0(w) = (w_1, v)$ とする．このとき t の値を $val(t)$ として，

$$g(u, w) = \begin{cases} 0 & t > s \text{ のとき} \\ (w_1, (val(t), v)) & t \leq s \text{ のとき} \end{cases}$$

と定義する．いま，w が Γ の witness であり，$t \leq s$ が成り立っているなら，(u, w) は $t \leq s, \Gamma$ の witness である．このとき，w_1 が Δ の witness であるか

$$Witness_{(\exists x \leq s)\varphi(x,\bar{a})}^{i,\bar{a}}((val(t), v), \bar{a})$$

であるかのいずれかが成り立つ．

(カット)

$$\frac{\Gamma \longrightarrow \Delta, \varphi \quad \Gamma, \varphi \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

上式の witness をそれぞれ $g_1(w) = (w_1, u)$, $g_2(v, w) = w_2$ とする．つまり例えば g_1 では w が Γ の witness のとき，w_1 は Δ の witness かまたは u は φ の witness となる．このとき

$$g(w) = \begin{cases} (g(w))_1 & Witness_\Delta^{i,\bar{b}}((g_1(w)), \bar{b}) \text{ のとき} \\ g_2((g_1(w))_2, w) & \text{それ以外} \end{cases}$$

とすると，

$$Witness_\Gamma^{i,\bar{b}}(w, \bar{b}) \rightarrow Witness_\Delta^{i,\bar{b}}(g(w), \bar{b})$$

が成り立つ．

(Σ_i^b-PIND) $\varphi(x) \in \Sigma_i^b$ として，

$$\frac{\Gamma, \varphi(\lfloor \frac{x}{2} \rfloor) \longrightarrow \varphi(x), \Delta}{\Gamma, \varphi(0) \longrightarrow \varphi(t), \Delta}$$

に対して，$g(w,u,x)=(u,w_0)$ が上式の witness であるとする．すなわち w が Γ の witness であり，u が $\varphi(\lfloor\frac{x}{2}\rfloor)$ の witness であるとき，v は $\varphi(x)$ の witness であるか，w_0 は Δ の witness であるかのいずれかが成り立つものとする．このとき，f をつぎのように BRN で定義する．

$$f(w,u,1)=\begin{cases}0 & \neg Witness^{i,\bar{b}}_{\varphi(0)}(u,\bar{b}) \text{ のとき}\\ g_0(w,u,1) & \text{それ以外}\end{cases}$$
$$f(w,u,2x)=g_0(w,(f(w,u,x))_1,2x)\quad x\neq 0 \text{ のとき}.$$

このとき，$f\in\Box^p_i$ であり，

$$g(w,u)=f(w,u,t)$$

とすれば，g は下式の witness となる． □

これにより S^i_2 で定義可能な関数の計算量が決定できる．

系 2 $i\geq 1$ とするとき，ある関数が S^i_2 で Σ^b_i-定義可能ならば それは $\Box^p_i$ の関数である．

（証明）ある $\varphi(x,y)\in\Sigma^b_i$ に対して定義されるとすると，

$$S^i_2\vdash(\forall x)(\exists y)\varphi(x,y)$$

が成り立つ．このとき定理 7 により，ある　$\mathcal{L}_{BA}$ の項 $t(a)$ が存在して，

$$S^i_2\vdash(\exists y\leq t(a))\varphi(a,y).$$

ここで定理 12 を $\longrightarrow(\exists y\leq t(a))\varphi(a,y)$ に適用すると，$f\in\Box^p_i$ に対して

$$PV_i\vdash Witness^{i,a}_{(\exists y\leq t(a))\varphi}(f(a),a)$$

が成り立つ．ここで $Witness^{i,a}_{\varphi}(w,a)$ の定義により，

$$Witness^{i,a}_{(\exists y\leq t(a))\varphi}(f(a),a)\Rightarrow Witness^{i,a,y}_{\varphi(y,a)}((f(a))_1,a,(f(a))_2)$$

が成り立つから，補題 1 により

$$PV_i\vdash\varphi(a,(f(a))_2)$$

であり，$g(x)=(f(x))_2\in\Box^p_i$ である． □

また，定義可能な述語についても次が得られる．

系 3 $i\geq 1$ とするとき，ある述語が S^i_2 で Δ^b_i-定義可能ならば，それは Δ^p_i に属する．

これ以外にも，定理 12 にはいろいろな応用があるが，ここでは次を述べておく．

系 4 S^1_2 は PV_1 の Σ^b_1-保存拡大である．$i\geq 1$ のとき S^{i+1}_2 は PV_1 と T^i_2 の Σ^b_{i+1}-保存拡大である

(証明) $\varphi(a) \in \Sigma^b_{i+1}$ に対して，$S^{i+1}_2 \vdash \varphi(a)$ とすると，定理 12 により，ある PV_{i+1} の関数 f が存在して

$$PV_{i+1} \vdash Witness^{i,a}_{\varphi}(f(a), a)$$

が成り立つ．このとき，補題 1 により，

$$PV_1 \vdash Witness^{i,a}_{\varphi}(f(a), a) \to A(a)$$

だから，$PV_{i+1} \vdash \varphi(a)$. □

Witnessing 定理については，上に紹介した証明の他にモデルを使った証明も得られている．これらについては Krajíček [15] および Hájek-Pudlák [8] に解説がある．

3.5 KPT witnessing

前節に結果により，S^i_2 が多項式時間階層の i 番目のクラスに対応していることがわかったわけであるが，これだけでは限定算術の分離問題と計算量クラスのそれとが関係しているかどうかは，定かではない．このことは以下に述べる KPT witnessing から示すことができる．

定理 13 (KPT witnessing) $i \geq 1$ とし $\varphi(a, x, y) \in \exists\Pi^b_i$ に対して，

$$T^i_2 \vdash (\exists x)(\forall y)\varphi(a, x, y)$$

が成り立つとする．このとき $k \in \mathbb{N}$ と $f_1, \ldots, f_k \in \square^p_i$ が存在して，

$$\varphi(a, f_1(a), b_1) \vee \varphi(a, f_2(a, b_1), b_2), \vee \cdots \vee \varphi(a, f_k(a, b_1, \ldots, b_{k-1}), b_k)$$

は T^i_2 で証明可能である．$i = 0$ のときは，PV_1 に対して同様のことが成り立つ．

(証明) $i \geq 1$ のとき，T^i_2 の代わりに PV_i を考えると，定理 10 によりこれは T^i_2 の保存拡大であり，定理 9 により Π^0_1 公理化可能であるから，Herbrand の定理により定理の主張が成り立つ．$i = 0$ のときも同様である． □

この形の witnessing 定理は，次の形の**反例計算 (counterexample computation)** としてとらえることができる．

定義 24 $\mathcal{C}_1$, $\mathcal{C}_2$ を計算量クラスとするとき，次の計算を反例数 l の $(\mathcal{C}_1, \mathcal{C}_2)$-反例計算という．

ステップ 1　生徒は入力に対して $\mathcal{C}_1$ のアルゴリズムで解の候補 a_1 を計算する．
先生は $\mathcal{C}_2$ でチェックできるような a_1 に対する反例の *witness* b_1 をオラクルとして与える．もしそれがなければ，a_1 を出力する．

ステップ 2　生徒は別の $\mathcal{C}_1$ のアルゴリズムで，元の入力と b_1 を使って解の候補 a_2 を計算する．
先生は a_2 に対する反例 b_2 がもしあれば，それをオラクルとして与える．

⋮

これを l 回繰り返し，解が見つかった時点でそれを出力する．

系 **5** $i \geq 1$ のとき，T_2^i で Σ_{i+2}^b-定義可能な関数は，反例数 $O(1)$ の $(\square_i^p, \Pi_{i+1}^b)$-反例計算で計算される．また PV_1 で Σ_2^b 定義可能な関数は，反例数 $O(1)$ の $(\square_1^p, \Pi_1^b)$-反例計算で計算される．

Krajíček, Pudlák, Takeuti [14] はこの定理を用いて次を示した．

定理 **14** $i \geq 1$ のとき，$T_2^i = S_2^{i+1}$ ならば，多項式時間階層 **PH** は $\Sigma_{i+1}^p = \Pi_{i+1}^p$ に一致する．同様に $PV_1 = S_2^1$ ならば，多項式時間階層は $\Sigma_2^p = \Pi_2^p$ に一致する．

証明はここでは省略する．

4　２種の限定算術

Buss の体系は自然数についての理論であり，そのモデルは自然数を土台とする構造である．これはペアノ算術などの，古典的な自然数の理論から派生したものと見ることができる．一方で，さまざまな計算モデルにおいては，入力や出力，またその計算などが２進列で与えられるため，これを Buss の体系内で扱うには，有限列のコーディングが必要になる．

Buss の体系ではこれを Σ_1^b-定義可能関数と，Δ_1^b-定義可能述語によるブートストラッピングという方法で解決してきたが，これとは別に最初から２進列を扱えるような言語において，形式体系を定義するという方法も考えられる．

ただし計算量の評価に際して，チューリング機械の計算ステップ数や回路のサイズなどを測るのに，自然数が扱えなければ，こんどは２進列で自然数をあらわすという全く逆の事態がおこってしまう．

このことを解決するためには、数と２進列の２種類の対象を扱うことができるような体系を考えればよいであろう．このような体系を考えるきっかけになったのは，すでに Buss の学位論文に現れていた２階の限定算術体系である．この体系は **PH** よりも強い計算量クラスに対応するものとして定義され，２階述語論理上で定義されていたが、のちにこのアイディアをもとに，１階述語論理の上で自然数の対象と２進列の対象を独立に扱ういわゆる２種の算術体系 **(two-sort system)** を扱う手法が定着した．

この体系は近年，Cook とその学生たちによって重点的に調べられ，特に **P** より弱いクラスに対応する算術体系を構成するための，極めて強力な手法となっている．

以下ではこの体系によって，様々な計算量クラスがどのように表現されるかについて解説する．

4.1　基本概念

まず始めに言語を定義する．２種の言語 $\mathcal{L}_2$ は以下の記号により構成される１階の言語とする．

- 数変数：$x_0, x_1, x_2, \ldots$
- 列変数：$X_0, X_1, X_2, \ldots$

- 定数記号：$0, 1$
- 関数記号：$x + y, x \cdot y, |X|$
- 述語記号 $x = y$, $x < y$, $x \in X$

列変数の意図するものは２進列であるが，２進列 X に対して，

$$x \in X \Leftrightarrow X \text{ の } x \text{ ビット目} = 1$$

として、これを有限集合と見なすこともできる．また $x \in X$ を $X(x)$ と表すこともある．

$\mathcal{L}_2$ は２種類の変数を持つ言語であるが，基礎となる論理は１階述語論理であることに注意する．したがって $\mathcal{L}_2$ の標準モデルは自然数と２進列の集合の組 $(\mathbb{N}, \Sigma^*)$ である．

数変数に対する量化子 $(\forall x), (\exists x)$ を**数量化子 (number quantifier)**，列変数に対する量化子を**列量化子 (string quantifier)** という．列に対する有界量化子を

$$(\forall X < t)\varphi(X) \Leftrightarrow (\forall X)(|X| < t \to \varphi(X))$$
$$(\exists X < t)\varphi(X) \Leftrightarrow (\exists X)(|X| < t \wedge \varphi(X))$$

で定義する．$\mathcal{L}_2$ の論理式はそこに含まれる量化子がすべて有界数量化子か，または有界列量化子のとき，有界論理式という．

Buss の体系の場合と同じように，有界論理式の階層を次のように定義する．

定義 25 $i \geq 0$ に対して，$\mathcal{L}_2$-論理式の集合 Σ_i^B, Π_i^B を以下を満たす最小の集合として定義する．

- $\Sigma_0^B = \Pi_0^B$ は，量化子がすべて有界数量化子であるような論理式の集合とする．
- Σ_i^B と Π_i^B は $\wedge, \vee$ と有界数量化子について閉じている．
- $\varphi \in \Sigma_{i+1}^B$（または Π_{i+1}^B），$\psi \in \Pi_{i+1}^B$（または Σ_{i+1}^B）のとき，$\varphi \to \psi, \neg\psi \in \Sigma_{i+1}^B$（または Π_{i+1}^B）
- $\varphi(X) \in \Sigma_{i+1}^B$ のとき，$(\exists X < t)\varphi(X) \in \Sigma_{i+1}^B$ かつ $(\forall X < t)\varphi(X) \in \Pi_{i+2}^B$
- $\varphi(X) \in \Pi_{i+1}^B$ のとき，$(\exists X < t)\varphi(X) \in \Pi_{i+1}^B$ かつ $(\forall X < t)\varphi(X) \in \Sigma_{i+2}^B$

4.2 体系 V-Φ

まず，２種の算術体系の一般的な形を定義する．

$BASIC_2$ は次の公理により構成されるものとする．

$x + 1 \neq 0$	$x + 1 = y + 1 \to x = y$
$x + 0 = x$	$x + (y + 1) = (x + y) + 1$
$x \cdot 0 = 0$	$x \cdot (y + 1) = (x \cdot y) + x$
$0 \leq x$	$x \leq x + y$
$x \leq y \wedge y \leq z \to x \leq z$	$x \leq y \wedge y \leq x \to x = y$
$x \leq y \vee y \leq x$	
$x \neq 0 \to (\exists y)(y + 1 = x)$	
$y \in X \to y < \|X\|$	$y + 1 = \|X\| \to y \in X$

定義 26 Φ を $\mathcal{L}_2$ 論理式の集合とするとき，$\mathbf{V}$-Φ は $BASIC_2$ にすべての $\varphi \in \Phi$ についてのビット内包公理 *(bit comprehension axiom)*

$$\Phi\text{-}COMP : (\exists X \leq b)(\forall z \leq b)(z \in X \leftrightarrow \varphi(z, \bar{a}, \bar{Y}))$$

を加えたものとする．また $\mathbf{V}^0 = \mathbf{V}\text{-}\Sigma_0^B$, $\mathbf{V}^1 = \mathbf{V}\text{-}\Sigma_1^B$ とする．

次に，$\mathbf{V}$-Φ についての基本的な性質を調べよう．

補題 2 Φ は数変数についての全称論理式すべてを含むとする．このとき次の最小値原理 *(least number principle)* は $\mathbf{V}$-Φ で証明可能である．

$$0 < |X| \rightarrow (\exists x < |X|)(X(x) \wedge (\forall y < x)\neg X(y))$$

(証明) Φ-COMP により

$$|Y| \leq |X|$$
$$(\forall z < |X|)(Y(z) \leftrightarrow (\forall i < |X|)(X(i) \rightarrow z < i)$$

を満たす Y が存在する．すなわち Y は，すべての X の要素より小さい数の集合である．このとき

$$X(|Y|) \wedge (\forall y < |Y|)\neg X(y)$$

は $BASIC_2$ から証明可能である． □

補題 3 Φ は数変数についての全称論理式すべてを含むとする．このとき次の帰納法原理 *(principle of induction)* は $\mathbf{V}$-Φ で証明可能である．

$$X(0) \wedge (\forall y < z)(X(y) \rightarrow X(y+1)) \rightarrow X(z)$$

(証明) 補題 2 により $\mathbf{V}$-Φ では最小値原理が成り立つ．最小値原理から帰納法原理が証明できることは例えば，Hájek-Pudlák[8] を参照のこと． □

系 6 Φ は数変数についての全称論理式すべてを含むとする．このとき，次の Φ-帰納法は $\mathbf{V}$-Φ で証明可能である．

$$\varphi(0) \wedge (\forall y < z)(\varphi(y) \rightarrow \varphi(y+1)) \rightarrow \varphi(z)$$

ここで，$\varphi \in \Phi$ とする．

(証明) Φ-COMP により，$X = \{y < z : \varphi(y)\}$ が存在する．この X に対して，補題 3 を適用すればよい． □

$\Sigma_0^B(\Phi)$ は Φ を含み，$\wedge, \vee, \neq$ と有界数量化子について閉じている最小の集合とする．このとき，

定理 15 $\mathbf{V}^0 \subseteq \mathbf{V}$-$\Phi$ ならば，$\mathbf{V}$-Φ において $\Sigma_0^B(\Phi)$ についての帰納法と内包公理は証明可能である．

(証明) $\varphi \in \Sigma_0^B(\Phi)$ についての帰納法による． □

4.3 制限された Σ_1^B による体系

体系 **V**-Φ は，とくに **FP** やその部分クラスに対応する算術体系として有効にはたらく．この基本的なアイディアは次のとおりである．

ある計算量クラス $\mathcal{C}$ がロジック Φ によって，語彙 τ 上でとらえられているとする．このとき Φ は τ 上の論理式の集合であるが，例えば τ として算術語彙を考えるとき，τ の論理式 φ は以下のようにして $\mathcal{L}_2$ の論理式 φ^* に翻訳することができる．

1. 原子論理式は，数変数の定数記号，関数記号と述語記号を使って書くことができる．例えば min は 0 とし，$+(x,y,z)$ は $x+y=z$ とする．
2. max は自由変数 n で翻訳する．φ に現れる 1 階の量化子 $(\forall x)$, $(\exists x)$ は $(\forall x < n+1)$, $(\exists x < n+1)$ で翻訳する．
3. 2 階変数 R は列変数で翻訳する．ただし R の引数が 2 つ以上のときは $R(x_1,\ldots,x_l)$ を $R^*(\langle x_1,\ldots,x_l\rangle)$ のようにする．2 階量化子 $(\forall X)$, $(\exists X)$ はそれぞれ $(\forall X < n+1)$, $(\exists X < n+1)$ で翻訳する．

この翻訳によって，例えば $SO\exists$ は Σ_1^B に翻訳される．

一方，**P** や **NL** などのクラスに対しては，定理 4 による特徴付けが与えられている．これを上記の翻訳によって $\mathcal{L}_2$ 論理式に直すとそれぞれ以下のようになる．

定義 27 量化子を含まない論理式 $\varphi(x_1,\ldots,x_k,P_1,\ldots,P_l)$ に対して，

$$(\exists P_1)\cdots(\exists P_l)(\forall x_1)\cdots(\forall x_k)\varphi(x_1,\ldots,x_k,P_1,\ldots,P_l)$$

の形の論理式を制限された **(restricted)**Σ_1^B という．

定義 28 量化子を含まない論理式が列変数 $P_1,\ldots,P_l$ について *Horn* であるとは，それが *CNF* であり，全てのクローズは $\neg P_i$ の形のリテラルを高々ひとつしか含まないときをいう．Σ_1^B-*Horn* は

$$(\exists P_1)\cdots(\exists P_l)(\forall x_1)\cdots(\forall x_k)\varphi(x_1,\ldots,x_k,P_1,\ldots,P_l,n,\bar{a},\bar{Y})$$

の形の論理式で，φ は $P_1,\ldots,P_l$ について *Horn* であるもの全体のクラスとする．

定義 29 量化子を含まない論理式が列変数 $P_1,\ldots,P_l$ について *Krom* であるとは，それが *CNF* であり，全てのクローズは P_i, または $\neg P_i$ の形のリテラルを高々ふたつしか含まないときをいう．Σ_1^B-*Krom* は

$$(\exists P_1)\cdots(\exists P_l)(\forall x_1)\cdots(\forall x_k)\varphi(x_1,\ldots,x_k,P_1,\ldots,P_l,n,\bar{a},\bar{Y})$$

の形の論理式で，φ は $P_1,\ldots,P_l$ について *Krom* であるもの全体のクラスとする．

定義 30 **V**-$Horn$ = **V**-Σ_1^B-*Horn*, **V**-$Krom$ = **V**-Σ_1^B-*Krom*.

このように定義された体系は対応する計算量クラス，すなわち **P** や **NL** に対応していると考えることは自然である．ところがこのためには，これらを関数のクラスとしてどのように定義するかということが，本質的な問題となる．

いま $\mathcal{C}$ に対応する関数のクラス $\mathcal{FC}$ を，

- ある多項式 $p(\bar{n})$ が存在して，全ての $\bar{X}$ に対して，$|F(\bar{X})| \leq p(|\bar{X}|)$，かつ
- 述語「$F(\bar{X})$ の i ビット目は 1 である 」は $\mathcal{C}$ で決定可能である

ような関数 F 全体のクラスとする．このとき **V**-$Horn$ や **V**-$Krom$ は $\mathcal{F}$**P** や $\mathcal{F}$**NL** を定義するような体系になっているであろうか．

実はこのことは，計算量クラスがある種の論理演算について閉じているかどうかということと，関わっている．たとえば **NL** は補集合演算について閉じているということは自明ではなく，このことは Immerman [11] と Szelepcsényi [19] によって独立に証明されている．このような性質を用いると，２種算術の体系と上記の関数のクラスの間に対応があることが示されるのであるが，次節においてこの一般的な議論を与える．

4.4 V-Φ での定義可能性と Witnessing

まず **V**-Φ で関数が定義されるということの，形式的な定義を与える．**V**-Φ では自然数と２進列の２種類の関数を扱うため，それぞれを値域とする関数を別々に定義する．

定義 31 数関数 *(number function)* とは

$$f : \mathbb{N}^k \times (\Sigma^*)^l \to \mathbb{N}$$

の形のものをいう．また列関数 *(string function)* とは

$$F : \mathbb{N}^k \times (\Sigma^*)^l \to \Sigma^*$$

の形のものをいう．

計算量クラスの関数バージョンは次のように定義される．

定義 32 $\mathcal{C}$ を計算量クラスとするとき，関数のクラス $\mathcal{FC}$ を次で定義する．

- 数関数 $f : \mathbb{N}^k \times (\Sigma^*)^l \to \mathbb{N}$ が $\mathcal{FC}$ の関数であるとは，$R \in \mathcal{C}$ と多項式 p が存在して，
$$f(\bar{x}, \bar{Y}) = \min_{i<p(\bar{x},|\bar{Y}|)} R(i, \bar{x}, \bar{Y})$$
となるときをいう．
- 列関数 $F : \mathbb{N}^k \times (\Sigma^*)^l \to \Sigma^*$ が $\mathcal{FC}$ の関数であるとは，$R \in \mathcal{C}$ と多項式 p が存在して，
$$F(\bar{x}, \bar{Y})(i) \Leftrightarrow i < p(\bar{x}, |\bar{Y}|) \wedge R(i, \bar{x}, \bar{Y})$$
となるときをいう．

関数や述語の体系 $\mathbf{V}$-Φ での定義可能性は，Buss の体系の場合と同様である．

定義 33 体系 $\mathbf{V}$-Φ が計算量クラス $\mathcal{C}$ に対応する[2]とは，その Σ_1^B-定義可能関数が $\mathcal{FC}$ に一致するときをいう．

定義 34 $\mathcal{L}_2$ 論理式の集合 Φ が計算量クラス $\mathcal{C}$ を表現する *(represent)* とは，Φ に対応する算術語彙上のロジック Φ' が $\mathcal{C}$ をとらえるときをいう．

$\mathbf{V}$-Φ についての Witnessing 定理では，次の性質が重要になる．

定義 35 $\mathcal{L}_2$ 論理式の集合 Φ は計算量クラス $\mathcal{C}$ を表現するものとする．このとき Φ が強く閉じている *(strongly closed)* とは，すべての $\varphi \in \Sigma_0^b(\Phi)$ に対して $\mathbf{V}$-$\Phi \vdash \varphi \leftrightarrow \varphi'$ となるような φ' が存在することをいう．

Φ が強く閉じているとするとき，特に $\mathbf{V}^0 \subseteq \mathbf{V}$-$\Phi$ であることに注意しよう．Σ_1^B-Krom や Σ_1^B-Horn などの制限された Σ_1^B は形式上は Σ_0^B を含まない．その一方で，$\mathbf{V}^0$ は Σ_0^B-COMP により公理化されており，Σ_0^B は FO に対応するクラスであるから，$\mathbf{V}^0$ は $\mathbf{AC}^0$ に対応するクラスと考えることができる．つまり，制限された Σ_0^B によって定義される体系をある計算量クラスに対応させるには，この条件があることが必要となる．

定義 36 $\mathcal{L}_2$ 論理式の集合 Φ は計算量クラス $\mathcal{C}$ を表現するものとする．このとき Φ が構成的である *(constructive)* とは，すべての $\varphi(\bar{a}, \bar{Y}) \in \Phi$ に対してある $\varphi'(\bar{a}, \bar{Y}) \in \Phi$ が存在して

- $\mathbf{V}$-$\Phi \vdash \varphi \leftrightarrow \neg\varphi'$ かつ，
- $\Sigma_0^b(\Phi)$ ビットグラフを持つ関数 $\bar{F}$ で $\bar{F}(\bar{a}, \bar{Y})$ が $\varphi(\bar{a}, \bar{Y}) \vee \varphi'(\bar{a}, \bar{Y})$ を *witness* するものが存在する

ときをいう．

つまり Φ が構成的であるとは，$\varphi \vee \varphi'$ の witness が $\mathcal{C}$ をオラクルとして $\mathbf{AC}^0$ で計算可能であるということであり，さらに Φ が強く閉じているときには，この witness は $\mathcal{C}$ で計算可能になる．したがって，とくに Φ が強く閉じているとするとき，Φ が構成的であるとは

> すべての $(\exists \bar{P})\varphi(\bar{P}) \in \Phi$ に対して $\mathbf{V}$-$\Phi \vdash (\exists \bar{P})\varphi(\bar{P})$ ならば，$\bar{P}$ を witness する関数 $\bar{F}$ でそのビットグラフが Φ に属するものが存在する

ことと同値になる．

さて，以上により $\mathbf{V}$-Φ が計算量クラス $\mathcal{C}$ を表現するための条件を，次のように述べることができる．

定理 16 (定義可能性定理 [13]) Φ は制限された Σ_1^B あるいは Σ_0^B で，構成的かつ $\mathcal{C}$ を表現するものとする．このとき，

[2] Kolokolova [13] では記述計算量と同様に「とらえる (capture)」が使われてるが，ここでは混同をさけるため,「対応する」とした．

- $\mathcal{FC}$ の関数はすべて $\mathbf{V}$-Φ で Σ_1^B-定義可能，かつ
- $\mathbf{V}$-Φ で Σ_1^B-定義可能な関数は $\mathbf{AC}^0(\mathcal{FC})$ に属する．

Φ がさらに強く閉じているとするとき，$\mathbf{V}$-Φ で Σ_1^B-定義可能な関数は $\mathcal{FC}$ に一致する．

証明は２つの部分にわけられる．

補題 4 Φ が構成的で $\mathcal{C}$ を表現するならば，$\mathcal{FC}$ の関数は Σ_1^B-定義可能である．

(証明) 列関数について考えることにする．$\mathcal{FC}$ の列関数 F に対して，

$$F(\bar{a},\bar{Y})(i) \leftrightarrow i < t(\bar{a},\bar{Y}) \wedge R(i,\bar{a},\bar{Y})$$

となる多項式 t と $R \in \mathcal{C}$ が存在する．Φ は $\mathcal{C}$ を表現するから，ある $\varphi \in \Phi$ に対して

$$F(\bar{a},\bar{Y})(i) \leftrightarrow i < t(\bar{a},\bar{Y}) \wedge \varphi(i,\bar{a},\bar{Y}).$$

よって Φ-COMP により $F(\bar{a},\bar{Y})$ の値が存在する．いま Φ は構成的だから，$\mathbf{V}$-$\Phi \vdash \varphi \leftrightarrow \varphi'$ となる $\varphi' \in \Sigma_1^B$ が存在する．このとき

$$\varphi^*(Z,\bar{a},\bar{Y}) \leftrightarrow (\forall i < |Z|)((Z(i) \wedge \varphi(i,\bar{a},\bar{Y})) \vee (\neg Z(i) \wedge \varphi'(i,\bar{a},\bar{Y})))$$

として φ^* を定義すると，これは F の Σ_1^B-定義を与える． □

２番目の部分は $\mathbf{V}$-Φ に対する witnessing 定理である．

定理 17 (一般化された witnessing 定理) Φ は 計算量クラス $\mathcal{C}$ を表現し，構成的であるとする．このとき $\varphi \in \Sigma_1^B$ に対して $\mathbf{V}$-$\Phi \vdash (\exists Z)\varphi(\bar{x},\bar{Y},Z)$ ならば，$\mathbf{AC}^0(\mathcal{FC})$ の列関数 $F(\bar{x},\bar{Y})$ が存在して

$$\mathbf{V}\text{-}\Phi, AX(F) \vdash \varphi(\bar{x},\bar{Y},F(\bar{x},\bar{Y})$$

となる．ここで $AX(F)$ は F の $\Sigma_0^B(\Phi)$ ビットグラフとする．Φ がさらに強く閉じているなら，ある $\psi \in \Phi$ に対して

$$\mathbf{V}\text{-}\Phi \vdash AX(F) \leftrightarrow \psi$$

が成り立つ．

定理 17 の証明は本質的に Buss の witnessing 定理と同じであるので，ここでは省略する．

4.5 定義可能性定理の応用

定義可能性定理（定理 16）の応用として，いくつかのクラス Φ について $\mathbf{V}$-Φ に対応する計算量クラスが決定できる．以下にその概略を示す．

定理 18 $\mathbf{V}^0 = \mathbf{V}\text{-}\Sigma_0^B$ は $\mathbf{AC}^0$ に対応する．

(証明) Σ_0^B は明らかに強く閉じており，$\mathbf{AC}^0$ を表している．また Σ_0^b 論理式には witness される量化子はないので、明らかに構成的である． □

定理 19 $\mathbf{V}$-$Horn$ は $\mathbf{P}$ に対応する．

以下に証明の概略を示す．まず次のことを証明する．

補題 5 すべての $\varphi \in \Sigma_1^B$-$Horn$ に対して $NEG_\varphi \in \Sigma_1^B$-$Horn$ が存在して

$$\mathbf{V}\text{-}Horn \vdash \neg\varphi \leftrightarrow NEG_\varphi$$

が成り立つ．

(証明の概略) 論理式 $RUN_\varphi(R, \tilde{R})$ を $(\exists R)(\exists \tilde{R})RUN_\varphi(R, \tilde{R}) \in \Sigma_1^B$-Horn で，次の２つが $\mathbf{V}$-$Horn$ で証明可能であるようなものとする．

$$(\exists R)(\exists \tilde{R})RUN_\varphi(R, \tilde{R}) \in \Sigma_1^B\text{-Horn},$$
$$RUN_\varphi(R, \tilde{R}) \rightarrow [(R(0) \leftrightarrow \varphi) \wedge (R(0) \leftrightarrow \varphi)].$$

この RUN_φ は Horn-SAT を決定する次のアルゴリズムを $\mathbf{V}$-$Horn$ の中で形式化することにより構成できる．

ステップ１：Horn 論理式 φ のすべての命題変数に $\bot$ を代入する．

ステップ２：充足されていないすべてのクローズについて，もしそれがポジティブなリテラルを含むなら，それに $\top$ を代入する．

ステップ３：ステップ２ができなくなるまで繰りかえし，ポジティブなリテラルを含まないクローズで充足されないものが残れば拒否，すべてのクローズが充足されれば受理する．

このとき，$NEG_\varphi \equiv RUN_\varphi(\top, \bot)$ とすればよい． □

これにより Σ_0^B-Horn は $\neg$ について閉じており，さらに強く閉じていることもわかる．また Σ_0^B-Horn 論理式は上に示したアルゴリズムにより，$\mathbf{V}$-$Horn$ において witness されることがわかる．

定理 20 $\mathbf{V}$-$Krom$ は $\mathbf{NL}$ に対応する．

この場合にも $\mathbf{V}$-$Krom$ の中で， $\mathbf{NL}$ が補集合演算（$\neg$）について閉じていることを示すのが本質的な部分になる．このことは Immmerman [11] と Szelepscényi [19] が独立に証明しているが，いずれも inductive counting とよばれる手法を用いて示されている．この手法は，ある有向グラフ G とその２つの頂点 s, t が与えられたとき，

$$G \text{ は } s \text{ から } t \text{ への道を持たない} \Leftrightarrow G' \text{ は } s' \text{ から } t' \text{ への道を持つ}$$

となるようなグラフ G' を構成するものである．

いま，$TrCl_\varphi(a, b)$ は (a, b) が２項関係 $\varphi(x, y)$ の推移的閉包に入っていることを表す述語とする．このとき $\mathbf{V}$-$Krom(TrCL)$ を $\mathbf{V}$-$Krom$ にすべての $\mathcal{L}_2$ の Σ_0^B 論理式 φ について述語記号 $TrCl_\varphi$ とその定義式をつけ加えた体系とする．このとき

補題 **6** $\mathbf{V}$-$Krom(TrCl)$ は $\mathbf{V}$-$Krom$ の保存拡大である．

が成り立つ．論理式 φ を有向グラフの辺を与える関係とするとき，$TrCl$ は頂点間の路を表すのでこれを使って inductive counting が $\mathbf{V}$-$Krom(TrCl)$ 内でできる．したがって

補題 **7** すべての $\mathcal{L}_2$ 論理式 $\varphi \in \Sigma_0^B$ に対して $\mathcal{L}_2$ 論理式 $\psi \in \Sigma_0^B$ が存在して，

$$\mathbf{V}\text{-}Krom(TrCl) \vdash TrCl_{\varphi}(a,b) \leftrightarrow \neg TrCl_{\psi}(a',b')$$

が成り立つ．

このことから

定理 **21** Σ_1^B-$Krom$ は強く閉じており，かつ構成的である．

が示される．

参考文献

[1] Buss. S. R., Bounded Arithmetic. Ph.D thesis. (1985) Published in 1986 by Bibliopolis, Naples.

[2] Clote, P., and Kranakis, E,. Boolean Functions and Computation Models. Springer (2001)

[3] Cobham, A., The intrinsic computational difficulty of functions. In Y. Bar-Hillel ed., Logic, Methodology and Philosophy of Science, pp.1–17.(1965)

[4] Cook, S. A., The complexity of theorem-proving procedures. In Proc. of the Third Annual ACM Symposium on the Theory of Computing (1971), pp.151–158.

[5] Fagin, R., Generalized first-order spectra and polynomial-time recognizable sets. In *Comlexity of Computation*, R. Karp, ed., SIAM-AMS Proceedings, 7 (1974), pp.43–73.

[6] Ferreira, F., Polynomial time computable arithmetic. In Logic and Computation. Contempurary Mathematics 106, American Mathematical Society (1987)

[7] Grädel, E., Capturing complexity classes by fragments of second order logic. Theoretical Computer Science, 101 (1992), pp.35–57.

[8] Hájek, P., and P. Pudlák, Metamathematics of First-Order Arithmetic. Springer-Verlag (1991).

[9] Hartmanis, J., and R. E. Sterns On the computational complexity of algorithms. Trans. AMS 117 (1965), pp.285–306.

[10] Håstad, J., Almost optimal lower bounds for small depth circuits. In: Randomness and Computation, ed. S. Micali, Ser.Adv.Comp.Res., 5 (1989) pp.143–70.

[11] Immerman, N., Nondeterministic space is closed under complementation. SIAM Journal on Computing, 17 (1988), pp.935–938.

[12] Immerman, N., Descriptive Complexity. Guraduate Texts in Computer Science, Springer (1999).

[13] Kolokolova, A., Systems of Bounded Arithmetic from Descriptive Complexity. Ph.D Dissertation, Toronto University, (2005).

[14] Krajíček, J., P. Pudlák, and G. Takeuti, Bounded arithmetic and the polynomial hierarchy, Annals of Pure and Applied Logic, 52, (1991), pp.143–153.

[15] Krajíček, J., Bounded Arithmetic, Propositional Logic, and Complexity Theory. Cambridge University Press (1995).

[16] Kuroda, S., On a theory for AC^0 and the strength of the induction scheme, Mathematical Logic Quarterly,44 pp.417-426 (1998).

[17] Libkin, L., Elements of Finite Model Theory. Springer (2004).

[18] Papadimitriou, C. Computational Complexity. Addison-Wesley. (1995).

[19] Szelepscényi, R., The method of forced enumeration for nondeterministic automata. Acta Informatica, 26 (1988) pp.279–284.

[20] Yao, Y., Separating the polynomial-time hierarchy by oracles, In: Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science, (1985) pp.1–10.