数理解析研究所講究録 1469 巻 2006 年 1-3

Second order bounded arithmetic and computational complexity

名古屋大学・情報科学研究科　安本　雅洋 (Masahiro Yasumoto)
School of Information Science,
Nagoya University

計算量理論における分離問題，特に **P** と **NP** の分離問題と関係の深い二階算術の未解決問題を紹介する．

1．$^*\mathbb{N}$ を $\mathbb{N}$ の elementary extension で ω_1-saturated, $n \in {}^*\mathbb{N} - \mathbb{N}$,

$$N = \{x \in {}^*\mathbb{N} | \, x < \overbrace{n\# \cdots \# n}^{k \text{ times}} \text{ for some } k \in \mathbb{N}\}$$

とする．ただし $\#$ は smash function，すなわち $n\#n = 2^{|n|^2} = 2^{\lceil \log_2(n+1) \rceil^2}$ で $|n|$ は n を 2 進数表示した時の桁数とする．$^*\mathbb{N}$ は N の endextension で N は smash function に関して閉じているので，

$$N \models \mathrm{I}\Sigma_0 + \Omega_1$$

ただし，$\Omega_1 \equiv \forall x \exists y (y = x\#x)$．$A$ を N の部分集合で

$$(N, A) \models \mathrm{I}\Sigma_0(A)$$

をみたすものとする．M を N の Σ_0-elementary substructure で N と cofinal，a を M の元，$\varphi(a, A)$ を $\Sigma_0(A)$-論理式で

$$(N, A) \models \varphi(a, A).$$

をみたすとする．

Open problem 1. M の部分集合 B で

$$(M, B) \models \mathrm{I}\Sigma_0(B) + \varphi(a, B).$$

となるものは存在するか？

この問題を考える時，最初に思いつくのは $B = M \cap A$ ではダメなのか？ということですが，次の例でわかるようにうまくいかない．

例. $c \in N - M, A = \{x \in N | 0 \leq x \leq c\}$

A には最大元 c があるが，$M \cap A$ にはない．すなわち，$c < a \in M$，$\varphi(a, A) \equiv \exists x < a(x \in A \wedge \forall y < a(y \in A \to y \leq x)$ とすると

$$(N, A) \models \varphi(a, A)$$

$$(M, M \cap A) \models \neg\varphi(a, M \cap A).$$

この例の A に対しては，B を次のようにとると Open Problem 1 は成立する．

M は N において cofinal だから $c < d$ となる M の元 d がある．$\varphi(a, A)$ の中の $v \in A$ を $v \leq c$ で置き換えてできる論理式を $\varphi'(a, c)$ と書くことにすると，$c \in N$ だから

$$N \models \exists x < d\varphi'(a, x).$$

M は N の Σ_0-elementary substructure だから，

$$M \models \exists x < d\varphi'(a, x)$$

$M \models \varphi'(a, b)$ をみたす $b \in M$ をとり，$B = \{x \in M | 0 \leq x \leq b\}$ とすると

$$(M, B) \models \mathrm{I}\Sigma_0(B) + \varphi(a, B).$$

Open problem 2. M の部分集合の集合 $\mathcal{M}$ で $(M, \mathcal{M}) \models U_2^1$ となるものは存在するか？

$\mathbf{P} = \mathbf{NP}$ を仮定すると，Open problem 2 の反例 (PTC(n)) が存在する ([]). 従って，Open problem 2 がどのような M に対して成立するか，ということが計算量理論における $\mathbf{P}$ と $\mathbf{NP}$ の分離問題を考える上で重要になる．

まず最初に，$M = N$ の場合を考える．この場合は Open problem 2 が成立することが次のようにして示される．$x \in {}^*\mathbb{N}$ に対して，

定義. $A_x = \{i \in {}^*\mathbb{N} |\ \mathrm{bit}(x, i) = 1\}$

とする．ここで，$\mathrm{bit}(x, i)$ は x を 2 進数表示した時の i 桁目を表す．$\mathcal{N} = \{A_x | \exists y \in N(x < 2^y)\}$ とすると，$(N, \mathcal{N}) \models U_2^1$ になる．

一般の $M \prec_{\Sigma_0} N$ の場合は，$(N, \mathcal{N}) \models U_2^1$ を使って $(M, \mathcal{M}) \models U_2^1$ となる $\mathcal{M} \subset \mathcal{P}(M)$ を構成することを考える．一階述語論理において elementary substructure を構成する方法 (skolem hull) を二階の構造である $\mathcal{N}$ に使おうとすると Open problem 1 を解決する必要が生じる．その時に重要なのは，M の部分集合 B で Σ_0-帰納法をみたすものをどのように作るかということであるが，このような方法としては forcing method がよく使われる ([1][2][3]). 特に [1] の方法を発展させて Open problem 1 を解決することが最も可能性があると考えられる．

2．Open problem 1 の A で具体的なものについて考える．x を $\mathbb{N}$ の元とする．

定義. *x is Σ_0-definable over M if there exists a Σ_0-formula $\psi(v,w)$ and $a \in M$ such that*

$$A_x = \{v \in N | N \models \psi(v,a)\}.$$

x が Σ_0-definable over M ならば, $\exists c \in M(x < 2^c)$. x, y が Σ_0-definable over M ならば, $x+y$ も Σ_0-definable over M である. 実際, $A_x = \{v \in N | N \models \psi(v,a)\}$, $A_y = \{v \in N | N \models \chi(v,b)\}$ とすると,

$$\begin{aligned} A_{x+y} = \{v \in N | N \models\ & (((\psi(v,a) \wedge \chi(v,b)) \vee (\neg\psi(v,a) \wedge \neg\chi(v,b))) \\ & \wedge \exists w < v(\psi(w,a) \wedge \chi(w,b) \\ & \quad \wedge \forall z < v(w < z \to ((\psi(v,a) \wedge \neg\chi(v,b)) \vee (\neg\psi(v,a) \wedge \chi(v,b))))) \\ & \vee (((\psi(v,a) \wedge \neg\chi(v,b)) \vee (\neg\psi(v,a) \wedge \chi(v,b))) \\ & \wedge \exists w < v(\neg\psi(w,a) \wedge \neg\chi(w,b) \\ & \quad \wedge \forall z < v(w < z \to ((\psi(v,a) \wedge \neg\chi(v,b)) \vee (\neg\psi(v,a) \wedge \chi(v,b)))))\}. \end{aligned}$$

Open problem 3. *x, y が Σ_0-definable over M ならば, $x \cdot y$ も Σ_0-definable over M になるか?*

Open problem 1 において $A = A_{x \cdot y}$ の場合を考える. もし Open problem 3 が正しければ, $B = A_{x \cdot y} \cap M$ とすればよい. しかし, Open problem 3 は正しくないと予想されるので, その場合 $B = A_{x \cdot y} \cap M$ としてよいかが問題になる.

Open problem 4. *x, y が Σ_0-definable over M ならば,*

$$(M, A_{x \cdot y} \cap M) \models \mathrm{I}\Sigma_0(A_{x \cdot y} \cap M).$$

さらにこの問題をもっと一般化して考える. $f \in$ FLogspace とする. ここで FLogspace は対数領域計算可能関数の集合を表す..

Open problem 5. *x が Σ_0-definable over M ならば,*

$$(M, A_{f(x)} \cap M) \models \mathrm{I}\Sigma_0(A_{f(x)} \cap M).$$

Open problem 5 がすべての $f \in$ FLogspace に対して成立するなら Flogspace≠FNP([4]).

References

1. Ajtai, M., *The complexity of the pigeonhole principle*, Combinatorica **14** (1992), 417-433.
2. Mostwski, A., *A remark on models of Gödel-Bernays axioms for set theory*, Studies in Logic and the Foundations of Math. **84** (1976), 325-340.
3. Paris, A. and Wilkie, A., *Counting problems in bounded arithmetic*, LNM **1130** (1985), 317-340.
4. Yasumoto M., *Separation of first and second order theories in bounded arithmetic*, Archive for Mathematical Logic **44** (2005), 685-688.