Proof Complexity and Computational Complexity-Part II
（命題論理証明の複雑さについて）

黒田 覚（群馬県立女子大学文学部総合教養学科（予定））

2008 年 9 月 18 日〜20 日
ラムダ計算と論理の晩夏セミナーに於いて

1　イントロダクション

命題論理証明の複雑さの問題は，Gödel が von Neumann へ宛てた手紙 [3] において初めて指摘されたとされる．この問題はその後，1975 年に Cook と Reckhow が定式化し，それ以降，様々な結果が得られている．

ここにおける基本的な問題は，与えられた命題論理証明体系における種々ののトートロジーの証明サイズがどの程度であるかということである．容易にわかることとして，ある命題がトートロジーかどうかは，それに含まれる命題変数の数の指数程度であれば調べられる．したがって問題は，それより本質的に短いサイズ（例えば多項式サイズ）の証明が存在するかどうかということになる．

特に，どのようなトートロジーに対しても多項式サイズの証明が存在するかどうか，という問題は，後述のように計算の複雑さについての基本的な問題と関係があり，これは否定的に解決されるだろうと予想されているが，一部の証明体系をのぞいては，その証明サイズが多項式を超えるようなトートロジーが存在することを証明するのは極めて難しいと考えられている．

したがって，証明の複雑さの理論においては，与えれられた証明体系に対してその証明が多項式を超えるようなトートロジーが存在することを示すことが，基本的な課題であるということができるだろう．

以下で，この分野の概略をみていくことにするが，基本的に証明は省くことにする．興味を持たれた場合は，関連する論文（たとえば [9], [10] など）を参照されたい．

2　基本事項

まず，命題論理についての基本的な定義と性質をについて触れる．命題論理式は，命題変数 $p_0, p_1, \ldots,$ から $\neg, \wedge, \vee$ を用いて作られる論理式である．命題変数はそれぞれが 0（偽）または 1（真）の値をとる．命題変数 $p_0, \ldots, p_k$ を含む論理式 $\varphi(p_1, \ldots, p_k)$ はその命題変数に対する真理値がすべて与えられたとき，真理表に従って真理値をとる．したがって命題論理式はブール値関数

$$f_\varphi : \{0,1\}^k \to \{0,1\}$$

に対応しているとみることができる．

命題論理式 φ はどのような真理値の与え方に対してもかならず真になるとき，**トートロジー**であるという．トートロジーの集合を TAUT で表す．

次に命題論理の証明体系とは何かについて考えよう．直感的には命題論理の証明とはある命題論理式がトートロジーであるかどうかをチェックするための手続きということになる．つまり与えられた手続きによるある論理式の『証明』が存在するときにその論理式はトートロジーであり（健全性），逆にトートロジーであれば必ず『証明』が存在する（完全性）ような体系を考えたい．このことを Cook と Reckhow は次のように形式化した：

定義 1 命題論理体系とは，多項式時間決定可能な 2 項関係 $P(x, y)$ で

$$\varphi \in \mathrm{TAUT} \Leftrightarrow \exists y P(\varphi, y)$$

となるようなものをいう．このとき y を φ の証明という．

すなわち論理式 φ に対して，与えられた列 y がその証明になっているかどうかを，多項式時間でチェックできるようなシステムのことを証明体系と呼ぶのである．この多項式時間という条件はいくらか恣意的にも思われるが，これによって次のようなきれいな関係が得られる：

定理 1 (Cook and Reckhow [5]) すべての $\varphi \in \mathrm{TAUT}$ に対して多項式サイズの証明が存在するような命題論理体系が存在することと，$NP = co\text{-}NP$ であることとは同値である．

定理 1 は TAUT が co-NP であることから証明される．

さてこのようにしてさまざまな命題論理体系を考えるとき，その間の強さを比較するための基準をもうけることにしよう．

定義 2 P, Q を命題論理体系とする．P が Q を *p-simulate* するとはある多項式時間計算可能関数 f が存在してすべての $\varphi \in \mathrm{TAUT}$ に対して

$$Q(\varphi, y) \leftrightarrow P(\varphi, f(y))$$

が成り立つことをいい，このことを $Q \leq_p P$ で表す．P と Q がお互いを *p-simulate* するとき $P \equiv_p Q$ で表す．

3　フレーゲ体系

フレーゲ体系とは通常の命題論理証明系をさす．その公理や推論規則はいろいろなものが採用されるが，以下にその一つの例を挙げる．

定義 3 体系 $\mathcal{F}$ は以下の公理を持ち，推論規則としてモーダス・ポーネンスのみを持つ体系である．

1. $A \to (B \to A)$
2. $A \wedge B \to B$
3. $(A \to B) \to (A \to B \to C) \to (A \to C)$
4. $A \wedge B \to A$
5. $A \to A \vee B$
6. $A \to B \to A \wedge B$
7. $(A \to B) \to (A \to \neg B) \to \neg A$
8. $B \to A \vee B$
9. $(A \to C) \to (B \to C) \to (A \vee B \to C)$
10. $\neg\neg A \to A$

$\mathcal{F}$ 証明とは命題論理式の列 $\varphi_1, \ldots, \varphi_m$ で各 φ_i は上の公理のうちのいずれかまたは φ_j, φ_k $(j, k < i)$ からモーダス・ポーネンスによって得られるかのいずれかであるようなものをいう．

定理 2 体系 $\mathcal{F}$ は完全かつ健全である．すなわちある命題論理式の $\mathcal{F}$ 証明が存在することと，それがトートロジーであることとは同値である．

フレーゲ体系における証明は，我々が「証明」と呼んでいるものの形式化としてはきわめて自然なものであるといえるだろう．さて，このような証明に対してその複雑さを定義しよう．

定義 4 φ を命題論理式とする．φ のサイズ $\mathrm{size}(\varphi)$ はそれに含まれる論理結合子の数とする．また深さ $\mathrm{depth}(\varphi)$ は次で帰納的に定義される：

- φ が命題変数のとき，$\mathrm{depth}(\varphi) = 0$,
- $\mathrm{depth}(\varphi \wedge \psi) = \mathrm{depth}(\varphi \vee \psi) = \max\{\mathrm{depth}(\varphi), \mathrm{depth}(\psi)\} + 1$,
- $\mathrm{depth}(\neg\varphi) = \mathrm{depth}(\varphi) + 1$,

ところで命題論理の証明は，その「入力」の長さによってことなるのが普通である．例として，鳩の巣原理 (PHP) を考えよう．これは非形式的には次のように定義される：

$n+1$ から n への単射は存在しない．

これを命題論理式であらわすと各自然数 n に対して次のようになる．

$$PHP_n \equiv \bigwedge_{0 \le i \le n} \bigvee_{0 \le j \le n-1} p_{ij} \to \bigvee_{0 \le i \le n} \bigvee_{0 \le j < k \le n-1} (p_{ij} \wedge p_{ik}).$$

したがって鳩の巣原理の命題論理証明とは，トートロジーの族 $\{PHP_n\}_{n \in \omega}$ に対する証明の族をさすのである．

さて $\mathcal{F}$ を制限した体系を考えよう．

定義 5 あるトートロジーの族の *cd-$\mathcal{F}$* 証明とは，$\mathcal{F}$ 証明で，それに含まれるすべての論理式の深さが命題変数の数に対して定数であるものをいう．

また $\mathcal{F}$ を拡張することによって,（少なくとも見かけ上は）より強い体系を考えることもできる．

定義 6 p を命題変数とし，φ を命題論理式とするとき $p \leftrightarrow \varphi$ を *extension axiom* という．拡張フレーゲ体系 $e\mathcal{F}$ は $\mathcal{F}$ に *extension axiom* を付け加えた体系とする．

また次のような規則によって拡張することもできる．

定義 7 $\varphi(p_1, \ldots, p_k)$ は命題変数 $p_1, \ldots, p_k$ を含む論理式で，$\theta_1, \ldots, \theta_k$ は論理式とする．代入規則 *(substitution rule)* とは $\varphi(p_1, \ldots, p_k)$ から $\varphi(\theta_1, \ldots, \theta_k)$ を導く規則とする．
$\mathcal{SF}$ は $\mathcal{F}$ に代入規則を付け加えた体系とする．

これらの体系に対して次のことは自明である．

命題 1 *cd-$\mathcal{F}$* $\leq_p \mathcal{F} \leq_p e\mathcal{F}$.

Krajíček-Pudlák [8] と Dowd [6] は独立に次のことを証明した．

定理 3 $e\mathcal{F} \equiv_p \mathcal{SF}$

4 導出原理

導出体系 (resolution system) $\mathcal{R}$ は命題論理式そのものではなく，クローズ (clause) を扱う証明体系である．クローズとは命題変数 p またはその否定 $\neg p$, すなわちリテラルの有限集合である．クローズ $\{l_1, \ldots, l_k\}$ は $l_1 \wedge \cdots \wedge l_k$ を意味するものとする．
導出規則 (resolution rule) とは，クローズ C_1, C_2 と命題変数 p に対して

$$\frac{C_1 \cup \{p\} \quad C_2 \cup \{\neg p\}}{C_1 \cup C_2}$$

となるような規則のことをいう．クローズの集合 $C = \{C_1, \ldots, C_k\}$ の導出反駁 (resolution refutation) とは，クローズの列 $D_1, \ldots, D_m$ で各 D_i は C に含まれるクローズか，D_j, D_k $(j, k < i)$ から導出規則によって得られるものをいう．
導出体系におけるトートロジーの証明を考えるには，まず与えられたトートロジー φ の否定 $\neg\varphi$ を CNF にすると，それはクローズの集合と考えられるので，これを反駁すればよいということになる．このとき次がなりたつ．

定理 4 導出体系は健全かつ完全である．すなわち論理式 φ がトートロジーであることと，その否定 $\neg\varphi$ の導出反駁が存在することは同値である．

導出体系において扱われる論理式はすべて深さが定数であり，次が成り立つ．

定理 5 $\mathcal{R} \leq_p cd\text{-}\mathcal{F}$.

フレーゲ体系と同様に，導出体系に対しても extension axiom を考えることができる．

定義 8 命題論理式 φ に対して命題変数 q_φ を割り当てる．このときクローズの集合 $Ext(\varphi)$ を次で定義する：

1. $\varphi \equiv p$ のとき $Ext(\varphi) = \{\{q_\varphi, \neg p\}, \{\neg q_\varphi, p\}\}$
2. $\varphi \equiv \neg\psi$ のとき $Ext(\varphi) = \{\{q_\varphi, q_\psi\}, \{\neg q_\varphi, \neg p_\psi\}\}$
3. $\varphi \equiv \psi_0 \vee \psi_1$ のとき $Ext(\varphi) = \{\{\neg q_\varphi, q_{\psi_0}, q_{\psi_1}\}, \{q_\varphi, \neg q_{\psi_0}\}\}, \{q_\varphi, \neg q_{\psi_1}\}$
4. $\varphi \equiv \psi_0 \wedge \psi_1$ のとき $Ext(\varphi) = \{\{q_\varphi, \neg q_{\psi_0}, \neg q_{\psi_1}\}, \{\neg q_\varphi, q_{\psi_0}\}\}, \{\neg q_\varphi, q_{\psi_1}\}$

$\mathcal{ER}$ は $\mathcal{R}$ にすべての φ に対して $Ext(\varphi)$ を公理として付け加えたものとする．

定理 6 $\mathcal{ER} \equiv_p e\mathcal{F}$.

5 鳩の巣原理

この節では，証明の複雑さの分析の例として代表的な，鳩の巣原理の下界性証明について触れることにする．ここで考えるのは次の問題である．

鳩の巣原理に関する基本問題 1 与えられた証明体系における鳩の巣原理 PHP_n の証明のできるだけよい下界をあたえよ．

次のことは容易にわかる．

定理 7 $e\mathcal{F}$ における多項式サイズの PHP_n の証明が存在する．

このことから $\mathcal{F}$ と $e\mathcal{F}$ を分離する命題の候補として，鳩の巣原理が考えられたが次のことを Buss が証明してこの可能性は否定された．

定理 8 (Buss [2]) $\mathcal{F}$ における多項式サイズの PHP_n の証明が存在する．

ではどの程度弱い体系まで，多項式サイズの証明を持つだろうか？まず Haken はこれについて，bottleneck counting と呼ばれる手法を使って，次のことを証明した．

定理 9 (Haken [7]) PHP_n^m を m から n への単射が存在しないことを表す命題論理式とする．$m > n$ とするとき $\neg PHP_n^m$ の導出反駁には少なくとも

$$2^{\Omega(\frac{n^2}{m})}$$

個のクローズが含まれる．

さらに Ajtai によって次のことが示された．

定理 10 (Ajtai [1]) d を定数とするとき，PHP_n の深さ d のフレーゲ証明には少なくとも

$$2^{n^{(1/6)^d}}$$

個の論理式が含まれる．

これらのことから次がわかる．

定理 11 $\mathcal{R} \leq_p cd\text{-}\mathcal{F} \leq_p \mathcal{F}$

6 限定算術との関係

最後に命題論理体系と限定算術との対応についてみてみよう．いま 2 種の算術における Σ_0^B 論理式 $\varphi(X)$ を考えるとき，これは次のようにして命題論理式の族に翻訳することができる．

定義 9 ([4]) $\varphi(X) \in \Sigma_0^B$ とし，$m \in \omega$ とする．変数 X に対して $p_0, p_1, \ldots$ を命題変数とし $\|\varphi(X)\|_m$ を以下のように帰納的に定義する．

1. $\varphi(X) \equiv X = X$ のとき $\|\varphi(X)\|_m = \top$,
2. $\varphi(X) \equiv t(|X|) = s(|X|)$ のとき

$$\|\varphi(X)\|_m = \begin{cases} \top & val(t(m)) = val(s(m)) \text{ のとき,} \\ \bot & \text{それ以外} \end{cases}$$

   ただし，$val(t)$ は t の値とする，
3. $\varphi(X) \equiv X(t|X|)$ のとき $j = t(m)$ として，

$$\|\varphi(X)\|_m = \begin{cases} p_j^X & j < m-1 \text{ のとき} \\ \top & j = m-1 \text{ のとき} \\ \bot & j > m-1 \text{ のとき} \end{cases}$$

4. $\varphi(X) \equiv \psi_0(X) \wedge \psi_0(X)$ のとき $\|\varphi(X)\|_m = \|\psi_0(X)\|_m \wedge \|\psi_1(X)\|_m$, ほかの論理結合子についても同様,

5. $\varphi(X) \equiv (\exists y \leq t(|X|)\psi(X)$ のとき

$$\|\varphi(X)\|_m = \bigvee_{i=0}^{m} \|\psi(i, X)\|_m$$

この翻訳について，次のことがわかる．

定理 12 $\varphi(X) \in \Sigma_0^B$ について $V^1 \vdash (\forall X)\varphi(X)$ ならば，$\|\varphi(X)\|_m$ の $e\mathcal{F}$ 証明で多項式サイズのものが存在する．

このことから $e\mathcal{F}$ は V^1 と少なくとも同程度に強い体系であるということがわかる．逆に次のことは $e\mathcal{F}$ が V^1 に比べて，それほど強くないということを示唆している．

定理 13 V^1 は $e\mathcal{F}$ の反映定理

> 命題論理式 φ の $e\mathcal{F}$-証明が存在するとき，φ はトートロジーである．

を V^1 の言語で形式化した命題を証明する．

参考文献

[1] M. Ajtai, The complexity of the pigeonhole principle, Combinatorica, 14(3) (1994) pp.417–433.

[2] S.R.Buss, The propositional pigeonhole princple has polynomial size Frege proofs, Journal of Symbolic Logic. 52 (1987). pp.916–27.

[3] Preface of "Arithmetic, Proof Theory and Computational Complexity", eds, P.Clote and J.Krajíček, Oxford Logic Guides 23 (1993)

[4] S.A.Cook and P.Nguyen, Logical Foundations of Proof Complexity, http://www.cs.toronto.edu/ sacook/homepage/book/

[5] S.A.Cook and R. Reckhow, The reltive efficiency of propositional proof systems, Journal of Symbolic Logic, 44(1) (1979) pp.36–50.

[6] M.Dowd, Propositional representations of arithmetic proofs, Ph.D. Thesis, University of Toronto (1979)

[7] A.Haken, The intractability of resolution, Theoretical Computer Science, 39 (1985), pp297–308.

[8] J.Krajíček and P.Pudlák, Propositional proof systems, the consistency of first order theories and the complexity of computations. Journal of Symbolic Logic, 54(3) (1989) pp.1063–79.

[9] J.Krajíček, Bounded Arithemtic, Propositional Logic, and Complexity Theory, Cambridge University Press, 1995.

[10] N.Segerlind The complexity of propositional proofs, Bulletin of Symbolic Logic, 13(4) (2007) pp.417–481.