# 線形推論規則に対するNP完全性の諸結果

近藤滉将
東京大学大学院数理科学研究科

## Deep inferenceとその意義

Deep inferenceとは，シークエント計算や自然演繹の類．修士論文では，古典命題論理のdeep inferenceのsystem SKSの重要な推論規則であるswitch規則とmedial規則に関する計算量の問題について議論した．

- Cook–Reckhowのプログラムは，弱い証明系から徐々に超多項式下界を示していくことで，最終的に$NP \neq coNP$の証明を試みるプログラムである．
- このプログラムは，Resolution [Hak85]や bounded-depth Frege system [Ajt94] など，比較的弱い証明系に対しては成功している一方で，より強い証明系であるカット付きLKに対しては進展していないため，カット付きLKを解析できる枠組みが望まれる．
- System SKSとカット付きLKは “同値” であり [BruGug09], switch規則とmedial 規則はSKSの “コア” [Brü03] である．

## Deep inferenceの推論の進め方

論理式とは，次で定められる記号列$R$のこと（$l$は任意のliteral）：

$$R ::= l \mid (R \wedge R) \mid [R \vee R]$$

Switch 規則とmedial 規則 （線形推論規則） は次の通り：

$$\frac{(A \wedge [B \vee C])}{[(A \wedge B) \vee C]}\,\mathrm{S} \qquad \frac{[(A \wedge B) \vee (C \wedge D)]}{([A \vee C] \wedge [B \vee D])}\,\mathrm{M}$$

線形推論規則からなる集合$S$について，論理式$\alpha$から論理式$\beta$が$S$によって導出可能 (derivable) であるとは，$S$に属する推論規則を$0$回以上適用することで，$\alpha$から$\beta$が得られるときをいう．

### 推論の例

$[a \vee b] \wedge [(c \wedge d) \vee (e \wedge f)]$から$[a \vee d \vee f] \wedge [b \vee c \vee e]$の導出の例.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[a \vee b] \wedge [(c \wedge d) \vee (e \wedge f)]}{[a \vee b] \wedge ([c \vee e] \wedge [d \vee f])}\,\mathrm{M}}{([a \vee b] \wedge [d \vee f]) \wedge [c \vee e]}\,\mathrm{IDENTITY}}{[a \vee (b \wedge [d \vee f])] \wedge [c \vee e]}\,\mathrm{S}}{(b \wedge [d \vee f]) \vee (a \wedge [c \vee e])}\,\mathrm{S}}{[a \vee d \vee f] \wedge [b \vee c \vee e]}\,\mathrm{M} \quad \frac{(A \wedge [B \vee C])}{[(A \wedge B) \vee C]}\,\mathrm{S} \quad \frac{[(A \wedge B) \vee (C \wedge D)]}{([A \vee C] \wedge [B \vee D])}\,\mathrm{M}$$

## 2つの計算量の問題

$S$をdeep inference の推論規則からなる集合とする．

### Derivability 問題

Input: $(\alpha, \beta)$ ($\alpha$と$\beta$は論理式)
Output: yes iff $\alpha$から$\beta$が$S$に属する規則のみで導出可能

### Criterion 問題

Input: $(\alpha, \beta)$ ($\alpha$と$\beta$は論理式で，$\alpha$と$\beta$に出現するliteralはそれぞれ相異なる．)
Output: yes iff $\alpha$から$\beta$が$S$に属する規則のみで導出可能

- Derivability 問題のような，証明可能性判定の計算量はそれ自体基本的な問いである．また，このような問題の計算量を明らかにすることで，証明探索の難易度の見当をつけることができる．また，Cook-Reckhowプログラムと関連して，下界証明の一手段であるfeasible interpolationが利用可能かどうかの目安になる．
- Criterion問題は，deep inferenceの発見に寄与した線形論理に関する問題に由来する．

## 既知の結果

| | switch | medial | switch + medial |
|---|---|---|---|
| derivability | NP完全 ([Kan94]) | ? | ? |
| criterion | P (e.g. [Mét94]) | P ([Str07]) | P でなさそう ([Das13]) |

## 私の貢献

| | switch | medial | switch + medial |
|---|---|---|---|
| derivability | NP完全 ([Kan94]) | NP完全 | NP完全 |
| criterion | P (e.g. [Mét94]) | P ([Str07]) | NP完全 |

## Derivability問題の結果について

NP性の証明には次の事実を用いた．

### Fact (folklore)

ある多項式$p$が存在して，次が成立する．任意の論理式$\alpha$に対し，$\alpha$から始まる*switch + medial* の証明のサイズは$p(|\alpha|)$以下である．

証明サイズが評価されているので，非決定的にproof-searchを行うことを考えることでNP性が示される．
NP 困難性は，すべて 3-Partition からの帰着．

### 3-Partition（NP 完全）

Input: $(A_1, A_2, \dots, A_{3n})$ （$n \in \mathbb{N}$，各$i$に対して $A_i \in \mathbb{N}$）
Output: yes iff $A_1, \dots, A_{3n}$ を $3$ つずつ $n$ 組に分割し，各組の和をすべて等しくできる

各 $A_i$ は unary 表記でも NP 完全（つまり例えば5を$*****$と表記してよい）

導出不可能を示すためには全ての導出を考える必要があるのが難しい．この困難を乗り越えるために，例えば次の考察を行った．

### observation

次の形の論理式はmedial 規則を適用しても同じ形を保つ．

$$\bigvee_i \left( [\bigvee_j l_{i,j}] \wedge [\bigvee_k l'_{i,k}] \right)$$

## Criterion問題の結果について

NP性はderivability問題のNP性より自明．NP困難性の証明は複雑であり，以下の通り，ある広義短調減少量に着目した．
$\alpha$を論理式とする．$\alpha$のliteralの出現であって，$\vee$に直接結ばれているものの個数を$i(\alpha)$で表す．また，$\alpha$を入力数無制限の$\wedge$ゲートと$\vee$ゲートからなる回路とみなしたとき，$\vee$ゲートであってliteralにのみ直接繋がれているものの個数を$s(\alpha)$で表す．

### 例

$i([a \vee b \vee c] \wedge [a \vee (e \wedge f)]) = 4$ (aが2回, bとcが1回ずつ.)
$s([a \vee b \vee c] \wedge [a \vee (e \wedge f)]) = 1$ ([a∨b∨c]の1つのみ.)

$$\Phi(\alpha) := 2(\alpha\text{に出現する} \wedge \text{の数}) + i(\alpha) - s(\alpha)$$

とおく．次の補題が鍵となった．

### lemma

$\alpha$から$\beta$がswitch+medialで導出可能ならば，$\Phi(\beta) \leq \Phi(\alpha)$.

## 今後の展望

Cook-Reckhowのプログラムに関連して，証明複雑性の分野で近年成功を収めているlifting手法のdeep inferenceへの適用を試みたい．

## 主要な参考文献

[Kan94] M. I. Kanovich, *The Complexity of Horn Fragments of Linear Logic*, Annals of Pure and Applied Logic **69** (1994)
[Das13] A. Das, *Rewriting with linear inferences in propositional logic*, in 24th International Conference on Rewriting Techniques and Applications (RTA 2013)