帰納法を用いた証明の分析
―暗号アルゴリズム Hermes の論理的可逆性の証明を対象として―

2018SE107 吉見颯
指導教員：横山哲郎

1　はじめに

プログラムの性質の証明で主に用いられる帰納法に，構造帰納法と導出に関する帰納法がある．証明したい命題によって，直接的に用いることができる帰納法が異なる．本研究では，帰納法を用いた証明の分析を行う．まず，構造帰納法と導出に関する帰納法を比較し，理解を深める．次に，論理的可逆性の証明が完成されていない，暗号アルゴリズム Hermes の形式仕様 $\Delta, \eta \models_S s : \sigma \rightsquigarrow \sigma' \Leftrightarrow \Delta, \eta \models_S I(s) : \sigma' \rightsquigarrow \sigma$ [1, 2] について着目する．Hermes は，小さなコンピューターや非力なデバイスに実装される軽量暗号を支援する可逆プログラミング言語である．任意の Hermes プログラムの論理的可逆性の証明を対象とし，帰納法を用いた証明の分析を行う．具体的には，Hermes プログラムの論理的可逆性を証明する上で，直接的に用いることができる帰納法は何か，任意の Hermes プログラムは論理的可逆性を満たしているか否か，の 2 点を研究課題として掲げる．

2　導出システム

導出システムは，論理式，プログラム，型などの議論の対象に対する様々な判断を推論規則に従って導くためのシステムである．導出システムを完成させるには，各判断を導くための推論規則が必要となる．「J_1ならば J_2」となる推論規則の J_1 を「前提」，J_2 を「結論」と呼ぶ．推論規則では，前提の判断 J_1 が既に導かれている場合のみ，J_2 の判断を導くことが可能である．

[推論規則 X]J_1かつ J_2かつ$\cdots$かつ J_nならば J_0である．

という推論規則は，

$$\frac{J_1 \ J_2 \cdots J_n}{J_0}(X)$$

のように表現される．前提の数 n は，前提のない規則の場合は 0 となる．導出は導出木という記法で表現する．導出木は，判断をノード，結論となる判断を根とする木構造がとられる．一般的に，判断 J_i を具体化したもの J_i' を結論とする $D_i (i = 1, \ldots, n)$ が得られており，また，推論規則 *Foo* 中のパラメータを具体化したもの

$$\frac{J_1' \cdots J_n'}{J_0'}$$

が得られたとすると，

$$\frac{D_1 \cdots D_n}{J_0'} Foo$$

は J_0' を結論とする導出である．また，前提のない推論規則 *Bar* を具体化したもの

$$\frac{}{J_0'} Bar$$

は導出である．

3　構造帰納法

構造帰納法は，ペアノ自然数や算術式などの BNF で定義される対象の性質を証明するのに用いることができる帰納法である．本節では，BNF を用いて算術式を定義し，算術式に関する構造帰納法について示す．

BNF を用いて，算術式を以下に定義する．

定義 3.1　算術式 (メタ変数 e) の集合 *Exp* は以下の構文で定義する．

$$e \in Exp \ ::= \ n \mid e + e \mid e * e$$

算術式に関する構造帰納法を以下に示す．算術式の性質についての述語 $P(e)$ に対し，以下の 3 つの条件が成り立つとき，述語 $P(e)$ は全ての算術式 e に成り立つとする．

(i) 任意のペアノ自然数 n に対して $P(n)$ が成り立つ．

(ii) 任意の算術式 e_1, e_2 に対して，$P(e_1)$ かつ $P(e_2)$ ならば $P(e_1$+$e_2)$ が成り立つ．

(iii) 任意の算術式 e_1, e_2 に対して，$P(e_1)$ かつ $P(e_2)$ ならば $P(e_1$*$e_2)$ が成り立つ．

上記のような証明法を算術式に関する構造帰納法という．

4　導出に関する帰納法

導出に関する帰納法は，導出の構造が本質的には木構造を持っていることに基づく帰納法の原理である．本節では，導出に関する帰納法の一例として，導出システム CompareNat1[3] を取り挙げ，CompareNat1 における判断の導出に関する帰納法について以下に示す．

自然数の大小を比較する導出システムを CompareNat として与える．この導出システムは，n_1 `is less than` n_2 という形式であり，「自然数 n_1 は自然数 n_2 より小さい.」という意味を持つ．

「〜より小さい」という概念は，様々な方法で規則化できるので，推論規則が 3 種類あり，そのひとつである導出システム CompareNat1 の推論規則を以下に与える．

$$\frac{}{n \ \texttt{is less than S(}n\texttt{)}} \text{ (L-SUCC)}$$

$$\frac{n_1 \ \texttt{is less than} \ n_2 \qquad n_2 \ \texttt{is less than} \ n_3}{n_1 \ \texttt{is less than} \ n_3} \text{ (L-TRANS)}$$

以下に CompareNat1 における判断 n_1 `is less than` n_2 の導出に関する帰納法の原理を示す．

ふたつのペアノ自然数と導出システムに関する述語 P に対し，以下のふたつの条件が成り立つとき，「任意のペアノ自然数 n_1, n_2，判断 n_1 `is less than` n_2 の導出 D に対して，$P(n_1, n_2, D)$」が成り立つとする．

(i) 任意のペアノ自然数 n に対して，以下が成り立つ．

$$P(\ n, \mathtt{S}(n), \frac{}{n \ \mathtt{is\ less\ than}\ \mathtt{S}(n)}\text{L-SUCC}\ )$$

(ii) 任意のペアノ自然数を n_1，n_2，n_3，
判断 n_1 `is less than` n_2 の導出を D_1，
判断 n_2 `is less than` n_3 の導出を D_2 とする．
これらに対して，$P(n_1, n_2, D_1)$ かつ $P(n_2, n_3, D_2)$ ならば，以下が成り立つ．

$$P(\ n_1, n_3, \frac{D_1 \qquad D_2}{n_1 \ \mathtt{is\ less\ than}\ n_3}\text{L-TRANS}\ )$$

5 Hermes の論理的可逆性の証明の分析

本節では，任意の Hermes プログラムの論理的可逆性についての証明の分析を行う．また，構造帰納法を用いた場合の Hermes の証明の分析を行う．

5.1 Hermes の論理的可逆性の証明の分析

任意のプロシージャ環境 Δ と環境 η，任意のロケーション λ について，文 s と反転した文 $I(s)$ が論理的可逆性を満たすということは，任意のストア σ_1, σ_2 について，

$$\begin{aligned}&\Delta, \eta, \lambda, \sigma_2(\lambda) \models_F s : \sigma_1 \rightleftharpoons \sigma_2 \quad \Longleftrightarrow \\ &\Delta, \eta, \lambda, \sigma_1(\lambda) \models_F I(s) : \sigma_2 \rightleftharpoons \sigma_1\end{aligned} \tag{1}$$

が成り立つことである．($\Longrightarrow$) を以下に示す．導出に関する帰納法を直接的に用いて証明を行うため，可能な導出の形に関する場合分けを行う．

意味規則 Loop1 が導出木の根で用いられた場合．意味規則 Loop1[1] より，任意の Δ, η について，

$$\frac{\sigma(\lambda) = v}{\Delta, \eta, \lambda, \sigma(\lambda) \models_F s : \sigma \rightleftharpoons \sigma}\ \text{Loop1} \tag{2}$$

が得られる．これは s を任意の文に置き換えても成立するので

$$\frac{\sigma(\lambda) = \sigma(\lambda)}{\Delta, \eta, \lambda, \sigma(\lambda) \models_F I(s) : \sigma \rightleftharpoons \sigma}\ \text{Loop1} \tag{3}$$

となり，結論が得られる．

意味規則 Loop2 が導出木の根で用いられた場合．論理的可逆性を満たしているとはいえない．なぜなら，**for**（x = e_1 ; e_2）において，$x = e_1$ を代入した後，$x = e_2$ に更新されるまで繰り返しの処理が行われるが，繰り返しの処理が始まってからは e_1 は確認することができないため，論理的可逆性を満たしているとはいえない．

5.2 構造帰納法を用いた場合の Hermes の証明の分析

任意のプロシージャ環境 Δ と環境 η について，文 s が前方決定的であるとは，任意のストア $\sigma_1, \sigma_2, \sigma_3$ について

$$\Delta, \eta \models_S s : \sigma_1 \rightleftharpoons \sigma_2 \wedge \Delta, \eta \models_S s : \sigma_1 \rightleftharpoons \sigma_3 \implies \sigma_2 = \sigma_3 \tag{4}$$

が成り立つことである．

直接的に構造帰納法を用いて証明する．$\Delta, \eta \models_S s : \sigma_1 \rightleftharpoons \sigma_2$ の場合．最後に用いる意味規則がひとつに定まらないので，Loop1，Loop2 に場合分けをする．Loop2 の場合において，形が定まらないストアを $\sigma_n (n = 1, 2, 3, \ldots)$ とすると，任意の導出 D_1，D_2，D_3，D_4 について

$$\frac{\sigma(\lambda) \neq v \quad D_3 \ D_4}{\Delta, \eta, \lambda, v \models_F s : \sigma_1 \rightleftharpoons \sigma_n}\text{Loop2} \tag{5}$$

$$D_3 = \frac{D_1}{\Delta, \eta \models_S s : \sigma_1 \rightleftharpoons \sigma_2}\ Va \tag{6}$$

$$D_4 = \frac{D_2}{\Delta, \eta, \lambda, v \models_F s : \sigma_2 \rightleftharpoons \sigma_n}\ Ve \tag{7}$$

となり，$\Delta, \eta, \lambda, v \models_F s : \sigma_n \rightleftharpoons \sigma_n$ と結論の形に関して分からないので，式 4 を示すことができない．

よって，任意の Hermes プログラムは構造帰納法を用いて証明することができないことが分かった．

6 おわりに

本研究では，プログラムの性質を証明するために主に用いられる構造帰納法と導出に関する帰納法について理解を深めた．Hermes プログラム [1] の性質において，Loop の意味規則の一部は論理的可逆性を満たしているといえないため，Hermes プログラムは一部論理的可逆性を満たしていないことが分かった．また，構造帰納法を用いて論理的可逆性を証明することができない Hermes プログラムがあることが分かった．

参考文献

[1] Mogensen, T.Æ.: Hermes: A Language for Light-Weight Encryption, *Reversible Computation* (Lanese, I. and Rawski, M., Eds.), Lecture Notes in Computer Science, Vol.12227, Cham, Springer International Publishing, pp.93–110 (2020).

[2] Mogensen, T.Æ.: Hermes: A Reversible Language for Writing Encryption Algorithms (Work in Progress), *Perspectives of System Informatics* (Bjørner, N., Virbitskaite, I. and Voronkov, A., Eds.), Lecture Notes in Computer Science, Vol.12227, Cham, Springer International Publishing, pp.243–251 (2019).

[3] 五十嵐淳：プログラミング言語の基礎概念，サイエンス社 (2020).