分離論理におけるエンテイルメント判定問題の決定不能性

飯田 晟樹　早乙女 献自　中澤 巧爾　（名古屋大学）

研究概要

エンテイルメント = 論理式間の含意関係

有限木幅条件 = 確立性 + 接続性 + 進行性

- 分離論理……ポインタ・プログラムの性質を証明するための，ホーア論理の拡張
- 分離論理によるプログラム検証のためには，エンテイルメントの妥当性判定が必要
- 再帰的データ構造を表す帰納的述語を含むエンテイルメント判定は難しい
  - 一般には決定不能 [Antonopoulos+ 2014] Postの対応問題を帰着
  - 有限木幅条件を満たす述語に制限すると決定可能 [Iosif+ 2013]
  - 有限木幅条件から確立性条件を除くと決定不能 [Tatsuta+ 2015] Postの対応問題を帰着

研究成果

- **分離論理のエンテイルメント判定問題の決定不能性の新しい証明 → 文脈自由文法の包含問題を帰着**
- **有限木幅条件のうち接続性を除くと決定不能になることを証明 → 文脈自由文法のグライバッハ標準形を利用**

分離論理

（項）　$t ::= nil \mid x$

（ストア論理式）　$\Pi, \Pi' ::= t = t' \mid t \neq t' \mid \Pi \wedge \Pi'$

（ヒープ論理式）　$\Sigma, \Sigma' ::= emp \mid t \mapsto t' \mid P(t \ldots) \mid \Sigma * \Sigma'$

（シンボリックヒープ）　$A ::= \Pi \wedge \Sigma$

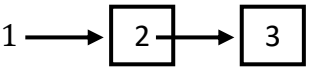
P：帰納的述語（別途，定義節集合が与えられている）

ヒープモデル (s,h)　ストア s：変数 → 値 ($\subseteq$ アドレス)，ヒープ h：アドレス $\rightarrow_{fin}$ 値

- $s,h \vDash emp$ iff $dom(h) = \emptyset$
- $s,h \vDash t \mapsto t'$ iff $dom(h) = \{s(t)\} \,\&\, h(s(t)) = s(t')$
- $s,h \vDash \Sigma * \Sigma'$ iff h は互いに素な h_1 と h_2 に分割でき $s,h_1 \vDash \Sigma \,\&\, s,h_2 \vDash \Sigma'$
- $A \vDash B$ iff $\forall (s,h).[s,h \vDash A$ ならば $s,h \vDash B]$

例：$s(x) = 1, s(y) = 2, s(z) = 3$
$h(1) = 2, h(2) = 3$

このヒープモデルは右図のヒープを表現し
$s,h \vDash x \mapsto y * y \mapsto z$ が成り立つ



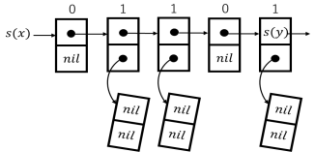
成果1　文脈自由文法の包含問題を用いたエンテイルメント判定問題の決定不能性証明

$\{0,1\}$上の文字列 w のエンコーディング

2引数帰納的述語 $w(x,y)$ を以下で定義

$\varepsilon(x,y) := x = y \wedge emp$
$0(x,y) := x \mapsto (y, nil)$
$1(x,y) := \exists u.[x \mapsto (y,u) * u \mapsto (nil, nil)]$
$ww'(x,y) := \exists z.[w(x,z) * w'(z,y)$

例：$s,h \vDash 01101(x,y)$



文脈自由文法 G のエンコーディング

各非終端記号 A について，2引数帰納的述語 $A(x,y)$ を考え
各生成規則 $A \rightarrow a \cdots b$ について，以下の定義節を与える
$A(x,y) := \exists z_1, \ldots, z_{n-1}.[a(x,z_1) * \cdots * b(z_{n-1}, y)]$

例：文脈自由文法 $G \begin{cases} S \rightarrow E \mid 0S1 \\ E \rightarrow \varepsilon \end{cases}$ のエンコーディング

$S(x,y) := E(x,y) \mid \exists z_1, z_2.[0(x,z_1) * S(z_1,z_2) * 1(z_2,y)]$
$E(x,y) := \varepsilon(x,y)$

定理1　G, G'を文脈自由文法，S, S'をそれぞれの開始記号とすると　$L(G) \subseteq L(G') \Leftrightarrow S(x,y) \vDash S'(x,y)$

（証明）文脈自由文法 G とその開始記号 S に対して $s,h \vDash S(x,y) \Leftrightarrow \exists w \in L(G).\ s,h \vDash w(x,y)$ が証明できる．□

定理1により，文脈自由文法の包含問題がエンテイルメント判定問題に帰着され，
文脈自由文法の包含問題が決定不能であることより，エンテイルメント判定問題の決定不能性が帰結する．

成果2　有限木幅条件の弱化による決定可能性の限界に関する分析

有限木幅条件 [Iosif+ 2013]　= 確立性，接続性，進行性

確立性 (establishment)：
各定義節中で存在量化された変数は述語展開によって必ず，ヒープ中に割当てられたメモリのアドレスになる

接続性 (connectivity)：
$P(x, \ldots)$の定義節が述語 $Q(y, \ldots)$を含むならば $x \mapsto (\ldots y \ldots)$ を含む

進行性 (progress)：
$P(x, \ldots)$ の定義節は $x \mapsto t$ の形の論理式を含み，この他に $\mapsto$ を含まない

定理2 有限木幅条件のうち，確立性と進行性を満たす述語に対するエンテイルメント判定問題は決定不能

（証明）文脈自由文法のグライバッハ標準形のエンコーディングで得られる述語は確立性と進行性を満たす．□

グライバッハ標準形：全ての生成規則 $A \rightarrow a \cdots b$ について，先頭の a が終端記号であるような文脈自由文法