制限された帰納的述語を含む分離論理の循環証明体系

名古屋大学大学院情報学研究科　石井沙織, 中澤巧爾

こんな話です

背景：分離論理＋循環証明体系はカットなし完全か？ → 述語の制限なしでは 完全でない[Kimura+ 2021]
→ 述語の制限によりカットなし完全になるか？

成果：1引数有界木幅条件[Iosif+ 2013]に制限した分離論理の循環証明体系について以下を示した

・成果1：一般にはカットなし完全でない
・成果2：1引数有界木幅条件＋決定性条件にすると**カットなし完全である**
・成果3：単一の述語のみを含む場合, 循環, カットなしで完全である

分離論理と循環証明体系

分離論理：ヒープ操作を含むプログラム検証のためのホーア論理の拡張

論理式：シンボリックヒープ $A := \Pi \wedge \Sigma$　　ストア論理式 $\Pi := true \mid t = t \mid t \neq t \mid \Pi \wedge \Pi$　（変数間の等価関係）
ヒープ論理式 $\Sigma := emp \mid t \mapsto t \mid \Sigma * \Sigma \mid P(t)$　（ヒープの状態）

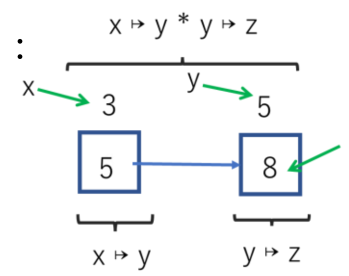
ヒープモデル：ストアsとヒープhの組．ストアsは変数の値を,ヒープhはある番地のヒープの中身を示す

$$s,\ h \models_\Phi t_0 \mapsto (t_1, \cdots, t_N) \overset{def}{\Leftrightarrow} dom(h) = \{s(t_0)\} \text{ かつ } h(s(t_0)) = (s(t_1), \cdots s(t_N))$$

$$s,\ h \models_\Phi \phi_1 * \phi_2 \overset{def}{\Leftrightarrow} h_1,\ h_2 \text{ が存在し } h = h_1 + h_2 \text{ かつ } s,\ h_i \models_\Phi \phi_i\ (i = 1,\ 2)$$

disjoint union

ヒープモデルの例：



$s(x) = 3$　$s(y) = 5$
$h(3) = 5$　$h(5) = 8$

エンテイルメント：$A \models B \overset{def}{\Leftrightarrow} \forall s, h[s, h \models A \text{ ならば } s, h \models B]$

循環証明体系：エンテイルメントのための証明体系．循環構造により帰納法を表現

$$\dfrac{\begin{array}{c}\vdots\\ x \mapsto y * ls(y,z) \vdash ls(x,z)\end{array} \qquad \dfrac{\dfrac{\dfrac{}{x \mapsto v \vdash x \mapsto v}\,Id \qquad ls(v,y) * ls(y,z) \vdash ls(v,z)}{x \mapsto v * ls(v,y) * ls(y,z) \vdash x \mapsto v * ls(v,z)}\,*}{x \mapsto v * ls(v,y) * ls(y,z) \vdash ls(x,z)}\,UR}{ls(x,y) * ls(y,z) \vdash ls(x,z)}\,UL$$

証明の循環構造

1引数有界木幅条件

有界木幅条件[Iosif+ 2013]を満たす1引数述語は以下の形の定義節で定義される

$$P(x) := \exists z_1 \cdots z_n (x \mapsto \vec{u} * Q_1(z_1) * \cdots * Q_n(z_n))$$
$$(\vec{u} \subseteq z_1, \cdots, z_n, x, nil, z_1 \cdots z_n \in (\vec{u})\ , n \geqslant 0)$$

例：以下は1引数有界木幅条件をみたす

$$list(x) = x \mapsto nil \mid \exists y\ (x \mapsto y * list(y))$$
$$tree(x) = x \mapsto (nil, nil) \mid \exists y, z\ (x \mapsto (y, z) * tree(y) * tree(z))$$

1引数有界木幅条件を満たす述語を含む分離論理の循環証明体系はカットなし完全か？

成果1：一般には完全ではない

定理：1引数有界木幅条件を満たす述語を含む分離論理の循環証明体系は、一般にカットなし完全でない

（証明）以下で定義される述語に対して $L(x) \models L_{eo}(x)$ は正しいエンテイルメントだが、カットなしで証明できない

$L(x) := x \mapsto \mathrm{nil} \mid \exists z(x \mapsto z * L(z))$　リスト
$L_o(x) := x \mapsto \mathrm{nil} \mid \exists z(x \mapsto z * L_e(z))$　奇数長のリスト
$L_e(x) := \exists z(x \mapsto z * L_o(z))$　偶数長のリスト
$L_{eo}(x) := x \mapsto \mathrm{nil} \mid \exists z(x \mapsto z * L_o(z)) \mid \exists z(x \mapsto z * L_e(z))$

成果3：単一の述語の場合

定理：1引数有界木幅条件と決定性条件をみたす述語を含む分離論理の循環証明体系について, 任意の述語 P , Q について「$P(x) \models Q(x)$ ならば $P = Q$」であるならば, 循環とカットなしで完全である

系：単一の述語のみを含む場合、循環とカットなしで完全である

成果2：決定性条件を課すと完全

定義（決定性条件）

（条件1）$P(x)$ の2つの異なる定義節

$$P(x) := \exists z_1 \cdots z_n (x \mapsto \vec{u} * \Sigma)$$
$$P(x) := \exists z'_1 \cdots z'_n (x \mapsto \vec{u'} * \Sigma')$$

に対して, $\vec{u}$ と $\vec{u'}$ は, 存在変数をすべて同一視した上で異なる

これらは決定性条件を満たす

（条件2）$P(x) \models Q(x)$ のとき, P の任意の定義節

$$P(x) := \exists z_1 \cdots z_n (x \mapsto \vec{u} * P_1(z_1) * \cdots * P_n(z_n))$$

に対して、Q の定義節

$$Q(x) := \exists z_1 \cdots z_n (x \mapsto \vec{u} * Q_1(z_1) * \cdots * Q_n(z_n))$$

で、$P_i(z_i) \models Q_i(z_i) (\forall i)$ となるものが存在する

定理：決定性と1引数有界木幅条件を満たす述語を含む分離論理の循環証明体系はカットなし完全である

（証明）正しいエンテイルメントの一般形は

$$\Sigma_1 * \cdots * \Sigma_n * \Sigma \vdash P_1(x_1) * \cdots * P_n(x_n) * \Sigma$$

（Σ_i は、$P_i(x_i)$ を展開した形）

で表せ、これらのエンテイルメントは循環証明体系においてカットなしで証明可能である