分離論理における記号ヒープのための
循環証明体系におけるカットの制限について

早乙女 献自（名古屋大学）中澤 巧爾（名古屋大学）木村 大輔（東邦大学）

こんな話です

背景：分離論理＋**循環証明**で**証明探索**がしたい ➡ **カット**が邪魔
しかし、**カット除去**することは出来ない [Kimura+ 2018] ➡ カットを**制限**できないか？

成果：カット論理式に対する制限として「**推測可能性**」を提案
推測可能な論理式にカットを制限すると、**証明能力が変わる**ことを証明

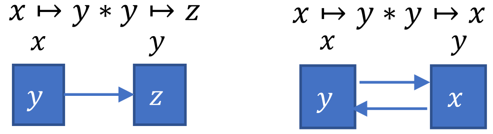
証明体系 CSL_1ID^ω

分離論理＋循環構造

分離論理

○ **ヒープメモリ**の構造を論理式で表す

$x \mapsto y * y \mapsto z$　　　$x \mapsto y * y \mapsto x$

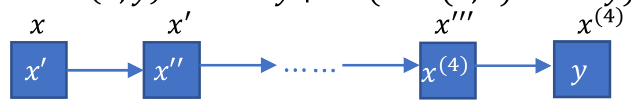


数学的帰納法に対応

○ 再帰的データ構造を帰納的述語で表現

$lsne(x,y) \coloneqq x \mapsto y \mid \exists z.(x \mapsto z * lsne(z,y))$

$slne(x,y) \coloneqq x \mapsto y \mid \exists z.(lsne(x,z) * z \mapsto y)$



記号ヒープ $\Pi \wedge \Sigma$の形の論理式を**記号ヒープ**という

Pure Part　$\Pi ::= \top \mid t = u \mid t \neq u \mid \Pi \wedge \Pi$

Spatial Part　$\Sigma ::= \mathrm{emp} \mid P(\boldsymbol{t}) \mid t \mapsto u \mid \Sigma * \Sigma$

循環証明

$$\dfrac{\dfrac{\dfrac{}{x \mapsto y \vdash x \mapsto y}}{x \mapsto y \vdash slne(x,y)}(PR) \qquad \dfrac{\dfrac{\dfrac{}{x \mapsto z \vdash x \mapsto z} \quad \underline{lsne(z,y)} \vdash slne(z,y)}{x \mapsto z * \underline{lsne(z,y)} \vdash \boldsymbol{x \mapsto z * slne(z,y)}}(*) \quad \dfrac{\dfrac{}{x \mapsto z * slne(z,y) \vdash x \mapsto z * slne(z,y)}}{\boldsymbol{x \mapsto z * slne(z,y)} \vdash slne(x,y)}(PR)}{x \mapsto z * \underline{lsne(z,y)} \vdash slne(x,y)}(\boldsymbol{cut})}{\underline{lsne(x,y)} \vdash slne(x,y)}(\boldsymbol{Case})$$

○ 規則(**Case**)は左辺の述語に関する展開の場合分けに対応

○ 「任意の**無限長パス**について，規則(Case)で無限に展開される述語（証明図下線）が存在する」
という条件（**Global Trace Condition**）を満たす証明木のみを証明図として許す

証明探索とカット

○ 証明図を**下から上**に探索する

○ カット規則は**カット論理式 C** が推測しづらい

$$\dfrac{A \vdash \boldsymbol{C} \qquad \boldsymbol{C} \vdash B}{A \vdash B}(\boldsymbol{cut})$$

○ カット論理式は循環証明体系で一般に除去できない
[Kimura+ 2019]

➡ 証明探索の邪魔にならない範囲に**制限**したい

推測可能なカット

○ カット以外の規則で証明木を作った時に
出てくる論理式を全て**推測可能**とする

○ **カット論理式**を**推測可能な論理式**に制限

➡ **推測可能なカット**

カット制限時の証明能力

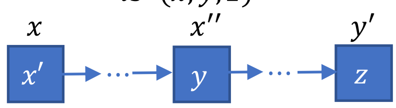
証明体系 CSL_1ID^ωにおいて

定理 1.　推測可能なカットを制限して証明することができるが、
[Kimura+ 2019] カットを使わずに証明できないシークエントが存在する
　　e.g.) $\mathrm{lsne}(x,y) \vdash slne(x,y)$

$$\begin{aligned}\mathrm{ls}^3(x,y,z) \coloneqq\ & x = y \wedge y = z \wedge \mathrm{emp} \\ & \mid \exists x'.(x = y \wedge y \neq z \wedge x \mapsto x' * \mathrm{ls}^3(x',x',z)) \\ & \mid \exists x'.(x \neq y\ \wedge\ x \mapsto x' * \mathrm{ls}^3(x',y,z)).\end{aligned}$$

定理 2.　カットを制限しないで証明することができるが、
[本研究]　推測可能なカットに制限すると証明できないシークエントが存在する

$ls^3(x,y,z)$



定理 2. の証明（概要）
反例として、$ls^3(x,y,x) \vdash ls^3(y,x,y)$ を用いた
　○カットフリーで証明可能なことは実際に証明図を書いて証明
　○カット制限下で証明不可能なことは背理法を用いて証明
　　「カット制限下で証明図が存在する」と仮定し、その証明図を調べる
　　➡ Global Trace Conditionを満たさないパスが発見される

$ls^3(x,y,x)$