

# 分離論理の 循環証明体系における 帰納的述語の制限と カット除去

名古屋大学 大学院 情報学研究科  
早乙女 献自 中澤 巧爾

# 背景

## 分離論理のエンテイルメントを 循環証明体系で自動証明したい

- **分離論理** ... ポインタ・プログラムのため、ホーア論理を拡張
- **循環証明体系** ... 証明の循環構造を許したLKスタイルの証明体系
- **エンテイルメント** ... 論理式の包含関係

e.g.)  $x \mapsto y * y \mapsto z \vdash ls(x, z)$

$x$ から $z$ のリスト断片

### 自動証明の例

$$\frac{\frac{x \mapsto y * y \mapsto z \vdash x \mapsto y * y \mapsto z}{x \mapsto y * y \mapsto z \vdash x \mapsto y * ls(y, z)} \text{(UR)}}{x \mapsto y * y \mapsto z \vdash ls(x, z)} \text{(右展開(UR))}$$

(公理(Axiom))

(UR)

# 自動証明とカット規則

分離論理のエンテイルメントを  
循環証明体系で自動証明したい



カット規則が邪魔になる

$$\frac{A \vdash C \quad C \vdash B}{A \vdash B} \text{ カット}$$

- 分離論理+循環証明では**カット除去できない**[Kimura+ 2019]
- 自動証明に適した範囲に**カットを制限することも難しい**[Saotome+ 2020]

➡ 証明対象を狭めて、カットの除去・制限を目指す

# 研究成果

- 帰納的述語を**帰納的命題**（0引数の帰納的述語）に制限しても**カット規則を除去できない**ことを示した
- 簡単な帰納的命題のみに制限した循環証明体系でカット除去できる例を示した
  - ➡ より複雑な帰納的述語に対して  
カット除去をする足がかりにしたい

**分離論理+循環証明**における  
エンテイルメント判定をしたい



カット規則を除去したい

**分離論理+循環証明**における  
エンテイルメント判定をしたい



カット規則を除去したい

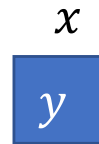
# 分離論理 [Reynolds 2002]

ホーア論理を**ヒープメモリ**のために拡張  
論理式でメモリ構造を表現する

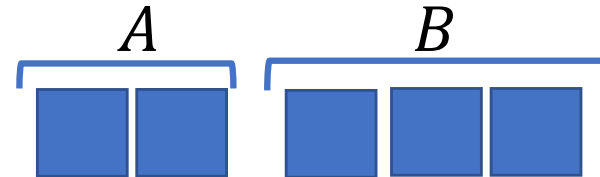
$emp$



$x \mapsto y$

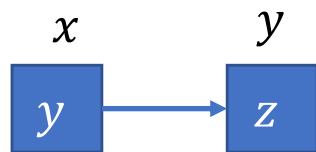


$A * B$

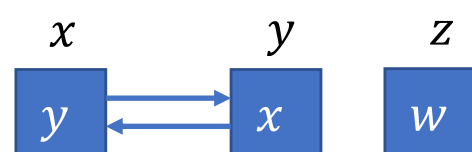


例

•  $x \mapsto y * y \mapsto z$



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



•  $x \mapsto y * x \mapsto y$  は **充足不能**

# 分離論理のための帰納的述語

再帰的データ構造を帰納的述語で表す


$$ls(x, y) := x = x \wedge emp \\ \vee \exists x'. (x \neq y \wedge x \mapsto x' * ls(x', y))$$



直観的には「 $x$  から  $y$  までのリスト断片」  
ただし、要素数0のリスト断片( $emp$ )を含む



# エンテイルメント判定

- エンテイルメント  $A \models B$  が成り立つか判定する
  - モデルを使う方法
  - **証明を生成する方法**  こっちに注目
- シークエント計算で証明することを考える
  - 全て証明することはできない
    - ➡ 扱う対象に制限を与える  
e.g.) Symbolic Heap
  - 帰納的述語を扱うので、帰納法も使いたい

# 分離論理の証明体系 (例)

**Definition 5** (Inference rules of  $CSL_1ID^\omega$ ). *The inference rules of  $CSL_1ID^\omega$  are the following.*

$$\begin{array}{c}
 \overline{A \vdash A} \text{ (Id)} \quad \overline{A * t \mapsto u_1 * t \mapsto u_2 \vdash B} \text{ (}\mapsto L\text{)} \quad \overline{t \neq t \wedge A \vdash B} \text{ (NEQL)} \\
 \\
 \frac{A \vdash C \quad C \vdash B}{A \vdash B} \text{ (cut)} \quad \frac{A \vdash B}{\Pi \wedge A \vdash B} \text{ (Wk)} \quad \frac{A \vdash C \quad B \vdash D}{A * B \vdash C * D} (*) \\
 \\
 \frac{t \neq u \wedge A \vdash B}{t \neq u \wedge A \vdash t \neq u \wedge B} \text{ (NEQR)} \\
 \\
 \frac{t = u \wedge A[u/x] \vdash B[u/x]}{t = u \wedge A[t/x] \vdash B[t/x]} \text{ (EQL)} \quad \frac{A \vdash B}{A \vdash t = t \wedge B} \text{ (EQR)} \\
 \\
 \frac{A \vdash B}{A * \text{emp} \vdash B} \text{ (EL1)} \quad \frac{A * \text{emp} \vdash B}{A \vdash B} \text{ (EL2)} \\
 \\
 \frac{A \vdash B}{A \vdash B * \text{emp}} \text{ (ER1)} \quad \frac{A \vdash B * \text{emp}}{A \vdash B} \text{ (ER2)} \\
 \\
 \frac{C_1(\mathbf{x}, \mathbf{y}_1) * A \vdash B \quad \cdots \quad C_n(\mathbf{x}, \mathbf{y}_n) * A \vdash B}{P(\mathbf{x}) * A \vdash B} \text{ (Case)} \quad \frac{A \vdash C_i(\mathbf{u}, \mathbf{t}) * B}{A \vdash P(\mathbf{u}) * B} \text{ (PR)},
 \end{array}$$

where the definition clauses of the predicate  $P$  are the following

$$P(\mathbf{x}) := \exists \mathbf{y}_1. C_1(\mathbf{x}, \mathbf{y}_1) \mid \cdots \mid \exists \mathbf{y}_n. C_n(\mathbf{x}, \mathbf{y}_n).$$

In (PR),  $i$  satisfies  $1 \leq i \leq n$ , and the terms  $\mathbf{t}$  are arbitrary. In (Case), the variables  $\mathbf{y}_i$  are fresh. The formula  $C$  in (cut) is called the cut formula.

# 循環証明<sup>[Brotherston+ 2006]</sup> と 証明探索

- 帰納法に相当する循環証明を導入
- 結論から前提に向かって証明を探す

$$ls(x, \underline{y}) * ls(y, z) \vdash ls(x, z)$$

# 循環証明<sup>[Brotherston+ 2006]</sup> と 証明探索

- 帰納法に相当する循環証明を導入
- 結論から前提に向かって証明を探す

$$\frac{\begin{array}{c} \overline{ls(y, z) \vdash ls(y, z)} \\ \vdots \end{array} \quad \boxed{x \neq y \wedge x \mapsto x' * ls(x', y)} * ls(y, z) \vdash ls(x, z)}{\boxed{ls(x, y)} * ls(y, z) \vdash ls(x, z)} \quad \boxed{(Case)}$$

# 循環証明<sup>[Brotherston+ 2006]</sup> と 証明探索

- 帰納法に相当する循環証明を導入
- 結論から前提に向かって証明を探す

$$\begin{array}{c}
 \overline{ls(y, z) \vdash ls(y, z)} \\
 \vdots \\
 \hline
 \end{array}
 \quad
 \frac{
 \begin{array}{c}
 x \neq y \wedge x \mapsto x' * ls(x', y) * ls(y, z) \vdash \boxed{x \neq y \wedge x \mapsto x' * ls(x', z)} \\
 \hline
 x \neq y \wedge x \mapsto x' * ls(x', y) * ls(y, z) \vdash \boxed{ls(x, z)}
 \end{array}
 }{
 ls(x, y) * ls(y, z) \vdash ls(x, z)
 }
 \begin{array}{c}
 (PR) \\
 (Case)
 \end{array}$$

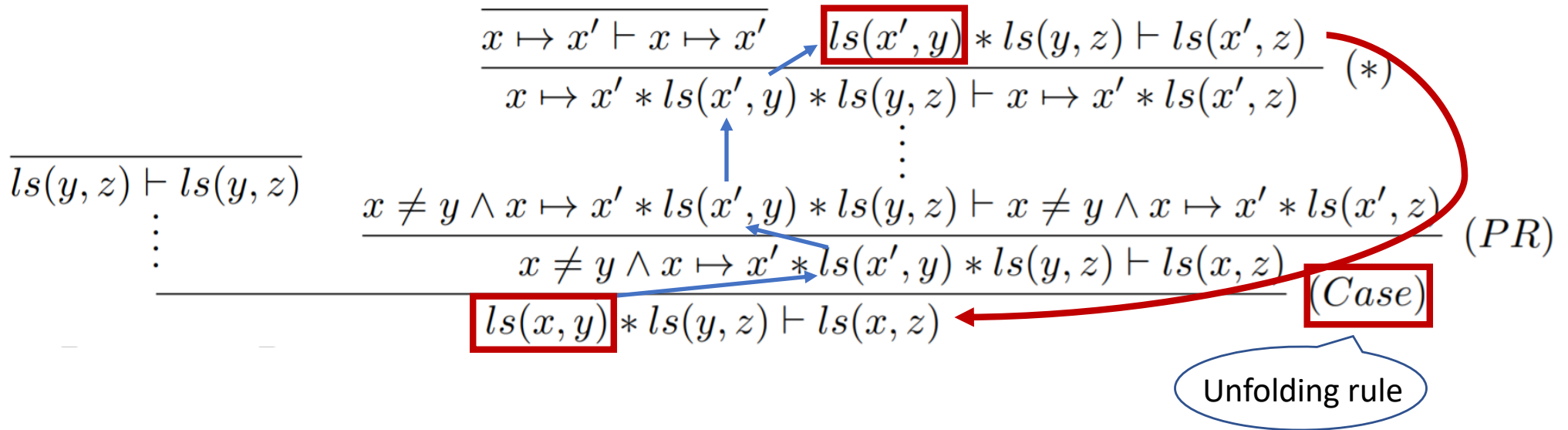
# 循環証明<sup>[Brotherston+ 2006]</sup> と 証明探索

- 帰納法に相当する循環証明を導入
- 結論から前提に向かって証明を探す

$$\begin{array}{c}
 \frac{\overline{x \mapsto x' \vdash x \mapsto x'} \quad ls(x', y) * ls(y, z) \vdash ls(x', z))}{x \mapsto x' * ls(x', y) * ls(y, z) \vdash x \mapsto x' * ls(x', z)} (*) \\
 \vdots \\
 \frac{\overline{ls(y, z) \vdash ls(y, z)} \quad \frac{x \neq y \wedge x \mapsto x' * ls(x', y) * ls(y, z) \vdash x \neq y \wedge x \mapsto x' * ls(x', z)}{x \neq y \wedge x \mapsto x' * ls(x', y) * ls(y, z) \vdash ls(x, z)} (PR)}{ls(x, y) * ls(y, z) \vdash ls(x, z)} (Case)
 \end{array}$$

# 循環証明<sup>[Brotherston+ 2006]</sup> と証明探索

- 帰納法に相当する循環証明を導入
- 結論から前提に向かって証明を探す



上(bud)の $ls(x', y)$ の長さより

下(companion)の $ls(x, y)$ の長さの方が一つ短い

➡ 帰納法に相当

# 証明探索とカット

探索時、結論から前提に向かって証明を探す

## カットと一般的な規則の差異

$$\frac{A \vdash D \quad B \vdash E}{A * B \vdash D * E} * \qquad \frac{A \vdash C \quad C \vdash B}{A \vdash B} \text{ カット}$$

- $*$ は前提の論理式がすべて結論に現れる
- カットは**カット論理式** $C$ の探索が必要

➡ カットは証明探索において不都合



# 背景

分離論理+循環証明における  
エンテイルメントチェッカーが作りたい



カット規則を除去したい

# カット除去可能性

## Definition カット除去可能性

ある証明体系 $S$ において、 $\Gamma \vdash \Delta$ が証明可能なとき、 $S - cut$ においても $\Gamma \vdash \Delta$ が証明可能であるならば、証明体系 $S$ は**カット除去可能である**という

- LKはカット除去可能である
- BIはカット除去可能である

**分離論理の循環証明体系はカット除去可能ではない**  
[Kimura+ 2020]

- LKやBIの循環証明体系については未解決  
ただし、どうやらカット除去出来なさそう

# 自動証明に向けた制限

カットは邪魔だが除去できない

➡ 何らかの制限を考える

大きく分けて以下の二通りが考えられる

- **カットそのもの**に制限を与える
  - カットの出現するタイミング
  - カット論理式の形 c.f.) 様相論理
- **証明対象**に制限を与える
  - シークエントに含まれる論理式
  - 帰納的述語の引数の形
  - 帰納的述語の定義の与え方
  - 帰納的述語同士の関係

# 自動証明に向けた制限

カットは邪魔だが除去できない

➡ 何らかの制限を考える

大きく分けて以下の二通りが考えられる

- **カットそのもの**に制限を与える
  - カットの出現するタイミング
  - カット論理式の形 c.f.) 様相論理
- **証明対象**に制限を与える
  - シークエントに含まれる論理式
  - **帰納的述語の引数の形**
  - 帰納的述語の定義の与え方
  - 帰納的述語同士の関係

# 帰納的述語の引数の制限

[Kimura+ 2020]のカット除去「できない」証明は以下のシーケントで行われた

$$lsne(x, y) \vdash slne(x, y)$$

- 両辺とも、空でないリスト断片
  - ただし展開の仕方が異なる
- 2引数の帰納的述語を用いている
  - ➡ 1引数や0引数の場合どうか？

# 研究成果

- 帰納的述語を**帰納的命題**（0引数の帰納的述語）に制限しても**カット規則を除去できない**ことを示した
- 簡単な帰納的命題のみに制限した循環証明体系でカット除去できる例を示した
  - ➡ より複雑な帰納的述語に対して  
カット除去をする足がかりにしたい

# カット除去可能性の反例

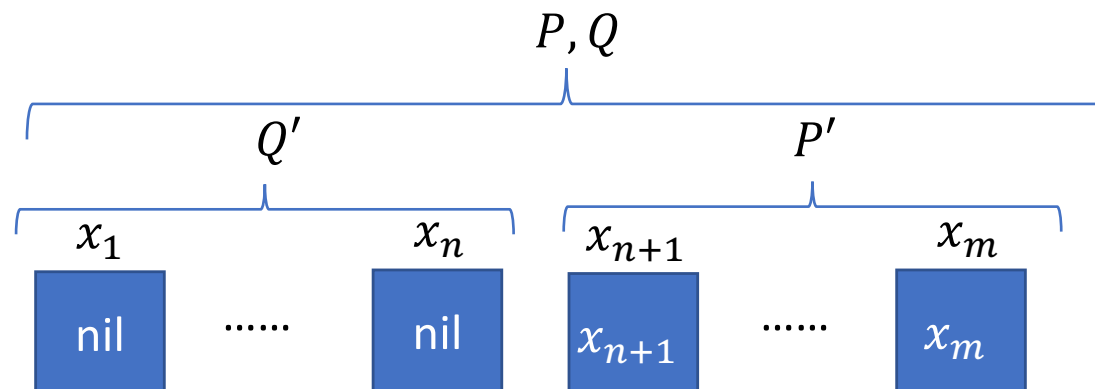
反例として用いるシーケントは以下の通り

$$P \vdash Q$$

今回考える帰納的述語は以下の4つ

$$P ::= P' \mid \exists x.(x \mapsto \text{nil} * P) \qquad Q ::= Q' \mid \exists x.(x \mapsto x * P)$$

$$P' ::= \text{emp} \mid \exists x.(x \mapsto x * P') \qquad Q' ::= \text{emp} \mid \exists x.(x \mapsto \text{nil} * Q')$$



# 循環証明体系の推論規則(1/2)

帰納的述語の展開規則以外の推論規則

c.f.) [Brotherston+ 2011]

$$\frac{}{A \vdash A} Id \quad \frac{}{x \mapsto u * x \mapsto u' * A \vdash B} Unsat \mapsto$$

$$\frac{A \vdash C \quad C \vdash B}{A \vdash B} Cut \quad \frac{A_1 \vdash B_1 \quad A_2 \vdash B_2}{A_1 * A_2 \vdash B_1 * B_2} *$$

$$\frac{A \vdash B}{A \vdash B * emp} EmpR \quad \frac{A \vdash B}{emp * A \vdash B} EmpL$$

$$\frac{A \vdash B * emp}{A \vdash B} EmpR' \quad \frac{emp * A \vdash B}{A \vdash B} EmpL'$$



# 循環証明体系の推論規則(2/2)

## 帰納的述語の展開規則

$$\begin{array}{l} \frac{P' * A \vdash B \quad x \mapsto nil * P * A \vdash B}{P * A \vdash B} \textit{Case} \quad \frac{A \vdash P' * B}{A \vdash P * B} \textit{PR} \quad \frac{A \vdash x \mapsto nil * P * B}{A \vdash P * B} \textit{PR} \\[10pt] \frac{emp * A \vdash B \quad x \mapsto x * P' * A \vdash B}{P' * A \vdash B} \textit{Case} \quad \frac{A \vdash emp * B}{A \vdash P' * B} \textit{P'R} \quad \frac{A \vdash x \mapsto x * P' * B}{A \vdash P' * B} \textit{P'R} \\[10pt] \frac{Q' * A \vdash B \quad x \mapsto x * Q * A \vdash B}{Q * A \vdash B} \textit{Case} \quad \frac{A \vdash Q' * B}{A \vdash Q * B} \textit{QR} \quad \frac{A \vdash x \mapsto c * Q * B}{A \vdash Q * B} \textit{QR} \\[10pt] \frac{emp * A \vdash B \quad x \mapsto nil * Q' * A \vdash B}{Q' * A \vdash B} \textit{Case} \quad \frac{A \vdash emp * B}{A \vdash Q' * B} \textit{Q'R} \quad \frac{A \vdash x \mapsto nil * Q' * B}{A \vdash Q' * B} \textit{Q'R} \end{array}$$

# カット除去不可能性(1/2)

## Theorem

帰納的述語を帰納的命題に制限しても  
前述の証明体系はカット除去可能でない

- このことから、引数に対する制限から  
 カット除去をするのは難しいことが分かる

証明  $P \vdash Q$  について以下の 2 つを証明する

- カットを用いて証明することが出来る
  - 実際に証明図を与えることで証明
  - カット論理式は  $x \mapsto nil * Q$
- カットなしで証明することが出来ない
  - 次スライドで説明

# カット除去不可能性(2/2)

## Lemma

シーケント  $P \vdash Q$  は  
カットなしで証明することが出来ない

- $P \vdash Q$  の証明図  $D$  を仮定し、背理法で証明
  - $D$  に出現する特定の path をたどっていくと、
    - Axiom に到達しない
    - 循環証明の条件を満たす Cycle が作れない
- ということが示せる
- Axiom に到達せず、循環構造も作れない path を含む場合  
証明図になっていないので仮定に矛盾

# カット除去可能性

## Theorem

帰納的述語を $P$ と $P'$ のみ、  
あるいは $Q$ と $Q'$ のみに制限すればカット除去できる

- 循環証明体系でカット除去できる、初めての制限

$P, P', Q, Q'$ をすべて許すとカット除去できないのに、  
 $P, P'$ だけや $Q, Q'$ だけならカット除去できる

➡ カット除去できる述語同士でも  
合わせるとカット除去できなくなる恐れがある

# まとめ

- 帰納的述語の引数を制限しても  
カット除去できないことがわかった
  - 簡単な帰納的述語でも、組み合わせ次第でダメ
  - 帰納的述語の定義の仕方や出現の仕方よりも  
その組み合わせに注目する必要がある可能性

ただし、カット除去できる例も見つかったので  
この手法を使ってより難しい述語でも、  
それ単体ならカット除去できる、  
ということが言えるかもしれない



おまけ

# モデルによるカット除去

準備するもの      証明体系 $S$     対応するモデル $M$

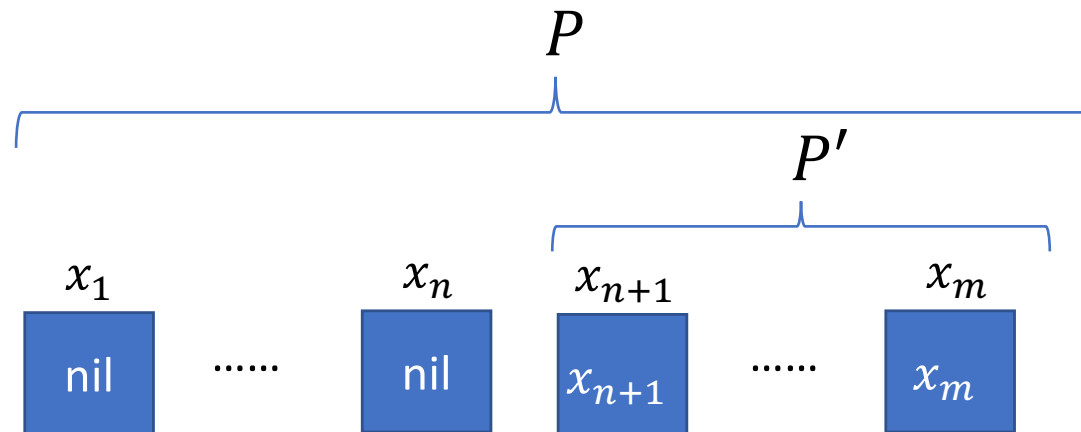
1. 任意のシークエント $\Gamma \vdash \Delta$ が $S$ で証明可能  
→  $\Gamma \vdash \Delta$ が $M$ でvalidを示す
2.  $\Gamma \vdash \Delta$ が $M$ でvalid  
→  $\Gamma \vdash \Delta$ が $S - cut$ で証明できることを示す
3. 上記2つから、  
 $\Gamma \vdash \Delta$ が $S$ で証明可能 →  $\Gamma \vdash \Delta$ が $S - cut$ で証明可能  
と言える

現在は帰納的述語を限定し、2.で  
シークエントを網羅的に調べる手法を考えている  
➡ 帰納的述語に幅を持たせると厳しい



# $P$ と $P'$ の定義 (再掲)

$$P ::= P' \mid \exists x. (x \mapsto \text{nil} * P)$$
$$P' ::= \text{emp} \mid \exists x. (x \mapsto x * P')$$



# $P$ と $P'$ のカット除去

準備するもの 証明体系 $S$  対応するモデル $M$

- $S$ は以下の規則+展開規則+cycleの体系
- $M$ は一般的なヒープモデル(帰納的述語は制限)

$$\begin{array}{c}
 \overline{A \vdash A} \text{ } Id \quad \overline{x \mapsto u * x \mapsto u' * A \vdash B} \text{ } Unsat \mapsto \\
 \\
 \frac{A \vdash C \quad C \vdash B}{A \vdash B} \text{ } Cut \quad \frac{A_1 \vdash B_1 \quad A_2 \vdash B_2}{A_1 * A_2 \vdash B_1 * B_2} * \\
 \\
 \frac{A \vdash B}{A \vdash B * emp} \text{ } EmpR \quad \frac{A \vdash B}{emp * A \vdash B} \text{ } EmpL \\
 \\
 \frac{A \vdash B * emp}{A \vdash B} \text{ } EmpR' \quad \frac{emp * A \vdash B}{A \vdash B} \text{ } EmpL'
 \end{array}$$

# $P$ と $P'$ のカット除去

1. 任意のシークエント  $\Gamma \vdash \Delta$  が  $S$  で証明可能  
→  $\Gamma \vdash \Delta$  が  $M$  で valid
  - 一般的な heap model で考えているので省略
  - 証明の高さに関する帰納法

# $P$ と $P'$ のカット除去

2.  $\Gamma \vdash \Delta$ が $M$ でvalid  
→  $\Gamma \vdash \Delta$ が $S - cut$ で証明できる

- $\Gamma$ 、 $\Delta$ の一般形を考える

$$(x \mapsto x)^{n_1} * (x \mapsto nil)^{n_2} * (x \mapsto t)^{n_3} * P^{n_4} * P'^{n_5} * emp$$

- どんな $\Gamma \vdash \Delta$ をとってきても  
invalid or cutなしで証明できる  
を示す( $n_i$ による場合分け)
- 帰納的述語に幅を持たせる場合、  
モデルを上手に選んでくる必要がある