Restriction on cut in cyclic proof system for symbolic heaps

Kenji Saotome (Nagoya)
Koji Nakazawa (Nagoya)
Daisuke Kimura (Toho)

This Talk

- Cyclic-Proof System for Separation Logic
  - Sequent-calculus style proof system
  - For automated inductive reasoning
  - Cut elimination fails ➡ Can we restrict?

- We show cuts cannot be restricted to **presumable cuts**
  - a cut formula is presumable if it may occur
    in cut-free proof segments of the goal sequent

Separation Logic [Reynolds 2002]

- Extension of Hoare logic
  - to verify programs manipulating heap memories
  - with **inductive predicates**
    to represent **recursively structured data** such as lists and trees

    e.g.) $ls(x, y)$ … list segment from x to y

- We have to tackle some problems
  - Loop invariant detection
  - Entailment checking

    e.g.)

    $$ls(x, z) * ls(z, y) \quad \vdash \quad ls(x, y)$$

Separation Logic [Reynolds 2002]

- Extension of Hoare logic
  - to verify programs manipulating heap memories
  - with **inductive predicates**
    to represent **recursively structured data** such as lists and trees

    e.g.) $ls(x, y)$ … list segment from x to y

- We have to tackle some problems
  - Loop invariant detection
  - **Entailment checking**

    e.g.)

$$ls(x, z) * ls(z, y) \quad \vdash \quad ls(x, y)$$

Cyclic-Proof Search

Cyclic proof = sequent-calculus style proof

[Brotherston+ 2006] with cyclic structure representing induction

$$ls(x, y) * ls(y, z) \vdash ls(x, z)$$

Cyclic-Proof Search

Cyclic proof = sequent-calculus style proof
[Brotherston+ 2006] with cyclic structure representing induction

$$\dfrac{\dfrac{\overline{ls(y,z) \vdash ls(y,z)}}{\vdots} \quad x \neq y \wedge x \mapsto x' * ls(x',y) * ls(y,z) \vdash ls(x,z)}{ls(x,y) * ls(y,z) \vdash ls(x,z)}\,(Case)$$

Cyclic-Proof Search

Cyclic proof = sequent-calculus style proof
[Brotherston+ 2006] with cyclic structure representing induction

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

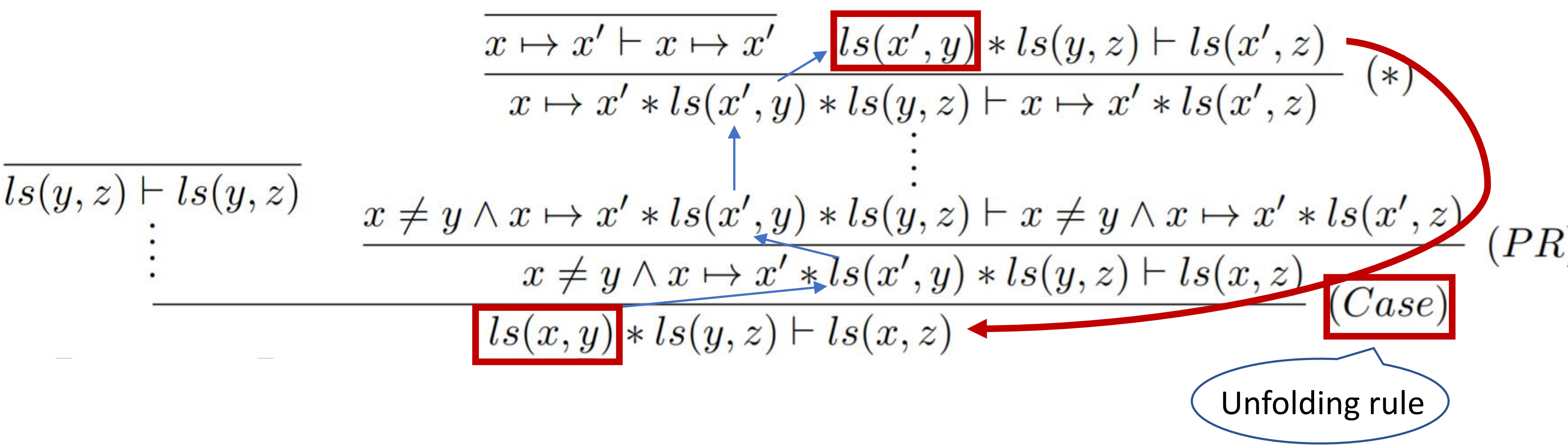
Cyclic-Proof Search

Cyclic proof = sequent-calculus style proof
[Brotherston+ 2006] with cyclic structure representing induction

$$\dfrac{\dfrac{}{ls(y,z) \vdash ls(y,z)} \quad \vdots \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{x \mapsto x' \vdash x \mapsto x'} \qquad ls(x',y) * ls(y,z) \vdash ls(x',z)}{x \mapsto x' * ls(x',y) * ls(y,z) \vdash x \mapsto x' * ls(x',z)}\,(*)}{\vdots \atop x \neq y \wedge x \mapsto x' * ls(x',y) * ls(y,z) \vdash x \neq y \wedge x \mapsto x' * ls(x',z)}}{x \neq y \wedge x \mapsto x' * ls(x',y) * ls(y,z) \vdash ls(x,z)}\,(PR)}{ls(x,y) * ls(y,z) \vdash ls(x,z)}\,(Case)$$

Cyclic-Proof Search

Cyclic proof [Brotherston+ 2006] = sequent−calculus style proof with cyclic structure representing induction



The length of $ls(x', y)$ is shorter than $ls(x, y)$

- The cycle represents a proof by induction

Cut in Cyclic Proof

$$\frac{A \vdash D \quad B \vdash E}{A * B \vdash D * E}\ (*) \qquad \frac{A \vdash \boldsymbol{C} \quad \boldsymbol{C} \vdash B}{A \vdash B}\ (\mathrm{cut})$$

- For $(*)$,
  all formulas in premises can be found in the conclusion
- For (cut), the **cut formula $\boldsymbol{C}$** is not in the conclusion

➡ To find cut formulas is hard
in automatic proof search

However…

Eliminating cut rule changes the provability[Kimura+ 2019]

Cut Restriction

Can we restrict cuts for cyclic-proof search?

$$\frac{A \vdash \boldsymbol{C} \quad \boldsymbol{C} \vdash B}{A \vdash B}\ (\mathrm{cut})$$

Example : modal logic $S5^*$

- $S5^*$ does **not** enjoy cut elimination

[Ohnishi+ 1959]

- We can restrict
  cut formulas $\boldsymbol{C}$ to subformulas of A and B [Takano 1992]

➡ Such restriction is good for proof search

Can we restrict cuts in cyclic-proof system like $S5^*$?

Our Result

It is hard to restrict cuts in cyclic-proof system for SL

- We define **presumable cut** for cut restriction
  - A cut is presumable if it may occur in cut-free proof segments of the conclusion (more relaxed restriction than $S5^*$)

main result

CSL_1ID^ω w/o cut $\subsetneq$ [Kimura+2019] CSL_1ID^ω with only presumable cut $\subsetneq$ (main result) CSL_1ID^ω (with cut)

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

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

Cyclic-Proof System

CSL_1ID^{ω}

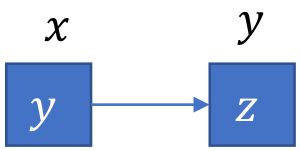
SL_1: Separation Logic for Symbolic Heaps

- Formulas represent structures of heap memories
  - $x \mapsto y \cdots$ the heap contains exactly one memory cell of the address x which stores the value y
  - $emp \cdots$ the heap contains no memory cells
  - $A * B \cdots$ the heap can be separated into two disjoint parts A and B

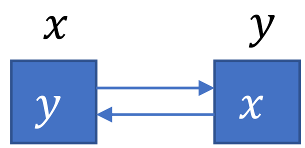
$$
\begin{array}{lll}
A ::= \Pi \wedge \Sigma & \cdots & \text{symbolic heaps} \\
\Pi ::= \top \mid t = u \mid t \neq u \mid \Pi \wedge \Pi & \cdots & \text{pure formulas} \\
\Sigma ::= emp \mid t \mapsto u \mid \Sigma * \Sigma \mid P(\vec{t}) & \cdots & \text{spatial formulas} \\
t ::= x \mid nil & \cdots & \text{terms} \\
e ::= A \vdash A & \cdots & \text{sequents}
\end{array}
$$

Examples of SL_1 formula

$x \mapsto y * y \mapsto z$



$x \mapsto y * y \mapsto x$



- $x \mapsto y * x \mapsto y$ is **not** satisfiable

Heap Model (s,h)

Store $s : \text{Variables} \rightarrow \mathbb{N}$

Heap $h: \mathbb{N} \setminus \{0\} \xrightarrow[fin]{} \mathbb{N}$

Example of heap

$$h(1) = 2, h(2) = 4, h(4) = 1$$

Address	1	2	4
Value	2	4	1

Semantics of SL_1 formulas

$$s, h \vDash t \mapsto u \Leftrightarrow dom(h) = \{s(t)\} \,\&\, h(s(t)) = s(u)$$

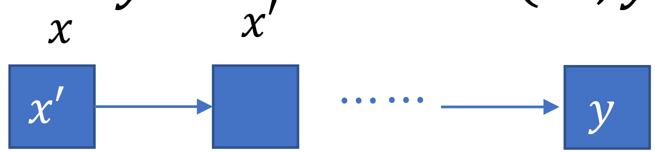
$$s, h \vDash A * B \Leftrightarrow \exists h_1, h_2. (h = h_1 \cup h_2, \ \mathrm{dom}(h_1) \cap \mathrm{dom}(h_2) = \emptyset, \ s, h_1 \vDash A, s, h_2 \vDash B)$$

$$A \vdash B \text{ is valid iff } \forall s, h. (s, h \vDash A \Rightarrow s, h \vDash B)$$

Inductive Definitions in SL_1

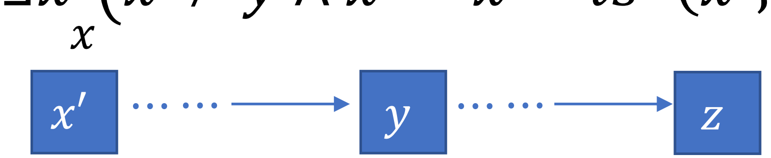
- $ls(x, y)$: list segment from x to y

$$ls(x,y) \coloneqq x = y \wedge emp$$
$$\mid \;\; \exists x'. \left(x \neq y \wedge x \mapsto x' * ls(x', y) \right)$$



- $ls^3(x, y, z)$: list segment from x to z containing y.

$$ls^3(x,y,z) \coloneqq x = y \wedge y = z \wedge emp$$
$$\mid \exists x'. \left(x = y \wedge y \neq z \wedge x \mapsto x' * ls^3(x', x', z) \right)$$
$$\mid \exists x' \left(x \neq y \wedge x \mapsto x' * ls^3(x', y, z) \right)$$



  - $ls^3(x, y, z)$ is equivalent to $ls(x, y) * ls(y, z)$

CSL_1ID^ω

- Cyclic-proof system for SL_1

Inference rules

$$\frac{A \vdash C \quad C \vdash B}{A \vdash B}\ (cut) \qquad \frac{A \vdash C \quad B \vdash D}{A * B \vdash C * D}\ (*)$$

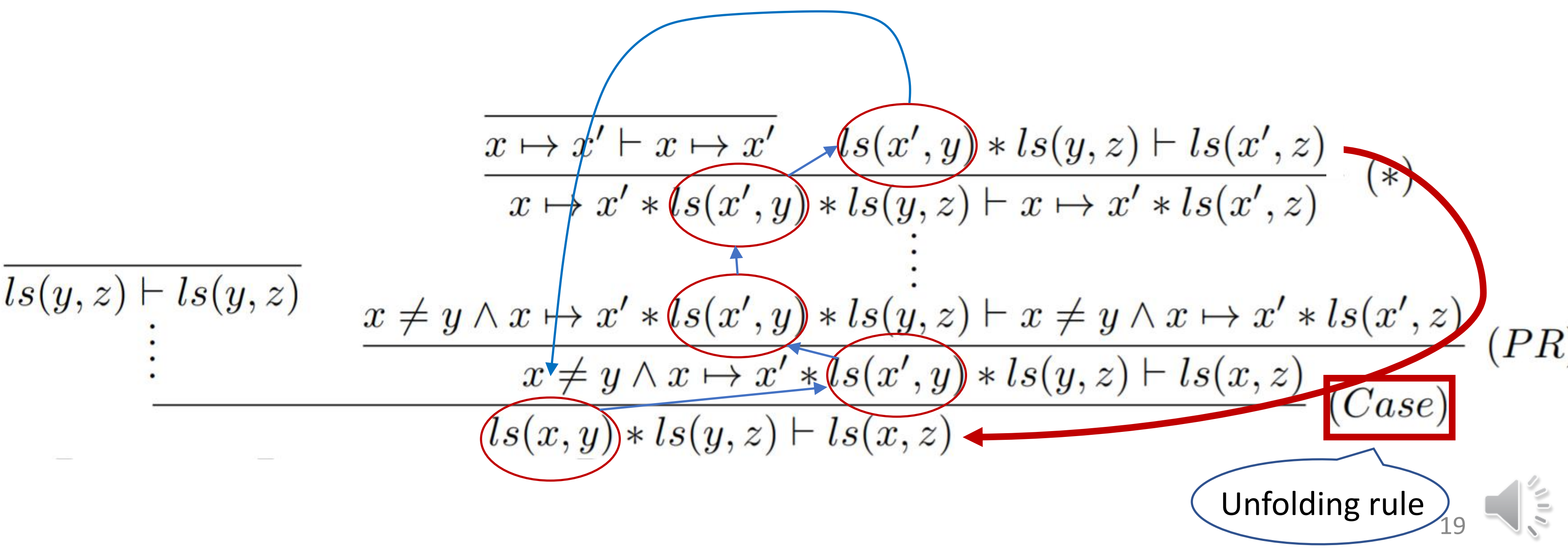
$$\frac{C_1(\boldsymbol{x}, \boldsymbol{y}_1) * A \vdash B \quad \cdots \quad C_n(\boldsymbol{x}, \boldsymbol{y}_n) * A \vdash B}{P(\boldsymbol{x}) * A \vdash B}\ (Case) \qquad \frac{A \vdash C_i(\boldsymbol{u}, \boldsymbol{t}) * B}{A \vdash P(\boldsymbol{u}) * B}\ (PR)$$

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

Global Trace Condition
[Brotherston+ 2006]

A cyclic−proof structure is really a proof if it satisfies the global trace condition

- Every infinite path contains
  a trace unfolded infinitely many times



Cut Restriction to Presumable Cuts

Cut Restriction

$$\frac{A \vdash \boldsymbol{C} \quad \boldsymbol{C} \vdash B}{A \vdash B} \ \text{(cut)}$$

To find cut formulas is hard for proof search

- **We cannot eliminate cut in $\boldsymbol{CSL_1ID^\omega}$** [Kimura+ 2019]

Can we restrict cuts in CSL_1ID^ω?

cf.) $S5^*$ can restrict cut formulas $\boldsymbol{C}$
to subformulas of A and B

Presumable Cut

- **presumable formula** from $A \vdash B$

$$\dfrac{\dfrac{A' \vdash C \quad A' \vdash D * E}{A' \vdash B}}{A \vdash B}$$

Incomplete proof tree

Cut-free proof segment

All of $A, A', B, C, D, E, D * E, \ldots$ are presumable from $A \vdash B$

- **presumable cut** = cut with presumable cut formula

Definition (Quasi cut-elimination property)

If every $A \vdash B$ which is provable with cuts can be proved with only $presumable\ cuts$, we say that the proof system satisfies the quasi **cut-elimination property**

cf.) Modal logic $S5^*$ satisfies quasi cut-elimination property

Examples of presumable formulas

From the sequent $ls(x,z) * ls(z,y) \vdash ls(x,y)$

$$\dfrac{\cdots \qquad \dfrac{\Pi_2 \wedge x \mapsto w * ls(w,z) * ls(z,y) \vdash \Pi_1 \wedge x \mapsto y * ls(y,y)}{ls(x,z) * ls(z,y) \vdash \Pi_1 \wedge x \mapsto y * ls(y,y)}\text{Case}}{ls(x,z) * ls(z,y) \vdash ls(x,y)}\text{PR}$$

Π_1 and Π_2 are pure parts

Presumable

$$ls(x,z) * ls(z,y), \qquad ls(x,y)$$
$$x \mapsto y, \qquad x \mapsto w * ls(w,z),$$
$$x \mapsto w * ls(w,z) * ls(z,y), \ldots$$

Not presumable

$$ls(x,z) * ls(z,w) * ls(w,y)$$

Main Theorem

- Theorem

CSL_1ID^ω **does not** satisfy
quasi cut-elimination property

- Proof

Counterexample : $ls^3(x,y,x) \vdash ls^3(y,x,y)$

1. We can prove $ls^3(x,y,x) \vdash ls^3(y,x,y)$ with cuts
2. There is no proof of $ls^3(x,y,x) \vdash ls^3(y,x,y)$ with only presumable cuts

main result

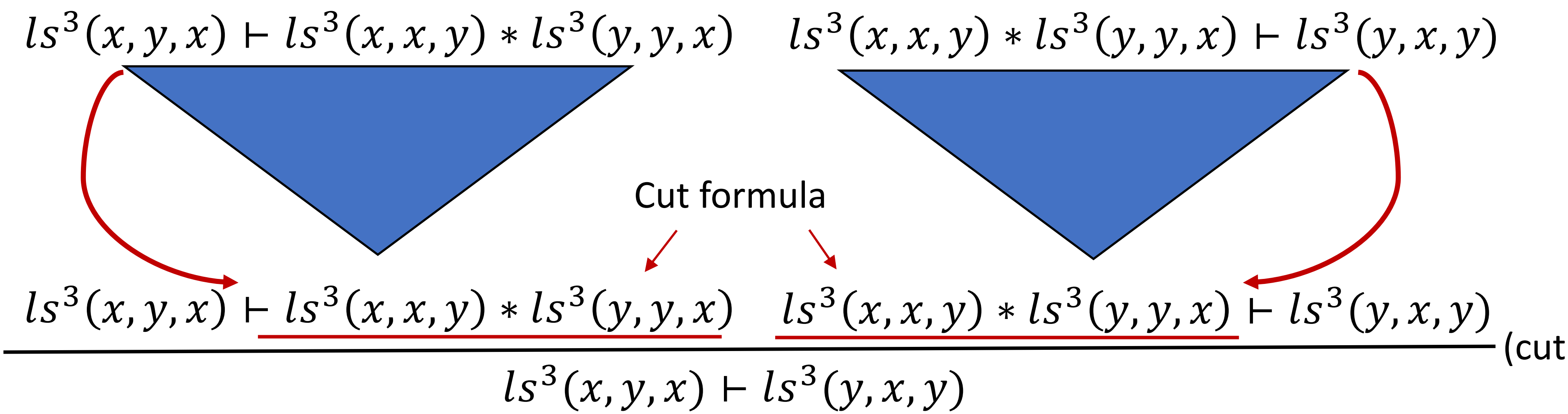
CSL_1ID^ω w/o cut $\subsetneq$ [Kimura+2019] CSL_1ID^ω with only presumable cut $\subsetneq$ (main result) CSL_1ID^ω (with cut)

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

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

Outline of Proof

1. We can prove $ls^3(x,y,x) \vdash ls^3(y,x,y)$ with cut



- We can prove $ls^3(x,y,x) \vdash ls^3(y,x,y)$ with cuts
- The cut formula $ls^3(x,x,y) * ls^3(y,y,x)$ is **not presumable** from the conclusion

Outline of Proof

2. There is no proof of $ls^3(x, y, x) \vdash ls^3(y, x, y)$ with only presumable cuts

- First, we assume existence of a cyclic proof of $ls^3(x, y, x) \vdash ls^3(y, x, y)$ with only presumable cuts
- Following a particular infinite path

⇒ the path has no trace unfolded infinitely many times

- Such an infinite path is not allowed because it does not satisfy the global trace condition

⇒ Contradiction

Related Work

- Automated Lemma Synthesis in Symbolic-Heap Separation Logic[Ta+ 2018]
  - Cuts with lemma generated automatically
- Automatic Induction Proofs of Data-Structures in Imperative Programs[Chu+ 2015]
  - Cuts with sequents occurring in proof search

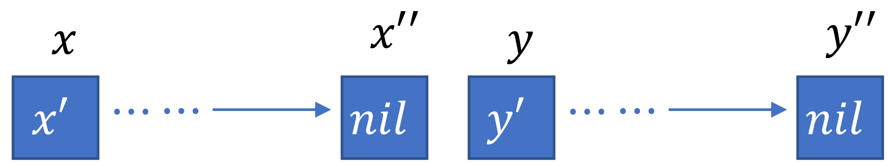
They have no discussed
theoretical properties on the provability

Conclusion

Theorem

We **can't restrict** cuts in CSL_1ID^ω **to presumable cuts**

- Counterexample : $ls^3(x, y, x) \vdash ls^3(y, x, y)$
  Another counterexample : $dl(x, y) \vdash dl(y, x)$
  - $dl(x, y)$ represent



  - We can prove $dl(x, y) \vdash dl(y, x)$
    with the cut formula $dl(x, nil) * dl(y, nil)$

Future work

- More relaxed restriction for proof search
- Restriction on inductive predicates to achieve (quasi) cut-elimination property