# Failure of Cut-Elimination in the Cyclic Proof System of Bunched Logic with Inductive Propositions

Kenji Saotome
(Nagoya)

Koji Nakazawa
(Nagoya)

Daisuke Kimura
(Toho)

MLA 2021 @ online

# Cyclic Proof System

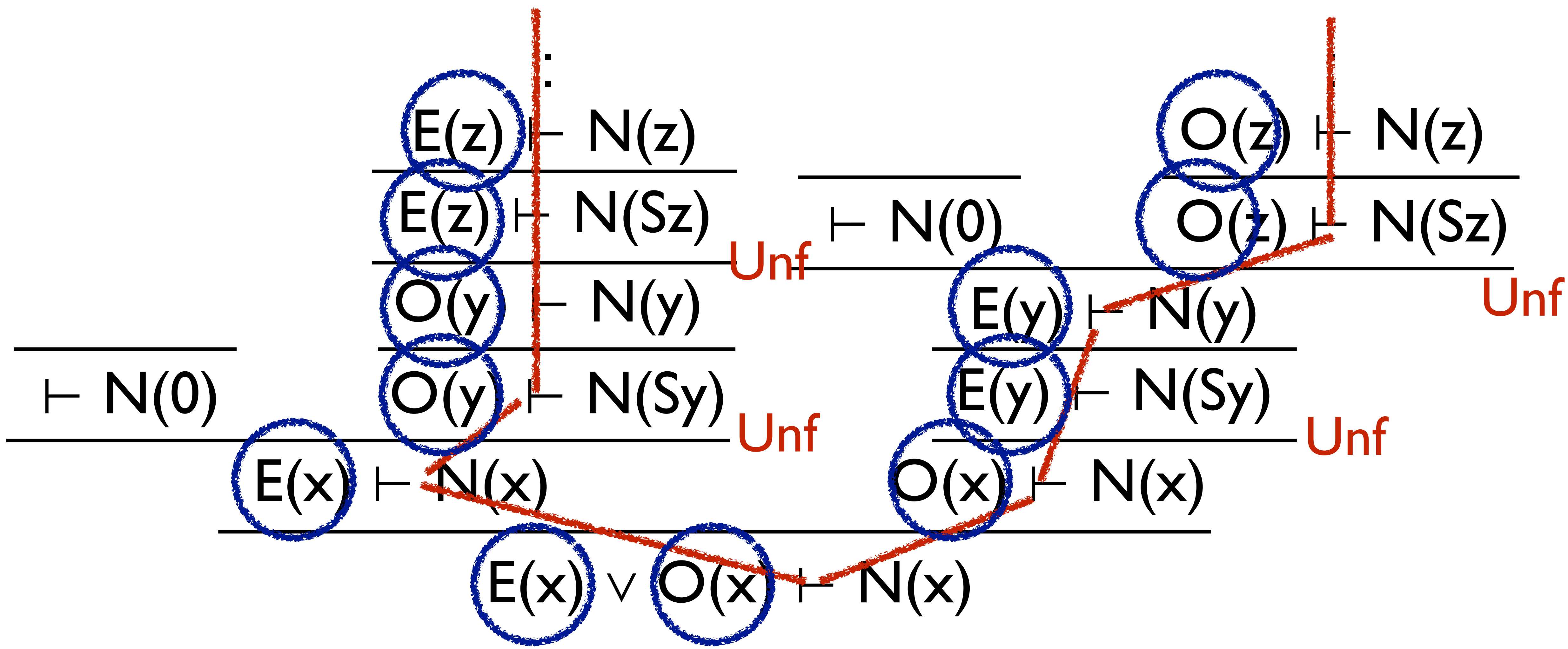
# Proof with Infinite Paths

- $\mathrm{LKID}_\omega$ [Brotherston'06] for inductive predicates
  - Extension of LK which admits infinite paths in proofs with some soundness condition (global trace condition)

$$
\dfrac{
  \dfrac{
    \dfrac{}{\vdash N(0)}
    \qquad
    \dfrac{
      \dfrac{
        \dfrac{
          \dfrac{\vdots}{E(z) \vdash N(z)}
        }{E(z) \vdash N(Sz)}
      }{O(y) \vdash N(y)}
    }{O(y) \vdash N(Sy)}
  }{E(x) \vdash N(x)}
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{}{\vdash N(0)}
        \qquad
        \dfrac{
          \dfrac{\vdots}{O(z) \vdash N(z)}
        }{O(z) \vdash N(Sz)}
      }{E(y) \vdash N(y)}
    }{E(y) \vdash N(Sy)}
  }{O(x) \vdash N(x)}
}{E(x) \vee O(x) \vdash N(x)}
$$

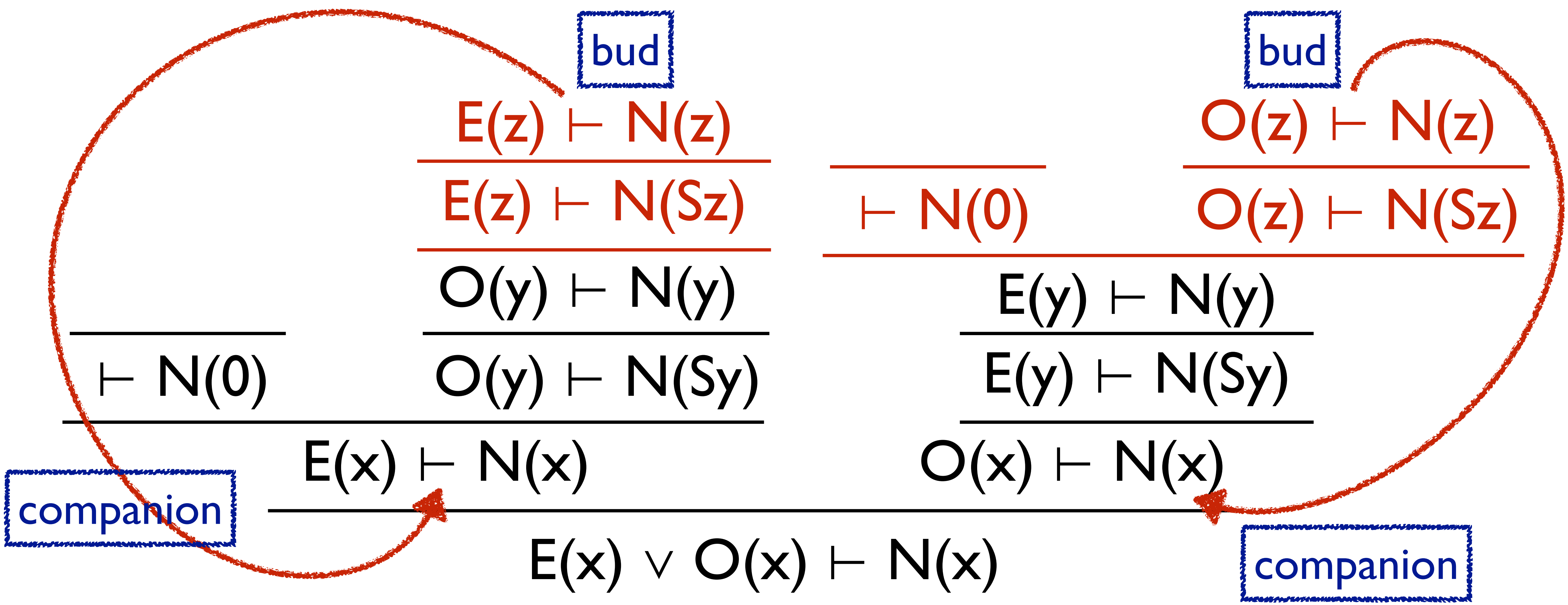
# Global Trace Condition

- Every infinite path has a trace (sequence of predicates on LHS) where unfolding rules are applied infinitely many times



# Cyclic Proofs

- CLKID$_\omega$ [Brotherston'06]
  - Regular representation of LKID$_\omega$ proofs by cyclic structure of proofs
  - Good for automation of (bottom-up) proof search



# Cut-Elimination in Cyclic Proof Systems

- Cut-elimination does not hold in the cyclic proof system for the symbolic-heap separation logic [Kimura+'19]
  - separation logic (SL) is for program analysis of pointer programs based on the bunched logic (BI)
  - symbolic heaps are restricted forms of the SL formulas
- Questions:
  - How about the cut-elimination in cyclic proof systems for other logics such as BI, LL, FOL,…?
  - Can we restrict predicates to recover the cut-elimination?

# This Talk

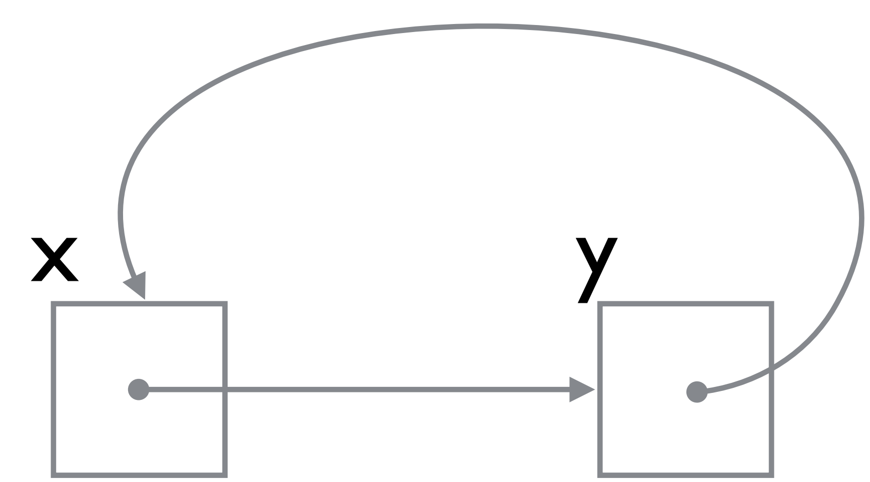
- Cut-elimination does not hold in cyclic BI
  - even if we consider only 0-ary predicates
    - [Kimura+'19]'s counterexample contains 2-ary predicates
  - using the proof unrolling for cyclic proofs
  - the proof can be adapted to SL and MLL

# Cut-Elimination Fails in Cyclic Proof System of Symbolic-Heap SL

**[Kimura+'19]**

# $SL_0$: Core Separation Logic

- Symbolic-heap formulas represent shape of heap memories
  - variables represent addresses of memory cells
  - $x \mapsto y$ means "the heap contains exactly one memory cell of address x which stores the value y"
  - $A * B$ means "the heap can be divided to two disjoint subheaps satisfying A and B, respectively"
- Example: $x \mapsto y * y \mapsto x$
  - implies $x \neq y$



# Symbolic Heaps in $SL_0$

$A ::= x \mapsto (t_1 \ldots t_n) \mid A * A' \mid P(t_1 \ldots t_n) \qquad (t ::= x \mid nil)$

- $P(x_1 \ldots x_m)$ is inductively defined by definition clauses
  - $\exists z_1 \ldots z_n A(x_1 \ldots x_m, z_1 \ldots z_n)$
- Examples of inductive definitions
  - $ls(x,y) = (x \mapsto y) \mid \exists z(x \mapsto z * ls(z,y))$
  - $sl(x,y) = (x \mapsto y) \mid \exists z(sl(x,z) * z \mapsto y)$

# $CSL_0ID_\omega$

- Cyclic-proof system for $SL_0$
  - $P(x) := \exists z D_1(x,z) \mid \ldots \mid \exists z D_n(x,z)$

$$\frac{}{A \vdash A}\,\mathrm{Id} \qquad \frac{A \vdash B \qquad B \vdash C}{A \vdash C}\,\mathrm{Cut} \qquad \frac{A_1 \vdash B_1 \qquad A_2 \vdash B_2}{A_1 * A_2 \vdash B_1 * B_2}\,*$$

$$\frac{A \vdash B * D_i(x,t)}{A \vdash B * P(x)}\,\mathrm{RU}$$

$$\frac{D_1(x,z) * A \vdash B \quad \ldots \quad D_n(x,z) * A \vdash B}{P(x) * A \vdash B}\,\mathrm{LU}\ \ (z \text{ is fresh})$$

# Example: ls * ls ⊢ ls

$$\dfrac{\dfrac{\dfrac{}{x\mapsto y * \mathrm{ls}(y,z) \vdash x\mapsto y * \mathrm{ls}(y,z)}\,\mathrm{Id}}{x\mapsto y * \mathrm{ls}(y,z) \vdash \mathrm{sl}(x,z)}\,\mathrm{UR} \qquad \dfrac{\dfrac{\dfrac{}{x\mapsto v \vdash x\mapsto v}\,\mathrm{Id} \qquad \mathrm{ls}(v,y) * \mathrm{ls}(y,z) \vdash \mathrm{ls}(v,y)}{x\mapsto v * \mathrm{ls}(v,y) * \mathrm{ls}(y,z) \vdash x\mapsto v * \mathrm{ls}(v,y)}\,*}{x\mapsto v * \mathrm{ls}(v,y) * \mathrm{ls}(y,z) \vdash \mathrm{ls}(x,z)}\,\mathrm{RU}}{\mathrm{ls}(x,y) * \mathrm{ls}(y,z) \vdash \mathrm{ls}(x,z)}\,\mathrm{LU}$$

# Theorem

- Theorem [Kimura+'19]:
  Cut-elimination does not hold in $CSL_0ID_\omega$
- Proof
  - $ls(x,y) \vdash sl(x,y)$ is
    - provable with cuts, and
    - not provable without cuts

# No Cut-Free Cyclic Proof

- We can chase a contradictory path in any cyclic proof of $ls(x,y) \vdash sl(x,y)$

invalid!

$$\frac{x \mapsto z_1 * \ldots * z_{n-1} \mapsto z_n * ls(z_n,y) \vdash sl(x,w) * w \mapsto y}{x \mapsto z_1 * \ldots * z_{n-1} \mapsto z_n * ls(z_n,y) \vdash sl(x,y)}\ \text{RU}$$

$$\vdots$$

$$\frac{\vdots \qquad \dfrac{\vdots \qquad x \mapsto z_1 * z_1 \mapsto z_2 * ls(z_2,y) \vdash sl(x,y)}{x \mapsto z_1 * ls(z_1,y) \vdash sl(x,y)}\ \text{LU}}{ls(x,y) \vdash sl(x,y)}\ \text{LU}$$

the rule * cannot be applied

it cannot be a bud

# Questions

- How about other cyclic proof systems?
  - Bunched logic (BI) contains additive conjunctions that admit structural rules (weakening and contraction)
- Can we restrict inductive predicates to recover the cut-elimination?
  - What happens if we restrict the arity to one or zero?

# Bunched Logic

# Bunched Logic [O'Hearn+'99]

- Logic with multiplicative (*) and additive ($\wedge$) conjunctions
  - for reasoning compositional properties of resources
  - SL is based on the bunched logic
- Lists of formulas in seuqents are extended by bunches
  - e.g.) $\underbrace{(A, B); (A, C)}_{\text{bunch}} \vdash A * (B \wedge C)$
    - intuitively means $(A * B) \wedge (A * C) \vdash A * (B \wedge C)$
    - cf.) In LJ, $A, B, C \vdash D$ means $A \wedge B \wedge C \vdash D$

# Formulas and Bunches

- Formulas: $A ::= I \mid T \mid P \mid A * A \mid A \wedge A$
  - I and T are proposition constants
  - P is an atomic or an inductive propositions (0-ary only)
- Bunches: $\Gamma ::= A \mid \Gamma , \Gamma \mid \Gamma ; \Gamma$
  - up to commutative monoid equations for (“,”, I) and ( “;”, T)
    e.g.) $I , \Gamma \simeq \Gamma \simeq T ; \Gamma$
- Intuitively, a bunch Γ means the formula φ(Γ):
  - $\varphi(A) = A \quad \varphi(\Gamma, \Delta) = \varphi(\Gamma) * \varphi(\Delta) \quad \varphi(\Gamma ; \Delta) = \varphi(\Gamma) \wedge \varphi(\Delta)$

# Multiset Models

- A multiset model $M = \{P_M \mid P : \text{an atomic proposition}\}$
- For a multiset m consisting of the elements in M,

  $m \models T$ always holds

  $m \models I \Leftrightarrow m = \{\ \}$

  $m \models P \Leftrightarrow m = \{P_M\}$ (for an atomic proposition P)

  $m \models A \wedge B \Leftrightarrow m \models A$ and $m \models A$

  $m \models A * B \Leftrightarrow m = m_1 + m_2$ (multiset sum),

  $m_1 \models A$ and $m_2 \models B$ hold for some $m_1, m_2$

  (the semantics of inductive preds are defined by lfp's)

# Multiset Models

- Example: For atomic propositions A, B, and inductive propositions $P_{AB} ::= P_B \mid P_{AB} * A \qquad P_B ::= I \mid P_B * B$
  - $\{ A_M, A_M, B_M \} \models A * A * B$
  - $\{ A_M, B_M \} \not\models A * A * B$
  - $\{ B_M, B_M \} \models P_B$
  - $\{ A_M, A_M, A_M, B_M, B_M, B_M \} \models P_{AB}$

# $\mathrm{CLBI}^{\omega}{}_{\mathrm{ID}}$ [Brotherston'07]

- A cyclic proof system for BI
- Rules for $*$ and $\wedge$

$$\frac{\Gamma(A\,,B) \vdash C}{\Gamma(A * B) \vdash C}\ L* \qquad \frac{\Gamma(A\,;B) \vdash C}{\Gamma(A \wedge B) \vdash C}\ L\wedge$$

$$\frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma, \Delta \vdash A * B}\ R* \qquad \frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma ; \Delta \vdash A \wedge B}\ R\wedge$$

- unfolding rules (same as $\mathrm{CSLID}_{\omega}$), and
- structural rules and cut

$$\frac{\Gamma(\Delta) \vdash A}{\Gamma(\Delta\,;\Delta') \vdash A}\ W \qquad \frac{\Gamma(\Delta\,;\Delta) \vdash A}{\Gamma(\Delta) \vdash A}\ C \qquad \frac{\Gamma \vdash A \qquad \Delta(A) \vdash B}{\Delta(\Gamma) \vdash B}\ Cut$$

# Soundness of $CLBI^{\omega}_{ID}$

- Theorem [Brotherston'07]:
  $CLBI^{\omega}_{ID}$ is sound for standard models

- In particular, for every sequent $\Gamma \vdash A$ in a cyclic proof,
  $m \models \varphi(\Gamma)$ implies $m \models A$ for any multiset m

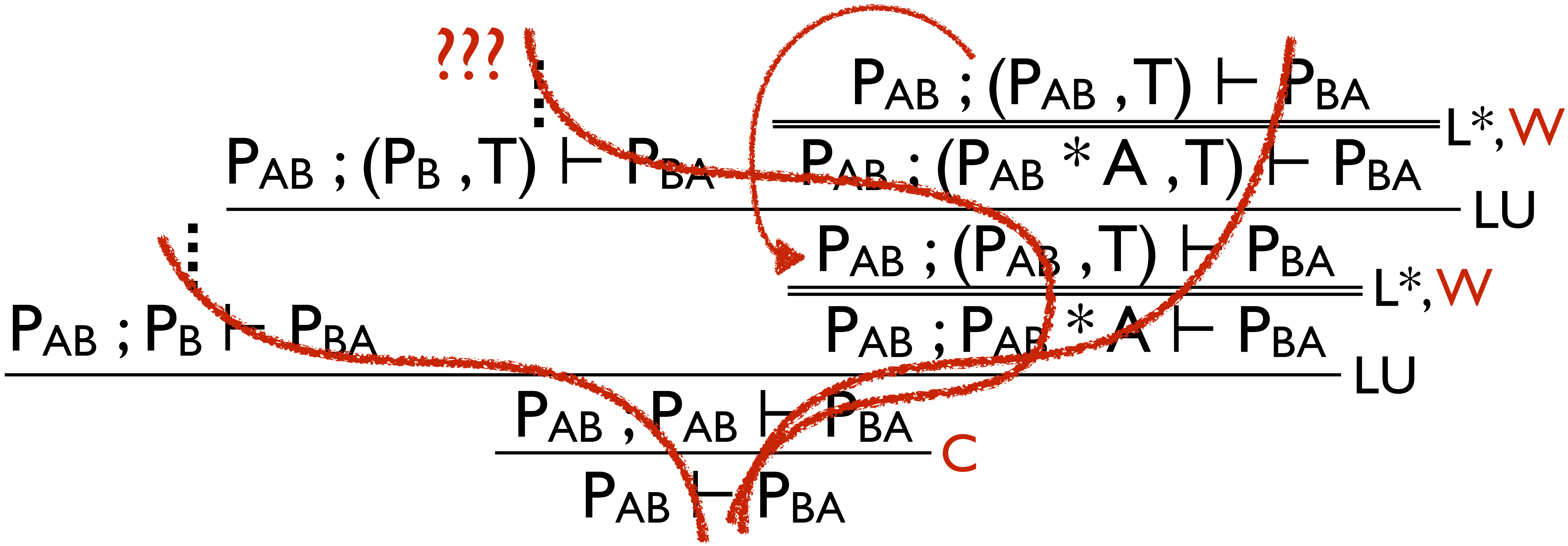
# Cut-Elimination Fails in $\mathrm{CLBI}^{\omega}_{\mathrm{ID}}$

# Theorem

- Theorem:
  Cut-elimination does not hold in $CLBI^{\omega}_{ID}$
  even if we restrict predicates to 0-ary ones

- Proof
  - A counterexample is $P_{AB} \vdash P_{BA}$
    with 0-ary predicates $P_{AB}$ and $P_{BA}$ defined by
    - $P_{AB} ::= P_B \mid P_{AB} * A \qquad P_A ::= I \mid P_A * A$
      $P_{BA} ::= P_A \mid P_{BA} * B \qquad P_B ::= I \mid P_B * B$
      (A and B are atomic propositions)

# Where is a Contradictory Path in a Cyclic Proof for BI?




- The leftmost and the rightmost paths contain no contradiction
- We have to chase the contradiction on the middle path

# Proof Unrolling

- Proposition: For a cyclic proof of $\Gamma \vdash A$,
  and a bunch $\Delta$ obtained by unfolding predicates in $\Gamma$,
  we can construct a non-cyclic proof of $\Delta \vdash A$

- Example: If we have a cyclic proof of $P_{AB} \vdash P_{BA}$,
  we can construct non-cyclic proofs of

  $$I * A * A * \ldots * A \vdash P_{BA}$$

  for any number of A's

# Proof Unrolling

Cycle is unrolled

$$P_{AB} ; (P_{AB}, T) \vdash P_{BA}$$
L*, W
$$P_{AB} ; (P_{AB} * A, T) \vdash P_{BA}$$
LU
$$P_{AB} ; (P_{AB}, T) \vdash P_{BA}$$
L*, W
$$P_{AB} ; P_{AB} * A \vdash P_{BA}$$

$$P_{AB} ; (P_B, T) \vdash P_{BA}$$

$$P_{AB} ; P_B \vdash P_{BA}$$

$$P_{AB} ; P_{AB} \vdash P_{BA}$$
C
$$P_{AB} \vdash P_{BA}$$

For LU, we choose a case depending on the unfolding tree to obtain I

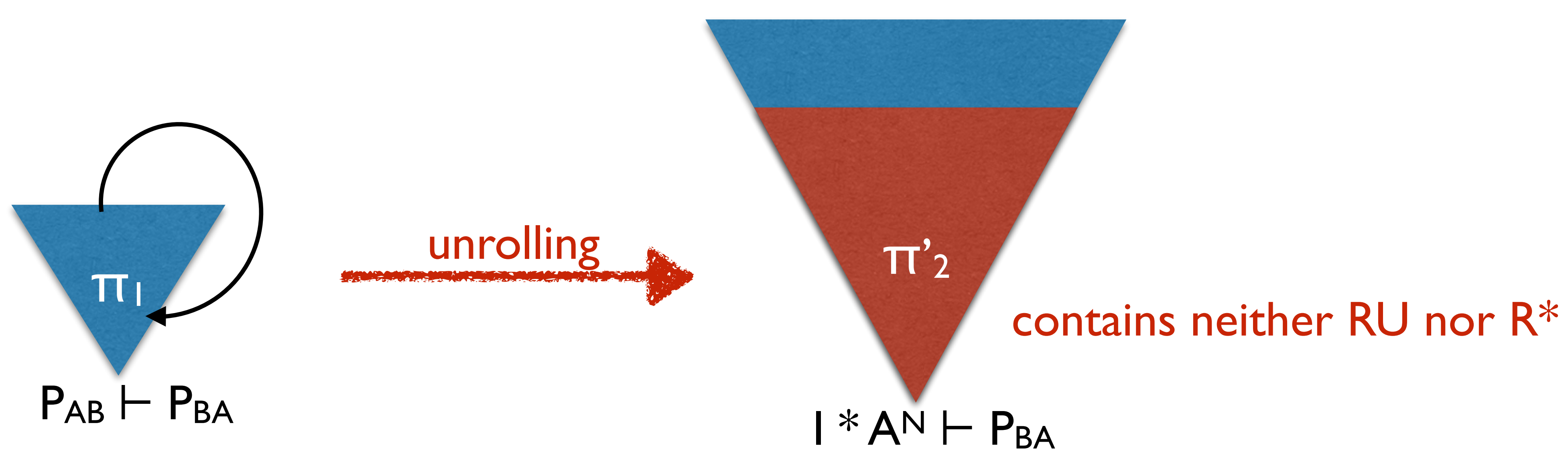
the unfolding tree to obtain I * A * A

For a sufficiently large number of A's, any path in unrolled proof is contradictory

$$I * A * A ; (I, T) \vdash P_{BA}$$
L*
$$I * A * A ; (I * A, T) \vdash P_{BA}$$
L*, W
$$I * A * A ; I * A * A \vdash P_{BA}$$
C
$$I * A * A \vdash P_{BA}$$

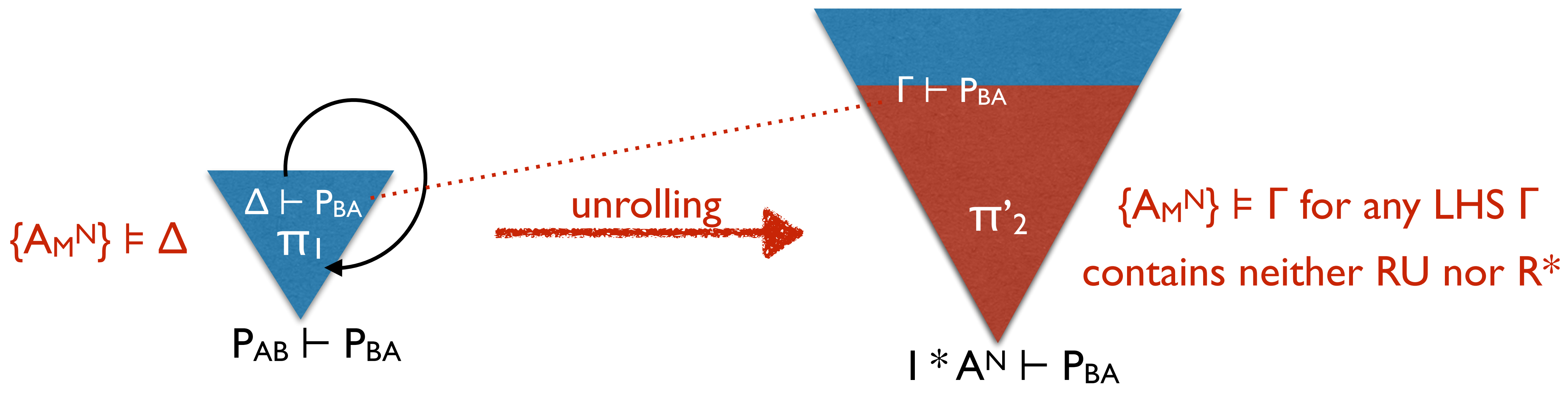
# $P_{AB} \vdash P_{BA}$ is Not Cut-Free Provable

- Assume a cyclic proof $\pi_1$ of $P_{AB} \vdash P_{BA}$
  - Let N = (the max size of LHS's of sequents in $\pi_1$) + 1
- By proof unrolling,
  we get a non-cyclic proof $\pi_2$ of $I * A^N \vdash P_{BA}$
- Let $\pi'_2$ be the right-rule free segment of $\pi_2$



# $P_{AB} \vdash P_{BA}$ is Not Cut-Free Provable

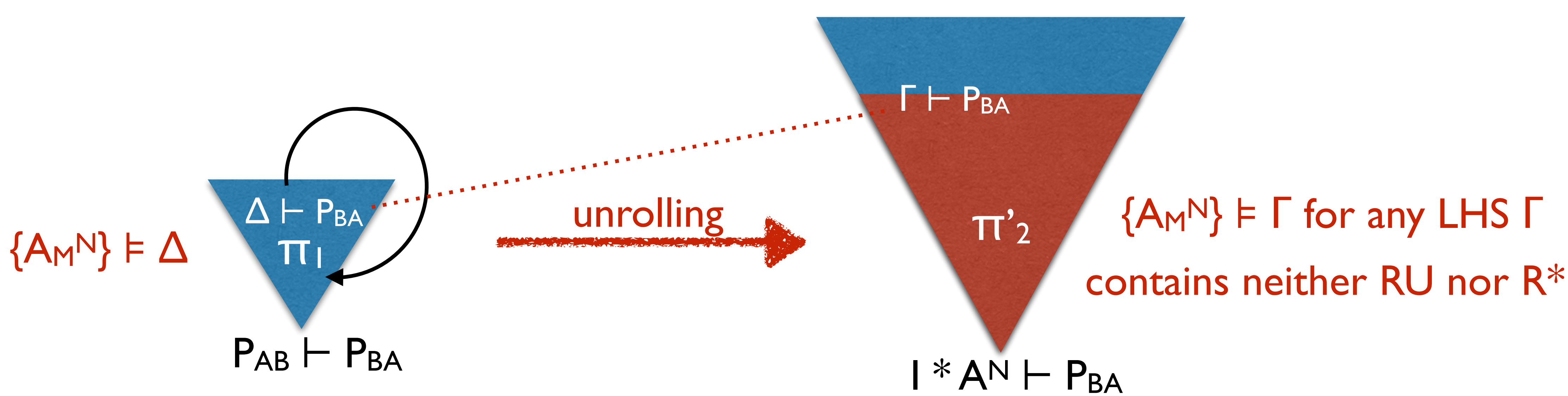
- For any sequent $\Gamma \vdash P_{BA}$ in $\pi'_2$, we have $\{A_M{}^N\} \models \Gamma$ in the multiset model
- Let $\Gamma \vdash P_{BA}$ be a top sequent in $\pi'_2$ and $\Delta \vdash P_{BA}$ be the corresponding sequent in $\pi_1$
  - Then, we have $\{A_M{}^N\} \models \Delta$ (since $\Gamma$ is obtained by unfolding predicates in $\Delta$)



# $P_{AB} \vdash P_{BA}$ is Not Cut-Free Provable

- Lemma: If $\Delta$ is a LHS in $\pi_I$ and $\{A_M{}^n\} \models \Delta$ for $n >$ (size of $\Delta$), then $\{A_M{}^n, B_M\} \models \Delta$
  - Hence, both $\{A_M{}^N\}$ and $\{A_M{}^N, B_M\}$ satisfy $\Delta$
- If $\Delta \vdash P_{BA}$ is a bottom sequent of RU, its assumption is either $\Delta \vdash P_A$ or $\Delta \vdash P_{BA} * B$, but both are invalid
- Since $P_{BA}$ contains no $*$, $\Delta \vdash P_{BA}$ is not a bottom sequent of R*
- It is easy to see that $\Delta \vdash P_{BA}$ is not an axiom

Contradiction!



# Conclusion

- Theorem:
  - Cut is not admissible in the cyclic proof system for BI even if we restrict inductive predicates to 0-ary ones
  - Proof by proof unrolling, easily adapted to SL and MLL
- How about the cyclic proof system for FOL?
  - Cut-elimination fails either
    - Proved by elaborated path chasing (Masuoka's talk!)
    - Can we use proof unrolling technique for FOL?