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

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

\[
\begin{align*}
\vdash & E(x) \lor O(x) \vdash N(x) \\
\vdash & E(x) \vdash N(x) \\
\vdash & O(x) \vdash N(x) \\
\vdash & N(0) \\
\vdash & O(y) \vdash N(Sy) \\
\vdash & E(z) \vdash N(z) \\
\vdash & E(z) \vdash N(Sz) \\
\vdash & O(y) \vdash N(y) \\
\vdash & E(y) \vdash N(y) \\
\vdash & O(z) \vdash N(Sz) \\
\vdash & E(y) \vdash N(Sy) \\
\vdash & O(z) \vdash N(Sz) \\
\vdash & E(z) \vdash N(0) \\
\vdash & O(z) \vdash N(0) \\
\vdash & E(x) \lor O(x) \vdash N(x)
\end{align*}
\]
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

\[
\vdash N(0) \quad O(y) \vdash N(y) \quad E(y) \vdash N(y) \\
O(z) \vdash N(z) \quad E(z) \vdash N(z) \quad O(z) \vdash N(Sy) \\
E(z) \vdash N(Sz) \quad E(y) \vdash N(Sy) \\
O(y) \vdash N(Sy) \\
E(x) \vdash N(x) \quad O(x) \vdash N(x) \\
E(x) \lor O(x) \vdash N(x)
\]
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 $y$"
- $A \ast B$ means "the heap can be divided to two disjoint subheaps satisfying $A$ and $B$, respectively"
- Example: $x \mapsto y \ast y \mapsto x$
- implies $x \neq y$
Symbolic Heaps in $SL_0$

$$A ::= x \mapsto (t_1 \ldots t_n) \mid A \ast A' \mid P(t_1 \ldots t_n) \quad (t ::= x \mid \text{nil})$$

- $P(x_1 \ldots x_m)$ 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
  - $ls(x, y) = (x \mapsto y) \mid \exists z (x \mapsto z \ast ls(z, y))$
  - $sl(x, y) = (x \mapsto y) \mid \exists z (sl(x, z) \ast z \mapsto y)$
\( \text{CSL}_0 \text{ID}_\omega \)

- Cyclic-proof system for \( \text{SL}_0 \)
- \( P(x) := \exists z D_1(x,z) \mid \ldots \mid \exists z D_n(x,z) \)

\[
\frac{A \vdash A}{\text{Id}} \quad \frac{A \vdash B \quad B \vdash C}{A \vdash C} \quad \frac{A_1 \vdash B_1 \quad A_2 \vdash B_2}{A_1 \ast A_2 \vdash B_1 \ast B_2}
\]

\[
\frac{A \vdash B \ast D_i(x,t)}{A \vdash B \ast P(x)} \quad \frac{D_1(x,z) \ast A \vdash B \ldots \quad D_n(x,z) \ast A \vdash B}{P(x) \ast A \vdash B} \quad \text{LU (} z \text{ is fresh)}
\]
Example: $ls * ls \vdash ls$
Theorem

• Theorem [Kimura+’19]:
  Cut-elimination does not hold in $\text{CSL}_0 \text{ID}_\omega$

• Proof

  • $\text{ls}(x,y) \vdash \text{sl}(x,y)$ 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 \( \text{ls}(x,y) \vdash \text{sl}(x,y) \)

\[
\begin{align*}
x \mapsto z_1 & \quad \ldots \quad z_{n-1} \mapsto z_n & \quad \text{ls}(z_n, y) \vdash \text{sl}(x, w) & \quad w \mapsto y \quad \text{RU} \\
x \mapsto z_1 & \quad \ldots \quad z_{n-1} \mapsto z_n & \quad \text{ls}(z_n, y) \vdash \text{sl}(x, y) \\
& \quad \vdots \\
& \quad \vdots \\
& \quad \text{x} \mapsto z_1 & \quad z_1 \mapsto z_2 & \quad \text{ls}(z_2, y) \vdash \text{sl}(x, y) \quad \text{LU} \\
& \quad \vdots \\
& \quad \text{x} \mapsto z_1 & \quad \text{ls}(z_1, y) \vdash \text{sl}(x, y) \quad \text{LU} \\
& \quad \text{ls}(x, y) \vdash \text{sl}(x, y) \quad \text{LU}
\end{align*}
\]

invalid!

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 sequents are extended by bunches

- e.g.) \((A, B); (A, C) \vdash A * (B \wedge C)\)

- 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: \( A ::= I \mid T \mid P \mid A \ast A \mid A \land A \)

- \( I \) 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 \( \Gamma \) means the formula \( \varphi(\Gamma) \):

  - \( \varphi(A) = A \)
  - \( \varphi(\Gamma, \Delta) = \varphi(\Gamma) \ast \varphi(\Delta) \)
  - \( \varphi(\Gamma ; \Delta) = \varphi(\Gamma) \land \varphi(\Delta) \)
Multiset Models

- A multiset model \( M = \{ P_M \mid P : \text{an atomic proposition} \} \)
- For a multiset \( m \) consisting of the elements in \( M \),
  \[
  m \models T \text{ always holds}
  \]
  \[
  m \models I \iff m = \{ \}
  \]
  \[
  m \models P \iff m = \{ P_M \} \quad (\text{for an atomic proposition } P)
  \]
  \[
  m \models A \land B \iff m \models A \text{ and } m \models B
  \]
  \[
  m \models A \star B \iff m = m_1 + m_2 \text{ (multiset sum)},
  \]
  \[
  \quad m_1 \models A \text{ and } m_2 \models B \text{ hold for some } m_1, m_2
  \]
  (the semantics of inductive preds are defined by lfp’s)
Multiset Models

- Example: For atomic propositions $A$, $B$, and inductive propositions

  $P_{AB} ::= P_B \mid P_{AB} * A \quad P_B ::= I \mid P_B * B$

- $\{A_M, A_M, B_M\} \models A * A * B$

- $\{A_M, B_M\} \not\models A * A * B$

- $\{B_M, B_M\} \models P_B$

- $\{A_M, A_M, A_M, B_M, B_M, B_M\} \models P_{AB}$
**CLBI\(_{\omega}^{I D}\) [Brotherston’07]**

- A cyclic proof system for BI
- Rules for \(\ast\) and \(\wedge\)

\[
\frac{\Gamma(A, B) \vdash C}{\Gamma(A \ast B) \vdash C} \quad \text{L}\ast \quad \frac{\Gamma(A ; B) \vdash C}{\Gamma(A \wedge B) \vdash C} \quad \text{L}\wedge
\]

\[
\frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \ast B} \quad \text{R}\ast \quad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma; \Delta \vdash A \wedge B} \quad \text{R}\wedge
\]

- Unfolding rules (same as CSLID\(_{\omega}\)), and
- **Structural rules** and cut

\[
\frac{\Gamma(\Delta) \vdash A}{\Gamma(\Delta ; \Delta') \vdash A} \quad \text{W} \quad \frac{\Gamma(\Delta ; \Delta) \vdash A}{\Gamma(\Delta) \vdash A} \quad \text{C} \quad \frac{\Gamma \vdash A \quad \Delta(A) \vdash B}{\Delta(\Gamma) \vdash B} \quad \text{Cut}
\]
Soundness of $\text{CLBI}^{\omega}_{\text{ID}}$

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

- In particular, for every sequent $\Gamma \vdash A$ in a cyclic proof, $m \vDash \varphi(\Gamma)$ implies $m \vDash A$ for any multiset $m$
Cut-Elimination Fails in $\text{CLBI}^{\omega}_{\text{ID}}$
Theorem

• Theorem:
Cut-elimination does not hold in CLBI^{(\omega,1)}
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

- \( P_{AB} ::= P_{B} \mid P_{AB} \ast A \)
- \( P_{A} ::= I \mid P_{A} \ast A \)
- \( P_{BA} ::= P_{A} \mid P_{BA} \ast B \)
- \( P_{B} ::= I \mid P_{B} \ast B \)

(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
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

$\Gamma \ast A \ast A \ast \ldots \ast A \vdash P_{BA}$

for any number of $A$'s
Proof Unrolling

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

For a sufficiently large number of $A$'s, any path in unrolled proof is contradictory
$P_{AB} \vdash P_{BA}$ is Not Cut-Free Provable

- Assume a cyclic proof $\pi_1$ of $P_{AB} \vdash P_{BA}$
- Let $N = (\text{the max size of LHS's of sequents in } \pi_1) + 1$
- 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 \( \{A_M^N\} \not\models \Gamma \) 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 \( \{A_M^N\} \not\models \Delta \) (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 $\Pi_1$ and $\{A_M^n\} \models \Delta$ for $n > (\text{size of } \Delta)$, then $\{A_M^n, B_M\} \not\models \Delta$

- 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 $\Delta \vdash P_{BA} \ast B$, but both are invalid

- Since $P_{BA}$ contains no $\ast$, $\Delta \vdash P_{BA}$ 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?