On Cut-elimination in Cyclic Proof Systems

Daisuke Kimura (Toho U.), Koji Nakazawa (Nagoya U.), Tachio Terauchi (Waseda U.), Hiroshi Unno (Tsukuba U.)
kmr@is.sci.toho-u.ac.jp knak@is.nagoya-u.ac.jp terauchi@waseda.jp uhiro@cs.tsukuba.ac.jp

Introduction

- Cyclic proof mechanism is a natural reasoning framework of inductive definitions. The framework plays important role in both logic and CS.
- However fundamental properties such as cut-elimination and completeness for cyclic proof systems are not well-known
- This work shows that cut-elimination fails in a cyclic proof system of very simple setting of separation logic

Simple Separation Logic SL_0

- Variables: $x, y, z, \dots$
- Inductive Predicates: $P_1(\vec{x_1}), \dots, P_n(\vec{x_n})$
- Formulas:

$$\begin{array}{rll} F, G ::= & x \mapsto y & \text{Points-to predicates} \\ | & P(\vec{x}) & \text{Ind. predicate} \\ | & F * G & \text{Separating conjunction} \end{array}$$

- Definition of Ind.Pred.: $P(\vec{x}) := F_{P,1}1(\vec{x}, \vec{z_1}) \mid \dots \mid F_{P,k}(\vec{x}, \vec{z_k})$
  $\vec{z_j}$ are implicitly existentially quantified
- Entailments: $F \vdash \Delta$ where $\Delta = G_1, \dots, G_n$ (multiset)

Examples

$ls(x, y) := x \mapsto y \mid x \mapsto z * ls(z, y)$ non-empty sll

$sl(x, y) := x \mapsto y \mid sl(x, z) * z \mapsto y$ non-empty sll-rev

Semantics

- Stores: s : Vars $\to \mathbb{N}$
- Heaps: $h : \mathbb{N} \setminus \{0\} \longrightarrow_{\mathrm{fin}} \mathbb{N}$
- Heap model: (s, h)

$s, h \models x \mapsto y \overset{\mathrm{def}}{\Longleftrightarrow} \mathrm{Dom}(h) = \{s(x)\}$ & $h(s(x)) = s(y)$

$s, h \models F_1 * F_2 \overset{\mathrm{def}}{\Longleftrightarrow} \exists h_1, h_2.(\ s, h_1 \models F_1$ & $s, h_2 \models F_2$ & $h = h_1 + h_2)$

$s, h \models P^{(0)}(\vec{y}) \overset{\mathrm{def}}{\Longleftrightarrow}$ Never

$s, h \models P^{(k+1)}(\vec{y}) \overset{\mathrm{def}}{\Longleftrightarrow} \exists \vec{a}, j.\ s[\vec{z} := \vec{a}], h \models F_{P,j}\,[\vec{P}^{(k)}/\vec{P}](\vec{y}, \vec{z})$

$s, h \models P(\vec{y}) \overset{\mathrm{def}}{\Longleftrightarrow} \exists k.\ s, h \models P^{(k)}(\vec{y})$

$s, h \models \Delta \overset{\mathrm{def}}{\Longleftrightarrow} \exists G \in \Delta. s, h \models G$

$F \vdash \Delta$ is valid (written $F \models \Delta$) $\overset{\mathrm{def}}{\Longleftrightarrow} \forall s, h.(s, h \models F$ implies $s, h \models \Delta)$

Derivation rules of $\mathrm{CSL}_0^M\mathrm{ID}\omega$

Inference Rules

$$\dfrac{}{F \vdash F}(\mathrm{Id}) \qquad \dfrac{F \vdash \Delta}{F \vdash \Delta, G}(\mathrm{Wk}) \qquad \dfrac{F \vdash \Delta, G, G}{F \vdash \Delta, G}(\mathrm{Ctr})$$

$$\dfrac{F_1 \vdash \Delta_1 \quad F_2 \vdash \Delta_2}{F_1 * F_2 \vdash \Delta_1 * \Delta_2}(*) \ \text{where } \Delta_1 * \Delta_2 = \{G_1 * G_2 \mid G_1 \in \Delta_1 \text{ and } G_2 \in \Delta_2\}$$

$$\dfrac{F \vdash \Delta_1, H \quad H \vdash \Delta_2}{F \vdash \Delta_1, \Delta_2}(\mathrm{Cut}) \qquad \dfrac{G \vdash \Delta, H * F_{P,j}(\vec{y}, \vec{w})}{G \vdash \Delta, H * P(\vec{y})}(\mathrm{UR})$$

$$\dfrac{G * F_{P,1}(\vec{y}, \vec{z_1}) \vdash \Delta \quad \dots \quad G * F_{P,m}(\vec{y}, \vec{z_m}) \vdash \Delta}{G * P(\vec{y}) \vdash \Delta}(\mathrm{UL}) \ \vec{z} \text{ are fresh}$$

Example: (UL) and (UR) rules for ls

$$\dfrac{F \vdash G * x \mapsto y}{F \vdash G * ls(x, y)}(\mathrm{UR}) \qquad \dfrac{F \vdash G * x \mapsto z * ls(z, y)}{F \vdash G * ls(x, y)}(\mathrm{UR})$$

$$\dfrac{F * x \mapsto y \vdash G \quad F * x \mapsto z * ls(z, y) \vdash G}{F * ls(x, y) \vdash G}(\mathrm{UL})$$

Cyclic proofs in $\mathrm{CSL}_0^M\mathrm{ID}\omega$

(Brotherston-style) cyclic proof

$$\dfrac{\dfrac{\dfrac{}{x \mapsto y * y \mapsto z \vdash x \mapsto y * y \mapsto z}}{x \mapsto y * y \mapsto z \vdash x \mapsto y * ls(y, z)}}{x \mapsto y * y \mapsto z \vdash ls(x, z)} \quad \dfrac{\dfrac{\dfrac{}{x \mapsto y \vdash x \mapsto y} \quad \overset{\textbf{Bud}}{y \mapsto w * \underline{ls(w, z)} \vdash ls(y, z)}}{x \mapsto y * y \mapsto w * \underline{ls(w, z)} \vdash x \mapsto y * ls(y, z)}}{x \mapsto y * y \mapsto w * \underline{ls(w, z)} \vdash ls(x, z)}$$
$$\overline{\textbf{Companion}\ x \mapsto y * \underline{ls(y, z)} \vdash ls(x, z)}\ (\mathrm{UL})$$

Preproof: derivation tree with bud-companion link

Proof graph: graph structure of preproof

Trace: a sequence of ind.preds. following a path of a proof graph (underlined ls)

Global trace condition: every inf.path contains a trace that passes inf.many (UL)

Cyclic proof: preproof which satisfies the global trace condition

Theorem (Soundness)

Every entailment in a cyclic proof is valid

Proposition

(1) $x \mapsto z * sl(z, y) \vdash sl(x, y)$ is provable

(2) $ls(x, y) \vdash sl(x, y)$ is provable in $\mathrm{CSL}_0^M\mathrm{ID}\omega$ using (Cut)

(1)

$$\dfrac{\dfrac{\dfrac{}{x \mapsto y \vdash x \mapsto y}}{x \mapsto y \vdash sl(x, y)}(\mathrm{UR}) \quad \dfrac{\dfrac{x \mapsto z * \underline{sl(z, w)} \vdash sl(x, w) \quad \dfrac{}{w \mapsto y \vdash w \mapsto y}}{x \mapsto z * \underline{sl(z, w)} * w \mapsto y \vdash sl(x, w) * w \mapsto y}}{x \mapsto z * \underline{sl(z, w)} * w \mapsto y \vdash sl(x, y)}(\mathrm{UR})}{x \mapsto z * \underline{sl(z, y)} \vdash sl(x, y)}(\mathrm{UL})$$

(2)

$$\dfrac{\dfrac{\dfrac{}{x \mapsto y \vdash x \mapsto y}}{x \mapsto y \vdash sl(x, y)} \quad \dfrac{\dfrac{\dfrac{}{x \mapsto z \vdash x \mapsto z} \quad \underline{ls(z, y)} \vdash sl(z, y)}{x \mapsto z * \underline{ls(z, y)} \vdash x \mapsto z * sl(z, y)} \quad \overset{(1)}{x \mapsto z * sl(z, y) \vdash sl(x, y)}}{x \mapsto z * \underline{ls(z, y)} \vdash sl(x, y)}(\mathrm{Cut})}{\underline{ls(x, y)} \vdash sl(x, y)}(\mathrm{UL})$$

Key idea

- **Connected Ls-form of** (x, y):
  $z_0 \mapsto z_1 * \dots * z_{m-1} \mapsto z_m * ls(z_m, y)$,
  where $x = z_0$ & $\vec{z}, y$ are distinguished
- **Partially conn.Ls-form of** (x, y):
  a formula obtained by removing some $z_i \mapsto z_{i+1}$ from a conn.Ls-form
- **Connected Sl-form of** (x, y):
  $sl(x, v_m) * v_m \mapsto v_{m-1} * \dots * v_1 \mapsto v_0$, where $v_0 = y$
- **Partially conn.Sl-form of** (x, y):
  a formula obtained by removing some $v_{i+1} \mapsto v_i$ from a conn.Sl-form
- Δ is **Sl-form**:
  For any $G \in \Delta$, G is a partially conn.Sl-form of (x, y) or $\mathop{\ast}_j z_j \mapsto w_j$
- $F \vdash \Delta$ is in **L-form** of (x, y)
  $\overset{\mathrm{def}}{\Longleftrightarrow}$ F is in partially conn.Ls-form of (x, y) and Δ is in Sl-form of (x, y)

Lemma1

Assume that $F \vdash \Delta$ is a valid L-form of (x, y). Then

(1) F is a connected Ls-form of (x, y)

(2) Δ contains $sl(x, y)$

Lemma2

Let entailment e be a L-form of (x, y).

Suppose that e appears in a cut-free cyclic proof as the conclusion of a rule r.

Then $r \neq (*)$ and r has a unique assump. which is a L-form of (x, y)

Main Theorem

$ls(x, y) \vdash sl(x, y)$ is not cut-free provable in $\mathrm{CSL}_0^M\mathrm{ID}\omega$.

Proof. Assume $\mathrm{e}_0 = ls(x, y) \vdash sl(x, y)$ has a cut-free cyclic proof.

- e_0 is a valid L-form of (x, y) by soundness.
- By Lemma2, a sequence $\mathrm{e}_0, \mathrm{e}_1, \dots, \mathrm{e}_\mathrm{N}$ of valid L-forms can be taken
- By Lemma1, e_N cannot be an axiom. Hence e_N is a bud
- Some e_k is the companion of e_N since every L-form appears in the sequence
- There is a (UL) between e_k and e_N
  since the inf.path $\mathrm{e}_\mathrm{k} \to^* \mathrm{e}_\mathrm{N} \to \mathrm{e}_\mathrm{k} \to^* \cdots$ contains a trace that passes inf.many (UL) by g.t.c.
- Define $\sharp(\mathrm{e}_\mathrm{i})$ by the number of $\mapsto$ in the antecedent of e_i
- $\sharp(\mathrm{e}_\mathrm{k}) \le \sharp(\mathrm{e}_\mathrm{m}) < \sharp(\mathrm{e}_{\mathrm{m}+1}) \le \sharp(\mathrm{e}_\mathrm{N}) = \sharp(\mathrm{e}_\mathrm{k})$
- Contradiction!

$$\begin{array}{c} \mathrm{e}_\mathrm{N} : F_N \vdash \Delta_N \\ \vdots \\ \dfrac{\mathrm{e}_{\mathrm{m}+1} : \mathop{\ast} z_i \mapsto z_{i+1} * z \mapsto z' * \underline{ls(z', y)} \vdash \Delta_m}{\mathrm{e}_\mathrm{m} : \mathop{\ast} z_i \mapsto z_{i+1} * \underline{ls(z, y)} \vdash \Delta_m}(\mathrm{UL}) \\ \vdots \\ \mathrm{e}_\mathrm{k} : F_k \vdash \Delta_k \\ \vdots \\ \dfrac{\cdot\ \cdot\ . \qquad \mathrm{e}_1 : F_1 \vdash \Delta_1}{\mathrm{e}_0 : ls(x, z) \vdash sl(x, y)} \end{array}$$

Corollary (Failure of Cut-Elimination in $\mathrm{CSL}_0^M\mathrm{ID}\omega$)

The cut-elimination property fails in $\mathrm{CSL}_0^M\mathrm{ID}\omega$

Future work

- Applying this proof technique to other cyclic proof systems
  - logic of bunched implications (Brotherston, 2007)
  - first-order logic (Brotherston, PhD thesis)
- Reconstructing positive results on cut-elimination
  - Reasonable restrictions on inductive predicates
  - Cut-elimination except cut rules against buds

This work is partially supported by JSPS KAKENHI Grant Number JP18K11161 and also by JSPS Core-to-Core Program (A. Advanced Research Networks).