마법봉 연산자를 포함한 분리 논리 정리 증명기 개발

POSTECH PL 이원열, 박성우

ROSAEC Workshop

2014.01.15

분리 논리

- 프로그램 □ □

- $\star$: separating conjunction
- $-\!\!\star$: separating implication, or magic wand

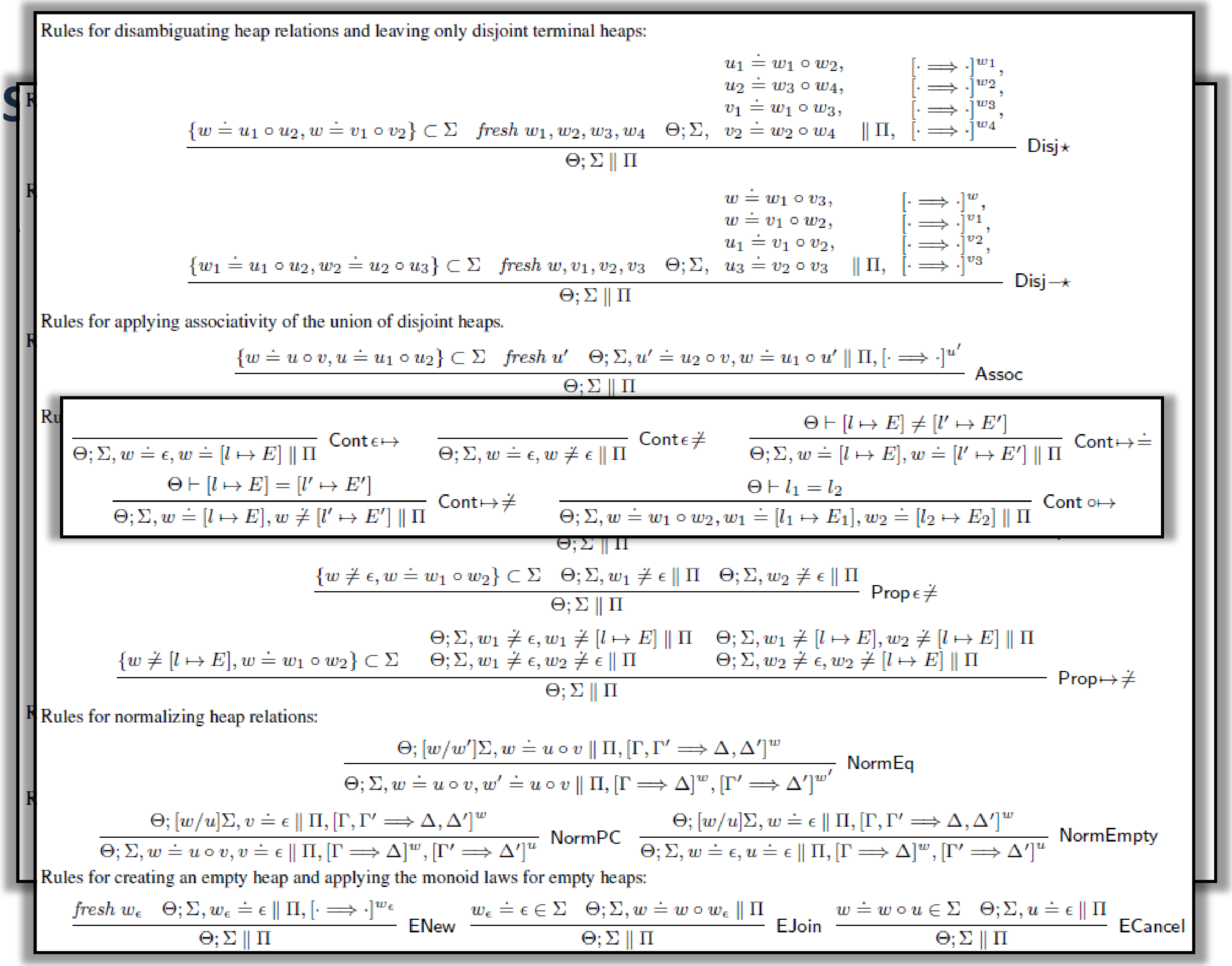
- □ □ □ □ □ □ □ □ □ …

분리 논리

- 프로그램 □ □

- ⋆ : separatir
- —⋆ : separatir nd

- □ □ □ □ □ □



Rules for disambiguating heap relations and leaving only disjoint terminal heaps:

$$\frac{\{w \doteq u_1 \circ u_2, w \doteq v_1 \circ v_2\} \subset \Sigma \quad \textit{fresh } w_1, w_2, w_3, w_4 \quad \Theta; \Sigma, \begin{array}{l} u_1 \doteq w_1 \circ w_2, \\ u_2 \doteq w_3 \circ w_4, \\ v_1 \doteq w_1 \circ w_3, \\ v_2 \doteq w_2 \circ w_4 \end{array} \parallel \Pi, \begin{array}{l} [\cdot \Longrightarrow \cdot]^{w_1}, \\ [\cdot \Longrightarrow \cdot]^{w_2}, \\ [\cdot \Longrightarrow \cdot]^{w_3}, \\ [\cdot \Longrightarrow \cdot]^{w_4} \end{array}}{\Theta; \Sigma \parallel \Pi} \ \mathsf{Disj}\star$$

$$\frac{\{w_1 \doteq u_1 \circ u_2, w_2 \doteq u_2 \circ u_3\} \subset \Sigma \quad \textit{fresh } w, v_1, v_2, v_3 \quad \Theta; \Sigma, \begin{array}{l} w \doteq w_1 \circ v_3, \\ w \doteq v_1 \circ w_2, \\ u_1 \doteq v_1 \circ v_2, \\ u_3 \doteq v_2 \circ v_3 \end{array} \parallel \Pi, \begin{array}{l} [\cdot \Longrightarrow \cdot]^{w}, \\ [\cdot \Longrightarrow \cdot]^{v_1}, \\ [\cdot \Longrightarrow \cdot]^{v_2}, \\ [\cdot \Longrightarrow \cdot]^{v_3} \end{array}}{\Theta; \Sigma \parallel \Pi} \ \mathsf{Disj}{-\!\star}$$

Rules for applying associativity of the union of disjoint heaps.

$$\frac{\{w \doteq u \circ v, u \doteq u_1 \circ u_2\} \subset \Sigma \quad \textit{fresh } u' \quad \Theta; \Sigma, u' \doteq u_2 \circ v, w \doteq u_1 \circ u' \parallel \Pi, [\cdot \Longrightarrow \cdot]^{u'}}{\Theta; \Sigma \parallel \Pi} \ \mathsf{Assoc}$$

Ru

$$\frac{}{\Theta; \Sigma, w \doteq \epsilon, w \doteq [l \mapsto E] \parallel \Pi} \ \mathsf{Cont}\,\epsilon\mapsto \qquad \frac{}{\Theta; \Sigma, w \doteq \epsilon, w \not\doteq \epsilon \parallel \Pi} \ \mathsf{Cont}\,\epsilon\not\doteq \qquad \frac{\Theta \vdash [l \mapsto E] \neq [l' \mapsto E']}{\Theta; \Sigma, w \doteq [l \mapsto E], w \doteq [l' \mapsto E'] \parallel \Pi} \ \mathsf{Cont}\mapsto\doteq$$

$$\frac{\Theta \vdash [l \mapsto E] = [l' \mapsto E']}{\Theta; \Sigma, w \doteq [l \mapsto E], w \not\doteq [l' \mapsto E'] \parallel \Pi} \ \mathsf{Cont}\mapsto\not\doteq \qquad \frac{\Theta \vdash l_1 = l_2}{\Theta; \Sigma, w \doteq w_1 \circ w_2, w_1 \doteq [l_1 \mapsto E_1], w_2 \doteq [l_2 \mapsto E_2] \parallel \Pi} \ \mathsf{Cont}\ \circ\!\mapsto$$

$\Theta; \Sigma \parallel \Pi$

$$\frac{\{w \not\doteq \epsilon, w \doteq w_1 \circ w_2\} \subset \Sigma \quad \Theta; \Sigma, w_1 \not\doteq \epsilon \parallel \Pi \quad \Theta; \Sigma, w_2 \not\doteq \epsilon \parallel \Pi}{\Theta; \Sigma \parallel \Pi} \ \mathsf{Prop}\,\epsilon\not\doteq$$

$$\frac{\{w \not\doteq [l \mapsto E], w \doteq w_1 \circ w_2\} \subset \Sigma \quad \begin{array}{l} \Theta; \Sigma, w_1 \not\doteq \epsilon, w_1 \not\doteq [l \mapsto E] \parallel \Pi \\ \Theta; \Sigma, w_1 \not\doteq \epsilon, w_2 \not\doteq \epsilon \parallel \Pi \end{array} \quad \begin{array}{l} \Theta; \Sigma, w_1 \not\doteq [l \mapsto E], w_2 \not\doteq [l \mapsto E] \parallel \Pi \\ \Theta; \Sigma, w_2 \not\doteq \epsilon, w_2 \not\doteq [l \mapsto E] \parallel \Pi \end{array}}{\Theta; \Sigma \parallel \Pi} \ \mathsf{Prop}\mapsto\not\doteq$$

Rules for normalizing heap relations:

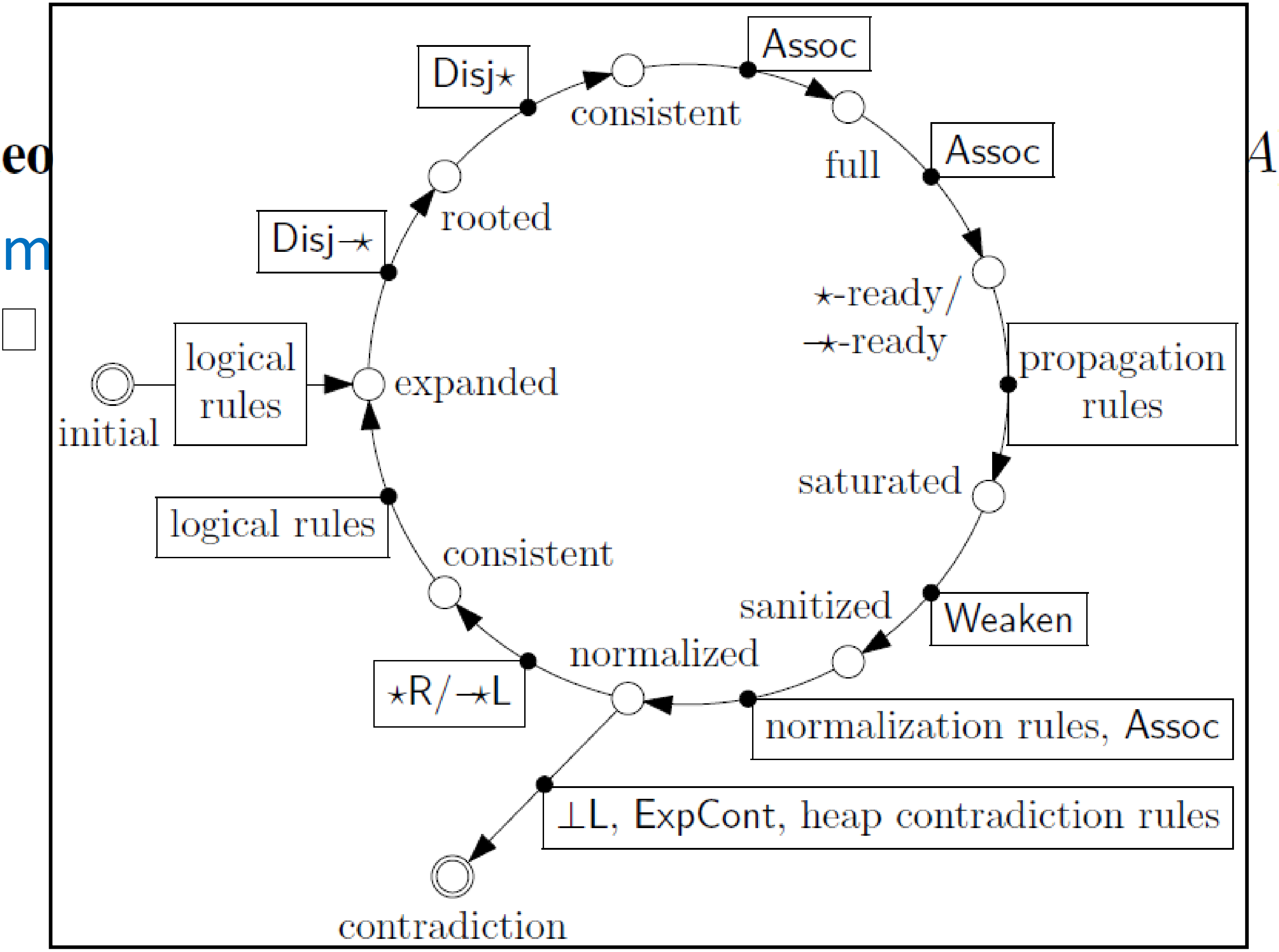
$$\frac{\Theta; [w/w']\Sigma, w \doteq u \circ v \parallel \Pi, [\Gamma, \Gamma' \Longrightarrow \Delta, \Delta']^{w}}{\Theta; \Sigma, w \doteq u \circ v, w' \doteq u \circ v \parallel \Pi, [\Gamma \Longrightarrow \Delta]^{w}, [\Gamma' \Longrightarrow \Delta']^{w'}} \ \mathsf{NormEq}$$

$$\frac{\Theta; [w/u]\Sigma, v \doteq \epsilon \parallel \Pi, [\Gamma, \Gamma' \Longrightarrow \Delta, \Delta']^{w}}{\Theta; \Sigma, w \doteq u \circ v, v \doteq \epsilon \parallel \Pi, [\Gamma \Longrightarrow \Delta]^{w}, [\Gamma' \Longrightarrow \Delta']^{u}} \ \mathsf{NormPC} \qquad \frac{\Theta; [w/u]\Sigma, w \doteq \epsilon \parallel \Pi, [\Gamma, \Gamma' \Longrightarrow \Delta, \Delta']^{w}}{\Theta; \Sigma, w \doteq \epsilon, u \doteq \epsilon \parallel \Pi, [\Gamma \Longrightarrow \Delta]^{w}, [\Gamma' \Longrightarrow \Delta']^{u}} \ \mathsf{NormEmpty}$$

Rules for creating an empty heap and applying the monoid laws for empty heaps:

$$\frac{\textit{fresh } w_\epsilon \quad \Theta; \Sigma, w_\epsilon \doteq \epsilon \parallel \Pi, [\cdot \Longrightarrow \cdot]^{w_\epsilon}}{\Theta; \Sigma \parallel \Pi} \ \mathsf{ENew} \qquad \frac{w_\epsilon \doteq \epsilon \in \Sigma \quad \Theta; \Sigma, w \doteq w \circ w_\epsilon \parallel \Pi}{\Theta; \Sigma \parallel \Pi} \ \mathsf{EJoin} \qquad \frac{w \doteq w \circ u \in \Sigma \quad \Theta; \Sigma, u \doteq \epsilon \parallel \Pi}{\Theta; \Sigma \parallel \Pi} \ \mathsf{ECancel}$$

P


Disj⋆
Assoc
consistent
Assoc
full
rooted
Disj—⋆
⋆-ready/
—⋆-ready
logical rules
expanded
propagation rules
initial
saturated
logical rules
consistent
sanitized
Weaken
normalized
⋆R/—⋆L
normalization rules, Assoc
⊥L, ExpCont, heap contradiction rules
contradiction

- **Theo** $A]^{w}$.
- Com

  □ □

현재 하고 있는 일

- 기본적인 □□ □□ □□ □□□□ □□ □...
  - Completeness□ □□□□ Proof Search□ □□□...
  - OCaml
- □□ □□
  - BBeye: A Theorem Prover for BBI
  - Coq Kernel
  - e.g. proof_tree, tactic, pftreestate, ...

현재 하고 있는 일

- 주의해야 □ □
  - Inference Rule□ □□ □□□□.
  - Inference Rule□ □□□□ □ □□□□ □□.

- □□ □□ □□…

해야 할 일

- 구현
  - Proof Search□ □ □ □ □ □ □ !
  - □ □ Data Structure□ □ □ □ □ □ □ !
  - Existential/Universal Quantifier □ □
- □ □ □ □
  - Inductive Predicate (e.g. list) □ □

감사합니다