Boolean BI를 위한 중첩 구조를 이용한 귀추 계산법

POSTECH 프로그래밍 언어 연구실 박종현

목표

일반적인 C 프로그램을 대상으로
사용하기 **편리**한 **연역 검증 도구** 개발

- 기존 방법 = Hoare 논리
- 일반적인 C 프로그램?
  - 동적 메모리 사용
  - 가명(alias) 문제 발생
- 새로운 대안 = 분리 논리

Hoare 논리 대 분리 논리

{ P } C { Q }
전조건 P가 만족된 상태에서,
프로그램 C가 **실행 후 종료**된다면,
후조건 Q가 만족된다.

- Hoare 논리?
  - 고전 논리

- 분리 논리?
  - 고전 논리
  - 선형 논리(E ↦ E, Emp / P * Q, P -* Q)

리스트 뒤집기

전: { List α_0 a }

```
b := nil
while a != nil do
  k := [a + 1];
  [a + 1] := b;
  b := a;
  a := k;
end while
```

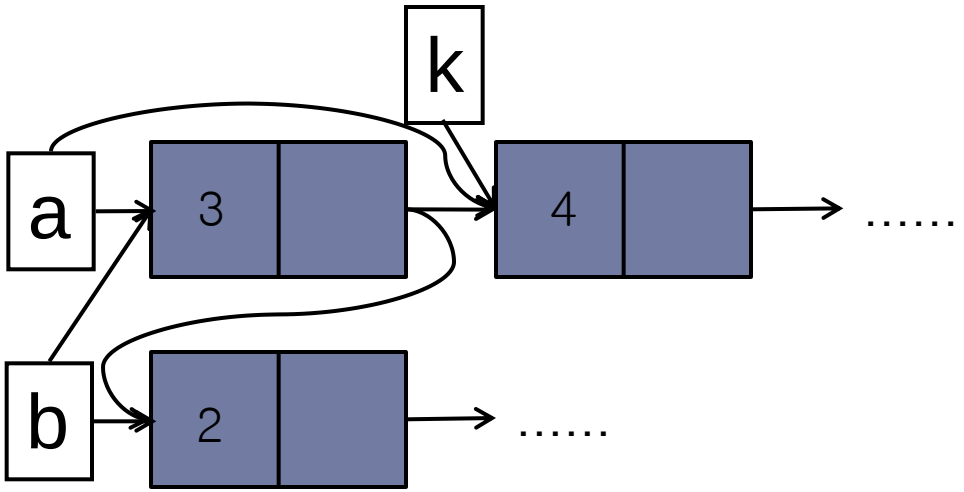
후: { List α_0^R b }

리스트 뒤집기

전: { List α_0 a }

```
b := nil
while a != nil do
  k := [a + 1];
  [a + 1] := b;
  b := a;
  a := k;
end while
```

후: { List α_0^R b }

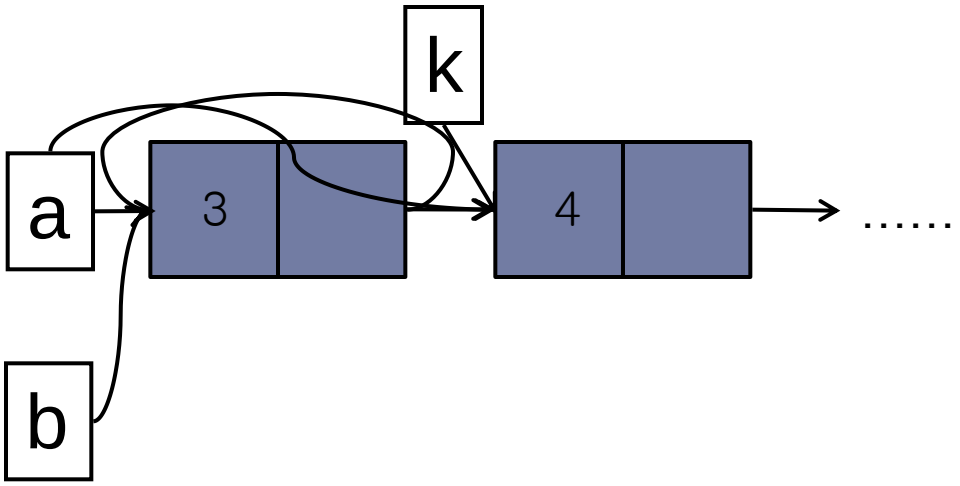


리스트 뒤집기: a = b?

전: { List α_0 a }

```
b := nil
while a != nil do
  k := [a + 1];
  [a + 1] := b;
  b := a;
  a := k;
end while
```

후: { List α_0^R b }



실제로는 발생하지 않음

리스트 뒤집기: a ≠ b! (Hoare 논리)

전: { List α_0 a }

```
b := nil
```

{ ∃α, β. List α a ∧ List β b ∧ $\alpha_0^R = \alpha^R \cdot \beta$) ∧
(∀k. Reach(a, k) ∧ Reach(b, k) ⇒ k = nil) }

```
while a != nil do
  k := [a + 1];
  [a + 1] := b;
  b := a;
  a := k;
end while
```

후: { List α_0^R b }

리스트 뒤집기: a ≠ b! (분리 논리)

전: { List α_0 a }

```
b := nil
```

{ ∃α, β. List α a * List β b ∧ α_0^R = α^R · β }

```
while a != nil do
  k := [a + 1];
  [a + 1] := b;
  b := a;
  a := k;
end while
```

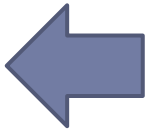
후: { List α_0^R b }

다른 리스트가 있을 때

전: { List α_0 a * List γ x }

```
b := nil
while a != nil do
  k := [a + 1];
  [a + 1] := b;
  b := a;
  a := k;
end while
```

후: { List α_0^R b * List γ x }



전: { List α_0 a }

```
b := nil
while a != nil do
  k := [a + 1];
  [a + 1] := b;
  b := a;
  a := k;
end while
```

후: { List α_0^R b }

분리 논리의 문제점?

- 고전 논리 + 선형 논리 ➔ 복잡한 상호 작용
- 기존 접근 방법
  - 자동 검증 도구 ➔ 분리 논리 일부분만 사용
  - 검증 보조 도구 ➔ 간단한 자동화 제공
- 우리의 접근 방법
  - 일반적인 분리 논리 사용 + 높은 수준의 자동화

Boolean BI

- 고전 논리 + 선형 논리

$$A \quad ::= \quad A \supset A \mid A \vee A \mid A \wedge A \mid \top \mid \bot \mid \neg A \mid A \mathrel{-\!\!\star} A \mid A \star A \mid \mathsf{I}$$

- 덧셈식 (고전 논리) $A \supset A,\ A \vee A,\ A \wedge A,\ \top,\ \bot,\ \neg A$
  - 귀류법 (proof by contradiction) 허용
- 곱셈식 (선형 논리) $A \mathrel{-\!\!\star} A,\ A \star A,\ \mathsf{I}$
  - 분리 논리에서와 같은 의미

핵심 문제: 컷-제거 귀추계산법

- 귀추 계산법 (sequent calculus)?
  - 자동 정리 증명 기법 연구를 위한 유용한 도구

$$\dfrac{\dfrac{}{A\ true}^{x}}{\dfrac{\begin{array}{c}\vdots\\ B\ true\end{array}}{A \supset B\ true}\supset I^{x}} \qquad \dfrac{A \supset B\ true \quad A\ true}{B\ true}\supset E$$

vs

$$\dfrac{\Gamma, A \supset B \longrightarrow A \quad \Gamma, A \supset B, B \longrightarrow C}{\Gamma, A \supset B \longrightarrow C}\supset L \qquad \dfrac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \supset B}\supset R$$

- 컷-제거 (cut-free) 성질 ≈ 보조 정리 규칙

$$\boxed{\text{If } \Gamma \longrightarrow A \text{ and } \Gamma, A \longrightarrow C, \text{ then } \Gamma \longrightarrow C.}$$

  - 귀추계산법의 건전성 증명에 필수

이전 연구 결과 (~2011.01)

첫 번째 시도

- 고전 논리 ➔ 참/거짓에 대한 논증
- 선형 논리 ➔ 부분 자원에 대한 논증

- 고전 논리 + 선형 논리?
  - 부분 자원에 대한 참/거짓 논증

- 새로운 형태의 귀추(world sequent) 이용

formula	A	$::=$	$P \mid \bot \mid A \wedge A \mid \neg A \mid \mathsf{I} \mid A \mathrel{-\!\!\star} A \mid A \star A$
boolean bunch	Δ	$::=$	$A \mid \emptyset_{\mathsf{a}} \mid \emptyset_{\mathsf{m}} \mid \Delta ; \Delta \mid W, W$
falsehood context	Ψ	$::=$	$\cdot \mid \Psi ; A$
world sequent	W	$=$	$\Delta \longrightarrow_{\mathsf{B}} \Psi$

첫 번째 컷-제거 귀추 계산법

$$\frac{A \text{ atomic}}{\omega[A \longrightarrow_{\mathsf{B}} A]}\ \mathit{Init}$$

$$\frac{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; \Delta' \longrightarrow_{\mathsf{B}} \Psi]}\ \mathsf{W} \qquad \frac{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi; A]}\ \mathsf{W}' \qquad \frac{\omega[\Delta; \Delta'; \Delta' \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; \Delta' \longrightarrow_{\mathsf{B}} \Psi]}\ \mathsf{C} \qquad \frac{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi; A; A]}{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi; A]}\ \mathsf{C}'$$

$$\frac{}{\omega[\bot \longrightarrow_{\mathsf{B}} \cdot]}\ \bot L \qquad \frac{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi; \bot]}\ \bot R \qquad \frac{\omega[\Delta \longrightarrow_{\mathsf{B}} A; \Psi]}{\omega[\Delta; \neg A \longrightarrow_{\mathsf{B}} \Psi]}\ \neg L \qquad \frac{\omega[\Delta; A \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta \longrightarrow_{\mathsf{B}} \neg A; \Psi]}\ \neg R$$

$$\frac{\omega[\Delta; A; B \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; A \wedge B \longrightarrow_{\mathsf{B}} \Psi]}\ \wedge L \qquad \frac{\omega[\Delta \longrightarrow_{\mathsf{B}} A; \Psi] \quad \omega[\Delta \longrightarrow_{\mathsf{B}} B; \Psi']}{\omega[\Delta \longrightarrow_{\mathsf{B}} A \wedge B; \Psi; \Psi']}\ \wedge R$$

$$\frac{\omega[\Delta; \emptyset_{\mathsf{m}} \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; \mathsf{I} \longrightarrow_{\mathsf{B}} \Psi]}\ \mathsf{I}L \qquad \frac{}{\omega[\emptyset_{\mathsf{m}} \longrightarrow_{\mathsf{B}} \mathsf{I}]}\ \mathsf{I}R$$

If $l_{\mathcal{D}} \sim l_{\mathcal{E}}$ *and* $l_{\mathcal{D}}[\Delta \longrightarrow_{\mathsf{B}} \Psi; C]$ *and* $l_{\mathcal{E}}[\Delta'; C \longrightarrow_{\mathsf{B}} \Psi']$, *then* $l_{\mathcal{D}} \cdot l_{\mathcal{E}}[\Delta; \Delta' \longrightarrow_{\mathsf{B}} \Psi; \Psi']$.

$$\frac{(\Delta \longrightarrow_{\mathsf{B}} \Psi), (A \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} B}{\omega[(\Delta \longrightarrow_{\mathsf{B}} A \multimap B; \Psi), (\Delta' \longrightarrow_{\mathsf{B}} \Psi'); \Delta'' \longrightarrow_{\mathsf{B}} \Psi'']}\ \multimap R$$

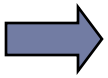
$$\frac{\omega[\Delta; (A \longrightarrow_{\mathsf{B}} \cdot), (B \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; A \star B \longrightarrow_{\mathsf{B}} \Psi]}\ \star L$$

$$\frac{\omega[\Delta''; (\Delta \longrightarrow_{\mathsf{B}} \Psi; A), (\Delta' \longrightarrow_{\mathsf{B}} \Psi') \longrightarrow_{\mathsf{B}} \Psi''] \quad \omega[\Delta''; (\Delta \longrightarrow_{\mathsf{B}} \Psi), (\Delta' \longrightarrow_{\mathsf{B}} \Psi'; B) \longrightarrow_{\mathsf{B}} \Psi'']}{\omega[\Delta''; (\Delta \longrightarrow_{\mathsf{B}} \Psi), (\Delta' \longrightarrow_{\mathsf{B}} \Psi') \longrightarrow_{\mathsf{B}} A \star B; \Psi'']}\ \star R$$

첫 번째 시도: 비결합적 Boolean BI 논리

- 비결합적(non-associative) 분리 연산자

$$A \star (B \star C) \supset (A \star B) \star C$$
$$(A \star B) \star C \supset A \star (B \star C)$$
$$A \star \mathsf{I} \supset A$$
$$A \supset A \star \mathsf{I}$$



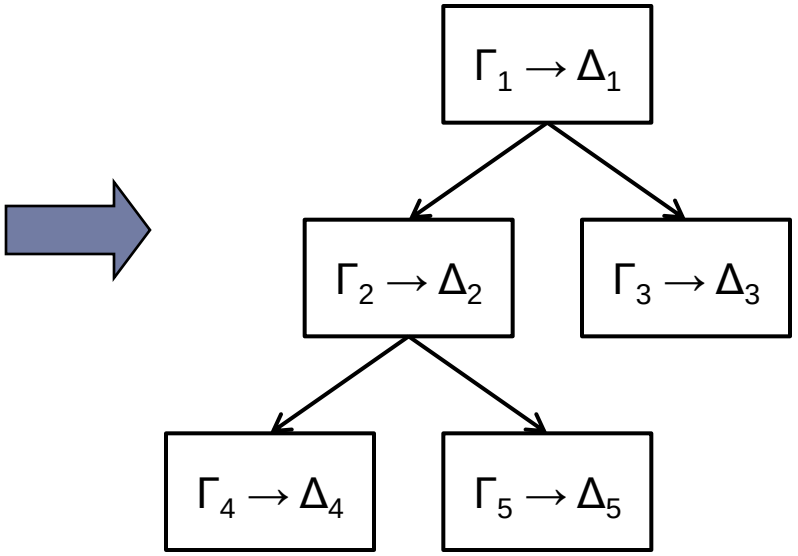
증명되지 않음

- 결론
  - Boolean BI와는 다른 논리
  - 분리 논리에 이용할 수 없음

비결합적 Boolean BI 논리 분석

- 나무 구조의 자원에 대해서만 적용 가능

$$
\begin{array}{lcl}
W & = & \Delta \longrightarrow_{\mathsf{B}} \Psi \\
\Delta & ::= & A \mid \emptyset_{\mathsf{a}} \mid \emptyset_{\mathsf{m}} \mid W, W \mid \Delta; \Delta \\
\Psi & ::= & \cdot \mid A \mid \Psi; \Psi
\end{array}
$$



Boolean BI의 자원 구조 ≠ 나무 구조

A ∨ B가 거짓이면?

A도 거짓이고 B도 거짓

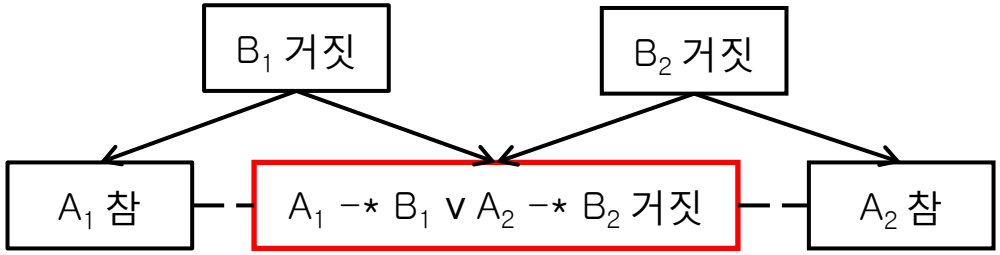
A −* B가 거짓이면?

A가 참인 어떤 이웃 자원과 결합할 경우 B가 거짓

$(A_1 -* B_1) \vee (A_2 -* B_2)$가 거짓이면?

A_1이 참인 **어떤 이웃 자원**과 결합할 경우 B_1이 거짓

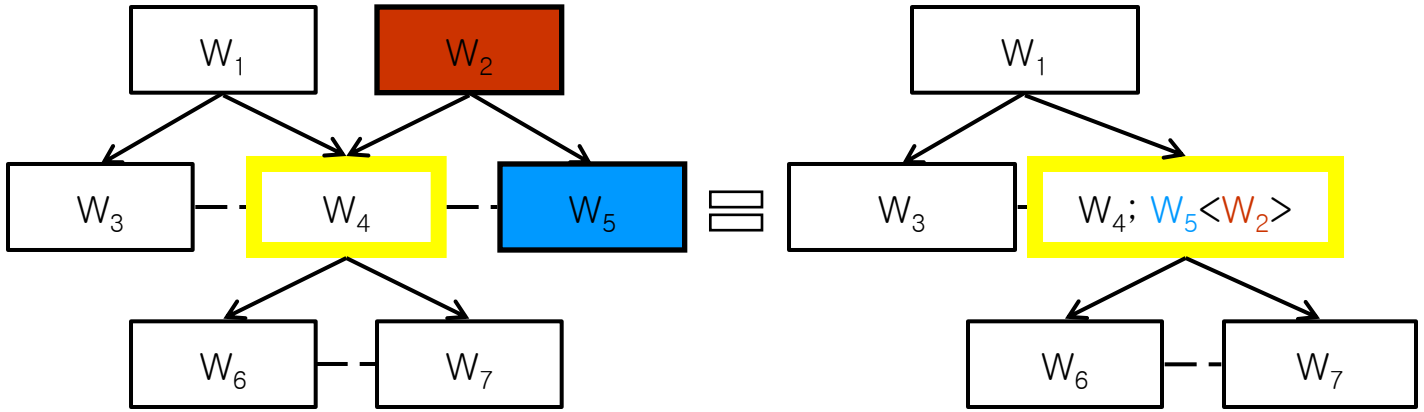
A_2가 참인 **어떤 이웃 자원**과 결합할 경우 B_2가 거짓



귀추 정의 확장

"이웃 자원"에 따른 "결합 자원" 가정 허용

$$
\begin{array}{lcl}
W & ::= & \Gamma \longrightarrow_{\mathsf{B}} \Delta \\
\Gamma & ::= & A \mid \emptyset_{\mathsf{a}} \mid \emptyset_{\mathsf{m}} \mid \Gamma;\Gamma \mid W, W \mid W\langle W\rangle \\
\Delta & ::= & \cdot \mid \Delta; A
\end{array}
$$



새로운 컷-제거 귀추 계산법

Structural rules:

$$\frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; S \Longrightarrow_{\mathcal{B}} \Delta}\ WL_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A}\ WR_{\mathcal{B}} \qquad \frac{\Gamma; S; S \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; S \Longrightarrow_{\mathcal{B}} \Delta}\ CL_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A; A}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A}\ CR_{\mathcal{B}}$$

$$\frac{\Gamma; S' \Longrightarrow_{\mathcal{B}} \Delta \quad S \equiv S'}{\Gamma; S \Longrightarrow_{\mathcal{B}} \Delta}\ E_{\mathcal{B}} \quad \text{where} \begin{cases} W, W' \equiv W', W & \text{(commutativity)} \\ (W_1, W_2 \Longrightarrow_{\mathcal{B}} \cdot), W_3 \equiv W_1, (W_2, W_3 \Longrightarrow_{\mathcal{B}} \cdot) & \text{(associativity)} \end{cases}$$

$$\frac{\Gamma_1; (\Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2), (\emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta_1}{\Gamma_1; \Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_1; \Delta_2}\ \emptyset_{\mathsf{m}} U_{\mathcal{B}} \qquad \frac{\Gamma_1; \Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_1; \Delta_2}{\Gamma_1; (\Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2), (\emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta_1}\ \emptyset_{\mathsf{m}} D_{\mathcal{B}}$$

Traverse rules:

$$\textit{If } \Gamma \Longrightarrow_{\mathcal{B}} \Delta; A \textit{ and } \Gamma'; A \Longrightarrow_{\mathcal{B}} \Delta', \textit{ then } \Gamma; \Gamma' \Longrightarrow_{\mathcal{B}} \Delta; \Delta'$$

$$\Gamma; (\Gamma_{\mathrm{c1}} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{c1}}), (\Gamma_{\mathrm{c2}} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{c2}}) \Longrightarrow_{\mathcal{B}} \Delta \qquad \Gamma; (\Gamma_{\mathrm{s}} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{s}}) \langle \Gamma_{\mathrm{p}} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{p}} \rangle \Longrightarrow_{\mathcal{B}} \Delta$$

Logical rules:

$$\frac{}{P \Longrightarrow_{\mathcal{B}} P}\ Init_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; \top \Longrightarrow_{\mathcal{B}} \Delta}\ \top L_{\mathcal{B}} \qquad \frac{}{\cdot \Longrightarrow_{\mathcal{B}} \top}\ \top R_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A}{\Gamma; \neg A \Longrightarrow_{\mathcal{B}} \Delta}\ \neg L_{\mathcal{B}} \qquad \frac{\Gamma; A \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; \neg A}\ \neg R_{\mathcal{B}}$$

$$\frac{\Gamma_1; A \Longrightarrow_{\mathcal{B}} \Delta_1 \quad \Gamma_2; B \Longrightarrow_{\mathcal{B}} \Delta_2}{\Gamma_1; \Gamma_2; A \vee B \Longrightarrow_{\mathcal{B}} \Delta_1; \Delta_2}\ \vee L_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A; B}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A \vee B}\ \vee R_{\mathcal{B}} \qquad \frac{\Gamma; \emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; \mathsf{I} \Longrightarrow_{\mathcal{B}} \Delta}\ \mathsf{I} L_{\mathcal{B}} \qquad \frac{}{\emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \mathsf{I}}\ \mathsf{I} R_{\mathcal{B}}$$

$$\frac{\Gamma; (A \Longrightarrow_{\mathcal{B}} \cdot), (B \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; A \star B \Longrightarrow_{\mathcal{B}} \Delta}\ \star L_{\mathcal{B}} \qquad \frac{\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1; A \quad \Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2; B}{(\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1), (\Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2) \Longrightarrow_{\mathcal{B}} A \star B}\ \star R_{\mathcal{B}}$$

$$\frac{\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1; A \quad \Gamma_2; B \Longrightarrow_{\mathcal{B}} \Delta_2}{(\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1) \langle \Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2 \rangle; A \mathrel{-\!\!\star} B \Longrightarrow_{\mathcal{B}} \cdot}\ \mathrel{-\!\!\star} L_{\mathcal{B}} \qquad \frac{\Gamma; (A \Longrightarrow_{\mathcal{B}} \cdot) \langle \cdot \Longrightarrow_{\mathcal{B}} B \rangle \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A \mathrel{-\!\!\star} B}\ \mathrel{-\!\!\star} R_{\mathcal{B}}$$

연구 결과 (~2011.06)

결과

- 컷-제거 성질 증명 (완료)
- Boolean BI와의 관계
  - 건전성 증명 (완료)
  - 완전성 증명 (완료)
- Boolean BI를 위한 컷-제거 귀추 계산법 완성

현재 상황

1단계	• Boolean BI 증명 이론 (완료)
2단계	• Boolean BI 증명 탐색 도구
3단계	• 분리 논리 증명 탐색 도구
4단계	• 분리 논리 기반 연역 검증 도구

진행 중: 증명 탐색

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Longrightarrow_{\mathcal{B}} A}\,Init_{\mathcal{B}}{}' \quad \dfrac{\dfrac{}{B \Longrightarrow_{\mathcal{B}} B}\,Init_{\mathcal{B}}{}'}{\cdot \Longrightarrow_{\mathcal{B}} B; \neg B}\,\neg R_{\mathcal{B}}}{(A \Longrightarrow_{\mathcal{B}} \cdot), (\cdot \Longrightarrow_{\mathcal{B}} B) \Longrightarrow_{\mathcal{B}} A \star \neg B}\,\star R_{\mathcal{B}}}{(A \Longrightarrow_{\mathcal{B}} \cdot), (\cdot \Longrightarrow_{\mathcal{B}} B) \Longrightarrow_{\mathcal{B}} A \star B; A \star \neg B}\,WR_{\mathcal{B}}}{S \Longrightarrow_{\mathcal{B}} B}\,\langle\rangle D_{\mathcal{B}} \quad \dfrac{}{A \Longrightarrow_{\mathcal{B}} A}\,Init_{\mathcal{B}}{}'}{(A \Longrightarrow_{\mathcal{B}} \cdot), (S \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} A \star B}\,\star R_{\mathcal{B}}}{(A \Longrightarrow_{\mathcal{B}} \cdot), (S \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} A \star B; A \star \neg B}\,WR_{\mathcal{B}}}{S; S \Longrightarrow_{\mathcal{B}} \cdot}\,\langle\rangle D_{\mathcal{B}}}{\emptyset_{\mathsf{m}}; S; S \Longrightarrow_{\mathcal{B}} \cdot}\,WL_{\mathcal{B}}}{\emptyset_{\mathsf{m}}; S \Longrightarrow_{\mathcal{B}} \cdot}\,CL_{\mathcal{B}}}{(A \Longrightarrow_{\mathcal{B}} \cdot), (\emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} A \star B; A \star \neg B}\,\langle\rangle U_{\mathcal{B}}}{A \Longrightarrow_{\mathcal{B}} A \star B; A \star \neg B}\,\emptyset_{\mathsf{m}} U_{\mathcal{B}}}{A \Longrightarrow_{\mathcal{B}} (A \star B) \vee (A \star \neg B)}\,\vee R_{\mathcal{B}}$$

where $S = (A \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} A \star B; A \star \neg B \rangle$