A Theorem Prover for Boolean BI

POSTECH 프로그래밍 언어 연구실
박종현 서정봉

목표

일반적인 C 프로그램을 위한 **연역 검증 도구** 개발

Hoare 논리

{ P } C { Q }

조건 P가 만족된 상태에서,

프로그램 C가 **실행** 후 **종료**된다면,

조건 Q가 만족된다.

분리 논리 = Hoare 논리의 확장

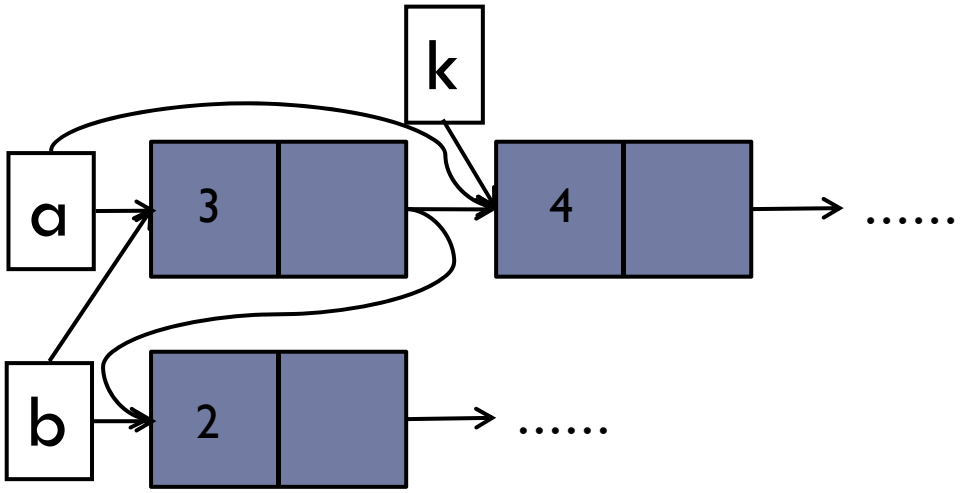
{ P } C { Q }

조건 P가 만족된 상태에서,
프로그램 C가 **실행** 후 **종료**된다면,
조건 Q가 만족된다.

동적 메모리와 관련된 성질을
분리 논리곱(*)과 **분리 함의(-*)** 연산자를 이용해서
직관적으로 기술 가능

리스트 뒤집기

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



리스트 뒤집기: 검증

{ List α_0 a }

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

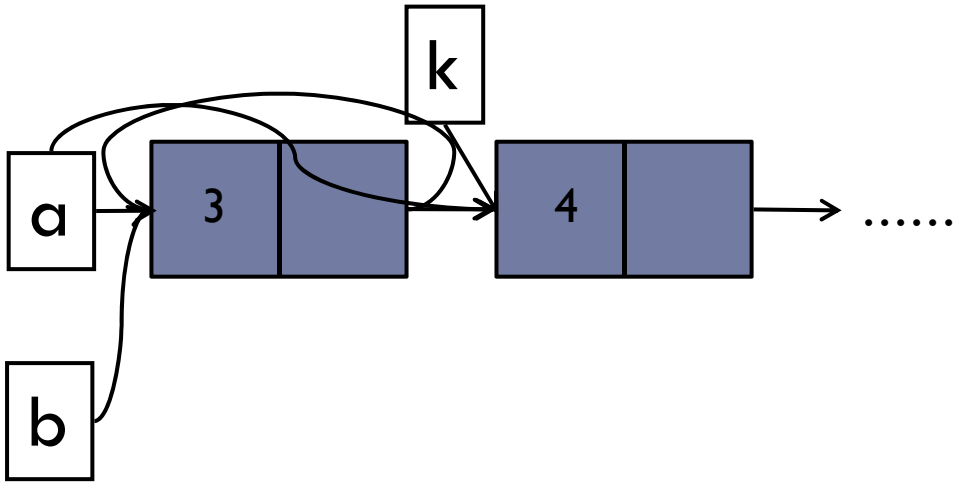
{ List α_0^R b }

리스트 뒤집기: a = b?

{ List α_0 a }

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

{ List α_0^R b }



실제로는 발생하지 않음

반복문 불변식 @ Hoare 논리

{ List α_0 a }

```
b := nil
```

{ $\exists \alpha, \beta$. List α a $\wedge$ List β b $\wedge$ $\alpha_0^R = \alpha^R \cdot \beta \wedge$
($\forall$ k. reachable(a, k) $\wedge$ reachable(b, k) $\Rightarrow$ k = nil) }

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

{ List α_0^R b }

반복문 불변식 @ 분리 논리

{ List α_0 a }

```
b := nil
```

{ $\exists \alpha, \beta.$ List α a * List β b $\wedge$ $\alpha_0^R = \alpha^R \cdot \beta$ }

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

{ List α_0^R b }

분리 논리에 기반한 검증 도구들

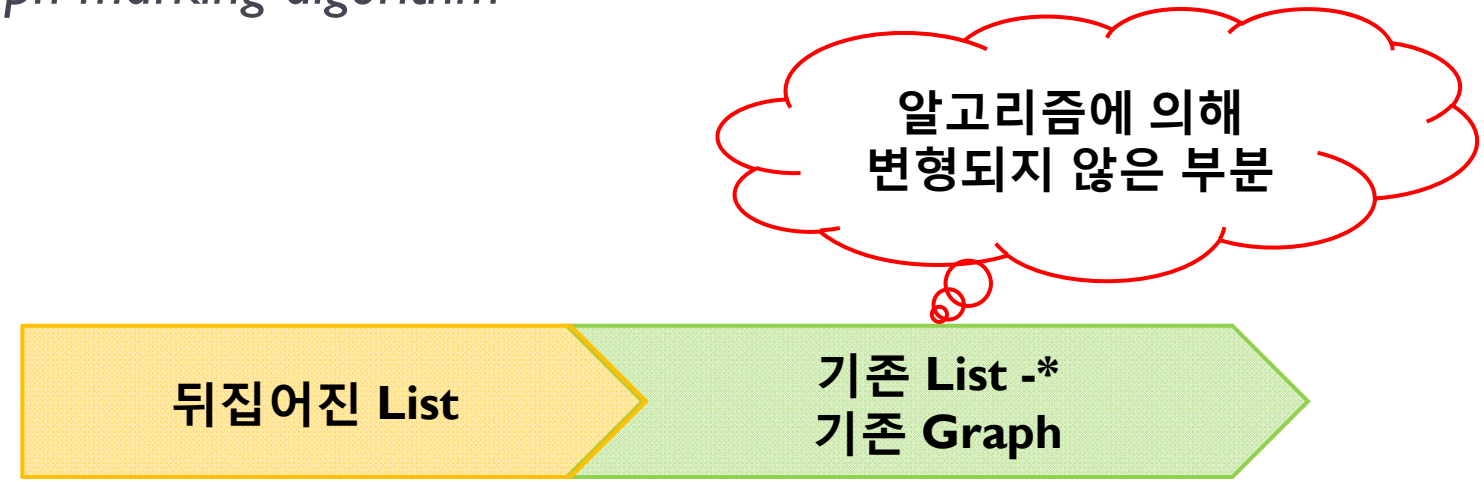
- Smallfoot (2005)
- ……
- Ynot (2008)
- ……

분리 논리곱(*) 연산자는 사용하지만,

분리 함의(-*) 연산자는 사용하지 않음

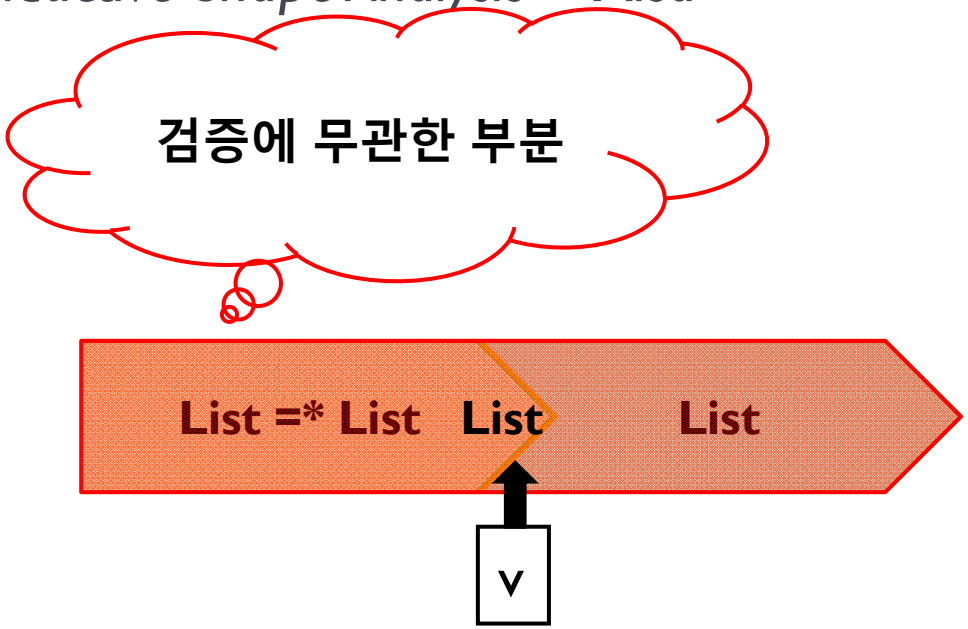
A -* B의 유용성: 직관적인 반복문 불변식

"An Example of Local Reasoning in BI pointer logic: the Schorr-Waite graph marking algorithm"



A -* B의 유용성: 메모리 상태 표현

"Relational Inductive Shape Analysis" - Xisa



왜냐하면…

- -*를 지원하는 자동 증명기가 존재하지 않음

This incompleteness could be dealt with if we instead used the backwards-running weakest pre-conditions of Separation Logic

A -* B도 지원하는 분리 논리 자동 증명기를 만들자!

*"Symbolic Execution with Separation Logic"*에서 인용

분리 논리 = Boolean BI의 특수한 경우

- Boolean BI?
  - 추상화된 "**자원**"에 대한 성질

A -* B도 지원하는 분리 논리 자동 증명기를 만들자!

Boolean BI 자동 증명기를 만들자!

기존 연구 결과 (~2011.06)

핵심 목표: 컷-제거 귀추계산법

- 귀추 계산법 (sequent calculus)?
  - 자동 증명기 설계를 위한 이론적 도구

$$\frac{\Gamma, A \supset B \longrightarrow A \quad \Gamma, A \supset B, B \longrightarrow C}{\Gamma, A \supset B \longrightarrow C} \supset L$$

$$\frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \supset B} \supset R$$

- 컷-제거 (cut-free) 성질 ≈ 보조 정리 규칙

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

새로운 귀추 계산법 S_{BBI}

Structural rules:

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

$$\frac{\Gamma; W', W \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; W, W' \Longrightarrow_{\mathcal{B}} \Delta}\ EC_{\mathcal{B}} \quad \frac{\Gamma; W_1, (W_2, W_3 \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; (W_1, W_2 \Longrightarrow_{\mathcal{B}} \cdot), W_3 \Longrightarrow_{\mathcal{B}} \Delta}\ EA_{\mathcal{B}}$$

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

Traverse rules:

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

Logical rules:

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

$$\frac{\Gamma; A \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; \neg A}\ \neg R_{\mathcal{B}} \quad \frac{\Gamma; A; B \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; A \wedge B \Longrightarrow_{\mathcal{B}} \Delta}\ \wedge L_{\mathcal{B}} \quad \frac{\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1; A \quad \Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2; B}{\Gamma_1; \Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_1; \Delta_2; A \wedge B}\ \wedge R_{\mathcal{B}}$$

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

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

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

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

S_{BBI}의 주요 성질

- 컷-제거(cut-free) 성질
  - $\Gamma \Rightarrow_{\mathcal{B}} \Delta; A$가 증명 가능하고,
  - $\Gamma; A \Rightarrow_{\mathcal{B}} \Delta$도 증명 가능하다면,
  - $\Gamma \Rightarrow_{\mathcal{B}} \Delta$도 또한 증명 가능하다.

- 안전성(soundness)
  - $\cdot \Rightarrow_{\mathcal{B}} A$가 증명 가능하면,
  - A는 Boolean BI에서 유효한 명제이다.

- 완전성(completeness)
  - A가 Boolean BI에서 유효한 명제라면,
  - $\cdot \Rightarrow_{\mathcal{B}} A$이 항상 증명 가능하다.

다음 목표: 증명 탐색

$$A \Longrightarrow_{\mathcal{B}} (A \star B) \vee (A \star \neg B)$$

연구 성과 (~2012.01)

목표 기반 단순 탐색 전략

- 귀추 $\Gamma \Longrightarrow_{\mathcal{B}} \Delta$ 주어졌을 때

1. 적용 가능한 [illegible]
2. 공리인가?
   $$\frac{}{P \Longrightarrow_{\mathcal{B}} P}\ Init_{\mathcal{B}}$$
   - 증명 완료
3. 다음 귀추를 계산한다.
4. [illegible]을 찾아본다.
5. $$\frac{\Gamma; A \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; \neg A}\ \neg R_{\mathcal{B}}$$
   - [illegible]
6. 1번부터 다시 수행 한다.

문제점은?

1. 적용 가능한 규칙이 너무 많습니다!

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

2. 규칙을 적용하는 방법도 너무 많습니다!

$$\frac{\Gamma_1; A \Longrightarrow_{\mathcal{B}} \Delta_1 \quad \Gamma_2; B \Longrightarrow_{\mathcal{B}} \Delta_2}{\underbrace{\Gamma_1; \Gamma_2}_{n}; A \vee B \Longrightarrow_{\mathcal{B}} \Delta_1; \Delta_2}\ \vee L_{\mathcal{B}}$$

또 다른 귀추 계산법 CS_{BBI}

Structural rules:

$$\frac{\Gamma;(\Gamma';W_1,W_2 \Longrightarrow_{\mathcal{B}} \Delta'),W_3;W_1',(W_2',W_3' \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma;(\Gamma';W_1,W_2 \Longrightarrow_{\mathcal{B}} \Delta'),W_3 \Longrightarrow_{\mathcal{B}} \Delta}\ EA_{\mathcal{C}}$$

$$\text{where } \begin{cases} W_1' = W_1 \oplus W_2\langle\Gamma';W_3\langle\Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle \Longrightarrow_{\mathcal{B}} \Delta'\rangle \\ W_2' = W_2 \oplus W_1\langle\Gamma';W_3\langle\Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle \Longrightarrow_{\mathcal{B}} \Delta'\rangle \\ W_3' = W_3 \oplus (\Gamma';W_1,W_2 \Longrightarrow_{\mathcal{B}} \Delta')\langle\Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle \end{cases}$$

$$\frac{\Gamma;W_2,W_1 \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma;W_1,W_2 \Longrightarrow_{\mathcal{B}} \Delta}\ EC_{\mathcal{C}} \qquad \frac{\Gamma;(\Gamma \Longrightarrow_{\mathcal{B}} \Delta),(\emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta}\ \emptyset_{\mathsf{m}}U_{\mathcal{C}}$$

$$\frac{\Gamma;(\Gamma_{c1} \Longrightarrow_{\mathcal{B}} \Delta_{c1}),(\Gamma_{c2};\emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \Delta_{c2});\Gamma_{c1};S \Longrightarrow_{\mathcal{B}} \Delta;\Delta_{c1}}{\Gamma;(\Gamma_{c1} \Longrightarrow_{\mathcal{B}} \Delta_{c1}),(\Gamma_{c2};\emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \Delta_{c2}) \Longrightarrow_{\mathcal{B}} \Delta}\ \emptyset_{\mathsf{m}}D_{\mathcal{C}}$$

$$\text{where } S = (\Gamma_{c2};\emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \Delta_{c2})\langle\Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle$$

Traverse rules:

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

Logical rules:

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

$$\frac{\Gamma;A;B \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma;A \wedge B \Longrightarrow_{\mathcal{B}} \Delta}\ \wedge L_{\mathcal{C}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta;A \quad \Gamma \Longrightarrow_{\mathcal{B}} \Delta;B}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta;A \wedge B}\ \wedge R_{\mathcal{C}} \qquad \frac{\Gamma;A \Longrightarrow_{\mathcal{B}} \Delta \quad \Gamma;B \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma;A \vee B \Longrightarrow_{\mathcal{B}} \Delta}\ \vee L_{\mathcal{C}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta;A;B}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta;A \vee B}\ \vee R_{\mathcal{C}}$$

$$\frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta;A \quad \Gamma;B \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma;A \to B \Longrightarrow_{\mathcal{B}} \Delta}$$

$$\frac{\Gamma;(A \Longrightarrow_{\mathcal{B}} \cdot),(B \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma;A \star B \Longrightarrow_{\mathcal{B}} \Delta}$$

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

$$\frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta;A \quad \Gamma \Longrightarrow_{\mathcal{B}} \Delta;B}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta;A \wedge B}\ \wedge R_{\mathcal{C}}$$

CS_{BBI}의 주요 성질

S_{BBI}에 대해서 안전하고 완전함

- 안전성(soundness)
  - $\Gamma \Rightarrow_{\mathcal{B}} \Delta$가 CS_{BBI}에서 증명 가능하면,
  - $\Gamma \Rightarrow_{\mathcal{B}} \Delta$는 S_{BBI}에서도 증명 가능하다.
- 완전성(completeness)
  - $\Gamma \Rightarrow_{\mathcal{B}} \Delta$가 S_{BBI}에서 증명 가능하면,
  - $\Gamma \Rightarrow_{\mathcal{B}} \Delta$는 CS_{BBI}에서도 증명 가능하다.

CS_{BBI} 첫 번째 성질: 도치 가능한 (invertible) 규칙들

- 도치 가능한 규칙이란?
  - 결론이 증명 가능하다면,
  - 전제도 항상 증명 가능하다.

$$\frac{\Gamma; A; B \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; A \wedge B \Longrightarrow_{\mathcal{B}} \Delta} \wedge L_{\mathcal{C}}$$

- 다시 말해서,
  - 어떤 규칙이 도치 가능하다면,
  - 해당 규칙이 적용 가능할 때,
  - 항상 적용 하면 된다!

- 모든 CS_{BBI} 규칙이 도치 가능

CS_{BBI} 두 번째 성질: 축약 없는(contraction-free) 증명 가능성

- 중복된 정보가 있는 상태에서 증명이 가능하면,
  중복된 정보가 제거된 상태에서도,
  항상 증명이 가능하다.
  - $\Gamma; S; S \Rightarrow_{\mathcal{B}} \Delta$ 증명 가능 ➔ $\Gamma; S \Rightarrow_{\mathcal{B}} \Delta$ 증명 가능
  - $\Gamma \Rightarrow_{\mathcal{B}} \Delta; A; A$ 증명 가능 ➔ $\Gamma \Rightarrow_{\mathcal{B}} \Delta; A$ 증명 가능

$$\frac{\Gamma; (\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1; A; A), (\Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2) \Longrightarrow_{\mathcal{B}} \Delta; A \star B \quad subgoal}{\Gamma; (\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1; A), (\Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2) \Longrightarrow_{\mathcal{B}} \Delta; A \star B} \star R_C$$

목표 기반 단순 탐색 전략

- 귀추 $\Gamma \Rightarrow_{\mathcal{B}} \Delta$ 주어졌을 때

1. 적용 가능한 규칙을 찾는다.
2. 공리인가?
   - 증명 완료
3. 다음 귀추를 계산한다.
4. 계산한 귀추에 대한 증명을 찾아본다.
5. 찾았는가?
   - 증명 완료
6. 1번부터 다시 수행 한다.

결과는?

- 다양한 예제들에 대해서 증명 탐색 성공!
  - $A \rightarrow (A \star B) \vee (A \star \neg B)$
  - $I \wedge A \rightarrow A \star A$
  - $\neg\left(\left(\left(A \star \left(C \mathrel{-\!\!\star} \left(\neg(\neg(A \mathrel{-\!\!\star} B) \star C)\right)\right)\right) \wedge \neg B\right) \star C\right)$
  - ……

손으로 증명할 경우

$$\overline{B \Longrightarrow_{\mathcal{B}} B}\ \mathit{Init}_{\mathcal{B}}$$

$$\overline{A \Longrightarrow_{\mathcal{B}} A}\ \mathit{Init}_{\mathcal{B}} \qquad B; (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} B\ \ \mathit{WL}_{\mathcal{B}}$$

$$S_1; A \mathrel{-\!\!\star} B \Longrightarrow_{\mathcal{B}} \cdot\ \ {\mathrel{-\!\!\star}}L_{\mathcal{B}}$$

$$S_1 \Longrightarrow_{\mathcal{B}} \neg(A \mathrel{-\!\!\star} B)\ \ \neg R_{\mathcal{B}}$$

$$S_1; A' \Longrightarrow_{\mathcal{B}} \neg(A \mathrel{-\!\!\star} B)\ \ \mathit{WL}_{\mathcal{B}} \qquad \overline{C \Longrightarrow_{\mathcal{B}} C}\ \mathit{Init}_{\mathcal{B}}$$

$$S_2 \Longrightarrow_{\mathcal{B}} \neg(A \mathrel{-\!\!\star} B) \star C\ \ {\star}R_{\mathcal{B}}$$

$$S_2; (A \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} \neg(A \mathrel{-\!\!\star} B) \star C\ \ \mathit{WL}_{\mathcal{B}}$$

$$\overline{C \Longrightarrow_{\mathcal{B}} C}\ \mathit{Init}_{\mathcal{B}} \qquad S_2; (A \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle; \neg(\neg(A \mathrel{-\!\!\star} B) \star C) \Longrightarrow_{\mathcal{B}} \cdot\ \ \neg L_{\mathcal{B}}$$

$$(C \Longrightarrow_{\mathcal{B}} \cdot)\langle S_2; (A \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} \cdot\rangle; A' \Longrightarrow_{\mathcal{B}} \cdot\ \ {\mathrel{-\!\!\star}}L_{\mathcal{B}}$$

$$(C \Longrightarrow_{\mathcal{B}} \cdot)\langle S_2; (A \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} \cdot\rangle; A'; S_1 \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{WL}_{\mathcal{B}}$$

$$S_2; S_2; (A \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{TC}_{\mathcal{B}}$$

$$S_2; (A \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{CL}_{\mathcal{B}}$$

$$(S_2 \Longrightarrow_{\mathcal{B}} \cdot), (A \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{TC}_{\mathcal{B}}$$

$$(A \Longrightarrow_{\mathcal{B}} \cdot), (S_2 \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{EC}_{\mathcal{B}}$$

$$((A \Longrightarrow_{\mathcal{B}} \cdot), (A'; S_1 \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \cdot), (C \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{EA}_{\mathcal{B}}$$

$$(A \Longrightarrow_{\mathcal{B}} \cdot), (A'; S_1 \Longrightarrow_{\mathcal{B}} \cdot); (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{TP}_{\mathcal{B}}$$

$$(A'; S_1 \Longrightarrow_{\mathcal{B}} \cdot), (A \Longrightarrow_{\mathcal{B}} \cdot); (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{EC}_{\mathcal{B}}$$

$$(A'; S_1 \Longrightarrow_{\mathcal{B}} \cdot), (A \Longrightarrow_{\mathcal{B}} \cdot); (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} B\ \ \mathit{WL}_{\mathcal{B}}$$

$$A'; S_1; S_1 \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{TP}_{\mathcal{B}}$$

$$A'; S_1 \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{CL}_{\mathcal{B}}$$

$$(A' \Longrightarrow_{\mathcal{B}} \cdot), (A \Longrightarrow_{\mathcal{B}} \cdot); (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} B\ \ \mathit{TC}_{\mathcal{B}}$$

$$(A \Longrightarrow_{\mathcal{B}} \cdot), (A' \Longrightarrow_{\mathcal{B}} \cdot); (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} B\ \ \mathit{EC}_{\mathcal{B}}$$

$$A \star A'; (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} B\ \ {\star}L_{\mathcal{B}}$$

$$A \star A'; \neg B; (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} \cdot\ \ \neg L_{\mathcal{B}}$$

$$(A \star A') \wedge \neg B; (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} \cdot\ \ {\wedge}L_{\mathcal{B}}$$

$$((A \star A') \wedge \neg B \Longrightarrow_{\mathcal{B}} \cdot), (C \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \cdot\ \ \mathit{TC}_{\mathcal{B}}$$

$$((A \star A') \wedge \neg B) \star C \Longrightarrow_{\mathcal{B}} \cdot\ \ {\star}L_{\mathcal{B}}$$

$$\cdot \Longrightarrow_{\mathcal{B}} \neg(((A \star A') \wedge \neg B) \star C)\ \ \neg R_{\mathcal{B}}$$

$$\text{where} \begin{cases} S_1 = (A \Longrightarrow_{\mathcal{B}} \cdot)\langle (C \Longrightarrow_{\mathcal{B}} \cdot)\langle \cdot \Longrightarrow_{\mathcal{B}} \cdot\rangle \Longrightarrow_{\mathcal{B}} B\rangle \\ S_2 = (A'; S_1 \Longrightarrow_{\mathcal{B}} \cdot), (C \Longrightarrow_{\mathcal{B}} \cdot) \end{cases}$$

하지만……

- $A \star B \star C \star D \rightarrow D \star C \star B \star A$
  - 26722.36초(≈ 7시간) 소모
  - 약 10만 번의 규칙 적용

첫 번째 문제점

항상 다시 적용 가능

같은 구조의 중복

$$\frac{\Gamma; (\Gamma'; W_1, W_2 \Longrightarrow_{\mathcal{B}} \Delta'), W_3; W_1', (W_2', W_3' \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; (\Gamma'; W_1, W_2 \Longrightarrow_{\mathcal{B}} \Delta'), W_3 \Longrightarrow_{\mathcal{B}} \Delta} \; EA_{\mathcal{C}}$$

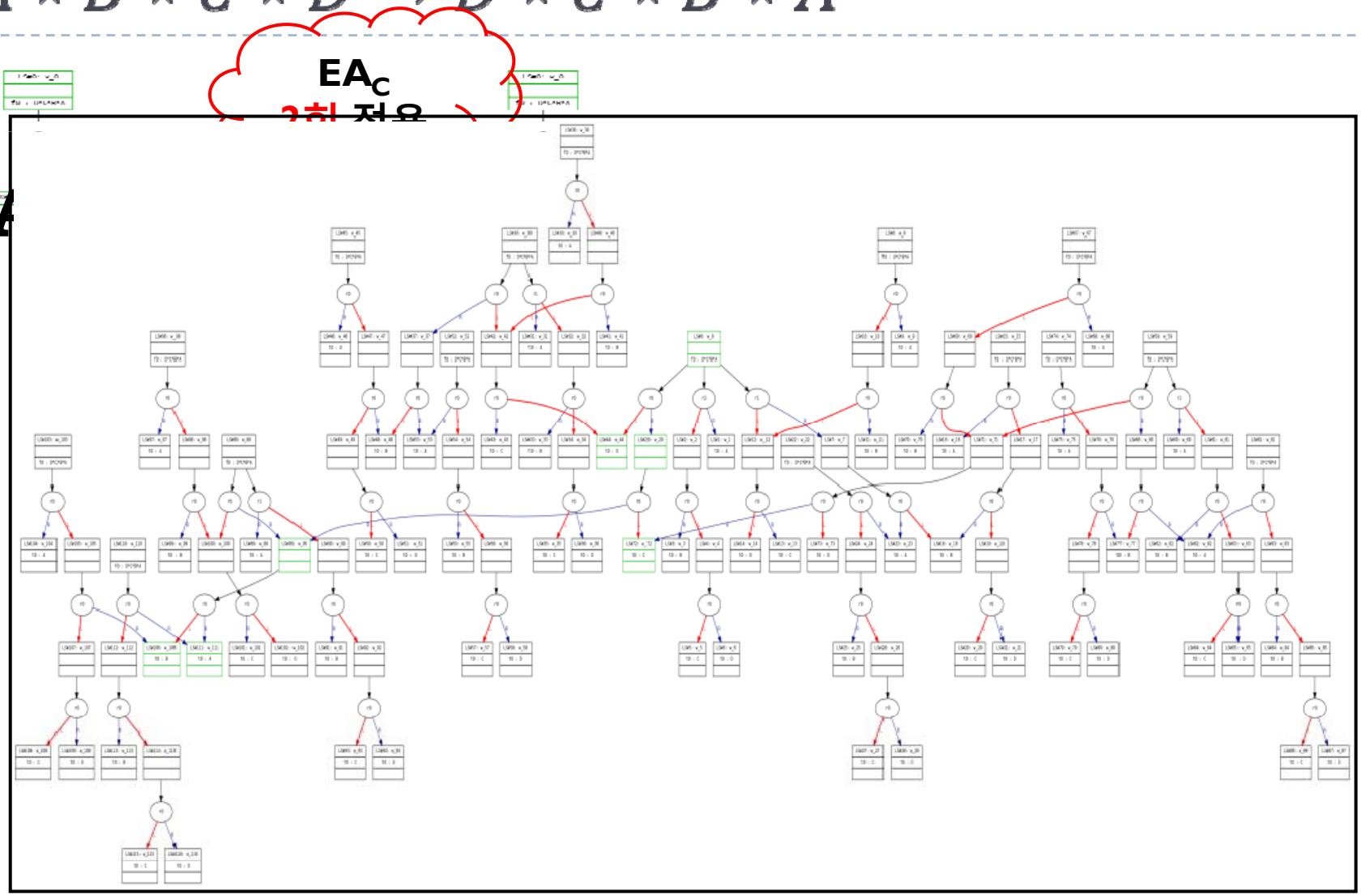
$$\text{where} \begin{cases} W_1' = W_1 \oplus W_2\langle \Gamma'; W_3\langle \Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle \Longrightarrow_{\mathcal{B}} \Delta'\rangle \\ W_2' = W_2 \oplus W_1\langle \Gamma'; W_3\langle \Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle \Longrightarrow_{\mathcal{B}} \Delta'\rangle \\ W_3' = W_3 \oplus (\Gamma'; W_1, W_2 \Longrightarrow_{\mathcal{B}} \Delta')\langle \Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle \end{cases}$$

$$\frac{\Gamma; W_2, \quad \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; W_1, \quad \Longrightarrow_{\mathcal{B}} \Delta} \; EC_{\mathcal{C}} \qquad \frac{\Gamma; (\Gamma \Longrightarrow_{\mathcal{B}} \Delta), (\emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta} \; \emptyset_{\mathsf{m}} U_{\mathcal{C}}$$

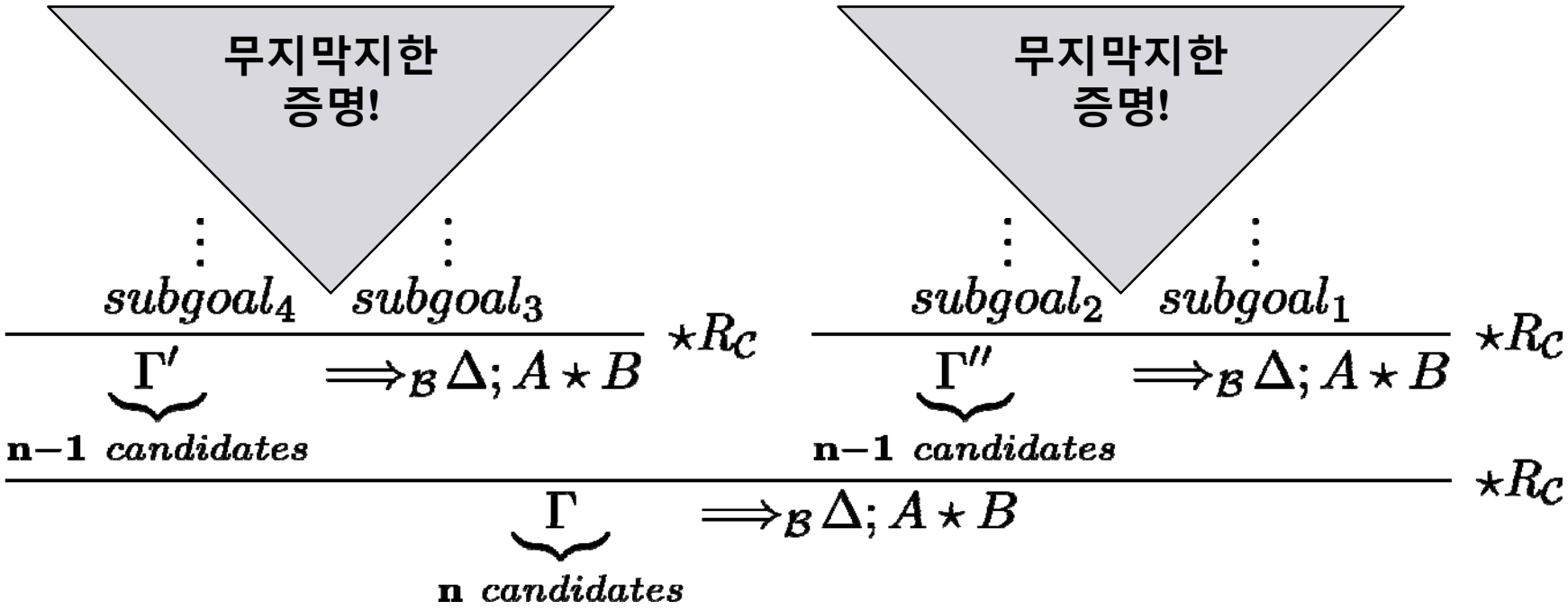
$$\frac{\Gamma; (\Gamma_{c1} \Longrightarrow_{\mathcal{B}} \Delta_{c1}), (\Gamma_{c2}; \emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \Delta_{c2}); \Gamma_{c1}; S \Longrightarrow_{\mathcal{B}} \Delta; \Delta_{c1}}{\Gamma; (\Gamma_{c1} \Longrightarrow_{\mathcal{B}} \Delta_{c1}), (\Gamma_{c2}; \emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \Delta_{c2}) \Longrightarrow_{\mathcal{B}} \Delta} \; \emptyset_{\mathsf{m}} D_{\mathcal{C}}$$

$$\text{where} \;\; S = (\Gamma_{c2}; \emptyset_{\mathsf{m}} \Longrightarrow_{\mathcal{B}} \Delta_{c2})\langle \Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle$$

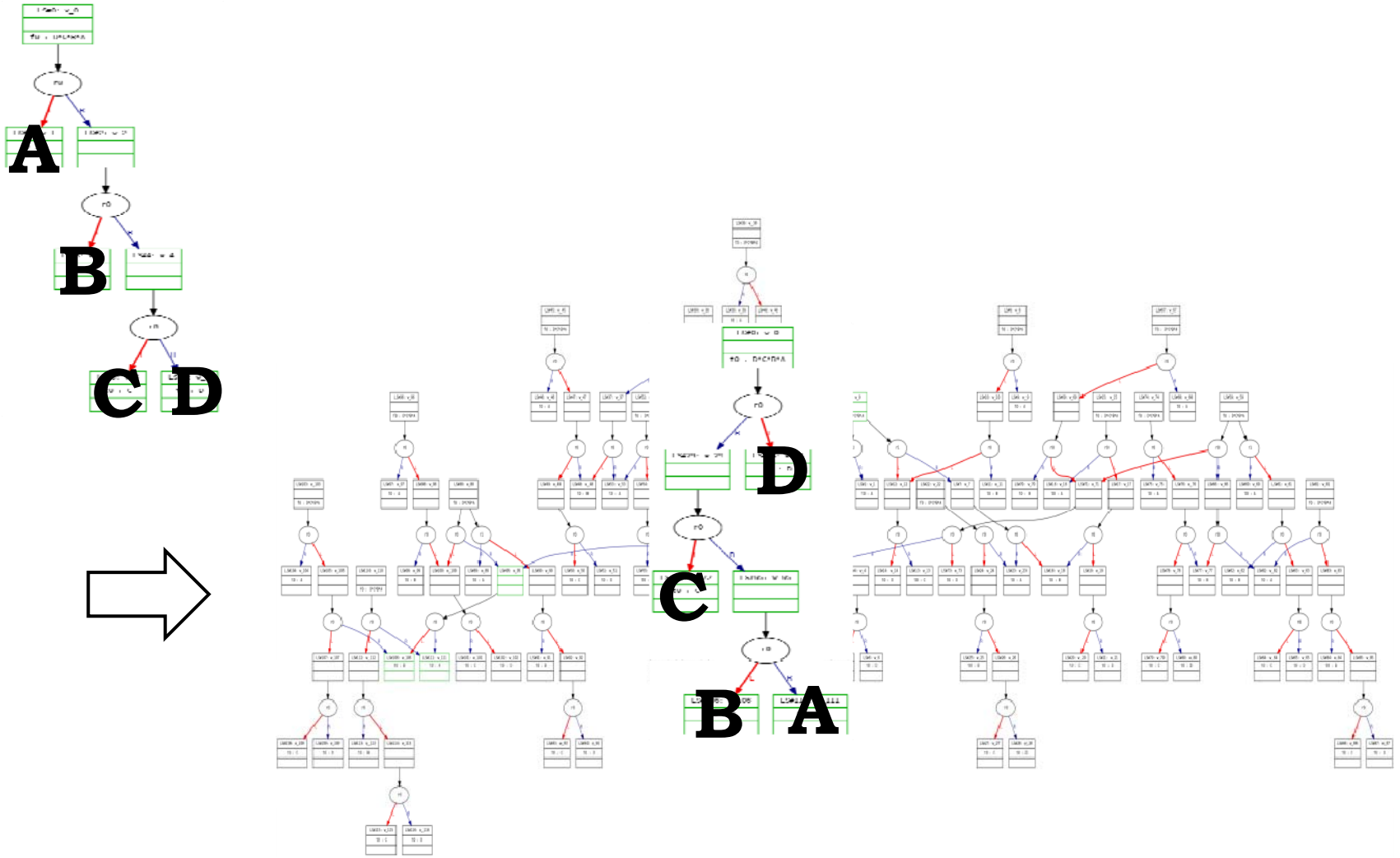
$$A \star B \star C \star D \rightarrow D \star C \star B \star A$$



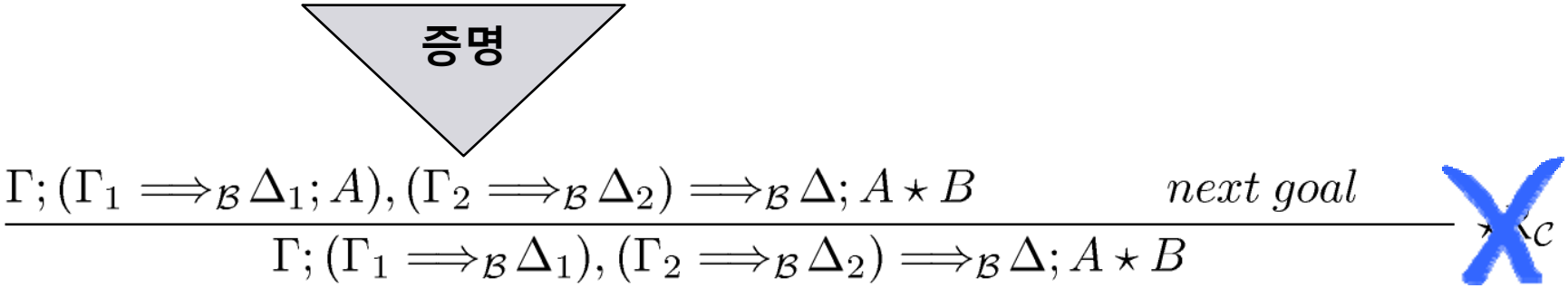
두 번째 문제점


무지막지한
증명!
무지막지한
증명!
$subgoal_4$ $subgoal_3$
Γ'
$\Longrightarrow_{\mathcal{B}} \Delta; A \star B$
$\star R_C$
$subgoal_2$ $subgoal_1$
Γ''
$\Longrightarrow_{\mathcal{B}} \Delta; A \star B$
$\star R_C$
n−1 candidates
n−1 candidates
Γ
$\Longrightarrow_{\mathcal{B}} \Delta; A \star B$
$\star R_C$
n candidates

해결 방법 1: 우선 순위를 주자!



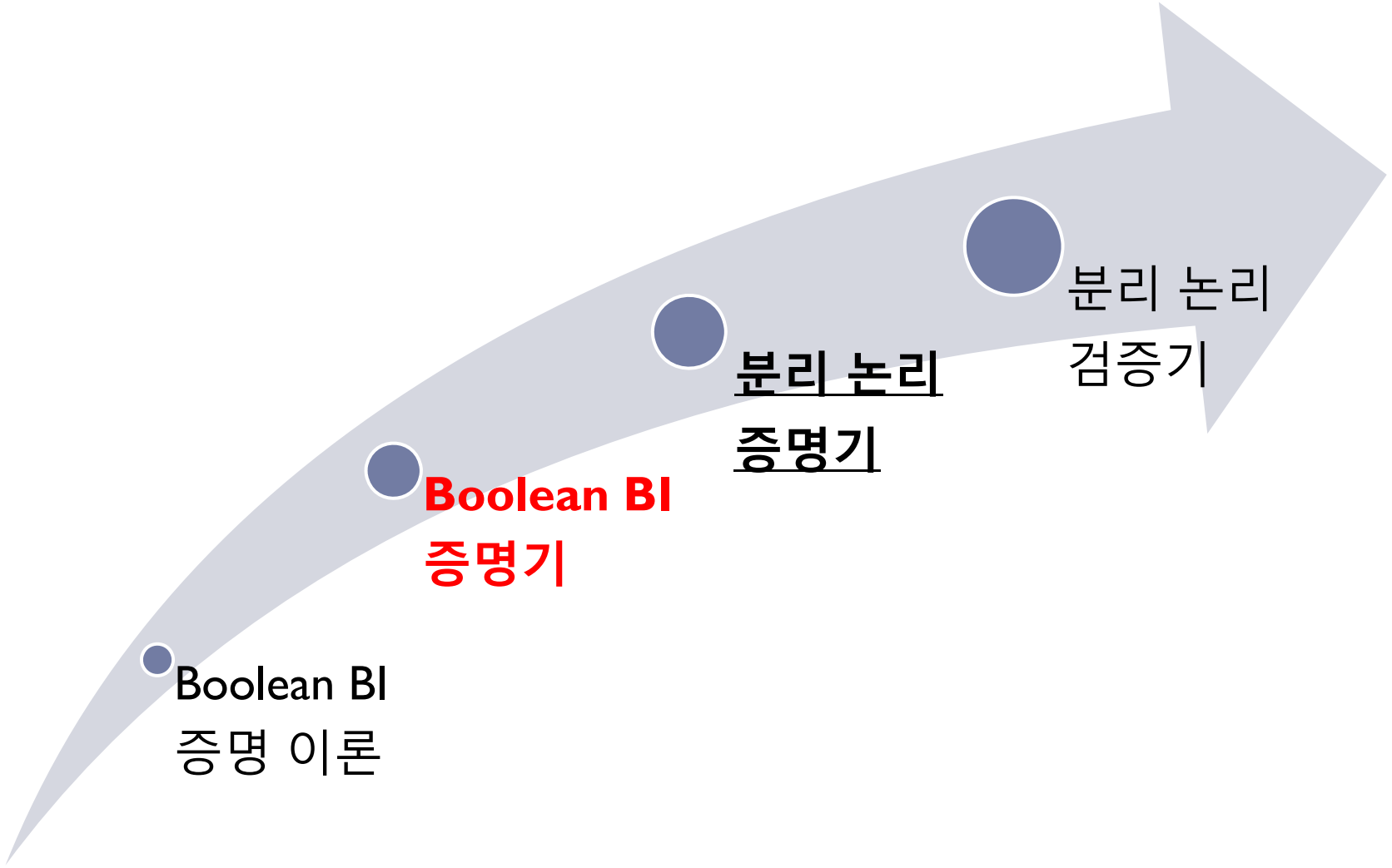
해결 방법 2: 재사용하자!


증명
$\Gamma; (\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1; A), (\Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2) \Longrightarrow_{\mathcal{B}} \Delta; A \star B$
$next\ goal$
$\Gamma; (\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1), (\Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2) \Longrightarrow_{\mathcal{B}} \Delta; A \star B$
$\star \backslash \mathcal{C}$

결과는?

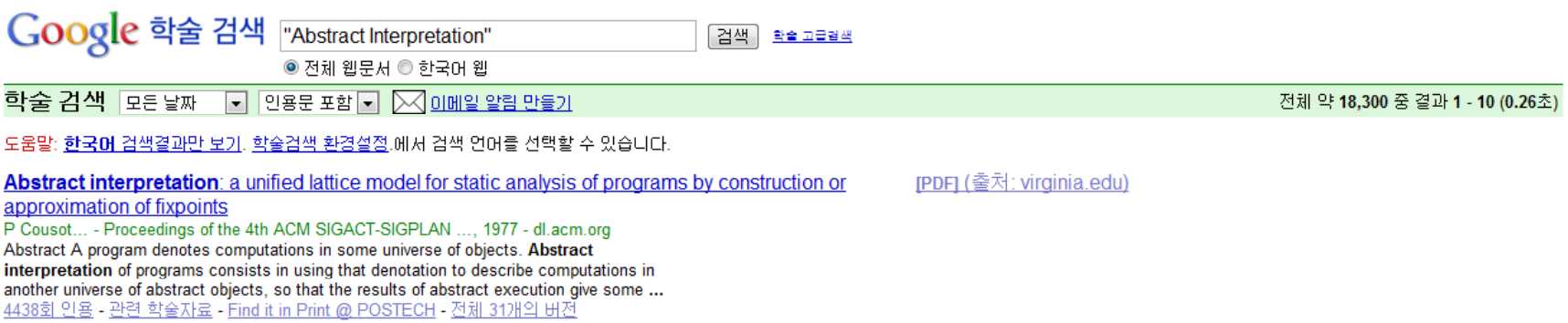
	최적화 (X)	최적화 (O)
$A \rightarrow (A \star B) \vee (A \star \neg B)$	< 0.01초	0.01초
$A \star B \star C \star D \rightarrow D \star B \star C \star A$	6.10초	0.01초
$A \star B \star C \star D \star E \rightarrow E \star D \star A \star B \star C$	67.87초	0.98초
$A \star B \star C \star D \star E \rightarrow E \star D \star B \star C \star A$	> 20000초	25.53초

현재 단계 및 향후 계획



POSTECH 프로그래밍 언어 연구실은……

- 멋쟁이 박성우 교수님의 지도하에,
- 주로, 다음과 같은 주제에 대한
  - 타입 이론
  - **증명 이론**
  - ……
- 연구를 주로 하고 있습니다.


Google 학술 검색
"Abstract Interpretation"
검색
학술 고급검색
전체 웹문서 한국어 웹
학술 검색
모든 날짜
인용문 포함
이메일 알림 만들기
전체 약 18,300 중 결과 1 - 10 (0.26초)
도움말: 한국어 검색결과만 보기. 학술검색 환경설정.에서 검색 언어를 선택할 수 있습니다.
Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints
[PDF] (출처: virginia.edu)
P Cousot... - Proceedings of the 4th ACM SIGACT-SIGPLAN ..., 1977 - dl.acm.org
Abstract A program denotes computations in some universe of objects. Abstract interpretation of programs consists in using that denotation to describe computations in another universe of abstract objects, so that the results of abstract execution give some ...
4438회 인용 - 관련 학술자료 - Find it in Print @ POSTECH - 전체 31개의 버전