A Theorem Prover for Boolean BI

POSTECH 프로그래밍 언어 연구실
박종현

목표

일반적인 C 프로그램을 위한 <u>**연역 검증 도구**</u> 개발

Hoare 논리

{ P } C { Q }

조건 P가 만족된 상태에서,

프로그램 C가 **실행**하면,

조건 Q가 만족된 상태에서 **종료**된다.

Hoare 논리 : 검증 방법

{ P } C { Q }

⇨

$Q_s \rightarrow Q$

또는

$P \rightarrow P_w$

분리 논리 = Hoare 논리의 확장

{ P } C { Q }

조건 P가 만족된 상태에서,
프로그램 C가 **실행**하면,
조건 Q가 만족된 상태에서 **종료**된다.

새로운 논리 연산자(⋆,−⋆)를 지원

리스트 뒤집기

$\{$ **List** α_0 **a** $\}$

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

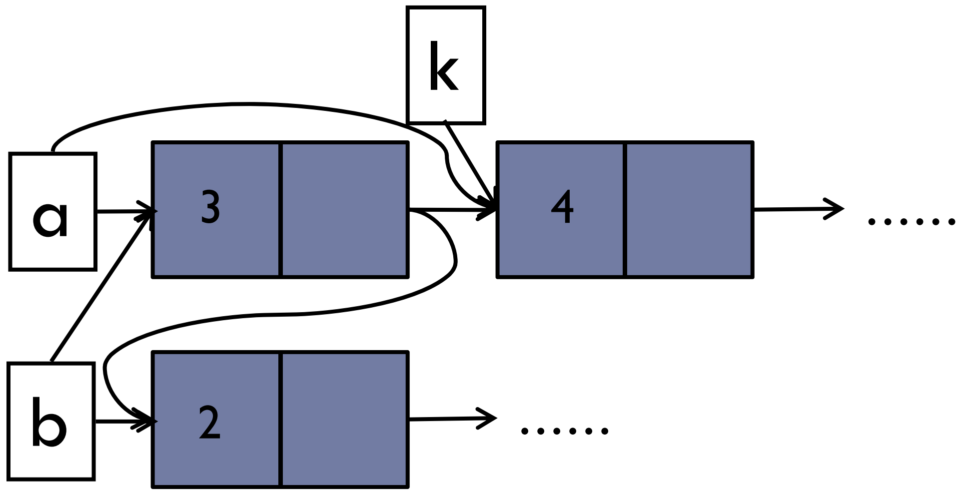
$\{$ **List** α_0^R **b** $\}$

리스트 뒤집기

{ 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 }

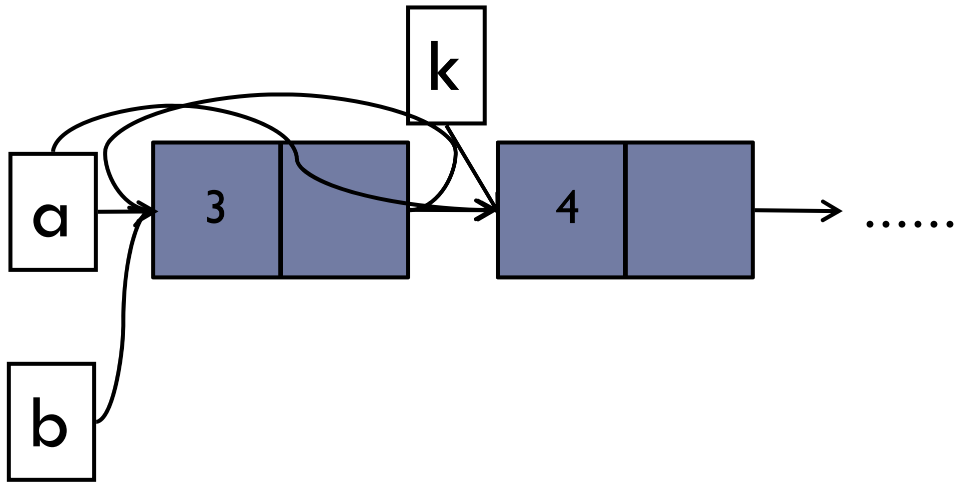


리스트 뒤집기: a = b?

{ 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

$\{ \text{List } \alpha_0 \text{ a} \}$

```
b := nil
```

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

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

$\{ \text{List } \alpha_0^R \text{ b} \}$

반복문 불변식 @ 분리 논리

$\{ \text{List } \alpha_0 \text{ a } \}$

```
b := nil
```

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

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

$\{ \text{List } \alpha_0^R \text{ b } \}$

분리 논리의 핵심

프로그램이
실제로 사용하는 메모리만
고려하면 된다!

$$\frac{\text{덖}P\text{덗}\ C\ \{Q\}}{\text{덖}P \star R\text{덗}\ C\ \{Q \star R\}}$$

다양한 검증 도구들

- Smallfoot
- ……

순방향(forward) 검증을 사용

왜냐하면...

- $-\!\!\ast$ 를 지원하는 자동 증명기가 존재하지 않음

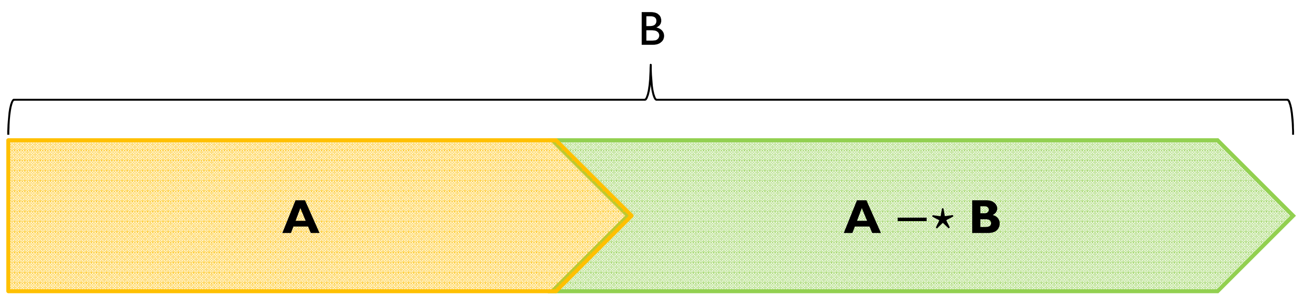
This incompleteness could be dealt with if we instead used the backwards running weakest pre-conditions of Separation Logic

$-\!\!\ast$ 도 지원하는 분리 논리 자동 증명기를 만들자!

"Symbolic Execution with Separation Logic"

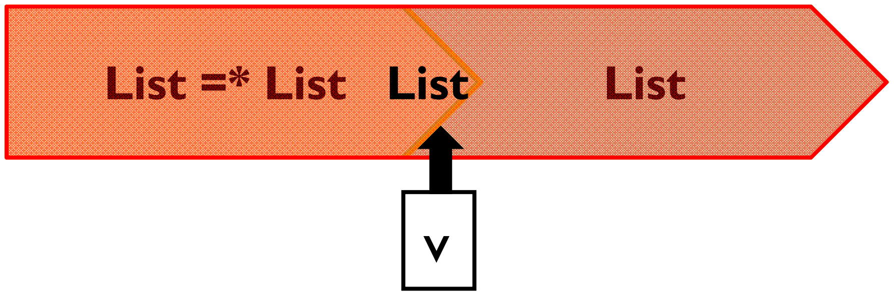
$-\!\!\star$의 유용성

B를 만족하는 메모리에서
A를 만족하는 부분을 제외한
메모리가 주어질 때……



Xisa

"Relational Inductive Shape Analysis"



분리 논리 = Boolean BI의 특수한 경우

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

Boolean BI 자동 증명기를 만들자!

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

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

귀추 계산법 $\mathrm{S}_{\mathrm{BBI}}$

Structural rules:

$$\frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; S \Longrightarrow_{\mathcal{B}} \Delta}\,\mathit{WL}_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A}\,\mathit{WR}_{\mathcal{B}} \qquad \frac{\Gamma; S; S \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; S \Longrightarrow_{\mathcal{B}} \Delta}\,\mathit{CL}_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A; A}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A}\,\mathit{CR}_{\mathcal{B}}$$

$$\frac{\Gamma; W', W \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; W, W' \Longrightarrow_{\mathcal{B}} \Delta}\,\mathit{EC}_{\mathcal{B}} \qquad \frac{\Gamma; W_1, (W_2, W_3 \Longrightarrow_{\mathcal{B}} \cdot) \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; (W_1, W_2 \Longrightarrow_{\mathcal{B}} \cdot), W_3 \Longrightarrow_{\mathcal{B}} \Delta}\,\mathit{EA}_{\mathcal{B}}$$

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

Traverse rules:

$$\frac{\Gamma_{\mathrm{c}1}; (\Gamma_{\mathrm{c}2} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{c}2})\langle \Gamma \Longrightarrow_{\mathcal{B}} \Delta \rangle \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{c}1}}{\Gamma; (\Gamma_{\mathrm{c}1} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{c}1}), (\Gamma_{\mathrm{c}2} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{c}2}) \Longrightarrow_{\mathcal{B}} \Delta}\,\mathit{TC}_{\mathcal{B}} \qquad \frac{\Gamma_{\mathrm{p}}; (\Gamma \Longrightarrow_{\mathcal{B}} \Delta), (\Gamma_{\mathrm{s}} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{s}}) \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{p}}}{\Gamma; (\Gamma_{\mathrm{s}} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{s}})\langle \Gamma_{\mathrm{p}} \Longrightarrow_{\mathcal{B}} \Delta_{\mathrm{p}} \rangle \Longrightarrow_{\mathcal{B}} \Delta}\,\mathit{TP}_{\mathcal{B}}$$

Logical rules:

$$\frac{}{P \Longrightarrow_{\mathcal{B}} P}\,\mathit{Init}_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma; \top \Longrightarrow_{\mathcal{B}} \Delta}\,\top L_{\mathcal{B}} \qquad \frac{}{\cdot \Longrightarrow_{\mathcal{B}} \top}\,\top R_{\mathcal{B}} \qquad \frac{}{\bot \Longrightarrow_{\mathcal{B}} \cdot}\,\bot L_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; \bot}\,\bot R_{\mathcal{B}} \qquad \frac{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A}{\Gamma; \neg A \Longrightarrow_{\mathcal{B}} \Delta}\,\neg L_{\mathcal{B}}$$

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

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

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

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

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

$\mathrm{S}_{\mathrm{BBI}}$의 주요 성질

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

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

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

역방향 단순 탐색 전략

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

1. 적용 가능한

$$\frac{}{P \Longrightarrow_{\mathcal{B}} P}\ Init_{\mathcal{B}}$$

2. 공리인가?
   - 증명 완료
3. 다음 귀추를 계산한다.
4.

$$\frac{\Gamma; A \Longrightarrow_{\mathcal{B}} \Delta}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; \neg A}\ \neg R_{\mathcal{B}}$$

을 찾아본다.

5.
   - 증명 완료
6. 1번부터 다시 수행 한다.

문제점

1. 적용 가능한 규칙이 너무 많습니다!

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

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 $\mathrm{CS}_{\mathrm{BBI}}$

Structural rules:

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

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

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

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

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

Traverse rules:

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

Logical rules:

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

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

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

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

$$\frac{\begin{array}{c}\Gamma; (\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1; A) \cdots \\ \Gamma; (\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1) \langle \Gamma \cdots \end{array}}{\Gamma; (\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1) \langle \Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2 \rangle; A \mathrel{-\!\!\star} B \Longrightarrow_{\mathcal{B}} \Delta}\ \mathrel{-\!\!\star} L_{\mathcal{C}} \qquad \frac{\cdots}{\Gamma \Longrightarrow_{\mathcal{B}} \Delta; A \mathrel{-\!\!\star} B}\ \mathrel{-\!\!\star} R_{\mathcal{C}}$$

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

CS_{BBI}의 주요 성질

S_{BBI}에 대해서 안전하고 완전함

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

$\mathrm{CS}_{\mathrm{BBI}}$ 유용한 성질

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,
  - 규칙이 적용 가능할 때,
  - 항상 적용 하면 된다!

$\mathrm{CS}_{\mathrm{BBI}}$ 유용한 성질 (계속)

증명 과정에서 같은 가정을 여러 번 사용할지라도,
같은 가정을 여러 번 도입할 필요는 없다.

- $\Gamma; S; S \Longrightarrow_{\mathcal{B}} \Delta$ 증명 가능 ➔ $\Gamma; S \Longrightarrow_{\mathcal{B}} \Delta$ 증명 가능

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

역방향 단순 탐색 전략

$\Gamma \Rightarrow_{\mathcal{B}} \Delta$가 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.

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

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

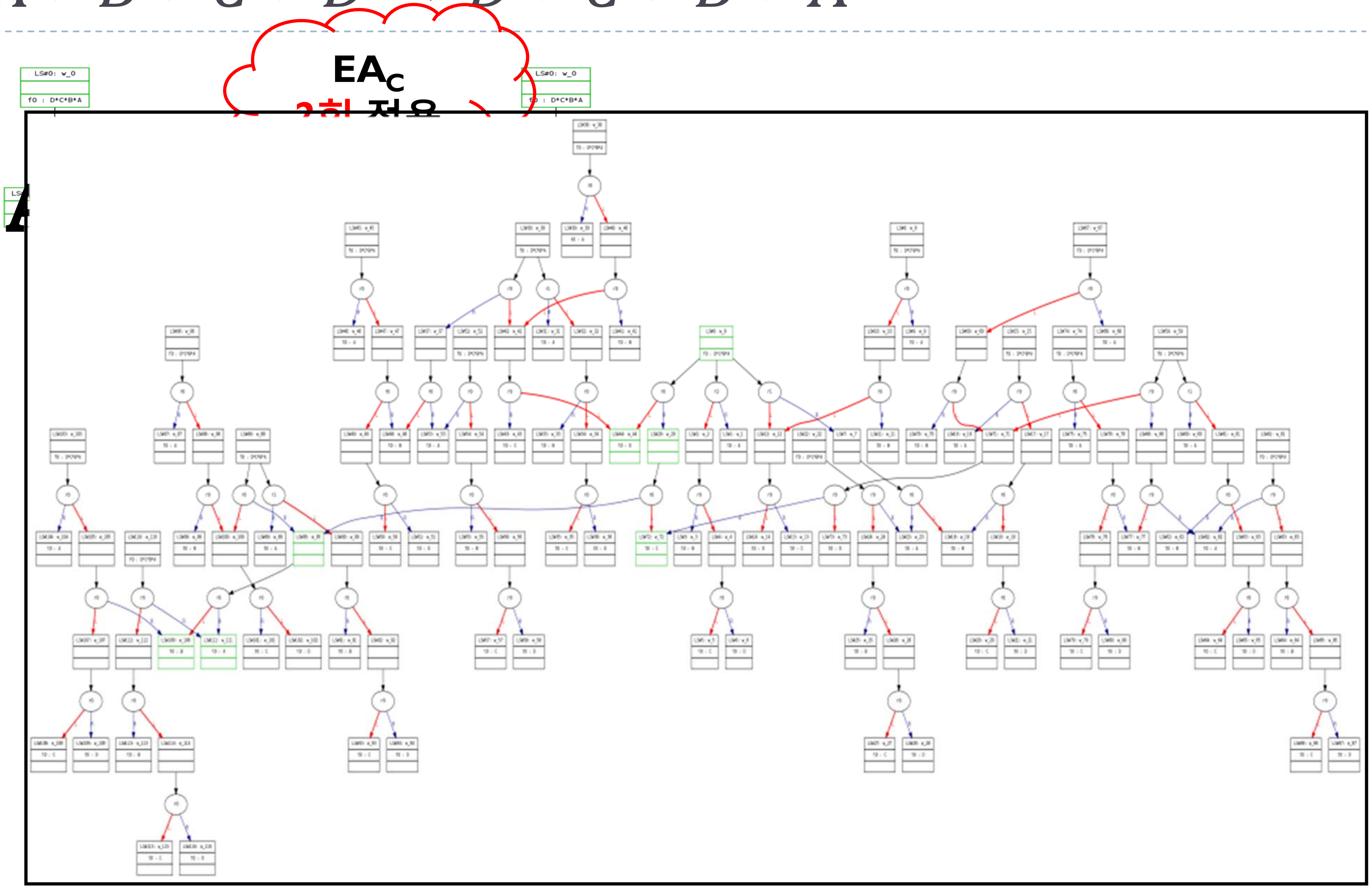
$$\text{where} \begin{cases} W_1' = W_1 \oplus W_2\langle \Gamma'; W_3\langle \Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle \Longrightarrow_{\mathcal{B}} \Delta'\rangle \\ W_2' = W_2 \oplus W_1\langle \Gamma'; W_3\langle \Gamma \Longrightarrow_{\mathcal{B}} \Delta\rangle \Longrightarrow_{\mathcal{B}}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

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

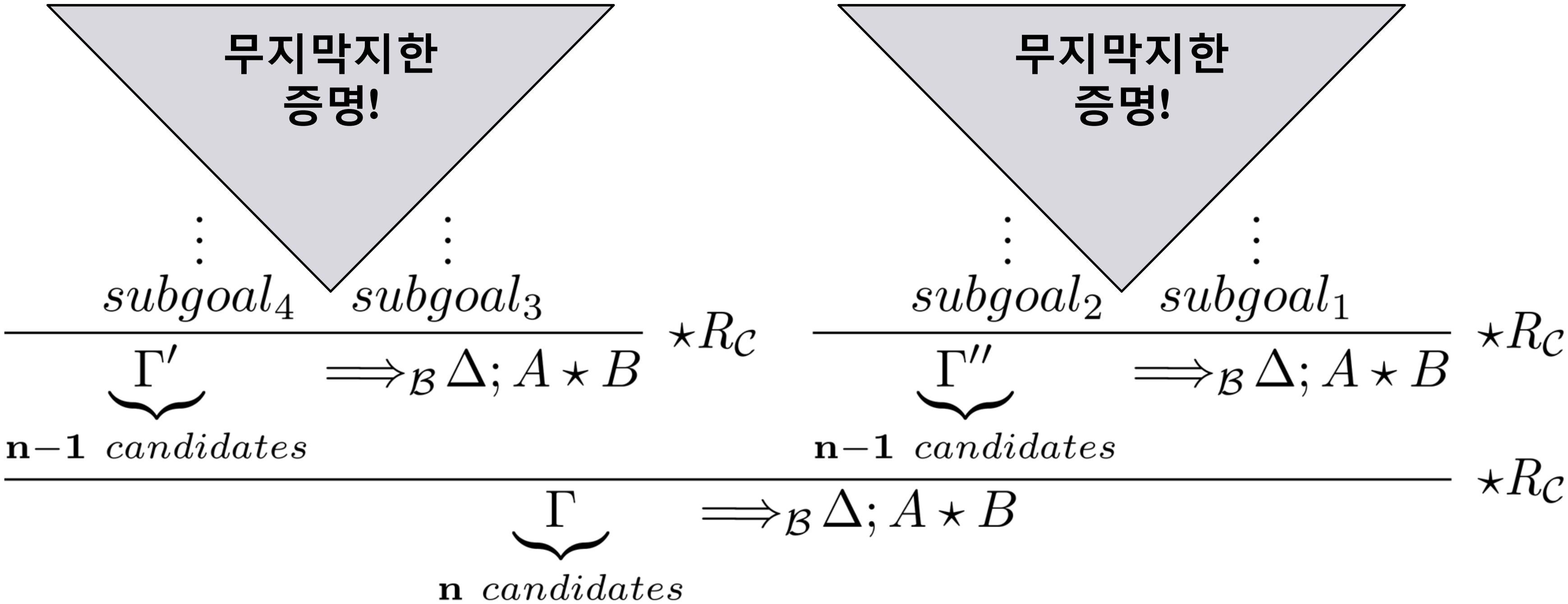
$$\frac{\Gamma; (\Gamma_{c1} \Longrightarrow_{\mathcal{B}} \Delta_{c1}), (\Gamma_{c2}; \emptyset_{\mathrm{m}} \Longrightarrow_{\mathcal{B}} \Delta_{c2}); \Gamma_{c1}; S \Longrightarrow_{\mathcal{B}} \Delta; \Delta_{c1}}{\Gamma; (\Gamma_{c1} \Longrightarrow_{\mathcal{B}} \Delta_{c1}), (\Gamma_{c2}; \emptyset_{\mathrm{m}}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

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

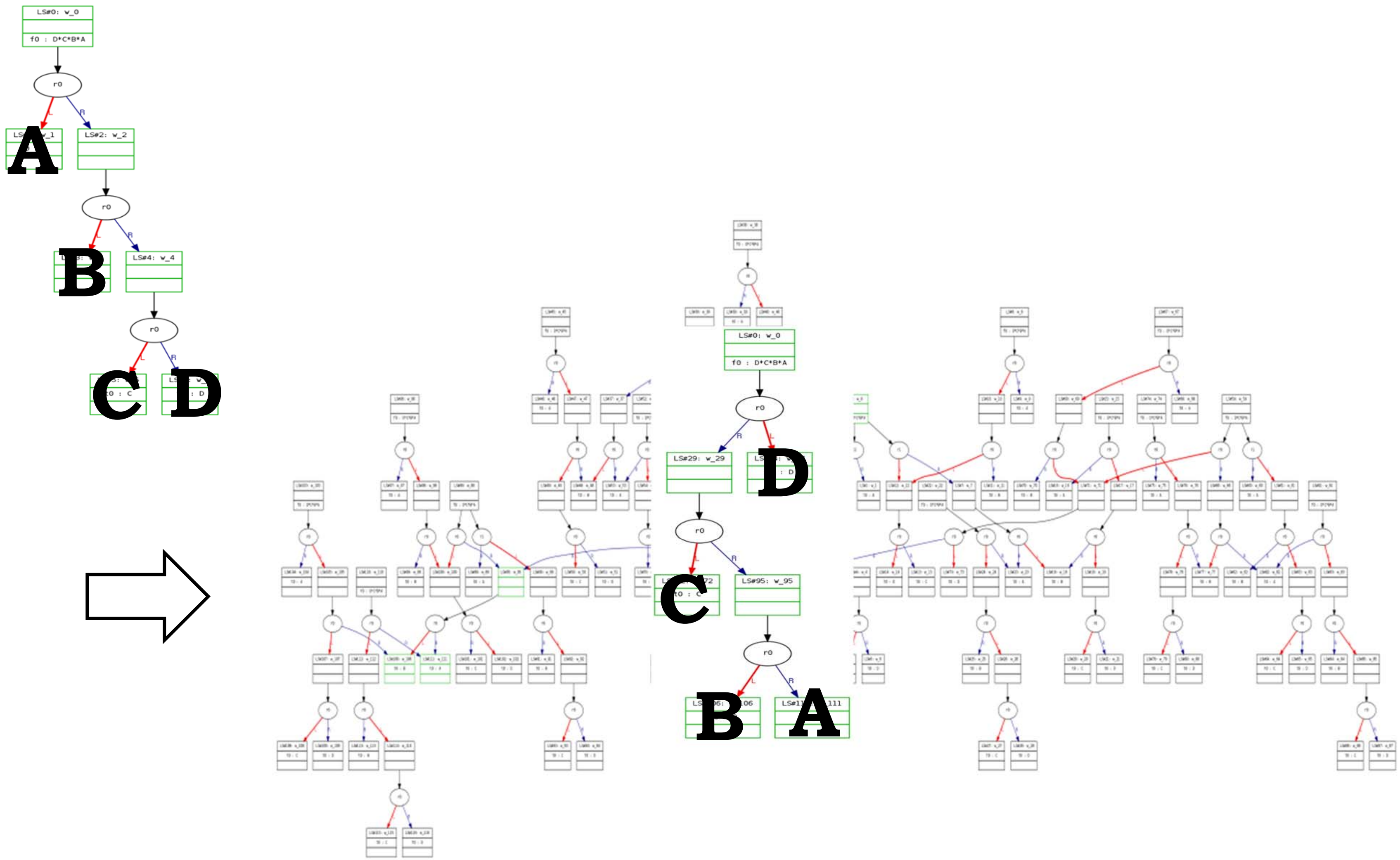
$A \star B \star C \star D \to D \star C \star B \star A$



두 번째 문제점


무지막지한 증명!
무지막지한 증명!
$subgoal_4$
$subgoal_3$
$subgoal_2$
$subgoal_1$
$\underbrace{\Gamma'}_{\mathbf{n-1}\ candidates} \Longrightarrow_{\mathcal{B}} \Delta; A \star B \quad \star R_{\mathcal{C}}$
$\underbrace{\Gamma''}_{\mathbf{n-1}\ candidates} \Longrightarrow_{\mathcal{B}} \Delta; A \star B \quad \star R_{\mathcal{C}}$
$\underbrace{\Gamma}_{\mathbf{n}\ candidates} \Longrightarrow_{\mathcal{B}} \Delta; A \star B \quad \star R_{\mathcal{C}}$

해결 방법 1: 우선 순위를 주자!



해결 방법 2: 재사용하자!

$$\frac{\Gamma; (\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1; A), (\Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2) \Longrightarrow_{\mathcal{B}} \Delta; A \star B \qquad \textit{next goal}}{\Gamma; (\Gamma_1 \Longrightarrow_{\mathcal{B}} \Delta_1), (\Gamma_2 \Longrightarrow_{\mathcal{B}} \Delta_2) \Longrightarrow_{\mathcal{B}} \Delta; A \star B} \; \cancel{\star R_{\mathcal{C}}}$$

홈페이지

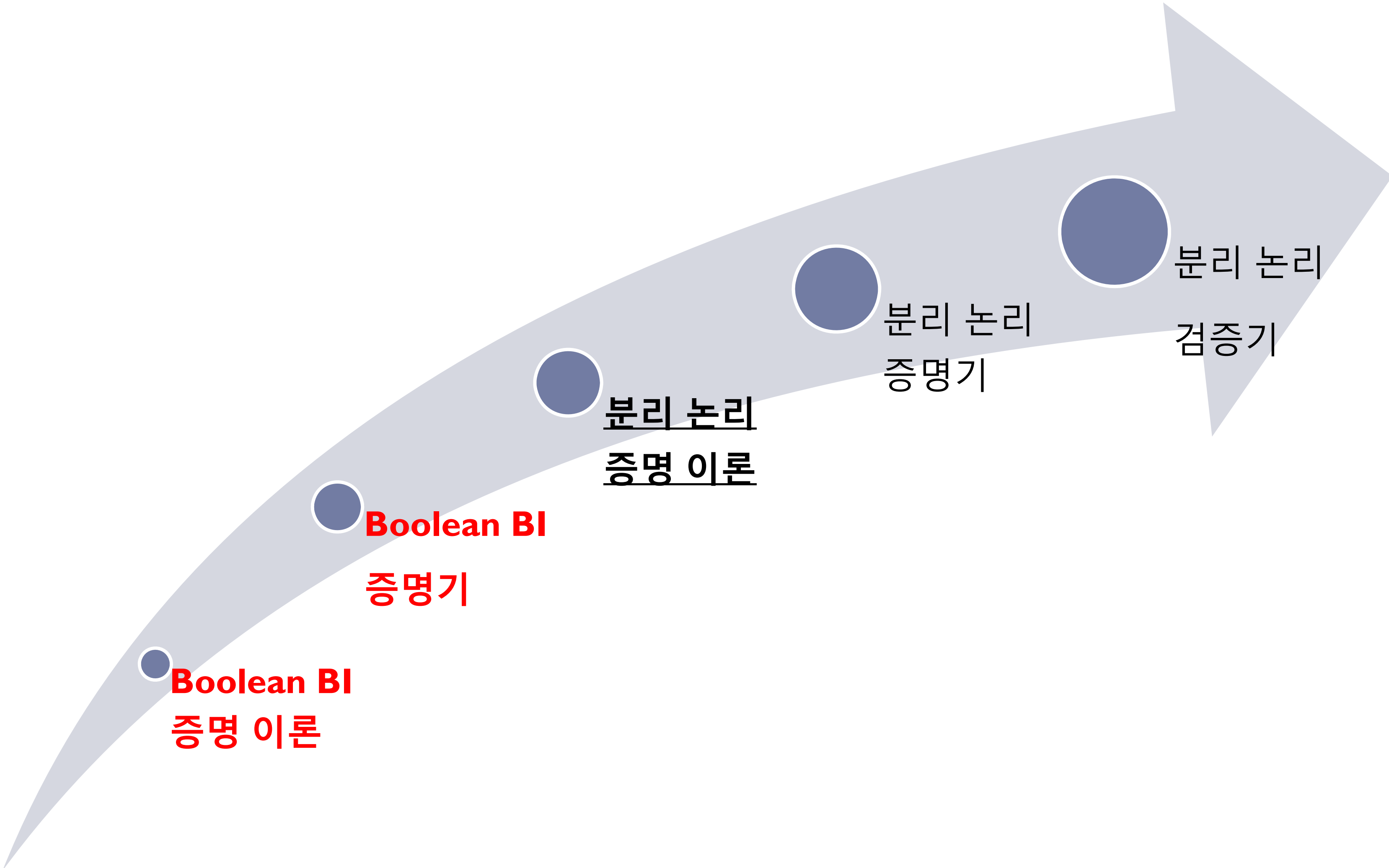
- http://pl.postech.ac.kr/BBI/

시연

시연

- http://pl.postech.ac.kr/BBI/web_prover/prover.php

진행 상황



목표

- $F, G, \cdots ::= l \mapsto \_ \mid \top \mid \neg F \mid F \vee G \mid F \star G \mid F -\!\!\star\, G$

- 일단은 간단한 문제부터……
  - $F, G, \cdots ::= l \mapsto \_ \mid \top \mid I \mid \boldsymbol{F \star G}$

- 보다 자세한 내용은 포스터 발표에서 ☺

감사합니다