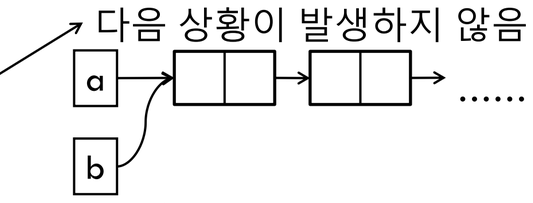
Boolean BI를 위한 컷-제거 귀추 계산법

POSTECH 프로그래밍 언어 연구실 박종현
ROSAEC 2011 동계 워크샵 @ 통영

연구 동기

- 포인터 프로그램의 연역 검증을 용이하게 만들어 주는 **분리 논리**

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



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

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

- 분리 논리에 대한 **증명 이론** 부재 ➔ **자동화**의 어려움
- 분리 논리 ≈ Boolean BI ➔ Boolean BI를 위한 증명 이론 설계!

관련 연구 – 직관 BI 논리

- 직관 BI 논리(= 직관 논리 + 선형 논리)를 위한 증명 이론은 존재
- 직관 BI 논리를 위한 귀추 계산법 **Γ→$_I$A**
  Γ가 성립하는 "자원"에서는 A를 할 수 있다.
- 핵심 아이디어? **"부분 독립 자원"**에 대한 가정 (Γ_1, Γ_2) 허용
  현재 자원을 Γ_1과 Γ_2가 성립하는 자원으로 분할 가능

$(\Gamma_1,\Gamma_2);\Gamma_3 \rightarrow_I A$ 〓

A 가능?

Γ_3	
Γ_1	Γ_2

- 컷-제거 성질 성립

비결합적 고전 BI 논리

- Boolean BI = 직관 BI 논리 + 고전 논리?
  - 고전 논리의 귀추 계산법 **Γ→Δ**
    Γ가 "**참**"이고 Δ가 "**거짓**"일 때 "모순"이 발생한다.
- 새로운 컷 제거 귀추 계산법 **Δ →$_B$ Ψ**
  - Δ가 "참"이고 Ψ가 "거짓"인 "자원"에서는 "모순"이 발생한다.
- 핵심 아이디어? 각 자원에 대한 독립적인 "**참**"/"**거짓**" 가정 허용
  현재 자원을 Δ_1이 "**참**"이고 Ψ_1가 "**거짓**"인 자원과 Δ_2이 "**참**"이고 Ψ_2가 "**거짓**"인 자원으로 분할 가능 ($\Delta_1 \rightarrow_B \Psi_1$, $\Delta_2 \rightarrow_B \Psi_2$)

$$(\Delta_1 \rightarrow_B \Psi_1,\ \Delta_2 \rightarrow_B \Psi_2);\ \Delta_3 \rightarrow_B \Psi_3$$

모순 발생?

〓

$\Delta_3 \rightarrow_B \Psi_3$	
$\Delta_1 \rightarrow_B \Psi_1$	$\Delta_2 \rightarrow_B \Psi_2$

컷-제거 귀추 계산법

$$\frac{A \text{ atomic}}{\omega[A \longrightarrow_B A]}\ Init \qquad \frac{\omega[\Delta \longrightarrow_B \Psi]}{\omega[\Delta;\Delta' \longrightarrow_B \Psi]}\ W \qquad \frac{\omega[\Delta \longrightarrow_B \Psi]}{\omega[\Delta \longrightarrow_B \Psi;A]}\ W'$$

$$\frac{\omega[\Delta;\Delta';\Delta' \longrightarrow_B \Psi]}{\omega[\Delta;\Delta' \longrightarrow_B \Psi]}\ C \qquad \frac{\omega[\Delta \longrightarrow_B \Psi;A;A]}{\omega[\Delta \longrightarrow_B \Psi;A]}\ C'$$

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

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

$$\frac{\omega[\Delta;\emptyset_m \longrightarrow_B \Psi]}{\omega[\Delta;\mathsf{I} \longrightarrow_B \Psi]}\ \mathsf{I}L \qquad \frac{}{\omega[\emptyset_m \longrightarrow_B \mathsf{I}]}\ \mathsf{I}R$$

$$\frac{\omega[(\Delta \longrightarrow_B \Psi),(\Delta' \longrightarrow_B \Psi';A);\Delta'' \longrightarrow_B \Psi''] \quad \omega[B;\Delta'' \longrightarrow_B \Psi'']}{\omega[(\Delta;A \mathrel{-\!\!\star} B \longrightarrow_B \Psi),(\Delta' \longrightarrow_B \Psi');\Delta'' \longrightarrow_B \Psi'']}\ \mathrel{-\!\!\star} L$$

$$\frac{\omega[(\Delta \longrightarrow_B \Psi),(\Delta';A \longrightarrow_B \Psi');\Delta'' \longrightarrow_B \Psi'';B]}{\omega[(\Delta \longrightarrow_B \Psi;A \mathrel{-\!\!\star} B),(\Delta' \longrightarrow_B \Psi');\Delta'' \longrightarrow_B \Psi'']}\ \mathrel{-\!\!\star} R$$

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

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

컷-제거 성질

$$\omega \quad ::= \quad [] \mid \omega, W;\Delta \longrightarrow_B \Psi$$

Theorem 4.1. *If* $\omega[\Delta \longrightarrow_B \Psi;C]$ *and* $\omega[\Delta;C \longrightarrow_B \Psi]$ *then* $\omega[\Delta \longrightarrow_B \Psi]$.

한 부분 자원에서
- C가 "참"일 때도, C가 "거짓"일 때도 모순이 발생한다면,
  언제나 "모순"이 발생한다.

문제점

- A —★ B의 의미?
  "이웃 자원"에서 A가 거짓이거나, 혹은 "부모 자원"에서 B가 참이다.
- 분리 논리에서의 —★ 활용

```
{ x ⇒ v ★ (x ⇒ 1 —★ P) }
x := 1
{ x ⇒ 1 ★ (x ⇒ 1 —★ P) }
{ P }
```

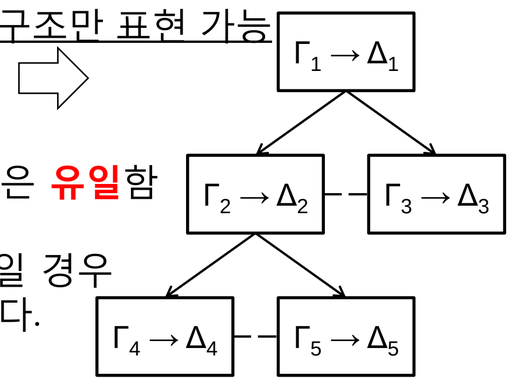
"이웃 자원"에서 x ⇒ 1이 거짓

"부모 자원"에서 P가 성립

원인

$$\begin{array}{lcl} W & = & \Delta \longrightarrow_B \Psi \\ \Delta & ::= & A \mid \emptyset_a \mid \emptyset_m \mid W, W \mid \Delta;\Delta \\ \Psi & ::= & \cdot \mid A \mid \Psi;\Psi \end{array}$$

나뭇가지 구조만 표현 가능



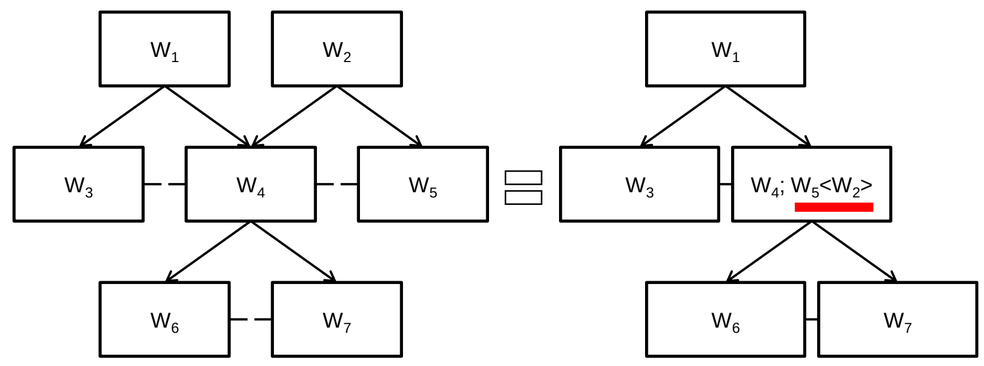
- 나뭇가지 구조에서는 **"이웃 자원"**은 **유일**함
- A —★ B의 의미
  A가 참인 "자원"이 "이웃 자원"일 경우
  그 "부모 자원"에서는 B가 참이다.

•복수의 "이웃 자원"과 "부모 자원"이 존재할 수 있음!
  • 나뭇가지 구조가 아닌 **비-순환 그래프 구조**가 필요

해결책

- "이웃 자원"에 따른 "부모 자원"에 대한 가정(W<W>) 허용

$$\begin{array}{lcl} W & ::= & \Gamma \longrightarrow_B \Delta \\ \Gamma & ::= & A \mid \emptyset_a \mid \emptyset_m \mid \Gamma;\Gamma \mid W, W \mid W\langle W\rangle \\ \Delta & ::= & \cdot \mid \Delta; A \end{array}$$



새로운 컷-제거 귀추 계산법

$$\frac{}{P \longrightarrow_B P}\ Init \qquad \frac{\Gamma \longrightarrow_B \Delta}{\Gamma;A \longrightarrow_B \Delta}\ WL \qquad \frac{\Gamma \longrightarrow_B \Delta}{\Gamma \longrightarrow_B \Delta;A}\ WR \qquad \frac{\Gamma;A;A \longrightarrow_B \Delta}{\Gamma;A \longrightarrow_B \Delta}\ CL \qquad \frac{\Gamma \longrightarrow_B \Delta;A;A}{\Gamma \longrightarrow_B \Delta;A}\ CR$$

$$\frac{\Gamma;\emptyset_a \longrightarrow_B \Delta}{\Gamma;\top \longrightarrow_B \Delta}\ \top L \qquad \frac{}{\emptyset_a \longrightarrow_B \top}\ \top R \qquad \frac{\Gamma \longrightarrow_B \Delta;A}{\Gamma;\neg A \longrightarrow_B \Delta}\ \neg L \qquad \frac{\Gamma;A \longrightarrow_B \Delta}{\Gamma \longrightarrow_B \Delta;\neg A}\ \neg R$$

$$\frac{\Gamma;A;B \longrightarrow_B \Delta}{\Gamma;A \wedge B \longrightarrow_B \Delta}\ \wedge L \qquad \frac{\Gamma \longrightarrow_B \Delta;A \quad \Gamma' \longrightarrow_B \Delta';B}{\Gamma;\Gamma' \longrightarrow_B \Delta;\Delta';A \wedge B}\ \wedge R$$

$$\frac{\Gamma;\emptyset_m \longrightarrow_B \Delta}{\Gamma;\mathsf{I} \longrightarrow_B \Delta}\ \mathsf{I}L \qquad \frac{}{\emptyset_m \longrightarrow_B \mathsf{I}}\ \mathsf{I}R$$

$$\frac{\Gamma;(A \longrightarrow_B \cdot),(B \longrightarrow_B \cdot) \longrightarrow_B \Delta}{\Gamma;A \star B \longrightarrow_B \Delta}\ \star L \qquad \frac{\Gamma' \longrightarrow_B \Delta';A \quad \Gamma'' \longrightarrow_B \Delta'';B}{(\Gamma' \longrightarrow_B \Delta'),(\Gamma'' \longrightarrow_B \Delta'') \longrightarrow_B A \star B}\ \star R$$

$$\frac{\Gamma' \longrightarrow_B \Delta';A \quad \Gamma'';B \longrightarrow_B \Delta''}{(\Gamma' \longrightarrow_B \Delta')\langle\Gamma'' \longrightarrow_B \Delta''\rangle;A \mathrel{-\!\!\star} B \longrightarrow_B \cdot}\ \mathrel{-\!\!\star} L \qquad \frac{\Gamma;(A \longrightarrow_B \cdot)\langle\emptyset_a \longrightarrow_B B\rangle \longrightarrow_B \Delta}{\Gamma \longrightarrow_B \Delta;A \mathrel{-\!\!\star} B}\ \mathrel{-\!\!\star} R$$

$$\frac{\Gamma'';(\Gamma \longrightarrow_B \Delta),(\Gamma' \longrightarrow_B \Delta') \longrightarrow_B \Delta''}{\Gamma;(\Gamma' \longrightarrow_B \Delta')\langle\Gamma'' \longrightarrow_B \Delta''\rangle \longrightarrow_B \Delta}\ \Uparrow \qquad \frac{\Gamma;(\Gamma' \longrightarrow_B \Delta')\langle\Gamma'' \longrightarrow_B \Delta''\rangle \longrightarrow_B \Delta}{\Gamma'';(\Gamma \longrightarrow_B \Delta),(\Gamma' \longrightarrow_B \Delta') \longrightarrow_B \Delta''}\ \Downarrow$$

컷-제거 성질

Lemma 1.8 *If* $\omega[\Gamma \longrightarrow_B \Delta;C]$ *and* $\omega'[\Gamma';C \longrightarrow_B \Delta']$, *then* $\Gamma;\Gamma';\Gamma_\omega;\Gamma_{\omega'} \longrightarrow_B \Delta;\Delta'$

한 부분 자원에서
- C가 "참"일 때도, C가 "거짓"일 때도 모순이 발생한다면,
  언제나 "모순"이 발생한다.