BI 논리체계 증명기 개발

박성우

ROSAEC Workshop

2009년 7월 11일

1st Workshop 발표 슬라이드

(2008. 11)

Theorem Prover for BI

- BI
  - Logic of Bunched Implications
  - Separation logic과 밀접한 관계
    - Separation logic이 BI 모델의 일종
- 기존의 theorem prover for BI
  - BILL
  - Inverse method prover [LPAR 2004]
- 목표
  - Inverse method + focusing

32

Logic 소개

진리표와 모델

- Model ***I*** ¼
  assignment of truth values (진리값)
  to propositions (명제)
  - ***I*** : Prop ! { T, F }

	A	B	$A \wedge B$
$\mathcal{I}_1$	T	T	T
$\mathcal{I}_2$	T	F	F
$\mathcal{I}_3$	F	T	F
$\mathcal{I}_4$	F	F	F

Disjunction & Implication

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

A	B	$A \supset B$
T	T	T
T	F	F
F	T	T
F	F	T

추론 시스템 (Inference System)

- Inference rules

$$\frac{A \qquad B}{A \wedge B}\wedge\mathrm{I} \qquad \frac{A \wedge B}{A}\wedge\mathrm{E_L} \qquad \frac{A \wedge B}{B}\wedge\mathrm{E_R}$$

$$\begin{array}{c}\overline{A}\\ \vdots \\ B \\ \hline A \supset B\end{array}\supset\mathrm{I} \qquad \frac{A \supset B \qquad A}{B}\supset\mathrm{E}$$

- Axioms

$$\frac{}{A \vee \neg A}\mathrm{EM}$$

모델 vs 추론 시스템

A	B	$B \supset A$	$A \supset (B \supset A)$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	T	T

$$\dfrac{\dfrac{\overline{A}^{y} \qquad \dfrac{\overline{B}^{x}}{\textit{(not used in the proof)}}}{B \supset A} \supset\mathrm{I}^{x}}{A \supset (B \supset A)} \supset\mathrm{I}^{y}$$

Classical Logic

- Concerned with:
  - "whether a given proposition is true or not."
- Logic from God's point of view
  - Every proposition is either true or false.
- Tautologies in classical logic

$A \vee \neg A$	Law of Excluded Middle
$\neg\neg A \supset A$	Double-negation elimination
$((A \supset B) \supset A) \supset A$	Peirce's law

Intuitionistic Logic

- Concerned with:
  - "how a given proposition becomes true."
- Logic from a human's point of view
  - we know only what we can prove.
- Not true in intuitionistic logic (for all *A* and *B*)

$A \vee \neg A$	Law of Excluded Middle
$\neg\neg A \supset A$	Double-negation elimination
$((A \supset B) \supset A) \supset A$	Peirce's law

Classical vs Intuitionistic

- Do you agree that for any two statements the first implies the second or the second implies the first?
  - 예:
    - first statement: "달에는 계수나무와 토끼가 있다"
    - second statement: "P = NP"
  - Yes?
  - No?

Logic of BI

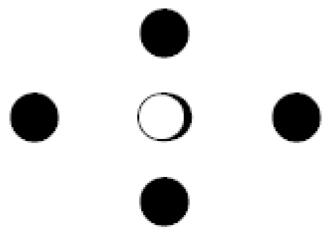
Separation Logic

- Hoare logic의 결점을 극복하는 논리체계
  - precondition, postcondition

$$\{x + 1 \leq N\}\ x := x + 1\ \{x \leq N\}$$

  - local reasoning on resources (esp., pointers)

$$\frac{\{P\}C\{Q\}}{\{P * R\}C\{Q * R\}}\ \text{Frame Rule}^{*}$$



- Ever increasing number of applications
  - E.g., Chang and Rival [POPL2008], Chin et al. [POPL2008], Parkinson and Bierman [POPL2008]

* O'Hearn CAV Tutorial, Princeton, July 2008

Logic of BI

- Logic of Bunched Implications (O'Hearn and Pym)
  - additive connectives
    - >, ?, :, Æ, Ç, !
    - either classically or intuitionistically
  - multiplicative connectives
    - *, -*
    - A * B : resource A and resource B
    - A -* B : resource A를 주면 resource B를 만든다

Separation Logic vs Logic of BI

- Separation Logic의 core = BI의 친척
  where
  - a **model** of BI based on pointers and heaps
  - additive connectives are interpreted **classically**
- Cf. *“Separation logic”* = *“BI's pointer logic”*

- 모델 vs 추론 시스템
) Separation logic vs Logic of BI

A	B	$B \supset A$	$A \supset (B \supset A)$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	T	T

$$\dfrac{\dfrac{\overline{A}^{y} \quad \overset{\overline{B}^{x}}{\text{(not used in the proof)}}}{B \supset A}\supset\mathrm{I}^{x}}{A \supset (B \supset A)}\supset\mathrm{I}^{y}$$

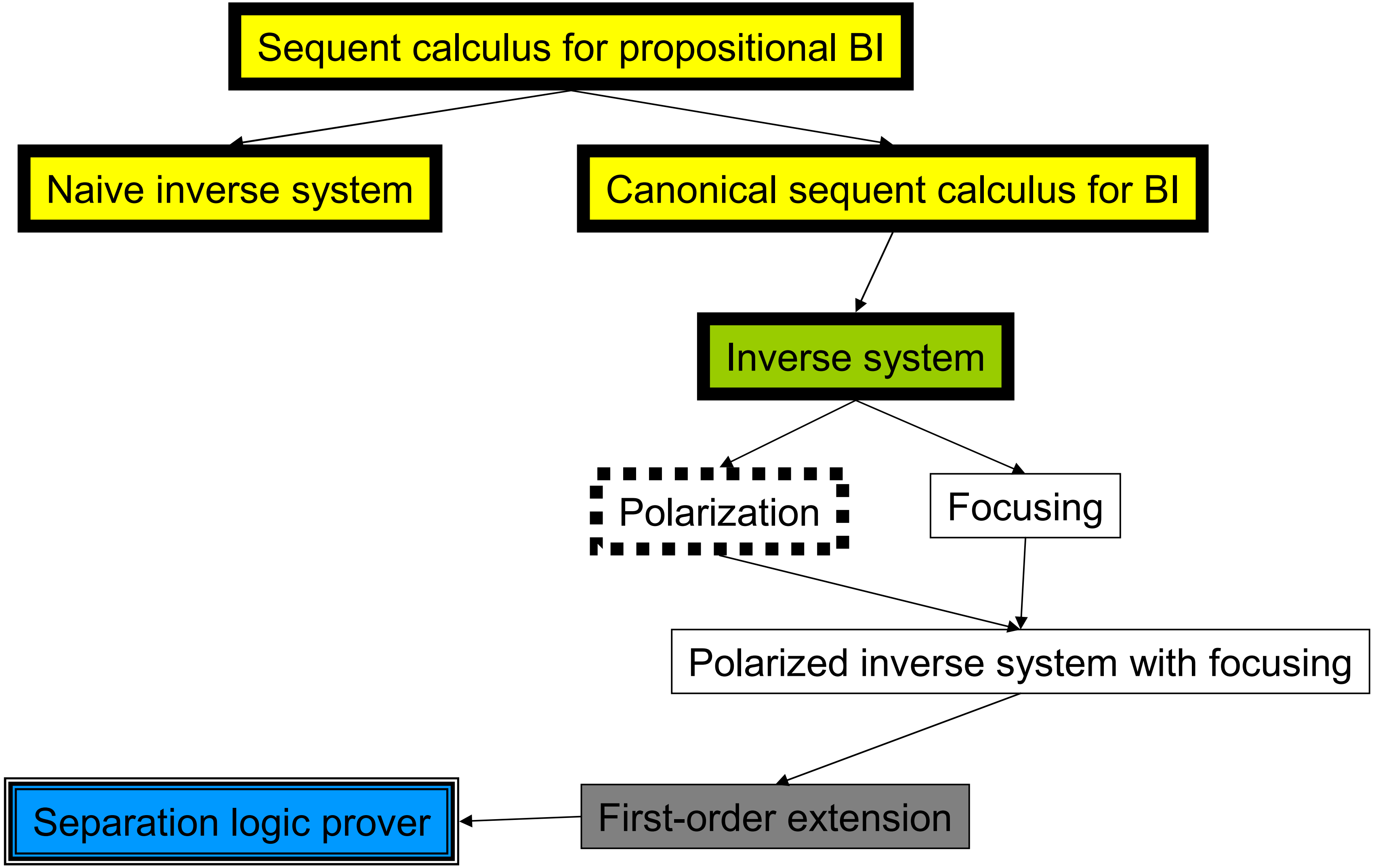
Prover for BI

$$(p * (q \wedge r)) \mathrel{-\!\!*} ((p * q) \wedge (p * r))$$

BI Prover

- 기존의 Prover (not very practical)
  – BILL (Galmiche and Mery, 2003)
    - Tableaux method
    - 증명 불가능하면 counter-model을 제시함
  – Inverse prover (Donnelly et al, 2004)
    - Proof theory를 이용한 prover
- Ideally a prover for (full first-order) BI
  – ¼ prover for separation logic
    - 프로그램 분석에 유용할 수 있음
  – fun to develop

Roadmap


Sequent calculus for propositional BI
Naive inverse system
Canonical sequent calculus for BI
Inverse system
Polarization
Focusing
Polarized inverse system with focusing
First-order extension
Separation logic prover

Sequent Calculus for BI

$$
\begin{array}{cccl}
\text{propositions} & A, B, C, \cdots & ::= & P \mid \top \mid \mathsf{I} \mid A \supset A \mid A \wedge A \mid A \mathrel{-\!\!\star} A \mid A \star A \mid A \vee A \\
\text{bunches} & \Gamma & ::= & A \mid \emptyset_{\mathsf{a}} \mid \emptyset_{\mathsf{m}} \mid \Gamma ; \Gamma \mid \Gamma , \Gamma \\
\text{contexts} & \gamma & ::= & [] \mid \Gamma ; \gamma \mid \Gamma , \gamma
\end{array}
$$

$$
\frac{\Gamma \longmapsto C \quad \Gamma \equiv \Gamma'}{\Gamma' \longmapsto C}\ E \qquad \frac{}{A \longmapsto A}\ \mathit{Init} \qquad \frac{\gamma(\Gamma) \longmapsto C}{\gamma(\Gamma ; \Gamma') \longmapsto C}\ \mathsf{W} \qquad \frac{\gamma(\Gamma ; \Gamma) \longmapsto C}{\gamma(\Gamma) \longmapsto C}\ \mathsf{C}
$$

$$
\frac{\gamma(\emptyset_{\mathsf{a}}) \longmapsto C}{\gamma(\top) \longmapsto C}\ \top L \qquad \frac{}{\emptyset_{\mathsf{a}} \longmapsto \top}\ \top R \qquad \frac{\gamma(\emptyset_{\mathsf{m}}) \longmapsto C}{\gamma(\mathsf{I}) \longmapsto C}\ \mathsf{I} L \qquad \frac{}{\emptyset_{\mathsf{m}} \longmapsto \mathsf{I}}\ \mathsf{I} R
$$

$$
\frac{\Gamma \longmapsto A \quad \gamma(\Gamma' ; B) \longmapsto C}{\gamma(\Gamma ; \Gamma' ; A \supset B) \longmapsto C}\ {\supset} L \qquad \frac{\Gamma ; A \longmapsto B}{\Gamma \longmapsto A \supset B}\ {\supset} R \qquad \frac{\gamma(A ; B) \longmapsto C}{\gamma(A \wedge B) \longmapsto C}\ {\wedge} L \qquad \frac{\Gamma \longmapsto A \quad \Gamma' \longmapsto B}{\Gamma ; \Gamma' \longmapsto A \wedge B}\ {\wedge} R
$$

$$
\frac{\gamma(A) \longmapsto C \quad \gamma(B) \longmapsto C}{\gamma(A \vee B) \longmapsto C}\ {\vee} L \qquad \frac{\Gamma \longmapsto A}{\Gamma \longmapsto A \vee B}\ {\vee} R_L \qquad \frac{\Gamma \longmapsto B}{\Gamma \longmapsto A \vee B}\ {\vee} R_R
$$

$$
\frac{\Gamma \longmapsto A \quad \gamma(\Gamma' , B) \longmapsto C}{\gamma(\Gamma , \Gamma' , A \mathrel{-\!\!\star} B) \longmapsto C}\ {-\!\!\star} L \qquad \frac{\Gamma , A \longmapsto B}{\Gamma \longmapsto A \mathrel{-\!\!\star} B}\ {-\!\!\star} R \qquad \frac{\gamma(A , B) \longmapsto C}{\gamma(A \star B) \longmapsto C}\ {\star} L \qquad \frac{\Gamma \longmapsto A \quad \Gamma' \longmapsto B}{\Gamma , \Gamma' \longmapsto A \star B}\ {\star} R
$$

Canonical BI

$$\frac{}{A \Longrightarrow A}\ Init \quad \frac{\phi[\![\Psi]\!] \Longrightarrow C}{\phi[\![\Psi;\Psi']\!] \Longrightarrow C}\ \mathsf{W} \quad \frac{\phi[\![\emptyset_{\mathsf{a}}]\!] \Longrightarrow C}{\phi[\![\Psi']\!] \Longrightarrow C}\ \mathsf{W} \quad \frac{\phi[\![\Psi;\Psi]\!] \Longrightarrow C}{\phi[\![\Psi]\!] \Longrightarrow C}\ \mathsf{C}$$

$$\frac{\phi[\![\emptyset_{\mathsf{a}}]\!] \Longrightarrow C}{\phi[\![\top]\!] \Longrightarrow C}\ \top L \quad \frac{}{\emptyset_{\mathsf{a}} \Longrightarrow \top}\ \top R \quad \frac{\phi[\![\emptyset_{\mathsf{m}}]\!] \Longrightarrow C}{\phi[\![\mathsf{I}]\!] \Longrightarrow C}\ \mathsf{I}L \quad \frac{}{\emptyset_{\mathsf{m}} \Longrightarrow \mathsf{I}}\ \mathsf{I}R$$

$$\frac{\Psi \Longrightarrow A \quad \phi[\![\Psi';B]\!] \Longrightarrow C}{\phi[\![\Psi;\Psi';A \supset B]\!] \Longrightarrow C}\ \supset L \quad \frac{\emptyset_{\mathsf{a}} \Longrightarrow A \quad \phi[\![\Psi';B]\!] \Longrightarrow C}{\phi[\![\Psi';A \supset B]\!] \Longrightarrow C}\ \supset L \quad \frac{\Psi \Longrightarrow A \quad \phi[\![B]\!] \Longrightarrow C}{\phi[\![\Psi;A \supset B]\!] \Longrightarrow C}\ \supset L \quad \frac{\emptyset_{\mathsf{a}} \Longrightarrow A \quad \phi[\![B]\!] \Longrightarrow C}{\phi[\![A \supset B]\!] \Longrightarrow C}\ \supset L$$

$$\frac{\Psi; A \Longrightarrow B}{\Psi \Longrightarrow A \supset B}\ \supset R \quad \frac{A \Longrightarrow B}{\emptyset_{\mathsf{a}} \Longrightarrow A \supset B}\ \supset R$$

$$\frac{\phi[\![A;B]\!] \Longrightarrow C}{\phi[\![A \wedge B]\!] \Longrightarrow C}\ \wedge L$$

$$\frac{\Psi \Longrightarrow A \quad \Psi' \Longrightarrow B}{\Psi;\Psi' \Longrightarrow A \wedge B}\ \wedge R \quad \frac{\Psi \Longrightarrow A \quad \emptyset_{\mathsf{a}} \Longrightarrow B}{\Psi \Longrightarrow A \wedge B}\ \wedge R \quad \frac{\emptyset_{\mathsf{a}} \Longrightarrow A \quad \Psi' \Longrightarrow B}{\Psi' \Longrightarrow A \wedge B}\ \wedge R \quad \frac{\emptyset_{\mathsf{a}} \Longrightarrow A \quad \emptyset_{\mathsf{a}} \Longrightarrow B}{\emptyset_{\mathsf{a}} \Longrightarrow A \wedge B}\ \wedge R$$

$$\frac{\phi[\![A]\!] \Longrightarrow C \quad \phi[\![B]\!] \Longrightarrow C}{\phi[\![A \vee B]\!] \Longrightarrow C}\ \vee L$$

$$\frac{\Phi \Longrightarrow A}{\Phi \Longrightarrow A \vee B}\ \vee R_L \quad \frac{\Phi \Longrightarrow B}{\Phi \Longrightarrow A \vee B}\ \vee R_R$$

$$\frac{\Delta \Longrightarrow A \quad \phi[\Delta', B]\!] \Longrightarrow C}{\phi[\![\Delta,\Delta',A -\!\!\star B]\!] \Longrightarrow C}\ -\!\!\star L \quad \frac{\emptyset_{\mathsf{m}} \Longrightarrow A \quad \phi[\![\Delta', B]\!] \Longrightarrow C}{\phi[\![\Delta',A -\!\!\star B]\!] \Longrightarrow C}\ -\!\!\star L \quad \frac{\Delta \Longrightarrow A \quad \phi[\![B]\!] \Longrightarrow C}{\phi[\![\Delta,A -\!\!\star B]\!] \Longrightarrow C}\ -\!\!\star L \quad \frac{\emptyset_{\mathsf{m}} \Longrightarrow A \quad \phi[\![B]\!] \Longrightarrow C}{\phi[\![A -\!\!\star B]\!] \Longrightarrow C}\ -\!\!\star L$$

$$\frac{\Delta, A \Longrightarrow B}{\Delta \Longrightarrow A -\!\!\star B}\ -\!\!\star R \quad \frac{A \Longrightarrow B}{\emptyset_{\mathsf{m}} \Longrightarrow A -\!\!\star B}\ -\!\!\star R$$

$$\frac{\phi[\![A,B]\!] \Longrightarrow C}{\phi[\![A \star B]\!] \Longrightarrow C}\ \star L$$

$$\frac{\Delta \Longrightarrow A \quad \Delta' \Longrightarrow B}{\Delta,\Delta' \Longrightarrow A \star B}\ \star R \quad \frac{\Delta \Longrightarrow A \quad \emptyset_{\mathsf{m}} \Longrightarrow B}{\Delta \Longrightarrow A \star B}\ \star R \quad \frac{\emptyset_{\mathsf{m}} \Longrightarrow A \quad \Delta' \Longrightarrow B}{\Delta' \Longrightarrow A \star B}\ \star R \quad \frac{\emptyset_{\mathsf{m}} \Longrightarrow A \quad \emptyset_{\mathsf{m}} \Longrightarrow B}{\emptyset_{\mathsf{m}} \Longrightarrow A \star B}\ \star R$$

Inverse System

Strictly weakening rules

$$\frac{\phi[\Omega] \Longrightarrow C}{\phi[\Omega;\Psi] \Longrightarrow C}\,\mathsf{W}_1 \quad \frac{\emptyset_{\mathsf{m}} \Longrightarrow C}{\emptyset_{\mathsf{m}};\Psi \Longrightarrow C}\,\mathsf{W}_2 \quad \frac{\phi[\Omega] \Longrightarrow C}{\phi[\Omega,(\emptyset_{\mathsf{m}};\Psi)] \Longrightarrow C}\,\mathsf{W}_3 \quad \frac{\phi[\emptyset_{\mathsf{a}}] \Longrightarrow C}{\phi[\Omega] \Longrightarrow C}\,\mathsf{W}_4 \quad \frac{\emptyset_{\mathsf{a}} \Longrightarrow C}{\emptyset_{\mathsf{m}} \Longrightarrow C}\,\mathsf{W}_5 \quad \frac{\phi[\Omega] \Longrightarrow C}{\phi[\Omega,\mathsf{I}] \Longrightarrow C}\,\mathsf{I}L_2$$

Strictly contracting rules

$$\frac{\phi[\Omega,\emptyset_{\mathsf{a}}] \Longrightarrow C}{\phi[\Omega] \Longrightarrow C}\,\mathsf{W}_6 \quad \frac{\phi[\phi_{\mathsf{am}}[\emptyset_{\mathsf{a}},\emptyset_{\mathsf{a}}]] \Longrightarrow C}{\phi[\emptyset_{\mathsf{m}}] \Longrightarrow C}\,\mathsf{W}_7 \quad \frac{\phi[\Omega,\phi_{\mathsf{am}}[\emptyset_{\mathsf{a}},\emptyset_{\mathsf{a}}]] \Longrightarrow C}{\phi[\Omega] \Longrightarrow C}\,\mathsf{W}_8 \quad \frac{\emptyset_{\mathsf{a}},\phi_{\mathsf{mm}}[\emptyset_{\mathsf{a}}] \Longrightarrow C}{\emptyset_{\mathsf{a}} \Longrightarrow C}\,\mathsf{W}_9$$

$$\frac{\phi[\Omega;(\emptyset_{\mathsf{a}},\phi_{\mathsf{mm}}[\emptyset_{\mathsf{a}}])] \Longrightarrow C}{\phi[\Omega] \Longrightarrow C}\,\mathsf{W}_{10} \quad \frac{\phi[\Omega;\Omega] \Longrightarrow C}{\phi[\Omega] \Longrightarrow C}\,\mathsf{C}_1 \quad \frac{\phi[\phi_{\mathsf{mm}}[\emptyset_{\mathsf{m}};\emptyset_{\mathsf{m}}]] \Longrightarrow C}{\phi[\emptyset_{\mathsf{m}}] \Longrightarrow C}\,\mathsf{C}_2 \quad \frac{\phi[\Omega,\phi_{\mathsf{mm}}[\emptyset_{\mathsf{m}};\emptyset_{\mathsf{m}}]] \Longrightarrow C}{\phi[\Omega] \Longrightarrow C}\,\mathsf{C}_3$$

$$\frac{\emptyset_{\mathsf{a}},\phi_{\mathsf{mm}}[\emptyset_{\mathsf{m}};\emptyset_{\mathsf{m}}] \Longrightarrow C}{\emptyset_{\mathsf{a}} \Longrightarrow C}\,\mathsf{C}_4 \quad \frac{\phi[\Omega;(\emptyset_{\mathsf{a}},\phi_{\mathsf{mm}}[\emptyset_{\mathsf{m}};\emptyset_{\mathsf{m}}])] \Longrightarrow C}{\phi[\Omega] \Longrightarrow C}\,\mathsf{C}_5$$

Rules without premisses

$$\frac{}{A \Longrightarrow A}\,Init \quad \frac{}{\emptyset_{\mathsf{a}} \Longrightarrow \top}\,\top R \quad \frac{}{\emptyset_{\mathsf{m}} \Longrightarrow \mathsf{I}}\,\mathsf{I}R$$

Non-focusing rules

$$\frac{\Psi \Longrightarrow A \quad \Psi' \Longrightarrow B}{\Psi;\Psi' \Longrightarrow A \wedge B}\,\wedge R \quad \frac{\Psi \Longrightarrow A \quad \emptyset_{\mathsf{a}} \Longrightarrow B}{\Psi \Longrightarrow A \wedge B}\,\wedge R \quad \frac{\emptyset_{\mathsf{a}} \Longrightarrow A \quad \Psi' \Longrightarrow B}{\Psi' \Longrightarrow A \wedge B}\,\wedge R \quad \frac{\emptyset_{\mathsf{a}} \Longrightarrow A \quad \emptyset_{\mathsf{a}} \Longrightarrow B}{\emptyset_{\mathsf{a}} \Longrightarrow A \wedge B}\,\wedge R$$

$$\frac{\Phi \Longrightarrow A}{\Phi \Longrightarrow A \vee B}\,\vee R_L \quad \frac{\Phi \Longrightarrow B}{\Phi \Longrightarrow A \vee B}\,\vee R_R$$

$$\frac{\Delta \Longrightarrow A \quad \Delta' \Longrightarrow B}{\Delta,\Delta' \Longrightarrow A \star B}\,\star R \quad \frac{\Delta \Longrightarrow A \quad \emptyset_{\mathsf{m}} \Longrightarrow B}{\Delta \Longrightarrow A \star B}\,\star R \quad \frac{\emptyset_{\mathsf{m}} \Longrightarrow A \quad \Delta' \Longrightarrow B}{\Delta' \Longrightarrow A \star B}\,\star R \quad \frac{\emptyset_{\mathsf{m}} \Longrightarrow A \quad \emptyset_{\mathsf{m}} \Longrightarrow B}{\emptyset_{\mathsf{m}} \Longrightarrow A \star B}\,\star R$$

Atomic focusing rules

$$\frac{\Psi \Longrightarrow A \quad \phi[B] \Longrightarrow C}{\phi[\Psi;A \supset B] \Longrightarrow C}\,\supset L \quad \frac{\emptyset_{\mathsf{a}} \Longrightarrow A \quad \phi[B] \Longrightarrow C}{\phi[A \supset B] \Longrightarrow C}\,\supset L \quad \frac{\Delta \Longrightarrow A \quad \phi[B] \Longrightarrow C}{\phi[\Delta, A \mathrel{-\!\!\ast} B] \Longrightarrow C}\,\mathrel{-\!\!\ast} L \quad \frac{\emptyset_{\mathsf{m}} \Longrightarrow A \quad \phi[B] \Longrightarrow C}{\phi[A \mathrel{-\!\!\ast} B] \Longrightarrow C}\,\mathrel{-\!\!\ast} L$$

$$\frac{A \Longrightarrow B}{\emptyset_{\mathsf{a}} \Longrightarrow A \supset B}\,\supset R \quad \frac{A \Longrightarrow B}{\emptyset_{\mathsf{m}} \Longrightarrow A \mathrel{-\!\!\ast} B}\,\mathrel{-\!\!\ast} R$$

Double-atomic focusing rule

$$\frac{\phi[A] \Longrightarrow C \quad \phi[B] \Longrightarrow C}{\phi[A \vee B] \Longrightarrow C}\,\vee L$$

Additive focusing rules

$$\frac{\Psi \Longrightarrow A \quad \phi[\Psi';B] \Longrightarrow C}{\phi[\Psi;\Psi';A \supset B] \Longrightarrow C}\,\supset L \quad \frac{\emptyset_{\mathsf{a}} \Longrightarrow A \quad \phi[\Psi';B] \Longrightarrow C}{\phi[\Psi';A \supset B] \Longrightarrow C}\,\supset L \quad \frac{\phi[A;B] \Longrightarrow C}{\phi[A \wedge B] \Longrightarrow C}\,\wedge L \quad \frac{\Psi;A \Longrightarrow B}{\Psi \Longrightarrow A \supset B}\,\supset R$$

감사합니다.