소프트웨어 개발에서 중요한 질문

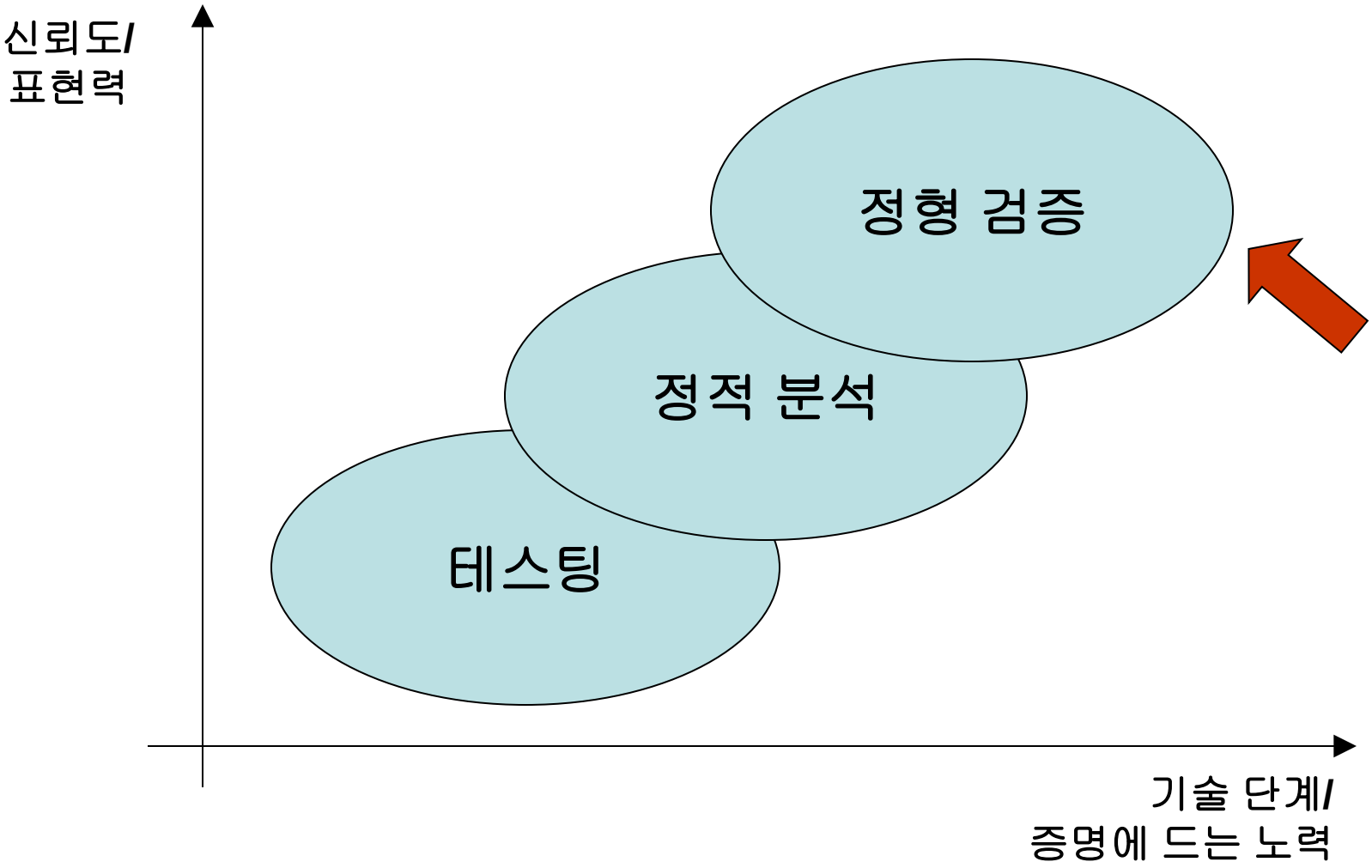
소프트웨어의

오류의 위치를 찾아주거나
오류가 없음을 확인해 주는

자동화된 도구가 있을까?

- 테스팅(testing)
- 정적 분석 (static nalysis)
- 정형 검증 (formal verification)

기술 지도



정형 검증 (Formal Verification)

- 장단점

  [+] 높은 신뢰도

  - 증명 (formal proof) 생성됨

  [+] Functional correctness까지 증명할 수 있음

  - "The program correctly sorts a given array.“

  [-] 사용하기 위해서 전문 지식이 필요함

- Hoare 논리 체계의 한계
- 분리 논리 (separation logic) 등장으로 반전

분리논리 (Separation Logic)

- A Logic for Shared Mutable Data Structures [Reynolds 2002]
  - 힙(메모리 할당)을 다루는 프로그램 분석에 적합
  - supports local reasoning

$$\frac{\{A\}\ \text{Program}\ \{B\}}{\{A \star C\}\ \text{Program}\ \{B \star C\}}$$

where Program does not access variables in C

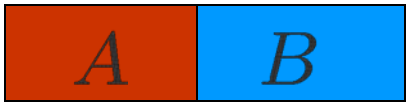
- 분리논리를 이용한 프로그램 검증도구
  - Smallfoot, Space Invader, THOR, SLAyer, HIP, VeriFast, jStar, Xisa, SeLoger, SLP, ...
  - Facebook의 Monoidics 합병
  - but focus only on separating conjunction $\star$.

분리논리 연산자

- Separating conjunction

$$A \star B$$

  - The current heap can be partitioned into two separate heaps;
  - A holds for one, and B holds for the other.



- Separating implication

$$A \mathrel{-\!\!\star} B$$

  - If the current heap is extended with a separate heap for which A holds,
  - then B holds for the combined heap.

  - 마법봉 (magic wand)

마법봉 연산자의 마력 $-\!\!\star$

- Schorr-Waite algorithm [Yang 2001]

$$
\begin{aligned}
&preLoopInvR(Stack, P, T, STree, root)\\
&\quad\equiv\ noDanglingR \wedge noDangling(T) \wedge noDangling(P)\\
&\qquad \wedge listMarkedNodesR(Stack, P) * (restoredListR(Stack, T) -\!\!* spansR(STree, root))\\
&\qquad \wedge markedR * \begin{pmatrix} unmarkedR \\ \wedge\ (\forall x.\ allocated(x) \rightarrow (reach(T, x) \vee reachRightChildInList(Stack, x))) \end{pmatrix}
\end{aligned}
$$

- Reasoning about iterators [Krishnaswami 2006]

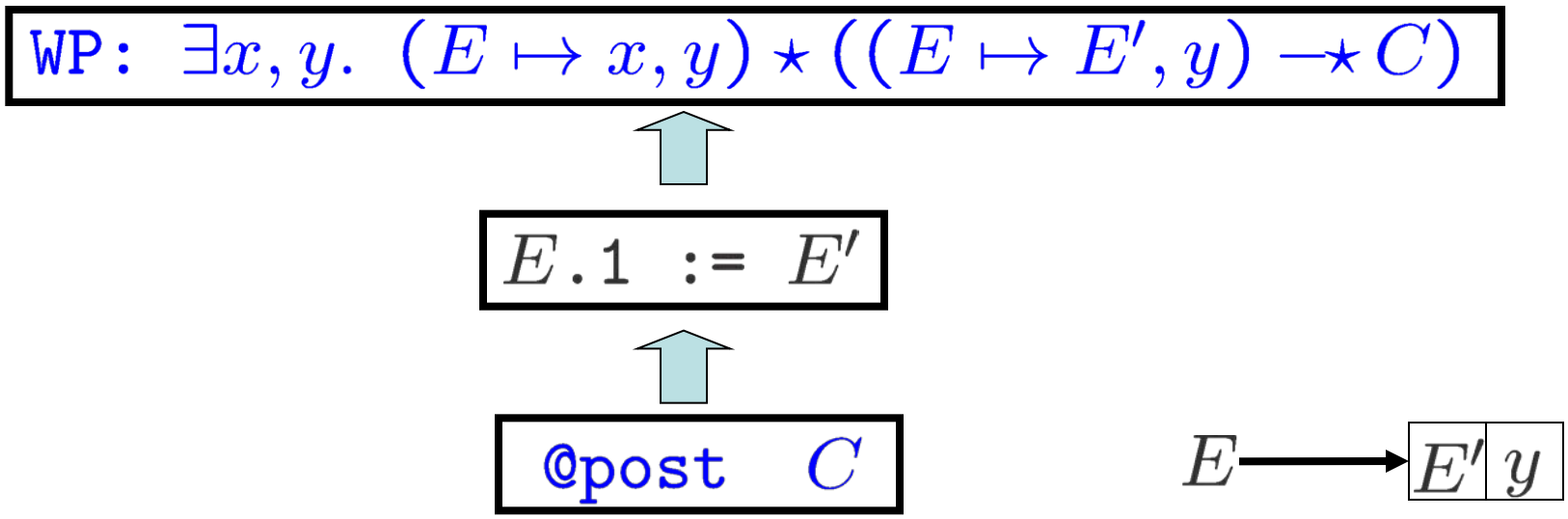
$$
\begin{aligned}
iter(i, c, xs, P) \supset [&coll(c, xs, P) * \\
&coll(c, xs, P) -\!\!* iter(i, c, xs, P)]
\end{aligned}
$$

- Ramification of sharing [Hobor and Villard 2013]

$$ramify(R, P, Q, R') \stackrel{\text{def}}{=} R \vdash P \mathbin{\text{-}\!\!\star} (Q \mathbin{\text{-}\!\!\star} R')$$

왜 마법봉 연산자가 필수적인가?

- 완전한 프로그램 검증 시스템 구현에 필수
  - weakest precondition 이용한 역방향 추론에 필수

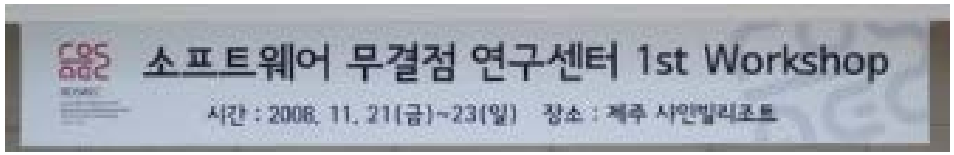


P_{SL} (Proof system for Separation Logic)

- 분리논리 증명체계
  - with separating conjunction $\star$
  - **also with magic wand** $-\!\!\star$
- Boolean BI 연구 연장
  - "A Theorem Prover for Boolean BI" [Park et al 2013]
- Sequent calculus 스타일
  - admissibility of cut
  - sound and complete

이야기의 시작은 2008년으로…

1회 2008.11 제주 샤인빌리조트



POSTECH PL 연구분야 소개

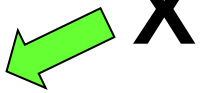
박성우

ROSAEC Kick-off Workshop

2008년 11월 22일

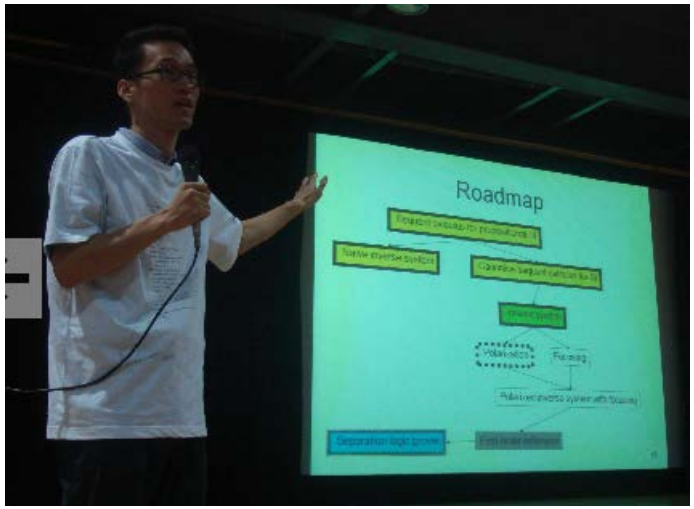
Theorem Prover for BI

- 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

2회 2009.7 지지향

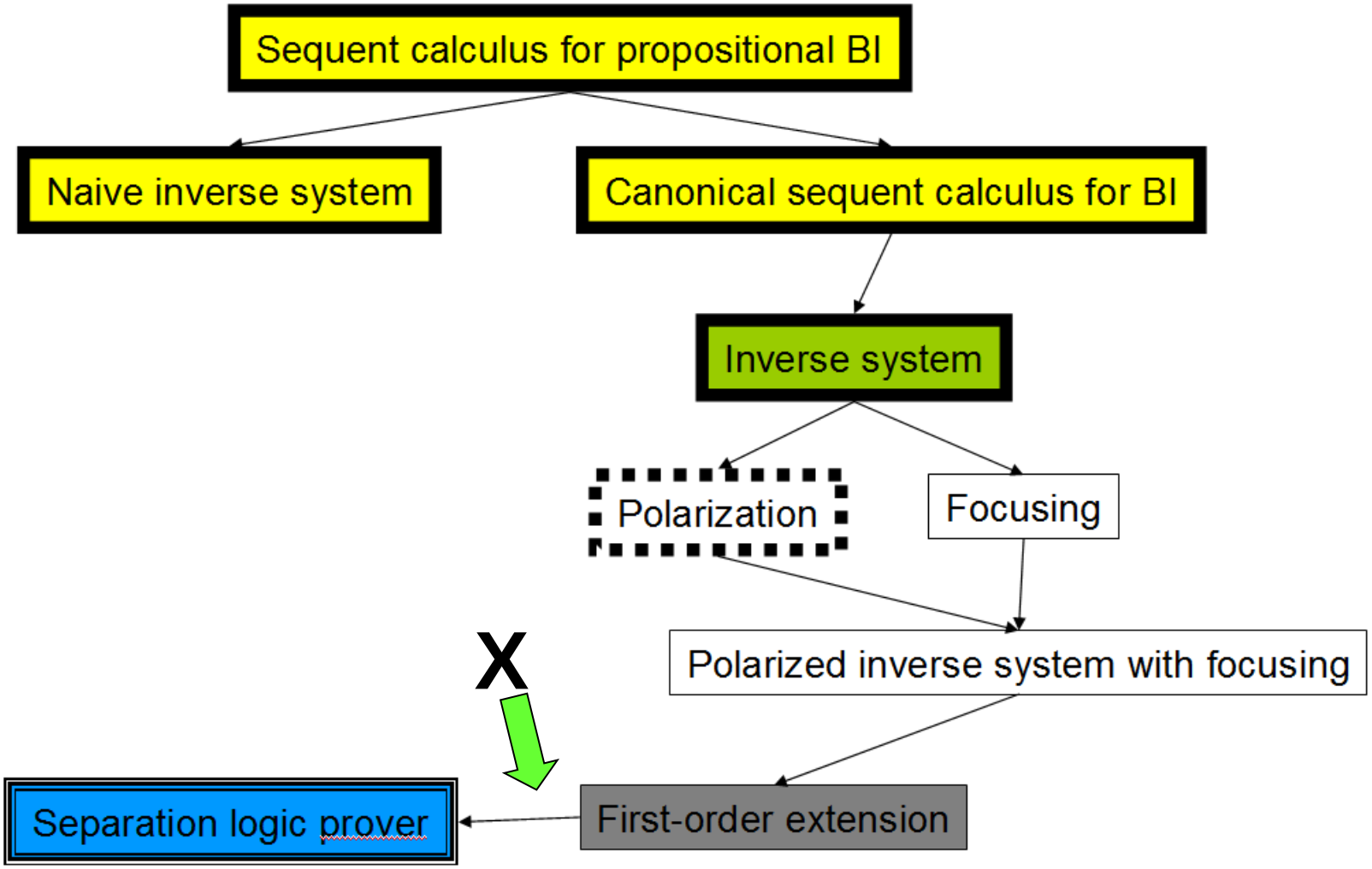


BI 논리체계 증명기 개발

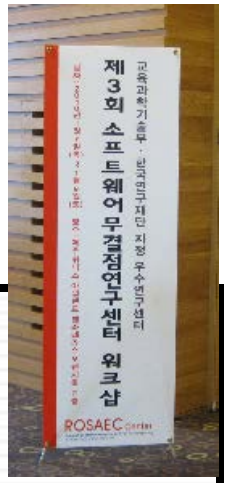
박성우

ROSAEC Workshop
2009년 7월 11일

Roadmap


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

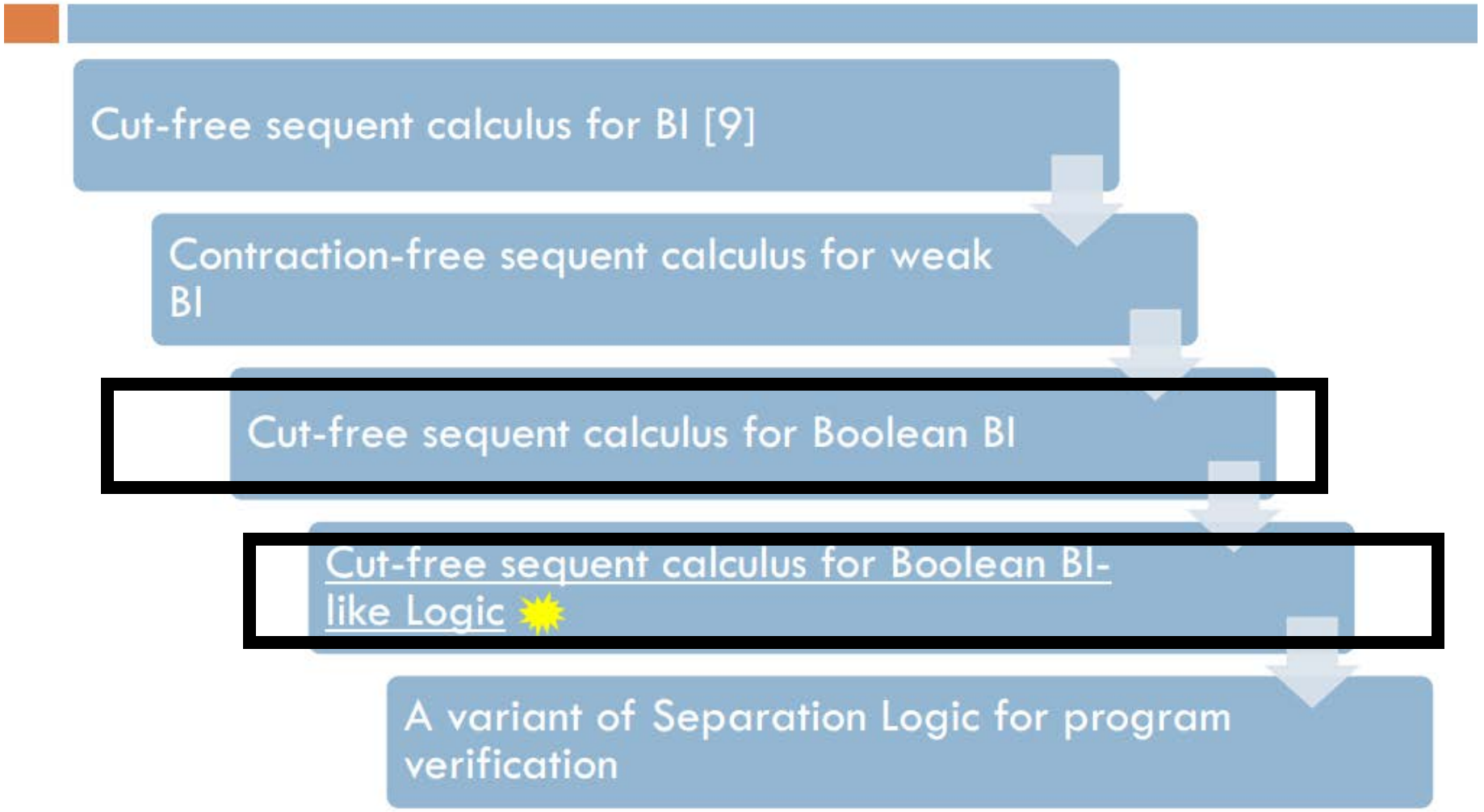
3회 2010.1 제주 피닉스아일랜드



A deductive verification tool for realistic programs

ROSEAC 2010 Workshop @ Jeju
POSTECH Programming Language Laboratory
Jonghyun Park

Current roadmap



4회 2010.8 설악산 대명콘도

A Theory of Non-associative Classical BI

포항공과대학교 프로그래밍 언어 연구실 박종현

진행 상황 (~2010. 08)

직관 BI 논리를 위한 컷 제거 귀추 계산법 연구

자동 정리 증명에 적합한 변형된 직관 BI 논리 개발

비결합적 고전 BI 논리를 위한 컷 제거 귀추 계산법 개발

분리 논리를 위한 자동 정리 증명기 개발

분리 논리에 기반한 연역 검증 도구 개발

Towards a Cut-free Sequent Calculus for Boolean BI

(A Cut-free Sequent Calculus for Non-associative Classical BI)

Sungwoo Park and Jonghyun Park
Pohang University of Science and Technology
Korea

PSPL 2010

July 10, 2010

Conclusion

- Cut-free sequent calculus for non-associative classical BI
  - additive connectives: classical
  - multiplicative connectives: classical
- Perhaps no cut-free sequent calculus for boolean BI

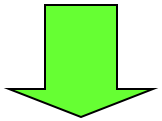
- *"Interpreting multiplicative connectives intuitionistically?"*
- Application of the logic?

Boolean BI 연구 포기

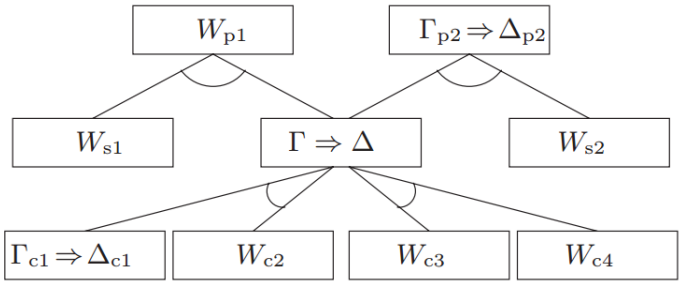
그러던 2010년 12월 어느날…

Breakthrough by 박종현

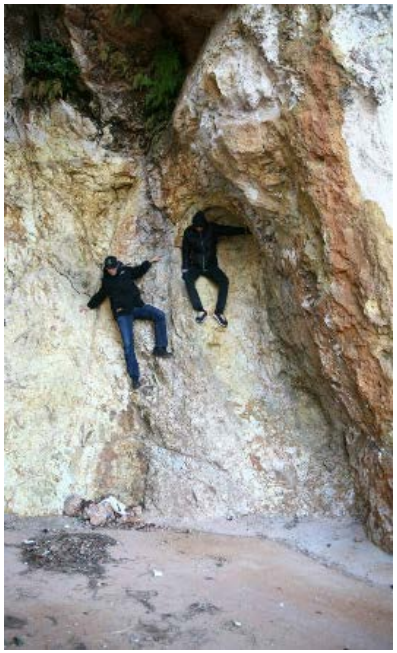
formula	$A, B, C, \cdots$	$::=$	$P \mid \top \mid \mathsf{I} \mid \bot \mid A \supset A \mid A \wedge A \mid A \mathrel{-\!\!\star} A \mid A \star A$
boolean bunches	Δ	$::=$	$A \mid \emptyset_{\mathsf{a}} \mid \emptyset_{\mathsf{m}} \mid \Delta;\Delta \mid W, W$
falsehood context	Ψ	$::=$	$\cdot \mid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



sequent	W	$=$	$\Gamma \Rightarrow \Delta$
truth context	Γ	$::=$	$\cdot \mid \Gamma; S$
falsehood context	Δ	$::=$	$\cdot \mid \Delta; A$
node state	S	$::=$	$A \mid \emptyset_{\mathsf{m}} \mid W, W \mid W \langle\langle W \rangle\rangle$



5회 2011.1 통영 금호마리나리조트



Boolean BI 논리를 위한 컷-제거 귀추 계산법

박종현, 박성우
POSTECH

소프트웨어무결점연구센터 워크샵
2011년 1월 7일

Boolean BI 컷-제거 귀추 계산법 완성

- 컷-제거 증명

$$If\ \omega[\Gamma \longrightarrow_{\mathsf{B}} \Delta; C]\ and\ \omega'[\Gamma'; C \longrightarrow_{\mathsf{B}} \Delta'],\ then\ \Gamma; \Gamma'; \Gamma_{\omega}; \Gamma_{\omega'} \longrightarrow_{\mathsf{B}} \Delta; \Delta'$$

- 비결합적 **classical BI**에 비해서
  - 정의가 더 간단
  - 컷-제거 증명이 더 간단
- 현재 진행 중
  - 컷-제거 증명 확인
  - **Boolean BI** 논리와의 관계 확인
  - 양 **20%** vs 질 **80%**

6회 2011.6 지지향

Boolean BI를 위한 중첩 구조를 이용한 귀추 계산법

POSTECH 프로그래밍 언어 연구실 박종현

무결점 음악회

- 서울대, 이승중, 피아노 [이루마 Indigo]
- 한양대, 최민영, 기타
  [오아시스 Wonder wall, 원스 OST Falling slowly]
- KAIST, 김지응, 클라리넷
- KAIST, 배성경, 만돌린, [박정현 이젠 그랬으면 좋겠어]

- KAIST, 김지응, 피아노
  경북대, 박민규, 기타
  서울대, 이원찬, 드럼
  } Canon

- 한양대, 도경구 교수님, 색소폰, My way, 베사메무쵸

무결점 나가수

- 서울대, 최원태, 담배가게아가씨
- 서울대, 정영범, 오래된 노래
- 서울대, 이원찬, 비상
- KAIST, 나현익, 고속도로 로망스
- KAIST, 허우람, 너를 위해
- POSTECH, 노한얼, Good Life
- 경북대, 박민규, 응급실
- POSTECH, Martin/Daniel/박진우/김동원,
  Starlight Moonlight

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

I am sorry to inform you that …

```
Date: Mon,  3 Oct 2011 12:04:40 -0400 (EDT)
From: POPL'12 PC Chair <mwh@cs.umd.edu>
To: Sungwoo Park <gla@postech.ac.kr>
Subject: [POPL 2012] Rejected paper #95 "Towards a Theorem Prover for Separation..."

    [ The following text is in the "utf-8" character set. ]
    [ Your display is set for the "EUC-KR" character set.  ]
    [ Some characters may be displayed incorrectly. ]

Dear Sungwoo Park,

I am sorry to inform you that your paper #95 has not been selected to
appear in the program of the 39th ACM SIGACT-SIGPLAN Symposium on
Principles of Programming Languages (POPL 2012)

       Title: Towards a Theorem Prover for Separation Logic (A Proof Theory
              for Boolean BI)
     Authors: Jonghyun Park (Pohang University of Science and Technology
              (POSTECH))
              Sungwoo Park (Pohang University of Science and Technology
              (POSTECH))
  Paper site: https://popl12.cs.umd.edu/paper.php?p=95

44 papers were accepted out of 201 submissions.
```

7회 2012.1 HKUST 홍콩

A Theorem Prover for Boolean BI

POSTECH 프로그래밍 언어 연구실
박종현 서정봉

5km 달리기

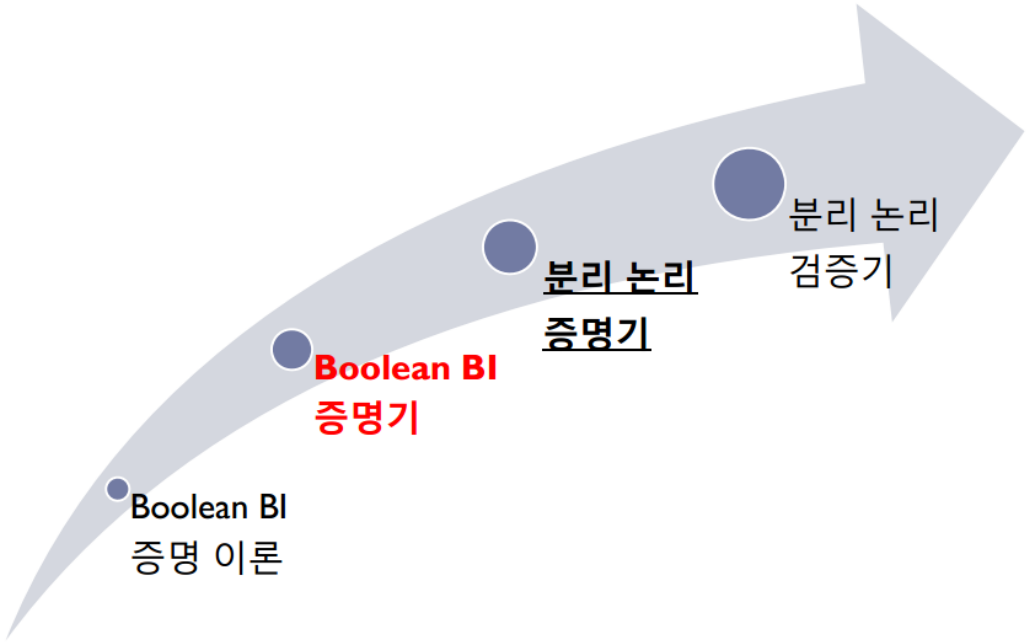
- 박진우 (22:04)
- 박봉주 (22:11)
- 김동원
- 이광근 교수님

- 완주: 황대연, Bui Hoang Duc, 한동균, 서현민, 김인, 이욱진 교수님, 이준, 도경구 교수님, 서정봉, *조소희*

결과는?

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

현재 단계 및 향후 계획



8회 2012.7 동원리더스아카데미

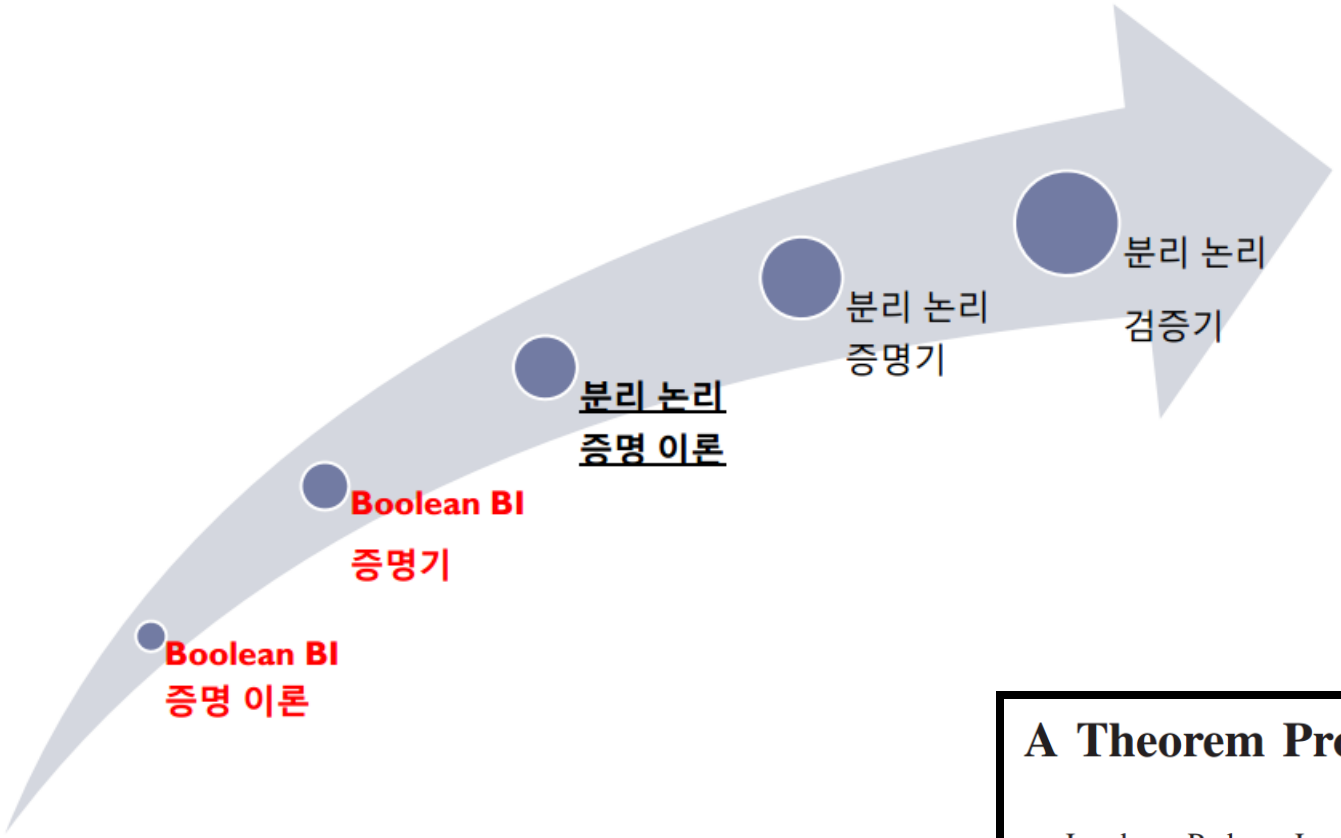
A Theorem Prover for Boolean BI

POSTECH 프로그래밍 언어 연구실
박종현

시연

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

진행 상황



A Theorem Prover for Boolean BI

Jonghyun Park Jeongbong Seo Sungwoo Park

Department of Computer Science and Engineering
Pohang University of Science and Technology (POSTECH)
Republic of Korea

{parjong,baramseo,gla}@postech.ac.kr

9회 2013.1 POSTECH

분리논리 자동정리증명기 개발
(A Theorem Prover for Separation Logic)

박성우
POSTECH

제9회 소프트웨어무결점연구센터 워크샵
2013년 1월 31일

CCeye: A Theorem Prover for Separation Logic

- 현재 설계 중

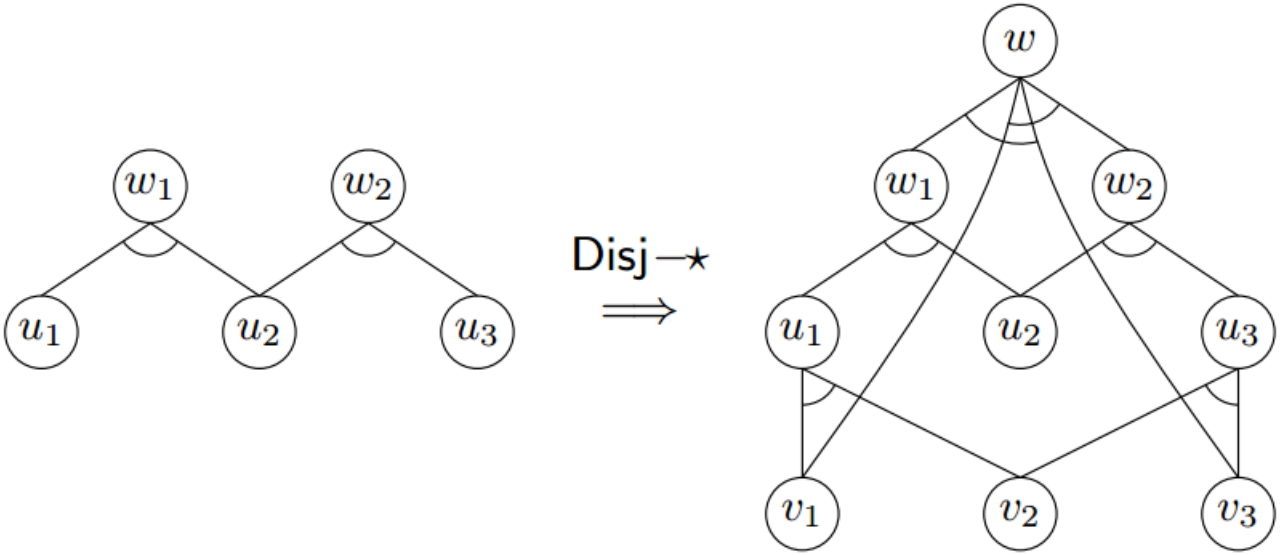
expression relation	θ	$::=$	$E = E' \mid E \neq E'$
expression relations	Θ	$=$	$\theta_1, \cdots, \theta_n$
heap variable	w, u, v		
heap relation	σ	$::=$	$w \doteq \epsilon \mid w \neq \epsilon \mid w \doteq [l \mapsto E] \mid$
			$w \neq [l \mapsto E] \mid w \doteq w' \circ w'' \mid w \doteq w'$
heap relations	Σ	$=$	$\sigma_1, \cdots, \sigma_n$
truth context	Γ	$::=$	$\cdot \mid \Gamma, A$
falsehood context	Δ	$::=$	$\cdot \mid \Delta, A$
heap sequent	$[\Gamma \Longrightarrow \Delta]^w$		
heap sequents	Π	$=$	$[\Gamma \Longrightarrow \Delta]^w, \cdots, [\Gamma' \Longrightarrow \Delta']^{w'}$
world description	$\Theta; \Sigma \parallel \Pi$		

- Challenge: Complexity 문제 처리

2013년 3월 이원열 등장

그냥 문제
던져주기만 하십시요

Breakthrough by 이원열



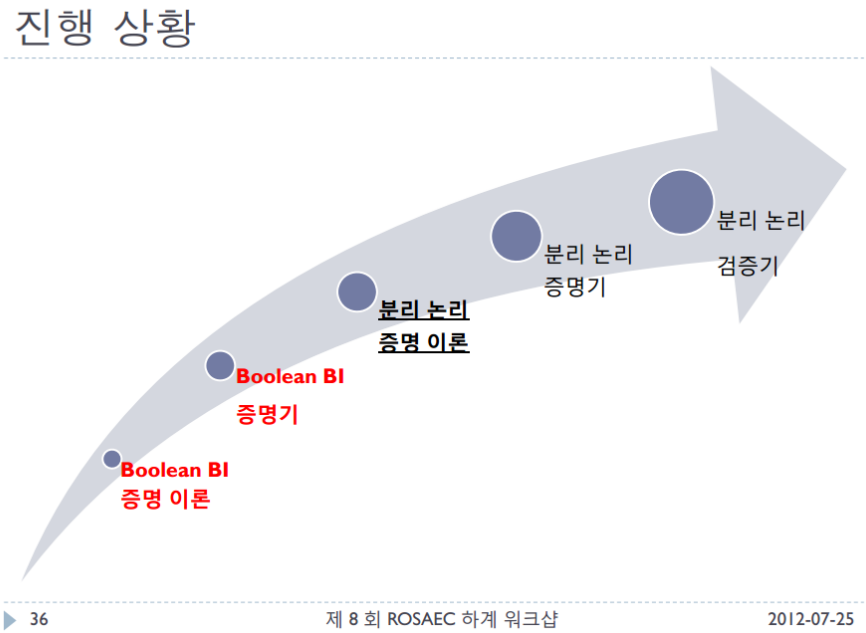
A Proof System for Separation Logic with Magic Wand

Wonyeol Lee Sungwoo Park

Department of Computer Science and Engineering
Pohang University of Science and Technology (POSTECH)
Republic of Korea
{leewy,gla}@postech.ac.kr

향후 목표

- Proof system 확장
  - inductive predicates
  - 외부 theorem prover와 연결
- Schorr-Waite algorithm [Yang 2001] 기계적 증명



마법봉 연산자를 포함한 분리 논리 증명 체계

이원열, 박성우
포항공과대학교 프로그래밍언어연구실

제10회 소프트웨어 무결점 연구센터 워크샵
지지향 2014년 1월 15일

감사합니다

자세한 내용은 포스터로 발표합니다