

Title	ToyWeb based prover
Author(s)	NISHIZAKI, Shin-ya; TAMANO, Hiroshi; SOYAMA, Yusuke
Citation	
Issue Date	2006-11-29
Type	Presentation
Text version	publisher
URL	http://hdl.handle.net/10119/8306
Rights	
Description	Theorem Proving and Provers Meeting(2nd TPP)での発表資料, 開催: 2006年11月29日~30日, 開催場所: JAIST 情報科学研究科棟II・Collaboration Room 7 (5F)

Toy Web based prover

Shin-ya NISHIZAKI

Tokyo Institute of Technology

Joint work with Hiroshi TAMANO and Yusuke SOYAMA.

Web based prover

Yusuke SOYAMA and Hiroshi TAMANO
Tokyo Institute of Technology

Joint work with Shin-ya NISHIZAKI

Overview

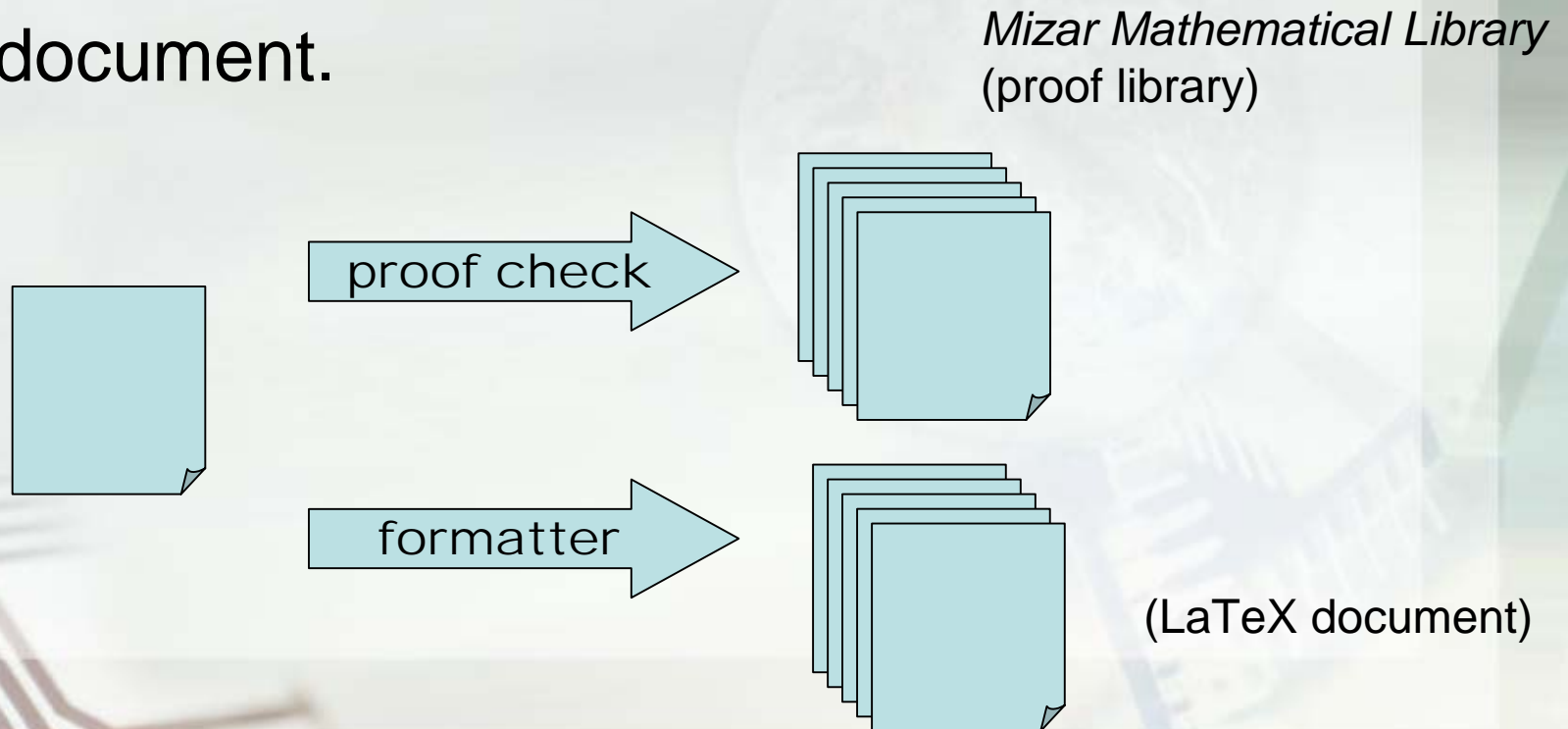
- Backgrounds
- PDIP
- Proof Archives and DoS-attack Resistance
- On going works
 - Trackback-based Checking

Backgrounds

- Mizar
 - Non-interactive prover
 - editing-latex-previewing loop*
 - Proof scripts in style of natural deduction
 - backward reasoning with tactics and tacticals
 - Amalgam of proofs and documents
 - Literated programming: web, weave and tangle
- Isabelle/Isar is influenced by Mizar.

Amalgam of proofs and documents

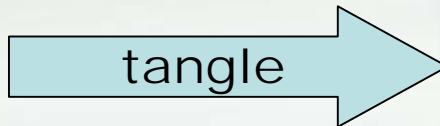
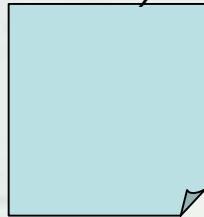
- A proof script has two aspects:
 - a proof
 - a document.



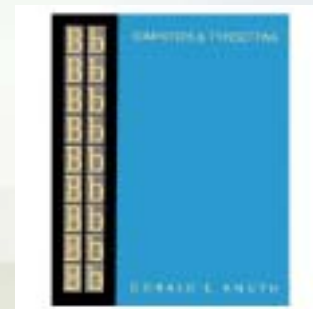
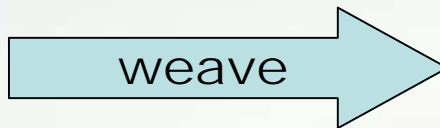
Literated Programming

- A WEB code has two aspects:
 - a program
 - a document

WEB code
(*CWEB code*)



Pascal code
(*C code*)



TeX document

Boomborg Project by Hagiya et al.

- Computing-As-Editing Paradigm (CAEP)
- Visibility
- Structure-Freedom

PDIP

- Proofs as Documents

Mizar, Literated Programming, Boomborg.

- implemented in HTML/JavaScript.

- another possibility

- Word/VBA: security..?

PDIP-rewrite

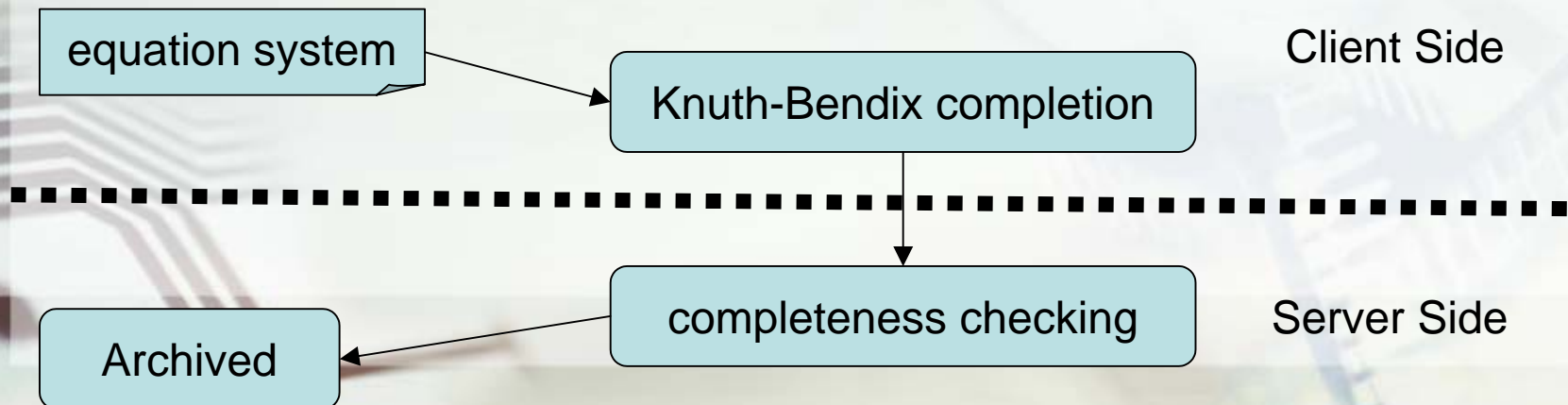
- We write an equation system and an expression to be rewrite in HTML.
- Redices appears as "buttons".
- If you push one of them, the redex is rewritten.

Points in implementation of PDIP-rewrite

- Stateless
 - The JavaScript code do not store states of a rewrite engine in JavaScript environments. Every states are expressed in HTML document tree.
c.f. Visibility in boomborg.

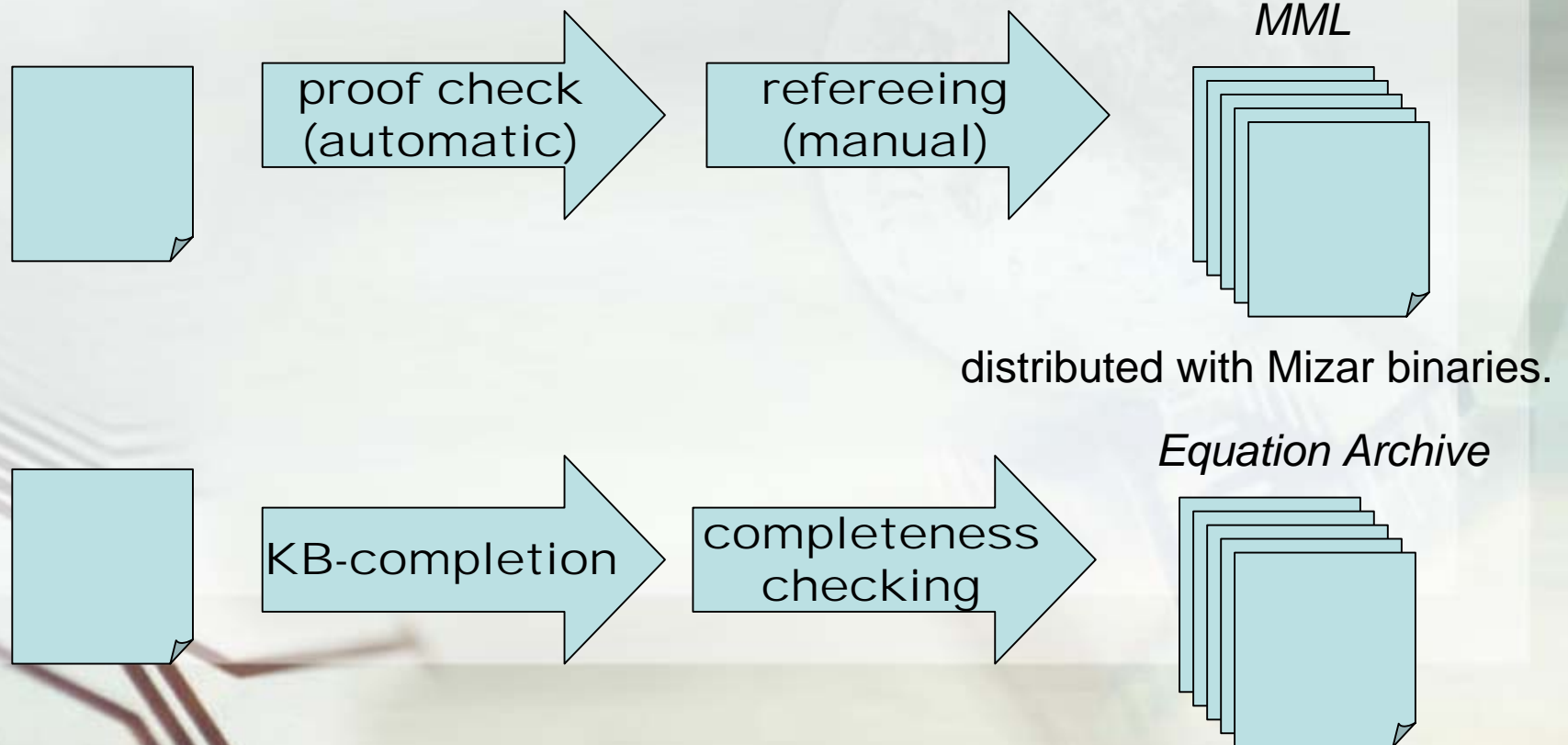
PDIP-KB and Equation Archive

- Knuth-Bendix completion with LPO is done in web browsers.
- Complete equation systems are filed in Equation Archive Server after checking their completeness in the server.



PDIP-KB and Equation Archive

- Similarity between Equation Archive and MML (Mizar Mathematical Library).

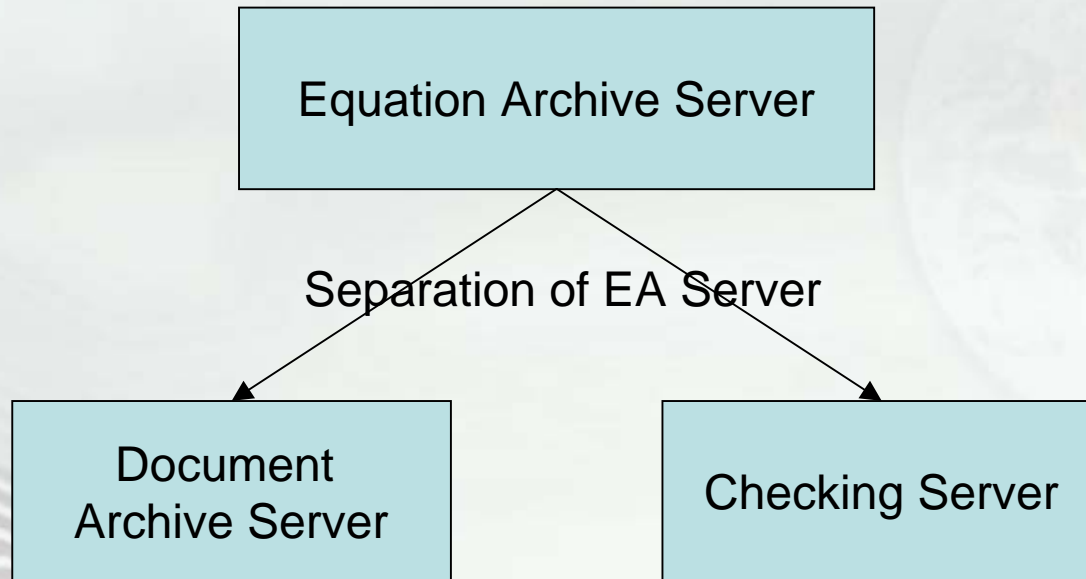


DoS Attack Resistance

- Completion is not decidable.
- Completeness checking is decidable.
- C.f.
 - Proving is not decidable.
 - Proof checking is decidable.
- If a client attaches a completeness proof with a equation system, then a server can estimate the computational cost.

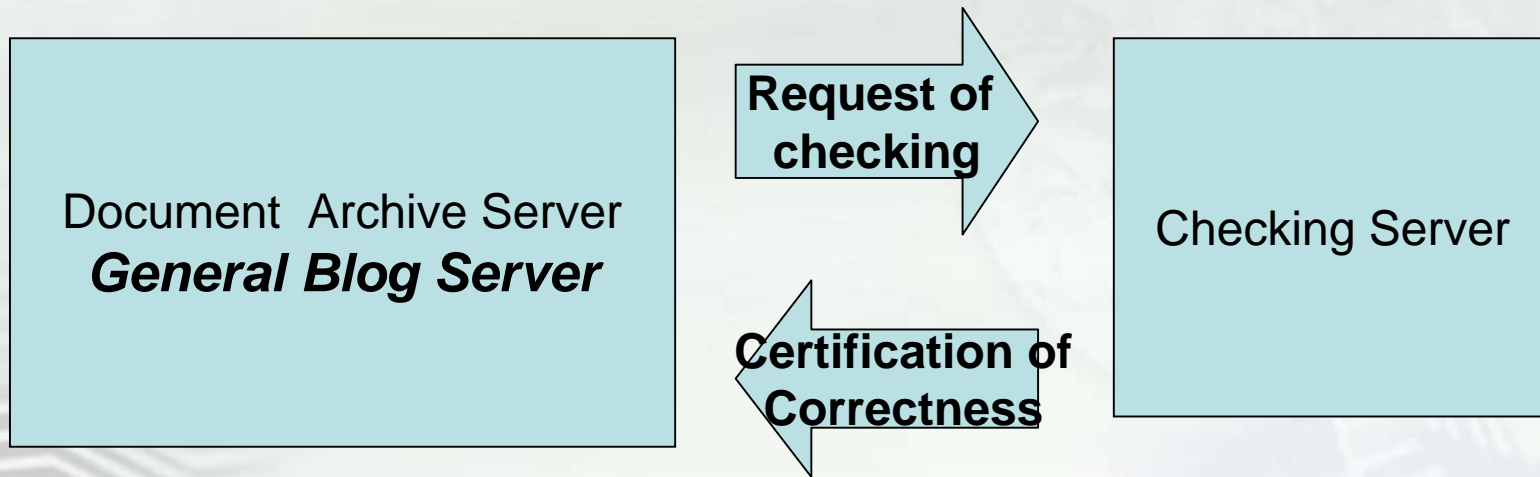
On-going work

- *Separation of Archiving and Checking*



Separation of Archiving and Checking

- *Cerifying Trackback*



Trackback Protocol

Future works

- Completion
 - Current implementation is too naive.
- Other logical systems
 - **prover!**
- PDIP on Wiki
- Proof checker on OpenOffice/JavaScript or MS Office/VBA.