UPPSALA UNIVERSITET

SWEDEN

Psi-calculi Workbench

Ramūnas Gutkovas

YR-CONCUR `12, Newcastle, 2012-09-03

Application areas

Authentication protocols
multicore programming
wireless sensor networks…

GAP

Fundamental models of computation

Turing machines
lambda-calculus
pi-calculus
modal logics…

Application areas

Authentication protocols

applied pi calculus
spi-calculus
concurrent constraint pi
others...

GAP

Fundamental models of computation

pi-calculus

lambda-calculus
pi-calculus
modal logics…

The Solution: Psi-calculi!

Applications

+ Cryptography

+ Eq Logics

+ Data structures

+ many other exts ...

Reusable

Ψ

Nominal Isabelle

Correct

framework for mobile process calculi

Part 1

Psi-Calculi

Introduction

Logical Methods in Computer Sci...
Vol. 7 (1:11) 2011, pp. 1–44
www.lmcs-online.org
...c. 30, 2009
..., 2011

**PSI-CALCULI:
A FRAMEWORK FOR MOBILE PROCESSES
WITH NOMINAL DATA AND LOGIC**

JESPER BENGTSON, MAGNUS JOHANSSON, JOACHIM PARROW, AND BJÖRN VICTOR

Department of Information Technology, Uppsala University, Sweden
e-mail address: {jesper.bengtson,magnus.johansson,joachim.parrow,bjorn.victor}@it.uu.se

...with nominal datatypes ...logical assertions and conditions. These can be transmitted between processes and their names can be statically scoped as in the standard pi-calculus. Psi-calculi can capture the same phenomena as other proposed extensions of the pi-calculus such as the applied pi-calculus, the spi-calculus, the fusion calculus, the concurrent con... ...calculi with... ...communication ch... ...is on par with the original pi-calculus.

Publications:

LICS'09, TPHOLs'09, LMCS'11, SOS'09, LICS'10, SEFM'11, JLAP'12, two PhD theses …

1. Introduction

...s a multitude of extensions where higher-level data struc... ...given as primitive. To mention only two there are the ...Abadi and Gordon [AG99] focusing on cryptographic primitives, and the applied pi-calculus of Abadi and Fournet [AF01] where agents can introduce statically scoped aliases of names for data, used e.g. to express how knowledge of an encryption is restricted. It is also... ...arbitrary... ...for expressing... ...tem for... ...with hu... ...rightly...

Receiv...
1998 ...
Key ...

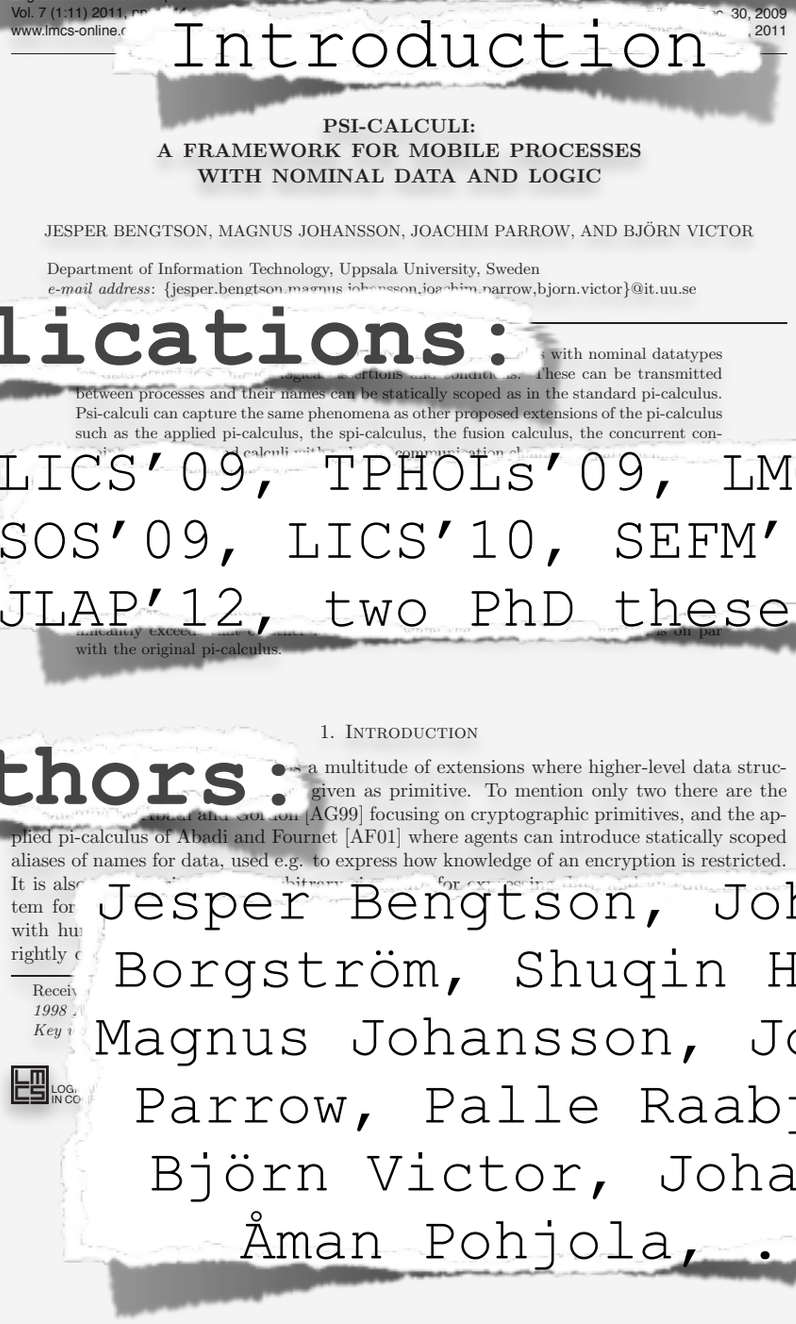
Authors:

Jesper Bengtson, Johannes Borgström, Shuqin Huang, Magnus Johansson, Joachim Parrow, Palle Raabjerg, Björn Victor, Johannes Åman Pohjola, ...

Part 1

Psi-Calculi

Introduction



Logical Methods in Computer Sci...
Vol. 7 (1:11) 2011, pp. ... 30, 2009
www.lmcs-online.org ... 2011

PSI-CALCULI:
A FRAMEWORK FOR MOBILE PROCESSES
WITH NOMINAL DATA AND LOGIC

JESPER BENGTSON, MAGNUS JOHANSSON, JOACHIM PARROW, AND BJÖRN VICTOR

Department of Information Technology, Uppsala University, Sweden
e-mail address: {jesper.bengtson,magnus.johansson,joachim.parrow,bjorn.victor}@it.uu.se

...s with nominal datatypes ... These can be transmitted between processes and their names can be statically scoped as in the standard pi-calculus. Psi-calculi can capture the same phenomena as other proposed extensions of the pi-calculus such as the applied pi-calculus, the spi-calculus, the fusion calculus, the concurrent con- ... calculi ... communication ... with the original pi-calculus.

1. Introduction

... a multitude of extensions where higher-level data struc- ... given as primitive. To mention only two there are the ... and Sorensen [AG99] focusing on cryptographic primitives, and the applied pi-calculus of Abadi and Fournet [AF01] where agents can introduce statically scoped aliases of names for data, used e.g. to express how knowledge of an encryption is restricted. It is also ... for expressing ... tem for ... with hu... rightly ...

Receiv... 1998 ... Key ...

LOGICAL METHODS IN CO...

Publications:

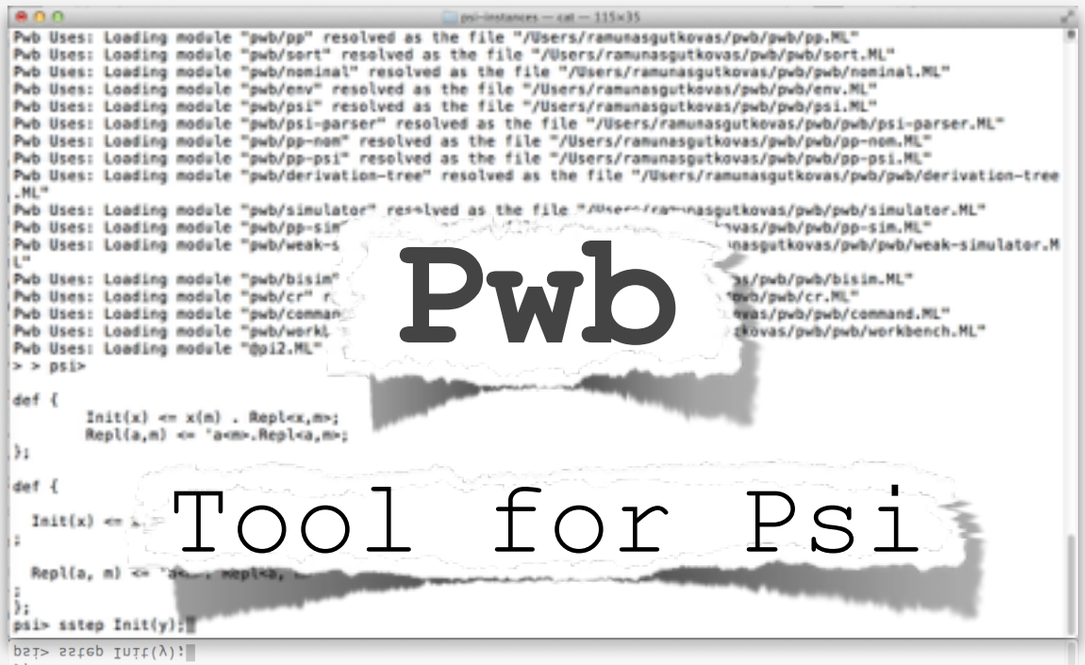
LICS'09, TPHOLs'09, LMCS'11, SOS'09, LICS'10, SEFM'11, JLAP'12, two PhD theses …

Authors:

Jesper Bengtson, Johannes Borgström, Shuqin Huang, Magnus Johansson, Joachim Parrow, Palle Raabjerg, Björn Victor, Johannes Åman Pohjola, ...

Part 2

Psi-Calculi Workbench



Pwb

Tool for Psi

Part 1

Psi-Calculi

Introduction

Psi by Example

pi-calculus (Informal)

ramunasgutkovas — bash — 80×24

nil	`0`
output	`'a<b>.P`
input	`a(x).P`
parallel	`P	Q`
replication	`!P`
restriction	`(new a)P`
match	`[a = b]P`
summation	`P + Q`

Psi by Example

pi-calculus (Informal)

ramunasgutkovas — bash — 80×24

nil	`0`
output	`'a<b>.P`
input	`a(x).P`
parallel	`P | Q`
replication	`!P`
restriction	`(new a)P`
match	`case [aa=bb]P: P`
summation	`case P true : P` `[] true : Q`

Psi by Example

Explicit Fusion (Informal)

Wischik & Gardner

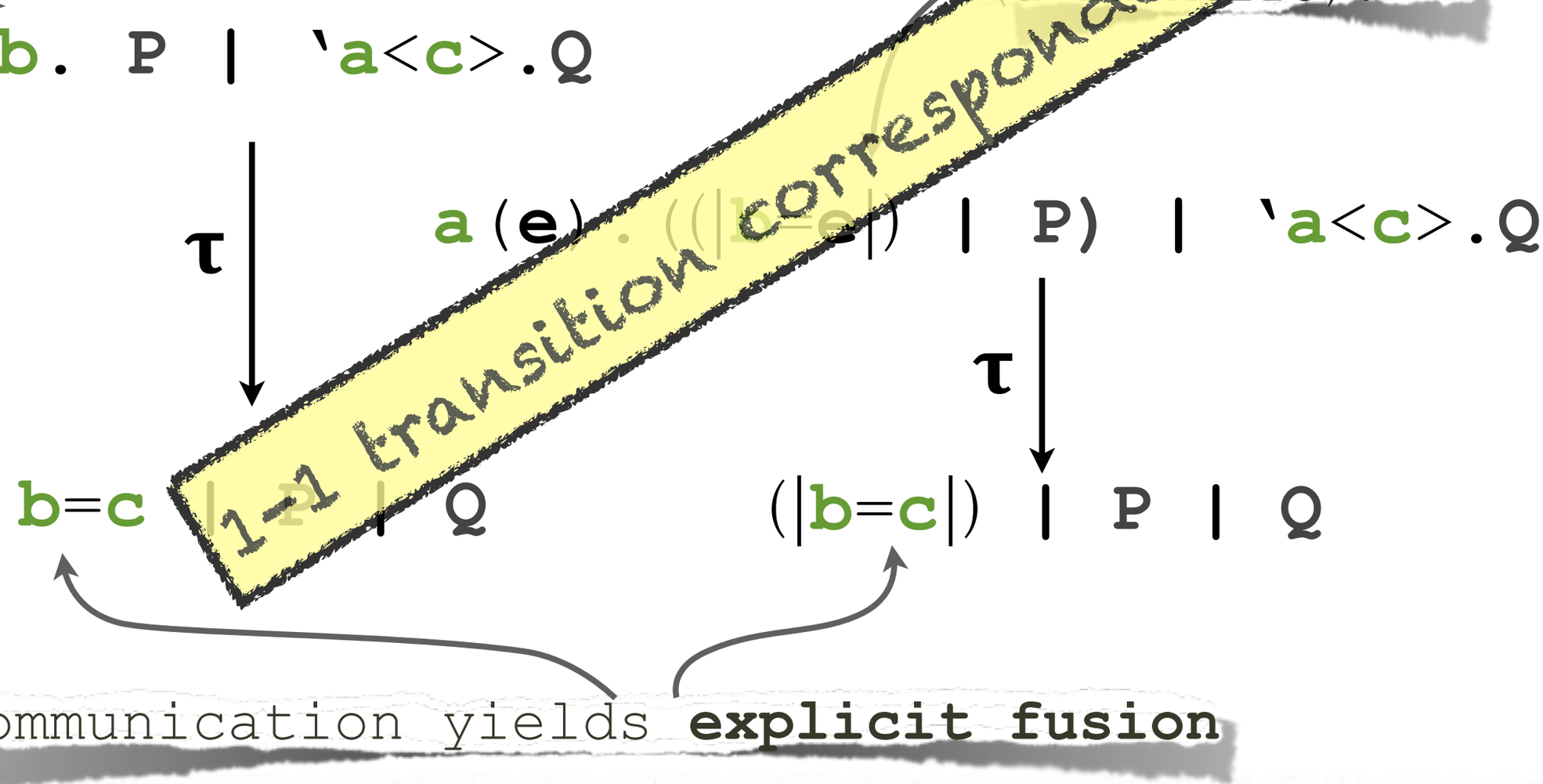
ramunasgutkovas — bash — 80×24

Input prefix **not** binding

Equatorial **Psi**

(a' la Merro):

1-1 transition correspondence



communication yields **explicit fusion**

Psi by Example

Crypto (A Closer Look)

Structured data: tuples with projection equations

```
fst(t(x,y)) = x
snd(t(x,y)) = y
```

```
'a<t(M,x)>  |
```

Facts about data: the secret **s** and message **M** hashes to **x**

```
(new s)
  (|hash(t(s,M)) = x|)  |
  a(y).if hash(t(s,fst(y))) = snd(y)
          then 'Ch(b)<fst(y)>
```

Structured channels

Equation as condition: checks if message and hash received via **a** is hashed with **s**

Psi-calculi

Parameterized Calculi

ramunasgutkovas — bash —

P, Q ::= (processes in ASCII notation)

Output: **'M<N>.P**

Input: **M(x).P**

Case: case **cnd$_1$:P$_1$** [] ... [] **cnd$_n$:P$_n$**

Assertion: (|**Psi**|)

T terms

C conditions

A assertions

Psi-calculi

Parameterized Calculi

ramunasgutkovas — bash — 80×24

```
P, Q ::=  (processes in ASCII notation)

  Output:   'M<N>.P          Input:   M(x).P

  Case: case cnd1:P1 [] ... [] cndn:Pn

  Assertion:  (|Psi|)

                Nil:  0

           Parallel:  P|Q

        Replication:  !P

        Restriction:  (new a)P
```

Psi-calculi

Defining a calculus

ramunasgutkovas — bash — 80×24

subst : T / C / A × List(name × T) → T / C / A

chaneq : T × T → C

entails : A × C → bool

compose : A × A → A

unit : A

Satisfy simple axioms, practically anything

terms are not necesseraly defined by a signature

Provide:

T terms
C conditions
A assertions

Example Psi-calculus
the pi-calculus (1)

ramunasgutkovas — bash — 80×24

T = names

terms are just names

C = {a == b : a, b in names}

conditions are equalities between names

A = {**unit**} = {1}

no facts in the environment

Example Psi-calculus

the pi-calculus (2)

ramunasgutkovas — bash — 80×24

T A

C

chaneq = λ(a,b).a == b

channel equivalence is formation of equality conditions

entails = λ(ψ,a == b).a = b

name equality is entailed whenever the names are the same

Example Psi-calculus

the pi-calculus (2)

ramunasgutkovas — bash — 80×24

$$\mathbf{chaneq} = \lambda(a,b).a == b$$

channel equivalence is formation of equality conditions

$$\mathbf{entails} = \lambda(\psi, a == b).a = b$$

name equality is entailed whenever the names are the same

$$\mathbf{unit} = 1 \qquad \mathbf{compose} = \lambda(\psi_1, \psi_2).1$$

assertions are trivial

Example Psi-calculus

the pi-calculus

ramunasgutkovas — ba

```
A = {unit} = {1}
T = names
C = {a == b : (a,b)}
chaneq = λ(a,b).a == b
entails = λ(Ψ,a == b).Ψ ⊢ a = b
compose = λ(Ψ1,Ψ2).Ψ1 ∧ Ψ2
unit = ⊤
```

~ coincides

1-1 correspondnce of →

That's the definition

machine-checked proofs

Example Psi-calculus

Fusion Calculus

ramunasgutkovas — bash — 80×24

$\mathbf{T} = \text{names}$

$\mathbf{C} = \{a = b : a,b \in \text{names}\}$

$\mathbf{A} = \text{pow}_{\text{fin}}(\{a = b : a,b \in \text{names}\})$

Done!

$\mathbf{chaneq} = \lambda(a,b).\ a = b$

$\mathbf{entails} = \lambda(\psi, a{=}b).\ (a,b) \in EQ(\psi)$

$\mathbf{compose} = \lambda(\psi_1, \psi_2).\ \psi_1 \cup \psi_2$

$\mathbf{unit} = \varnothing$

equivalence closure

Example Psi-calculus

crypto

ramunasgutkovas — bash — 80×24

Σ = {hash(•), enc(•,•), dec(•,•),
pk(•), sk(•), …}

$\mathbf{E}$ = {dec(enc(x,y),y) = x, …}

$\mathbf{T}$ = {f(M_1,…,M_n) : $M_i \in T$ & f$\in\Sigma$} U names

$\mathbf{C}$ = {M=N : M,N ∈ T}

$\mathbf{A}$ = pow({M=N : M,N ∈ T})

Done!

chaneq = λ(M,N) . M=N

entails = λ(ψ,M=N). $\mathbf{E}$Uψ $\vdash_{eq}$ M=N

compose = λ(ψ_1,ψ_2) . ψ_1 U ψ_2

unit = ∅

Psi-Calculi

Expressiveness

- **Psi-calculi can capture**
  - Cryptography, like applied pi-calculus (Abadi, Fournet 2001)
  - **Fusion**, like the explicit fusion calculus (Wischik, Gardner 2005)
  - **Concurrent constraints**, like concurrent constraint pi (Buscemi, Montanari 2007)
  - **Polyadic synchronisation** (Carbone, Maffeis 2003)
  - **pattern matching, higher-order values** (various)

Extensions

+ Higher Order

+ Broadcast

+ Sorts, match

+ Types (Hüttel, CONCUR'11)

Part 1

Psi-Calculi

Introduction

Logical Methods in Computer Science
Vol. 7 (1:11) 2011, pp. 1–11
www.lmcs-online.org

Submitted Dec. 30, 2009
Published Mar. 29, 2011

**PSI-CALCULI:
A FRAMEWORK FOR MOBILE PROCESSES
WITH NOMINAL DATA AND LOGIC**

JESPER BENGTSON, MAGNUS JOHANSSON, JOACHIM PARROW, AND BJÖRN VICTOR

Department of Information Technology, Uppsala University, Sweden
e-mail address: {jesper.bengtson,magnus.johansson,joachim.parrow,bjorn.victor}@it.uu.se

...ing the framework for bisimulation and congruence properties in the pi-calculus with nominal datatypes for data structures and for logical assertions and conditions. These can be transmitted between processes and their names can be statically scoped as in the standard pi-calculus. Psi-calculi can capture the same phenomena as other proposed extensions of the pi-calculus such as the applied pi-calculus, the spi-calculus, the fusion calculus, the concurrent constraint pi-calculus and calculi with bulk communication channels or data matching ... Psi-calculi can be ... more general ... without a structural congruence. We establish minimal requirements on the nominal data ... and prove general algebraic properties ... of which have ... mically exceeds that of other formalisms, while the purity of the semantics is on par with the original pi-calculus.

1. Introduction

... has a multitude of extensions where higher-level data structures ... are given as primitive. To mention only two there are the spi-calculus by Abadi and Gordon [AG99] focusing on cryptographic primitives, and the applied pi-calculus of Abadi and Fournet [AF01] where agents can introduce statically scoped aliases of names for data, used e.g. to express how knowledge of an encryption is restricted. It is also parametrised by an arbitrary signature for expressing data and an equality system for ... Psi-calculi is compatible with hundreds of papers applying or developing the formalisms. As Abadi and Fournet rightly observe, there is a trade-off between "purity", meaning the simplicity and elegance

Received by the editors April 1, 2011.
1998 ACM Subject Classification: F.1.2, F.3.1, F.3.2.
Key words and phrases: ... nominal ... theorem prover.

Publications:

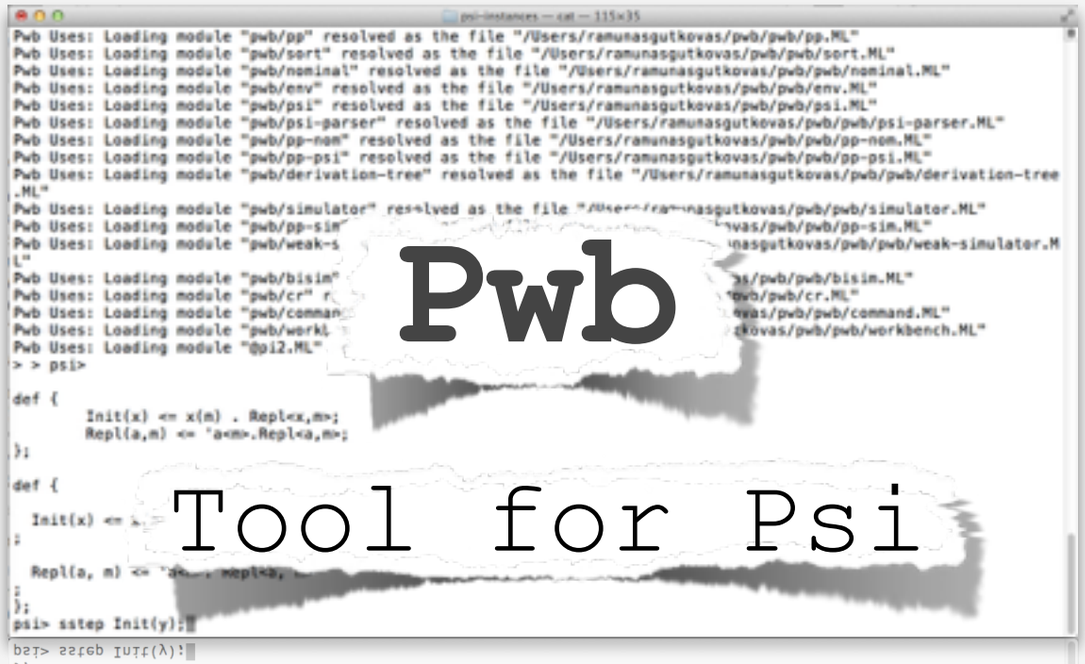
LICS'09, TPHOLs'09, LMCS'11, SOS'09, LICS'10, SEFM'11, JLAP'12, two PhD theses …

Authors:

Jesper Bengtson, Johannes Borgström, Shuqin Huang, Magnus Johansson, Joachim Parrow, Palle Raabjerg, Björn Victor, Johannes Åman Pohjola, ...

Part 2

Psi-Calculi Workbench

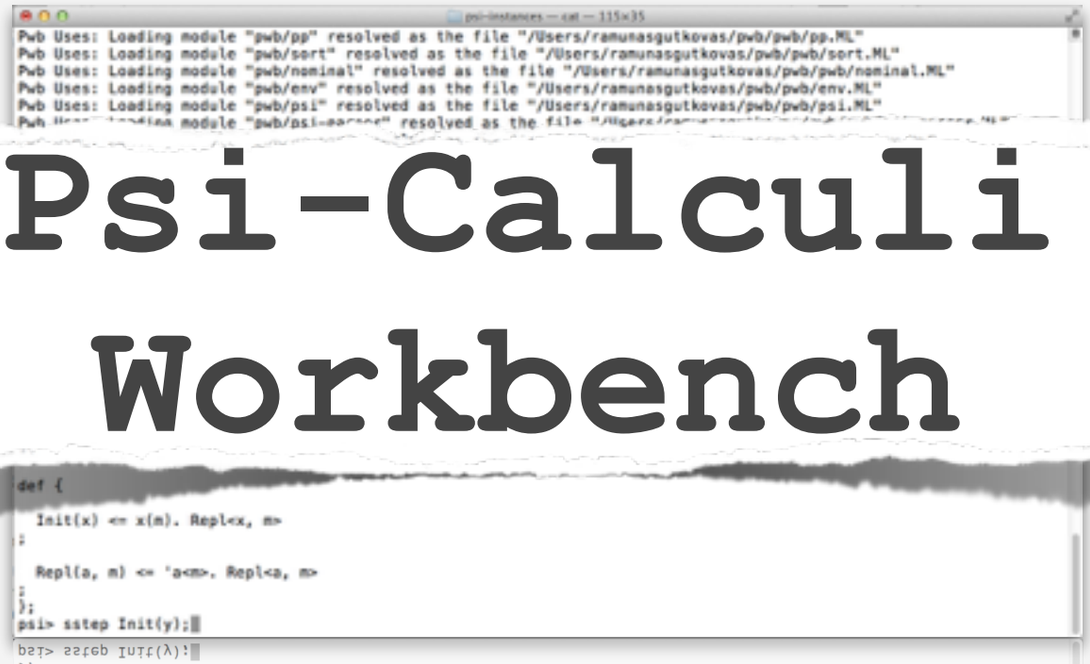


Pwb

Tool for Psi

Part 2

Psi-Calculi Workbench



Tool for Psi

Psi-Calculi Workbench

ramunasgutkovas — bash — 80×24

Framework for **implementing** **Psi-Calculi** instances

Experimental Platform for **experimentation** with **semantics** and pi-calculus **extensions**

Free

Implemented in **SML** (**PolyML**)

For **every psi** implementation **includes**

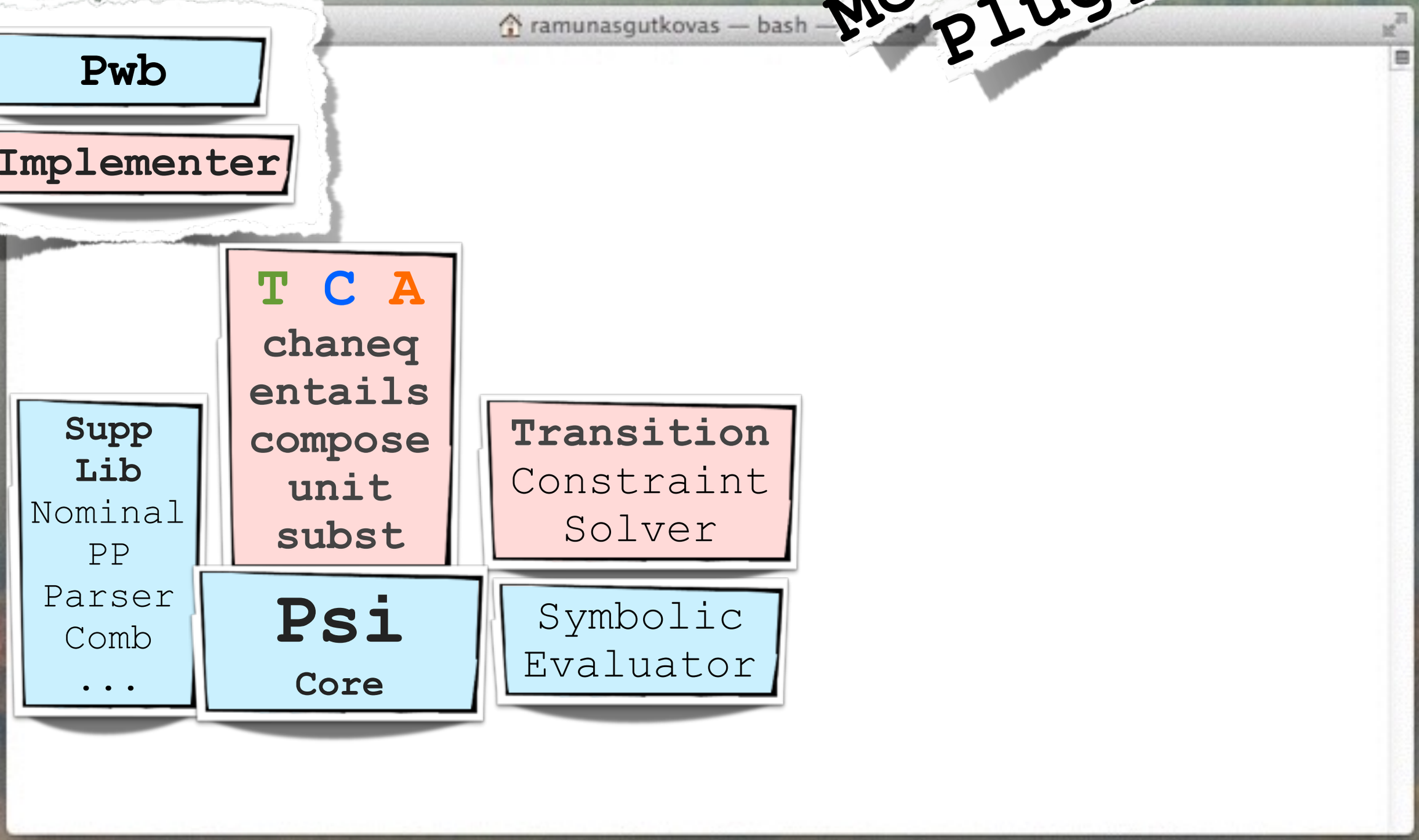
Transition simulator

Weak bisim generator

Psi-Calculi Workbench

Architecture

Modular
Pluggable



Psi-Calculi Workbench

Constraint Solver

Pwb

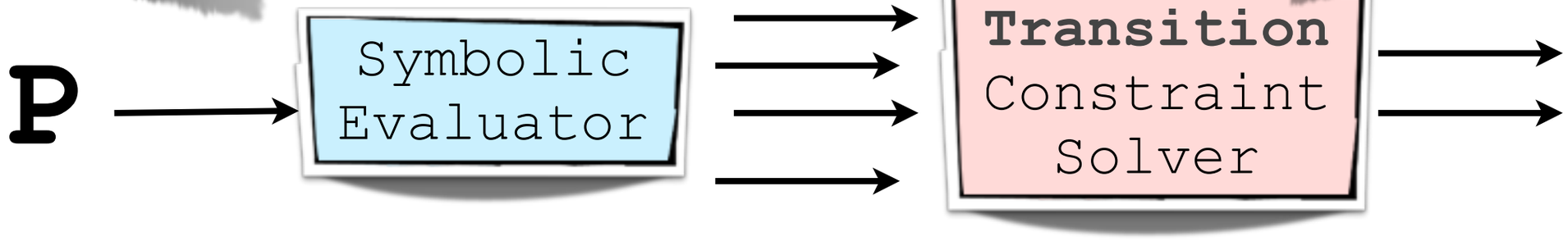
Implementer

ramunasgutkovas — bash — 80×24

Transition Derivative **Constraint**

Transition Derivative Constraint **Solution**

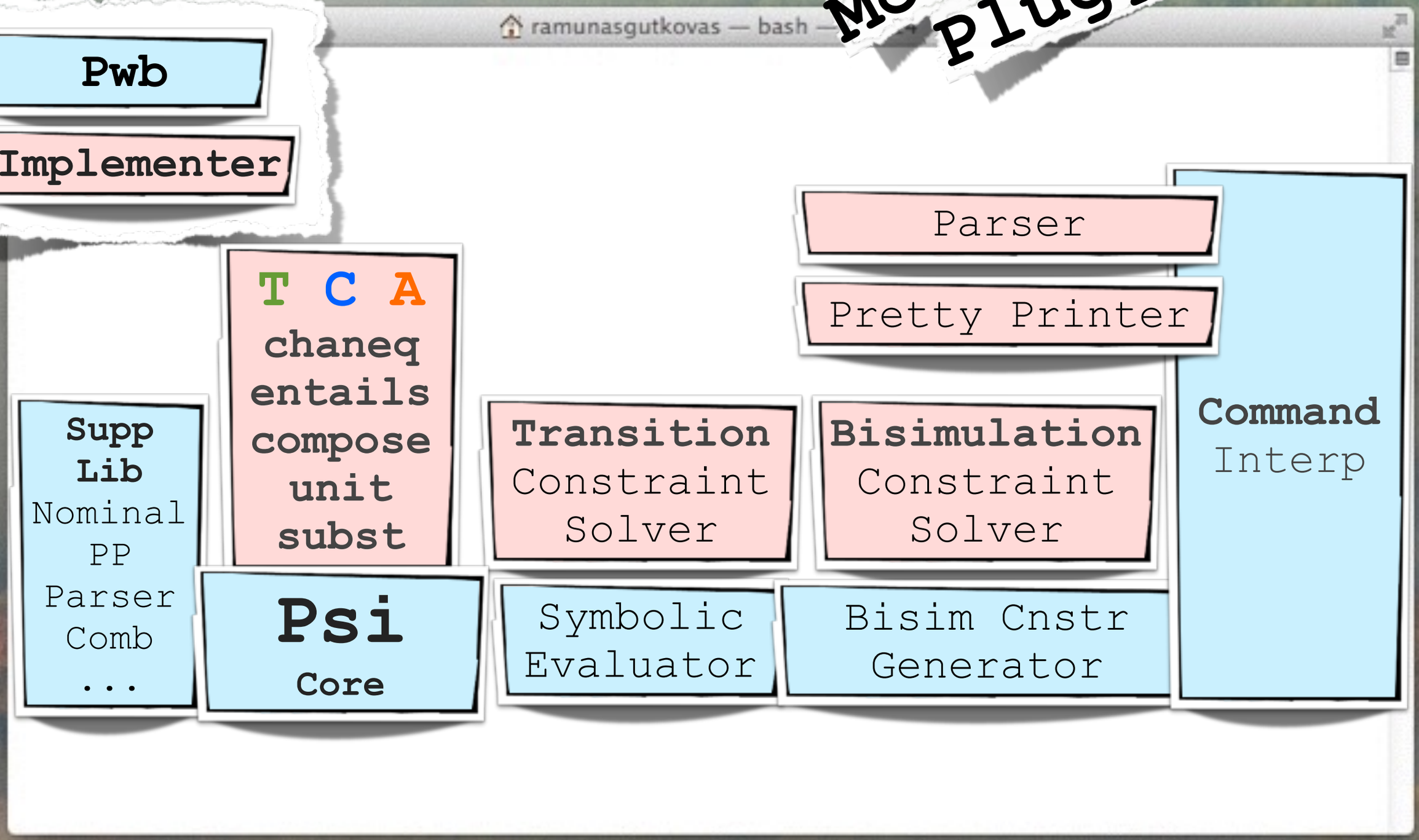
Process

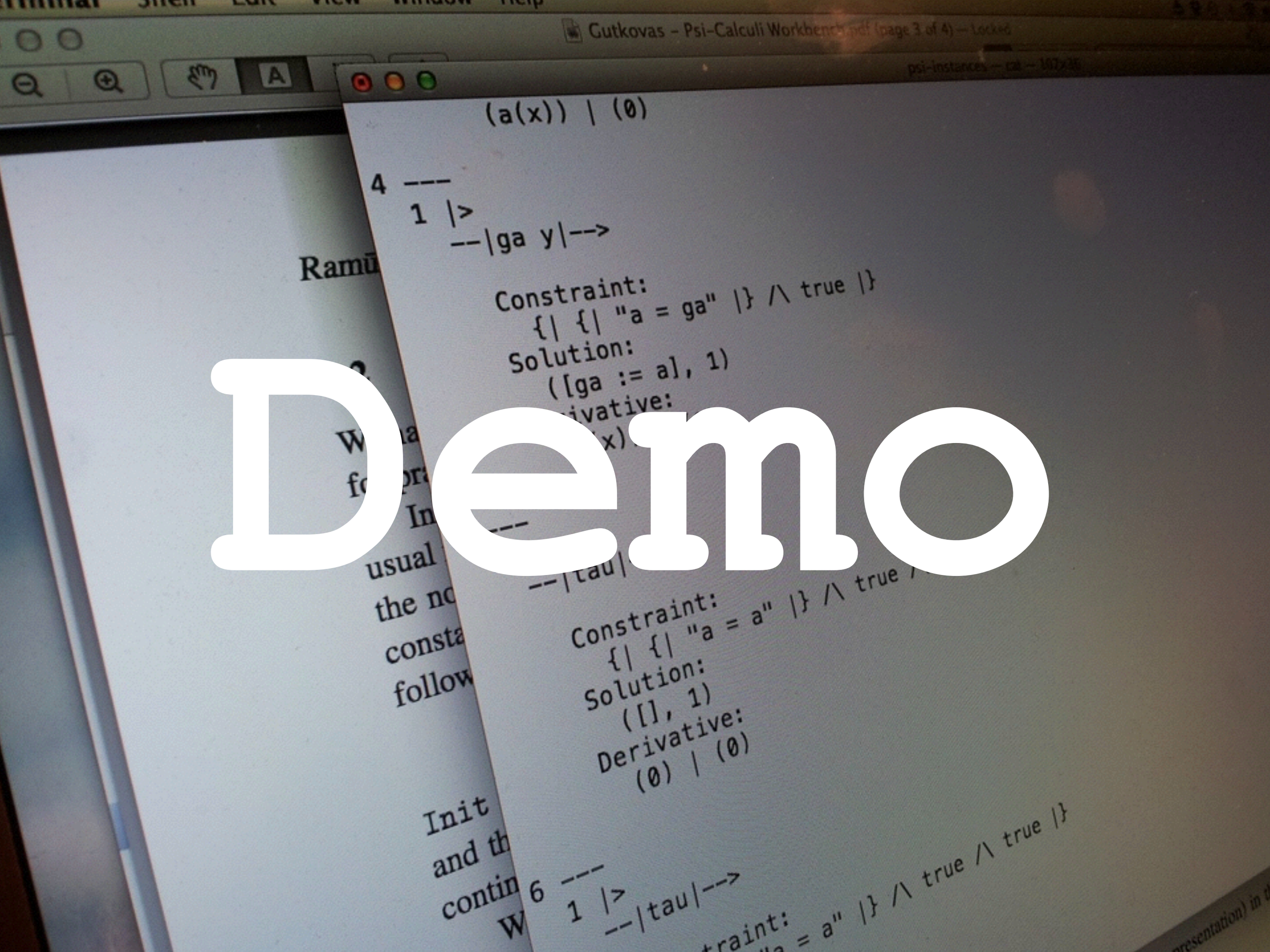


Psi-Calculi Workbench

Architecture

Modular
Pluggable




Gutkovas – Psi-Calculi Workbench.pdf (page 3 of 4) — Locked
psi-instances — cat — 107×36
(a(x)) | (0)
4 ---
1 |>
--|ga y|-->
Constraint:
{| {| "a = ga" |} /\ true |}
Solution:
([ga := a], 1)
Derivative:
(x)
--|tau|
Constraint:
{| {| "a = a" |} /\ true
Solution:
([], 1)
Derivative:
(0) | (0)
Ramū
usual
the no
consta
follow
Init
and th
contin
6 ---
1 |>
--|tau|-->
Demo

Psi-Calculi

Extensions (in progress)

ramunasgutkovas — bash — 80×24

+ Nominal Free Algebras

+ Broadcast communication

Johannes Borgström

+ Hüttel's Types

Amin Khorsandi, MSc Thesis

References

ramunasgutkovas — bash — 80×24

Get Pwb at

$ wget www.it.uu.se/research/group/mobility/applied/psiworkbench

Take a look

$ wget www.it.uu.se/research/group/mobility

Read

LICS'09, TPHOLs'09, **LMCS'11**, SOS'09, LICS'10, SEFM'11, JLAP'12

Exercising Psi-calculi: A Psi-calculi workbench (my MSc Thesis)