Mobility and Threads in Ambients

Xudong GUAN

Shanghai Jiao Tong University

In this talk …

Part I. Introducing myself

Part II. Mobility and threads in Ambients

Who, Where, What

- Xudong GUAN, Ph.D.
- Shanghai Jiao Tong University, Shanghai, China
- Thesis: Ambients
- Other interests: Web Usage Mining, Wiki

Thesis: Ambients

- Robust Ambients: coaction parameters
- Evolving Type System: mobility and threads
- Algebraic proof of pi-encoding in pure ambients

Web Usage Mining

- Preprocessing
- Association: improving the pattern interestingness
- Clustering: fast session and page clustering
- Destination prediction and recommendation

Wiki - “The Writable Web”

- Collaborative Document Authoring
  - ⇨ Project documentation
  - ⇨ Resource and knowledge sharing
- Personal knowledge storage
  - ⇨ Bookmarking and comments
  - ⇨ Experiences recording
  - ⇨ Resource keeping

Part II Mobility and Threads in Ambients

<u>1. Motivation</u>

2. The type system: ETS-MT

3. Equational laws under ETS-MT

4. The new encoding

Motivation

- Levi and Sangiorgi, 00: algebraic proof of renaming, firewall-crossing, pi-encoding, ...
- Zimmer, 00: pi-encoding in pure ambients, non-algebraic proof, leaving one conjecture -- all the auxiliary reductions are confluent.
- Problem: Can we make use of the equational laws already developed in LS00 to prove the conjecture?

What we have: a review of the equational laws

- Untyped laws
  - ⇨ simple but restrictive
- Single-threadness laws
  - ⇨ the two interacting ambients must be single-threaded
- Uniform receptiveness laws
  - ⇨ built on single-threadness and immobility

What we want: a review of the encoding and the auxiliary reductions

- Channel name => *n*[*allowIO n* | *server read* . ...]
- Variable name => *x*[*allowIO x* | *fwd M'*]
- input process => *read*[*request read M* . ...]
- output process => *write*[*request write M* . ...]
- Communication steps:
  - ⇨ redirection: *r/w-in-x* *enter-in-r/w r/w-open-enter r/w-out-x*
  - ⇨ meet: *r/w-in-n* *enter-in-read read-open-enter enter-out-read*
  - ⇨ construction: *enter-in-write* *write-open-enter read-be-p write-in-p p-open-write read-out-n p-be-read p-out-read read-be-x p-out-x open-p*

Classification of the auxiliary reductions

- *read* / *write* entering and exiting *n* / *x*
  - ⇨ *n* / *x* : imm;   read, write : ST
- *enter* entering and exiting *read* / *write*
  - ⇨ *enter*, *read*, *write* : ST
- opening *enter*, *read*, *write*, and *p*
  - ⇨ *enter*, *read*, *write*, *p* : ST
- Is this possible?

The problem of typing

- *read* is mobile, must be ST
- communication makes the resulting variable ambient *x*[*fwd M* | *allowIO x*], which is not ST. As a result, it must be immobile.
- two renamings: from *read* to *p* and from *p* to *x*
- ---- the type systems in LS00 is difficult to handle here.

Solution: a small type system + a few trivial modifications to the encoding

- able to record mobility and threads of ambients and processes
  - ⇨ *n* is mobile: *n* may exercise *in/out* at some point
  - ⇨ threads of ambient: maximum number of concurrent top-level actions of the process inside
- special treatment to the *open/co-open* capabilities
  - ⇨ distinguish the behavior before and after opening
  - ⇨ e.g. *write* is mobile and *x* is immobile, *x* can open *write* to get *fwd M*

Part II Mobility and Threads in Ambients

1. Motivation

2. The type system: ETS-MT

3. Equational laws under ETS-MT

4. The new encoding

ETS-MT: grammar

- only records threads and mobility information

$\Gamma = \{n{:}T \mid \ldots\}$

$\Gamma \mid\!\!-\!\!- P{:}T \quad \Gamma \mid\!\!-\!\!- n{:}T$

$\Gamma \mid\!\!-\!\!- M{:}W$

$T\ (type) ::= \bot \mid U \mid U[T]$

$U\ (pre\text{-}type) ::= Z^{Y}$

$Z\ (mobility) ::= \underline{\vee} \mid \curvearrowright$

$Y\ (threads) ::= 0 \mid 1 \mid \omega$

$W\ (context) ::= \ --$
$\quad \mid\ U \cdot_t W$
$\quad \mid\ T \mid_t W$
$\quad \mid\ U[W]$

Current type and future type (ex. in SA)

$U[T]$ U: current type, current behavior

T: future type, behavior after being opened

$\mathbf{0} : \underline{\vee}^{0}$ $\mathbf{in}\ read\ .\ \mathbf{0} : \curvearrowright^{1}$

$\mathbf{in}\ read\ .\ \overline{\mathbf{open}}\ write\ .\ \mathbf{0} : \curvearrowright^{1}[\ \underline{\vee}^{0}\ ]$

$\overline{\mathbf{open}}\ n\ .\ \overline{\mathbf{open}}\ m\ .\ !\ \overline{\mathbf{in}}\ p : \underline{\vee}^{1}[\ \underline{\vee}^{1}[\ \underline{\vee}^{\omega}\ ]\ ]$

$\mathbf{open}\ m \mid m[\ \mathbf{open}\ n \mid n[\ \overline{\mathbf{open}}\ n\ .\ \overline{\mathbf{open}}\ m\ .\ !\ \overline{\mathbf{in}}\ p\ ]\ ]$

$\rightarrow\ \rightarrow\ !\ \overline{\mathbf{in}}\ p\ : \underline{\vee}^{\omega}$

Subtyping

$\underline{V} \le \curvearrowright$ $0 \le 1 \le \omega$

e.g.

$$\underline{V}^0 \le \begin{array}{c}\curvearrowright^0 \\ \underline{V}^1\end{array} \le \curvearrowright^1$$

$$\underline{V}^0[\underline{V}^0] \le \underline{V}^1[\underline{V}^0] \le \underline{V}^1[\curvearrowright^1]$$

Type operators

$\bullet_t$

$$\textbf{in}\ m\ .\ \overline{\textbf{out}}\ n\ .\ \mathbf{0} : \curvearrowright^{1}$$

$$\curvearrowright^{1} \bullet_t \underline{V}^{1} \bullet_t \underline{V}^{0} = \curvearrowright^{1}$$

$|_t$

$$\textbf{in}\ m \mid \overline{\textbf{out}}\ n : \curvearrowright^{\omega}$$

$$\curvearrowright^{1} \ |_t\ \underline{V}^{1} = \curvearrowright^{\omega}$$

$$\textbf{in}\ m \mid n[P] : \curvearrowright^{1}$$

$$\curvearrowright^{1} \ |_t\ \underline{V}^{0} = \curvearrowright^{1}$$

Typing of co-open

$\mathbf{in}\ \mathit{read}\ .\ \overline{\mathbf{open}}\ \mathit{write}\ .\ \mathbf{0} : \curvearrowright^{1}[\ \underline{\vee}^{0}\ ]$

$\overline{\mathbf{open}}\ \mathit{write}\ .\ \mathbf{0} : \underline{\vee}^{1}[\ \underline{\vee}^{0}\ ]$

$\overline{\mathbf{open}}\ \mathit{write}\ .\ P : \underline{\vee}^{1}[\ T_{P}\ ]$

$\overline{\mathbf{open}}\ n : \underline{\vee}^{1}[\ \text{--}\ ]$

Typing of parallel co-opens

$$\textbf{in}\ m\ .\ \mathbf{0} \mid \overline{\textbf{open}}\ n\ .\ \mathbf{0} : \curvearrowright^{\omega}[\curvearrowright^{1}]$$

$$\curvearrowright^{1} \mid_t \underline{\vee}^{1}[\underline{\vee}^{0}]$$

$$= (\curvearrowright^{1} \mid_t \underline{\vee}^{1})[\curvearrowright^{1} \mid_t \underline{\vee}^{0}]$$

$$= \curvearrowright^{\omega}[\curvearrowright^{1}]$$

$$\overline{\textbf{open}}\ n\ .\ \overline{\textbf{open}}\ n\ .\ \mathbf{0} : \underline{\vee}^{1}[\underline{\vee}^{1}[\underline{\vee}^{0}]]$$

$$\overline{\textbf{open}}\ n\ .\ \mathbf{0} \mid \overline{\textbf{open}}\ n\ .\ \mathbf{0} : \underline{\vee}^{1}[\underline{\vee}^{1}[\underline{\vee}^{0}]]$$

$$M_1\ .\ \overline{\textbf{open}}\ n\ .\ P_1 \mid M_2\ .\ \overline{\textbf{open}}\ n\ .\ P_2 : U_1[T_1] \mid_t U_2[T_2] = ?$$

Typing of open

$$\textbf{open}\ n\ .\ \mathbf{0} \mid n\,[\overline{\textbf{open}}\ n\ .\ \mathbf{0}\ ] \quad \rightarrow \quad \mathbf{0}$$

$$n : \underline{\vee}^{1}[\ \underline{\vee}^{0}\ ] \qquad \textbf{open}\ n\ .\ \mathbf{0} : \ \underline{\vee}^{1} \cdot_t \underline{\vee}^{0}$$

$$\textbf{open}\ n\ .\ \mathbf{0} \mid n\,[\overline{\textbf{open}}\ n\ .\ Q\ ] \quad \rightarrow \quad Q$$

$$n : \underline{\vee}^{1}[T_Q] \qquad \textbf{open}\ n\ .\ \mathbf{0} : \ \underline{\vee}^{1} \cdot_t T_Q$$

$$\textbf{open}\ n\ .\ P \mid n\,[\overline{\textbf{open}}\ n\ .\ Q\ ] \quad \rightarrow \quad P \mid Q$$

$$P : T_P \quad n : \underline{\vee}^{1}[T_Q] \qquad \textbf{open}\ n\ .\ P : \underline{\vee}^{1} \cdot_t (T_P \mid_t T_Q)$$

$$\textbf{open}\ n : \quad \underline{\vee}^{1} \cdot_t (\text{--}\ \mid_t T_Q)$$

Relating ETS-MT and grave interference

grave interference ==> $\curvearrowright^{\omega}$

Part II Mobility and Threads in Ambients

1. Motivation

2. The type system: ETS-MT

3. Equational laws under ETS-MT

4. The new encoding

Single-threadness and immobility

- $Current(U)=U$, $Current(U[T])=U$
- $Future(U[T])=T$
- ST: $P/n:T$ and $Current(T).threads <= 1$
- I: $P/n:U$ and $U.mobility = \underline{\vee}$

Six uniform receptiveness structures

- $read\ [\mathbf{in}\ n\ .\ P_1 \mid Q_1] \mid n\ [\mathbf{!}\overline{\mathbf{in}}\ n\ .\ P_2 \mid Q_2]$

  ⇨ $read$: ST, n : I

- $\mathbf{!}\ enter[\mathbf{in}\ read\ .\ P_1 \mid Q_1] \mid read\ [\overline{\mathbf{in}}\ read\ .P_2 \mid Q_2]$

  ⇨ $read$: ST

- other 4 cases:

  $\mathbf{!}n\mathbf{[out}\ \ldots\mathbf{]},\ n\mathbf{[!}\overline{\mathbf{out}}\ldots\mathbf{]},\ \mathbf{!open}\ n\ldots,\ \mathbf{!}n\mathbf{[}\overline{\mathbf{open}}\ldots\mathbf{]}$

Part II Mobility and Threads in Ambients

1. Motivation

2. The type system: ETS-MT

3. Equational laws under ETS-MT

4. The new encoding

Single-threaded encoding in pure SA

- some results:
  - ⇨ *read*, *write*, *enter* : ST
  - ⇨ *n*, *x* : I
  - ⇨ no renaming
- the encoding:

$$\{(\nu n)P\} \triangleq (\nu n{:}\underline{V}^{\omega})$$
$$(n[\ \mathit{allowIO}\ n \mid n_1[\mathit{allowIO}\ n_1]$$
$$\mid \mathit{server}\ \mathit{write}\ .\ \mathbf{in}\ n_1\ .\ \mathbf{in}\ \mathit{read}\ .\ \overline{\mathbf{open}}\ \mathit{write}$$
$$\mid \mathit{server}\ \mathit{read}\ .\ \mathbf{in}\ n_1\ .\ \overline{\mathbf{in}}\ \mathit{read}\ .\ \mathbf{out}\ n_1\ .\ \mathbf{out}\ n\ .\ \overline{\mathbf{out}}\ \mathit{read}$$
$$.\ \mathbf{open}\ \mathit{write}\ .\ \overline{\mathbf{out}}\ \mathit{read}\ .\ \mathbf{open}\ r_2\ .\ \overline{\mathbf{open}}\ \mathit{read}\ ]$$
$$\mid \{\mathrm{P}\})$$

$$\{M(x).P\} \triangleq \mathit{read}\ [\ \mathit{request}\ \mathit{read}\ M$$
$$\mid (\nu x{:}\underline{V}^{\omega})$$
$$(\ c_1\ [\mathbf{out}\ \mathit{read}\ .\ \overline{\mathbf{open}}\ c_1\ .\ \{P\}]$$
$$\mid r_1[\overline{\mathbf{in}}\ r_1\ .\ \mathbf{in}\ x\ .\ \overline{\mathbf{open}}\ r_1]$$
$$\mid x\ [\overline{\mathbf{in}}\ x\ .\ \mathbf{open}\ r_1\ .\ \mathbf{open}\ w_1$$
$$.\ (\ \mathit{allowIO}\ x \mid r_2\ [\mathbf{out}\ x\ .\ \overline{\mathbf{open}}\ r_2\ ]\ )\ ]\quad)\ ]$$
$$\mid \mathbf{open}\ c_1 \mid \mathbf{open}\ c_2 \mid \mathbf{open}\ \mathit{read}$$

$$\{M\langle M'\rangle.P\} \triangleq \mathit{write}[\ \mathit{request}\ \mathit{write}\ M$$
$$\mid c_2\ [\mathbf{out}\ \mathit{read}\ .\ \overline{\mathbf{open}}\ c_2\ .\ \{P\}]$$
$$\mid w_1\ [\mathbf{in}\ r_1\ .\ \overline{\mathbf{open}}\ w_1\ .\ \mathit{fwd}\ M'\ ]\ \ ]$$

$$\{\mathbf{0}\} \triangleq \mathbf{0}$$
$$\{P|Q\} \triangleq \{P\}|\{Q\}$$
$$\{!P\} \triangleq\ !\{P\}$$

Typing of the encoding

$$
\begin{aligned}
\{(\nu n)P\} \;\triangleq\; & (\nu n{:}\underline{V}^{\omega}) \\
& (n[\, allowIO\ n \mid n_1\, [allowIO\ n_1\,] \\
& \quad \mid server\ write\ .\ \mathbf{in}\ n_1\ .\ \mathbf{in}\ read\ .\ \overline{\mathbf{open}}\ write \\
& \quad \mid server\ read\ .\ \mathbf{in}\ n_1\ .\ \overline{\mathbf{in}}\ read\ .\ \mathbf{out}\ n_1\ .\ \mathbf{out}\ n\ .\ \overline{\mathbf{out}}\ read \\
& \qquad\qquad .\ \mathbf{open}\ write\ .\ \overline{\mathbf{out}}\ read\ .\ \mathbf{open}\ r_2\ .\ \overline{\mathbf{open}}\ read\ ] \\
& \mid \{\mathrm{P}\})
\end{aligned}
$$

$$enter : \curvearrowright^{1} [\, \curvearrowright^{1} [\, \underline{V}^{0} \,]\,]$$

$$read,\ write,\ r_1,\ r_2,\ w_1 : \curvearrowright^{1} [\, \underline{V}^{0} \,]$$

$$c_1,\ c_2 : \curvearrowright^{1} [\, \underline{V}^{\omega} \,] \qquad\qquad n_1 : \underline{V}^{\omega}$$

$$n,\ x : \underline{V}^{\omega} \qquad\qquad \{P\} : \underline{V}^{\omega}$$

The result

- Auxiliary reductions, and even some primary reductions are confluent, the only interference is the mutual selections of *read*s and *write*s inside channels.

Conclusion

- verification made easy by typing, but
- typing is not easy

$$m\,[\,\overline{\mathbf{out}}\;n \mid n\,[\,\mathbf{out}\;m\,.\,(!\,\overline{\mathbf{in}}\;n \mid !\,\overline{\mathbf{out}}\;n) \mid p[P]\,]\,]$$

--- *The End* ---