(Not that) **Old and New Results**
on
**Probabilistic Intersection Type Systems**

Flavien BREUVART, Ugo Dal Lago

Focus, Inria team, Bologna

GdR-LL: June 12-13 2016
Randomized Programming

Motivations

Randomized Algorithmics
- Efficiency analysis

Cryptography
- Security

Machine Learning
- Modeling

Probabilistic λ-calculus
(Weak head-reduction)

\[ M, N ::= x | \lambda x. M | M \ N | M \oplus N \]

\[ (\lambda x. M) \ N \xrightarrow{1} M[N/x] \]

\[ M \oplus N \xrightarrow{1/2} M \]

\[ M \oplus N \xrightarrow{1/2} N \]

\[ A ::= \lambda u x. x(\lambda y. (u(Sx) \oplus y))I \]

\[ \text{Prob}(YA0 \downarrow) < 1 \]
Probability of Normalization: A difficult problem

Problem PConv:
What is the probability $p$ of convergence of a given program $M$?

PConv is $\Pi^0_2$-complete: one derivation is insufficient

The following (and any variation) is impossible to get from r.e. type systems:

$$\text{Prob}(M \downarrow) = p \iff \frac{\pi}{\vdash M : p \cdot \alpha}$$

Probabilistic dependency is not type dependency

**Probabilistic Dependency**
- non-uniform; randomized;
- only propagate dependency

**Type Dependency**
- uniform; non-deterministic;
- waiting for data to propagate
Some Recursion Theory

<table>
<thead>
<tr>
<th>The lower-bound problem is $\Sigma^0_1$-complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asking whether $\text{Prob}(M \downarrow) &gt; p$ is recursively enumerable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The upper-bound problem is $\Sigma^0_2$-complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asking whether $\text{Prob}(M \downarrow) &lt; p$ is a problem of the form:</td>
</tr>
<tr>
<td>$\exists x \forall y, \phi(x, y)$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The exact bound problem (PConv) is $\Pi^0_2$-complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asking whether $\text{Prob}(M \downarrow) = p$ is a problem of the form:</td>
</tr>
<tr>
<td>$\forall x \exists y, \phi(x, y)$</td>
</tr>
</tbody>
</table>
Non deterministic IT systems:
Idempotent Intersection Types

Grammar

(types) \( \alpha, \beta \) := \* | \( a \rightarrow \alpha \)

(intersections) \( a, b \) finite sets of types

(context) \( \Gamma, \Delta \) := \_ | \( x : a, \Gamma \)

(sequent) \( s \) := \( \Gamma \vdash M : \alpha \)

Weak head reduction

Rule furnishing a type to \( \lambda x.\Omega \)
Non-deterministic IT systems: Non-idempotent IT [De Carvalho]

Grammar

(types) \( \alpha, \beta := \ast | a \rightarrow \alpha \)

(intersections) \( a, b \) finite multisets of types

(context) \( \Gamma, \Delta := \_ | x : a, \Gamma \)

(sequent) \( s := \Gamma \vdash M : \alpha \)

\[
\begin{align*}
\Gamma \vdash M : \alpha & \quad \Gamma \vdash N : \alpha \\
\Gamma \vdash M \oplus N : \alpha & \quad \Gamma \vdash M \oplus N : \alpha \\
\Gamma \vdash \lambda x.M : \ast & \\
\Gamma ; x : a \vdash M : \alpha & \quad \Gamma \vdash M : a \rightarrow \beta \quad \left[ \Delta_\alpha \vdash N : \alpha \mid \alpha \in a \right]
\end{align*}
\]

Multisets of intersections
Multiplicities corresponding to different uses
Probabilistic IT systems:  
Weight monad [Ehrhard et al]

| Grammar |
|---|---|
| (types) | $\alpha, \beta := \ast \mid a \rightarrow p \cdot \alpha$ |
| (intersections) | $a, b$ finite multisets of types |
| (weight) | $p, q \in \{0, \ldots, 1\}$ |
| (context) | $\Gamma, \Delta := \_ \mid x : a, \Gamma$ |
| (sequent) | $s := \Gamma \vdash M : p \cdot \alpha$ |

| Probability |
|---|---|
| for the function to get this result |

| Sums |
|---|---|
| weighted but non-deterministic |

\[
\begin{align*}
\Gamma \vdash M : p \cdot \alpha & \quad \Gamma \vdash N : \alpha \\
\Gamma \vdash M \oplus N : \frac{p}{2} \cdot \alpha & \quad \Gamma \vdash N \oplus M : \frac{p}{2} \cdot \alpha \\
\vdash \lambda x.M : 1 \cdot \ast & \\
\Gamma ; x : a \vdash M : p \cdot \alpha & \quad \Gamma \vdash M : p \cdot (a \rightarrow q \cdot \beta) \\
\Gamma \vdash \lambda x.M : 1 \cdot (a \rightarrow p \cdot \alpha) & \quad \Gamma + \sum \Delta \vdash M \ N : pq(\prod i ; r_i) \cdot \beta
\end{align*}
\]
Probabilistic IT systems: Weight monad [Ehrhard et al]

Grammar

| (types)     | \( \alpha, \beta \) : = \ast \mid \mathit{a} \rightarrow p \cdot \alpha |
| (intersections) | \( a, b \) finite multisets of types |
| (weight)    | \( p, q \) \in \{0, \ldots, 1\} |
| (context)   | \( \Gamma, \Delta \) : = \_ \mid x : \mathit{a}, \Gamma |
| (sequent)   | \( s \) : = \Gamma \vdash M : p \cdot \alpha |

A derivation is an execution
the weight is the probability to get this execution

\[ M : \frac{1}{2^3} \cdot \alpha \rightarrow^1 \cdot \]

\[ \lambda x. N : 1 \cdot \alpha \]
Summing all possible executions?

The (naive) theorem

\[
\text{Prob}(M \Downarrow) = \sum \left[ p \mid \frac{\pi}{\vdash M : p \cdot \alpha} \right]
\]

Not summing too much

**Issue:**

\[
\vdash \lambda x.x : 1 \cdot * \\
x : [\alpha] \vdash x : 1 \cdot \alpha \\
\vdash \lambda x.x : 1 \cdot ([\alpha] \rightarrow 1 \cdot \alpha)
\]

**Solution:**

\[
\sum \left[ p \mid \frac{\pi}{\vdash M : p \cdot *} \right]
\]

Summing all of them

**Issue:**

\[
M : [\alpha, \alpha] \rightarrow * \\
N_1 : 1 \cdot \alpha \\
N_2 : 1 \cdot \alpha \\
N_1 \oplus N_2 : \frac{1}{2} \alpha \\
N_1 \oplus N_2 : \frac{1}{2} \alpha \\
M \ (N_1 \oplus N_2) : \frac{1}{4} \cdot *
\]

**Solution:**

Use keyed-multisets
Theorem and implications

The theorem

\[ \text{Prob}(M \downarrow) = \sum W(M) \]

where \( W(M) = \left[ p \, \right| \, \frac{\pi}{\vdash M : p \cdot *} \] \)

Lower-bound problem (\( \Sigma^0_1 \))

Prob. of conv. of \( M > q \) \iff \( \exists P \subseteq_f W(M), \sum_{p \in P} p > q \)

Upper-bound problem (\( \Sigma^0_2 \))

Prob. of conv. of \( M < q \) \iff \( \exists q', \forall P \subseteq_f W(M), \sum_{p \in P} p < q' < q \)

The exact bound problem is \( \Pi^0_2 \)
Sketching the proof

**Cut Elimination**

\[
\begin{array}{c}
\pi \\
\vdash M : p \cdot * \\
\sim \mapsto \\
\vdash M' : \frac{p}{q} \cdot *
\end{array}
\]

such that:

- \( M \xrightarrow{q} M' \),
- \( \sim \mapsto \) is normalizing and deterministic

**Small-step distrib.**

\[
\begin{array}{c}
\Lambda_R \\
\xrightarrow{\text{deriv.}} \\
\Pi_R \\
\vdash V : 1 \cdot *
\end{array}
\]

**Value determinism**

\[
\forall \text{ normal form } V, \quad \text{Unicity of derivation} \\
\vdash V : 1 \cdot *
\]

**Big-step distribution**

\[
\begin{array}{c}
\Lambda \\
\xleftarrow{\text{eval}} \\
\Pi \\
\vdash \Lambda \rightarrow M \\
\vdash \Pi \\
\vdash \Lambda_V \\
\xrightarrow{\text{deriv.}} \\
\Pi_V
\end{array}
\]

**Conclusion**

\[
\sum_{V} P(M \rightarrow V) = \sum_{W} W(M)
\]
## Toward distributions of derivations

### Unsatisfactory completeness

<table>
<thead>
<tr>
<th>Uninformative derivations</th>
<th>Quantifying over ALL derivations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each derivation carries the information regarding one possible execution.</td>
<td>Distinguishing derivations and looking for new one is not really computationally-friendly.</td>
</tr>
</tbody>
</table>
Toward distributions of derivations

Unsatisfactory completeness

**Uninformative derivations**
Each derivation carries the information regarding **one** possible execution.

**Quantifying over ALL derivations**
Distinguishing derivations and looking for new one is not really computationally-friendly.

---

A monad of probabilistic distributions over types

- (types) \( \alpha, \beta \) := \* \mid a \rightarrow \tau
- (intersections) \( a, b \) finite multisets of types
- (monadic distributions) \( \rho, \tau \) finite distribution over types

---

A comonad of probabilistic distributions over intersections

- (types) \( \alpha, \beta \) := \* \mid A \rightarrow p \cdot \alpha
- (intersections) \( a, b \) finite multisets of types
- (comonadic distributions) \( A, B \) finite distribution over intersections
An unavoidable issue: Probabilistic dependency

\[ \vdash (\lambda x. c_\alpha \oplus x) (c_\beta \oplus \Omega) : \frac{1}{2} \alpha + \frac{1}{4} \beta \]
An unavoidable issue: Probabilistic dependency

\[ \vdash c_\beta \oplus \Omega : \frac{1}{2} \beta \]

\[ \vdash (\lambda x. c_\alpha \oplus x) \ (c_\beta \oplus \Omega) : \frac{1}{2} \alpha + \frac{1}{4} \beta \]
An unavoidable issue: Probabilistic dependency

\[
\begin{align*}
\frac{1}{2}[] + \frac{1}{2}[^{\beta}] & \vdash c_{\alpha} \oplus x : \frac{1}{2} \alpha + \frac{1}{2} \beta \\
\vdash \lambda x. c_{\alpha} \oplus x : \left\{ \frac{1}{2}[] + \frac{1}{2}[^{\beta}] \right\} \rightarrow \left\{ \frac{1}{2} \alpha + \frac{1}{2} \beta \right\} & \vdash c_{\beta} \oplus \Omega : \frac{1}{2} \beta \\
\vdash (\lambda x. c_{\alpha} \oplus x) (c_{\beta} \oplus \Omega) : \frac{1}{2} \alpha + \frac{1}{4} \beta
\end{align*}
\]
An unavoidable issue: Probabilistic dependency

Forgotten dependency

\[
\begin{align*}
    x : \frac{1}{2}[] + \frac{1}{2}[\beta] & \vdash c_\alpha \oplus x : \frac{1}{2}\alpha + \frac{1}{2}\beta \\
    \vdash \lambda x. c_\alpha \oplus x : \left\{\frac{1}{2}[] + \frac{1}{2}[\beta]\right\} & \rightarrow \left\{\frac{1}{2}\alpha + \frac{1}{2}\beta\right\} & \vdash c_\beta \oplus \Omega : \frac{1}{2}\beta \\
    \vdash (\lambda x. c_\alpha \oplus x) (c_\beta \oplus \Omega) : \frac{1}{2}\alpha + \frac{1}{4}\beta
\end{align*}
\]

No such a rule

No reasonable and systematic rule can perform this step.
### Distributions over sequents

#### Grammar

<table>
<thead>
<tr>
<th>(types)</th>
<th>$\alpha, \beta : = ^* \mid a \rightarrow \alpha$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(intersections)</td>
<td>$a, b$ finite multisets of types</td>
</tr>
<tr>
<td>(context)</td>
<td>$\Gamma, \Delta : = _ \mid x : a, \Gamma$</td>
</tr>
<tr>
<td>(logical sequent)</td>
<td>$l : = \overline{\Gamma} \vdash \alpha$</td>
</tr>
<tr>
<td>(sequent distributions)</td>
<td>$L$ Distributions over logical sequents</td>
</tr>
<tr>
<td>(type sequent)</td>
<td>$s : = (\tilde{x}, M) \vdash D$</td>
</tr>
</tbody>
</table>

### Rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Premise</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x, x) \vdash {[\alpha] \vdash \alpha}$</td>
<td>$M \vdash D \quad N \vdash E$</td>
<td>$M \oplus N \vdash \frac{1}{2} D + \frac{1}{2} E$</td>
</tr>
<tr>
<td>$M \vdash {p_i \cdot (\Gamma_i; x : a_i \vdash \alpha_i) \mid i \leq n}$</td>
<td>$\lambda x. M \vdash {p_i \cdot \Gamma_i \vdash a_i \rightarrow \alpha_i \mid i \leq n} + {(1 - \sum_i p_i) \cdot ^*}$</td>
<td></td>
</tr>
<tr>
<td>$M \vdash {p \cdot (\Gamma \vdash [\alpha_{i,1}, \ldots, \alpha_{i,m_i}] \rightarrow \beta) \mid i \leq n}$</td>
<td>$\forall i, j, N \vdash D_{i,j}$</td>
<td></td>
</tr>
<tr>
<td>$M \vdash {p_i \prod_{j \leq m_i} D_{i,j}(\Delta_{i,j} \vdash \alpha_{i,j})} \cdot (\Gamma + \sum_j \Delta_{i,j} \vdash \beta_i) \mid \forall (\Delta_{i,j})_j$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flavien BREUVART, Ugo Dal Lago

Focus Probabilistic Intersection Type Systems
Distributions over sequents

Grammar

(types) \( \alpha, \beta \) := \( \ast \mid a \rightarrow \alpha \)

(intersections) \( a, b \) finite multisets of types

(context) \( \Gamma, \Delta \) := \_ \mid x : a, \Gamma

(logical sequent) \( l \) := \( \Gamma \vdash \alpha \)

(sequent distributions) \( L \) Distributions over logical sequents

(type sequent) \( s \) := \( (\vec{x}, M) \vdash D \)

Theorem

\[
\text{Prob}(M \Downarrow) = \text{Sup} \left\{ D(\vdash \ast) \mid \frac{\pi}{M \vdash D} \right\}
\]
Conclusion

Past

[Ehr, Pag, Tas]
A fully abstract model for $\Lambda_{\oplus}$.
Sketched intersection type system.

Now

Refinement of the ITS.
Combinatorial and simpler proof of completeness.
Collapsed intersection type system.

Future

Fixpoint/coninductive proofs
$\rightsquigarrow$ unbounded terms:
while coin continue $\Sigma^0_1$, checkable or inferenceable fragments