(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

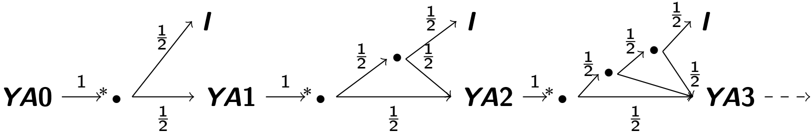
Modeling

Probabilistic λ-calculus (Weak head-reduction)

$$M, N \;:=\; x \mid \lambda x.M \mid M\ N \mid M \oplus N$$

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

$$M \oplus N \xrightarrow{\frac{1}{2}} M \qquad M \oplus N \xrightarrow{\frac{1}{2}} N$$



$$\boldsymbol{A} := \lambda ux.x(\lambda y.(u(\boldsymbol{S}x) \oplus y)\boldsymbol{I}$$

$$\mathrm{Prob}(\boldsymbol{YA0} \Downarrow) < 1$$

Probability of Normalization: A difficult problem

Problem PConv:

What is the probability p of convergence of a given program M?

PConv is Π^0_2-complete: one derivation is insufficient

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

$$\mathrm{Prob}(M \Downarrow) = p \quad \Leftrightarrow \quad \frac{\pi}{\vdash M : p{\cdot}\alpha}$$

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

The lower-bound problem is Σ_1^0-complete

Asking whether $\text{Prob}(M \Downarrow) > p$ is recursively enumerable.

The upper-bound problem is Σ_2^0-complete

Asking whether $\text{Prob}(M \Downarrow) < p$ is a problem of the form:

$$\exists x \forall y, \phi(x, y)$$

The exact bound problem (PConv) is Π_2^0-complete

Asking whether $\text{Prob}(M \Downarrow) = p$ is a problem of the form:

$$\forall x \exists y, \phi(x, y)$$

Non deterministic IT systems: Idempotent Intersection Types

Grammar

(types)	α, β	:=	$* \mid a \to \alpha$
(intersections)	a, b		finite sets of types
(context)	Γ, Δ	:=	$\_ \mid x : a, \Gamma$
(sequent)	s	:=	$\Gamma \vdash M : \alpha$

Weak head reduction

Rule furnishing a type to $\lambda x.\Omega$

$$\frac{}{\Gamma, x : \{\alpha\} \vdash x : \alpha} \qquad \frac{\Gamma \vdash M : \alpha}{\Gamma \vdash M \oplus N : \alpha} \qquad \frac{\Gamma \vdash N : \alpha}{\Gamma \vdash M \oplus N : \alpha} \qquad \frac{}{\Gamma \vdash \lambda x.M : *}$$

$$\frac{\Gamma ; x : a \vdash M : \alpha}{\Gamma \vdash \lambda x.M : a \to \alpha} \qquad \frac{\Gamma \vdash M : a \to \beta \qquad \left\{ \Gamma \vdash N : \alpha \,\middle|\, \alpha \in a \right\}}{\Gamma \vdash M\ N : \beta}$$

Non-deterministic IT systems: Non-idempotent IT [De Carvalho]

Grammar

(types)	α, β	$:=$	$* \mid a \to \alpha$
(intersections)	a, b		finite multisets of types
(context)	Γ, Δ	$:=$	$\_ \mid x : a, \Gamma$
(sequent)	s	$:=$	$\Gamma \vdash M : \alpha$

Multisets of intersections

Multiplicities corresponding to different uses

$$\frac{}{x : [\alpha] \vdash x : \alpha} \qquad \frac{\Gamma \vdash M : \alpha}{\Gamma \vdash M \oplus N : \alpha} \qquad \frac{\Gamma \vdash N : \alpha}{\Gamma \vdash M \oplus N : \alpha} \qquad \frac{}{\vdash \lambda x.M : *}$$

$$\frac{\Gamma; x : a \vdash M : \alpha}{\Gamma \vdash \lambda x.M : a \to \alpha} \qquad \frac{\Gamma \vdash M : a \to \beta \qquad \left[\Delta_\alpha \vdash N : \alpha \,\middle|\, \alpha \in a\right]}{\Gamma + \sum \Delta_\alpha \vdash M\ N : \beta}$$

Probabilistic IT systems: Weight monad [Ehrhard et al]

Grammar

(types)	α, β	$:= \; * \mid a \to p \cdot \alpha$
(intersections)	a, b	finite multisets of types
(weight)	p, q	$\in \; \{0, ..., 1\}$
(context)	Γ, Δ	$:= \; \_ \mid x : a, \Gamma$
(sequent)	s	$:= \; \Gamma \vdash M : p \cdot \alpha$

Probability

for the function to get this result

Sums

weighted but non-deterministic

$$\frac{}{x : [\alpha] \vdash x : 1 \cdot \alpha} \qquad \frac{\Gamma \vdash M : p \cdot \alpha}{\Gamma \vdash M \oplus N : \frac{p}{2} \cdot \alpha} \qquad \frac{\Gamma \vdash N : \alpha}{\Gamma \vdash M \oplus N : \frac{p}{2} \cdot \alpha} \qquad \frac{}{\vdash \lambda x.M : 1 \cdot *}$$

$$\frac{\Gamma; x : a \vdash M : p \cdot \alpha}{\Gamma \vdash \lambda x.M : 1 \cdot (a \to p \cdot \alpha)} \qquad \frac{\Gamma \vdash M : p \cdot (a \to q \cdot \beta) \qquad \left[\Delta_\alpha \vdash N : r_\alpha \cdot \alpha \;\middle|\; \alpha \in a \right]}{\Gamma + \sum \Delta_\alpha \vdash M \; N : pq(\prod_i r_i) \cdot \beta}$$

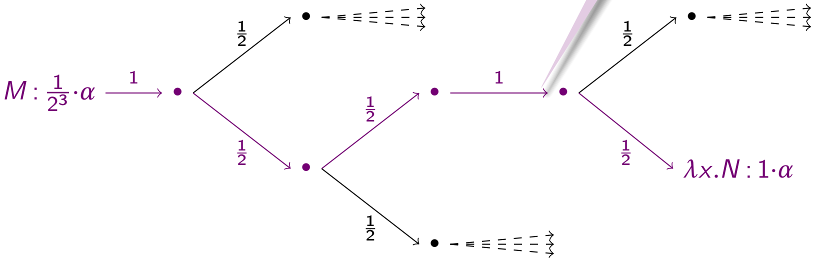
Probabilistic IT systems: Weight monad [Ehrhard et al]

Grammar

(types)	α, β	$:= \ * \mid a \to p \cdot \alpha$
(intersections)	a, b	finite multisets of types
(weight)	p, q	$\in \{0, \dots, 1\}$
(context)	Γ, Δ	$:= \ \_ \mid x : a, \Gamma$
(sequent)	s	$:= \ \Gamma \vdash M : p \cdot \alpha$

A derivation is an execution

the weight is the probability to get this execution



Summing all possible executions?

The (naive) theorem

$$\mathrm{Prob}(M \Downarrow) = \sum \left[p \;\middle|\; \frac{\pi}{\vdash M : p{\cdot}\alpha} \right]$$

Not summing too much

Issue:

$$\frac{}{\vdash \lambda x.x : 1{\cdot}*}$$

$$\frac{x : [\alpha] \vdash x : 1{\cdot}\alpha}{\vdash \lambda x.x : 1{\cdot}([\alpha] \to 1{\cdot}\alpha)}$$

Solution:

$$\sum \left[p \;\middle|\; \frac{\pi}{\vdash M : p{\cdot}*} \right]$$

Summing all of them

Issue:

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

Solution:

Use keyed-multisets

Theorem and implications

The theorem

$$\text{Prob}(M \Downarrow) \;=\; \sum W(M)$$

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

Lower-bound problem (Σ_1^0)

Prob. of conv. of M $> q$ iff

$$\exists P \subseteq_f W(M), \quad \sum_{p \in P} p > q$$

Upper-bound problem (Σ_2^0)

Prob. of conv. of M $< q$ iff

$$\exists q', \forall P \subseteq_f W(M), \quad \sum_{p \in P} p < q' < q$$

The exact bound problem is Π_2^0

Sketching the proof

Cut Elimination

$$\frac{\pi}{\vdash M : p\cdot *} \rightsquigarrow \frac{\pi'}{\vdash M' : \frac{p}{q}\cdot *}$$

such that:

- $M \xrightarrow{q} M'$,
- $\rightsquigarrow$ is normalizing and deterministic

Small-step distrib.

$$\begin{array}{ccc} \Lambda_R & \xrightarrow{\text{deriv.}} & \Pi_R \\ \downarrow \text{red} & & \downarrow \text{red} \\ \Lambda & \xrightarrow{\text{deriv.}} & \Pi \end{array}$$

Value determinism

$\forall$ normal form V,

Unicity of derivation

$$\vdash V : 1\cdot *$$

$$\frac{}{\vdash \lambda x.M : 1\cdot *}$$

Big-step distribution

$$\begin{array}{ccc} \Lambda & \xrightarrow{\text{deriv.}} & \Pi \\ \downarrow \text{eval} & & \downarrow \text{eval} \\ \Lambda_V & \xrightarrow{\text{deriv.}} & \Pi_V \end{array}$$

Conclusion

$$\sum_V P(M \to V) = \sum W(M)$$

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.

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)	α, β	$:= \ * \mid a \to \tau$
(intersections)	a, b	finite multisets of types
(monadic distributions)	ρ, τ	finite distribution over types

A comonad of probabilistic distributions over intersections

(types)	α, β	$:= \ * \mid A \to p{\cdot}\alpha$
(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

$$\frac{\vdash c_\beta \oplus \Omega \;:\; \frac{1}{2}\beta}{\vdash (\lambda x.c_\alpha \oplus x)\;(c_\beta \oplus \Omega) \;:\; \frac{1}{2}\alpha + \frac{1}{4}\beta}$$

An unavoidable issue: Probabilistic dependency

$$\dfrac{\dfrac{x : \frac{1}{2}[] + \frac{1}{2}[\beta] \vdash c_\alpha \oplus x \ : \ \frac{1}{2}\alpha + \frac{1}{2}\beta}{\vdash \lambda x.c_\alpha \oplus x \ : \ \left\{\frac{1}{2}[] + \frac{1}{2}[\beta]\right\} \to \left\{\frac{1}{2}\alpha + \frac{1}{2}\beta\right\}} \qquad \vdash c_\beta \oplus \Omega \ : \ \frac{1}{2}\beta}{\vdash (\lambda x.c_\alpha \oplus x)\ (c_\beta \oplus \Omega) \ : \ \frac{1}{2}\alpha + \frac{1}{4}\beta}$$

An unavoidable issue: Probabilistic dependency

Forgotten dependency

$$\dfrac{\dfrac{x : \frac{1}{2}[] + \frac{1}{2}[\beta] \vdash c_\alpha \oplus x \;:\; \frac{1}{2}\alpha + \frac{1}{2}\beta}{\vdash \lambda x.c_\alpha \oplus x \;:\; \left\{\frac{1}{2}[] + \frac{1}{2}[\beta]\right\} \to \left\{\frac{1}{2}\alpha + \frac{1}{2}\beta\right\}} \qquad \vdash c_\beta \oplus \Omega \;:\; \frac{1}{2}\beta}{\vdash (\lambda x.c_\alpha \oplus x)\ (c_\beta \oplus \Omega) \;:\; \frac{1}{2}\alpha + \frac{1}{4}\beta}$$

No such a rule

No reasonable and systematic rule can perform this step.

Distributions over sequents

Grammar

(types)	α,β	$:= \ * \mid a \to \alpha$
(intersections)	a, b	finite multisets of types
(context)	Γ,Δ	$:= \ \_ \ \mid \ x : a, \Gamma$
(logical sequent)	l	$:= \ \Gamma \vdash \alpha$
(sequent distributions)	L	Distributions over logical sequents
(type sequent)	s	$:= \ (\vec{x}, M) \Vdash D$

$$\frac{}{(x,x) \Vdash \{[\alpha] \vdash \alpha\}} \qquad \frac{M \Vdash D \qquad N \Vdash E}{M \oplus N \Vdash \frac{1}{2} D + \frac{1}{2} E} \qquad \frac{}{M \Vdash \{\}}$$

$$\frac{M \Vdash \{p_i \cdot (\Gamma_i; x : a_i \vdash \alpha_i) \mid i \leq n\}}{\lambda x.M \Vdash \{p_i \cdot \Gamma_i \vdash a_i \to \alpha_i \mid i \leq n\} + \{(1 - \sum_i p_i) \cdot *\}}$$

$$\frac{M \Vdash \left\{p \cdot (\Gamma \vdash [\alpha_{i,1}, \ldots, \alpha_{i,m_i}] \to \beta) \,\middle|\, i \leq n\right\} \qquad \forall i,j,\ N \Vdash D_{i,j}}{M \ \ N \Vdash \sum_{i \leq n} \left\{(p_i \prod_{j \leq m_i} D_{i,j}(\Delta_{i,j} \vdash \alpha_{i,j})) \cdot (\Gamma + \sum_j \Delta_{i,j} \vdash : \beta_i) \,\middle|\, \forall (\Delta_{i_j})_j\right\}}$$

Distributions over sequents

Grammar

(types)	α, β	$:= \ * \mid a \rightarrow \alpha$
(intersections)	a, b	finite multisets of types
(context)	Γ, Δ	$:= \ \_ \ \mid \ x : a, \Gamma$
(logical sequent)	l	$:= \ \Gamma \vdash \alpha$
(sequent distributions)	L	Distributions over logical sequents
(type sequent)	s	$:= \ (\vec{x}, M) \Vdash D$

Theorem

$$\mathrm{Prob}(M \Downarrow) \ = \ \mathrm{Sup}\left\{ D(\vdash *) \middle| \frac{\pi}{M \Vdash D} \right\}$$

Conclusion

Past

[Ehr,Pag,Tas]

A fully abstract model for $\Lambda_\oplus$.

Sketched intersection type system.

Now

Refinment of the ITS.

Combinatorial and simpler proof of completeness.

Collapsed intersection type system.

future

Fixpoint/conindunctive proofs

$\rightsquigarrow$ unbounded terms: `while coin continue`

Σ^0_1, cherckable or inferenceable fragments