On Higher-Order Probabilistic Subrecursion

Flavien BREUVART, Ugo DAL LAGO, Agathe HERROU

Focus, Inria team, Bologna[1]

LC&A: 2016 September 6

[1] I am now based at University Paris 13

What Is the Result of a Probabilistic Computation?

A probabilistic distribution

What Is the Result of a Probabilistic Computation?

A probabilistic distribution

What distributions are generated by arbitrary terminating programs?

What Is the Result of a Probabilistic Computation?

A probabilistic distribution

What distributions are generated by arbitrary terminating programs?

Any recursively approximable function $f : \mathbb{N} \to \mathbb{R}$ summing to 1.
(Due to almost sure termination)

What Is the Result of a Probabilistic Computation?

A probabilistic distribution

What distributions are generated by arbitrary terminating programs?

Any recursively approximable function $f:\mathbb{N}\to\mathbb{R}$ summing to 1.
(Due to almost sure termination)

- **support(f) can be any r.e. set**
- **$f(0)$ can be any computable real**

Probability of termination $=1$.
eg:

```
x := 0;
while (coin = 0) do x++;
ret 1 !
```

What Is the Result of a Probabilistic Computation?

A probabilistic distribution

What distributions are generated by arbitrary terminating programs?

Any recursively approximable function $f : \mathbb{N} \to \mathbb{R}$ summing to 1.
(Due to almost sure termination)

A sole randomized result

What can be computed by arbitrary randomized algorithms?

What Is the Result of a Probabilistic Computation?

A probabilistic distribution

What distributions are generated by arbitrary terminating programs?

Any recursively approximable function $f : \mathbb{N} \to \mathbb{R}$ summing to 1.
(Due to almost sure termination)

A sole randomized result

What can be computed by arbitrary randomized algorithms?

Only recursive programs...
(Due to Church Thesis)

What Is the Result of a Probabilistic Computation?

A probabilistic distribution

What distributions are generated by arbitrary terminating programs?

Any recursively approximable function $f : \mathbb{N} \to \mathbb{R}$ summing to 1.
(Due to almost sure termination)

A sole randomized result

What can be computed by arbitrary randomized algorithms?

Only recursive programs...
(Due to Church Thesis)

How does this extends for sub-recursive classes?

Extensional Approach

Are all distributions deterministically representable?

Intentional Approach

Can we always perform a derandomization?

When is Probabilistic Choice Necessary?

Are all distributions deterministically representable?

Finite Representation

$$\texttt{prob}\Big(P \rightsquigarrow k\Big) = P^*(k) \quad \in \mathbb{Q}$$

Functional Representation

$$\texttt{prob}\Big(P \rightsquigarrow k\Big) = \lim_{n\to\infty} P^*(n,k)$$

$$\text{s.t. } \sum_k \mathrm{Err}(P^*(n,k)) \leq \frac{1}{n}$$

Parametrization

For $P : \mathbb{N} \to \mathbb{N}$

Can we always perform a derandomization?

Monte Carlo

$f(n)$ reached with probability $> \frac{1}{2} + \epsilon$

Las Vegas

$f(n)$ reached and ascertained with probability $> \epsilon$

Dynamic/Strict bounds

Make ϵ dynamic/null

Different classes

Complexity **Primitive Rec.** **HO Prim. Rec.** **Recursive**

When is Probabilistic Choice Necessary?

Are all distributions deterministically representable?

Finite Representation

$$\mathtt{prob}\Big(P \rightsquigarrow k\Big) = P^*(k) \ \in \mathbb{Q}$$

Functional Representation

$$\mathtt{prob}\Big(P \rightsquigarrow k\Big) = \lim_{n\to\infty} P^*(n,k)$$

$$\text{s.t. } \sum_k \mathrm{Err}(P^*(n,k)) \leq \frac{1}{n}$$

Parametrization

For $P : \mathbb{N} \to \mathbb{N}$

Can we always perform a derandomization?

Monte Carlo

$f(n)$ reached with probability $> \frac{1}{2} + \epsilon$

Las Vegas

$f(n)$ reached and ascertained with probability $> \epsilon$

Dynamic/Strict bounds

Make ϵ dynamic/null

Different classes

Complexity **Primitive Rec.** **HO Prim. Rec.** **Recursive**

When is Probabilistic Choice Necessary?

Are … determinis… able?

Exponential Blow Up

Finite Representation

$$\mathtt{prob}\Big(P \rightsquigarrow k\Big) = P^*(k) \;\in \mathbb{Q}$$

Functional Representation

$$\mathtt{prob}\Big(P \rightsquigarrow k\Big) = \lim_{n\to\infty} P^*(n,k)$$

$$\text{s.t. } \sum_k \mathrm{Err}(P^*(n,k)) \leq \frac{1}{n}$$

Parametrization

For $P : \mathbb{N} \to \mathbb{N}$

Can we always perform a derandomization?

BPP

Monte Carlo

$f(n)$ reached with probability $> \frac{1}{2} + \epsilon$

ZPP

Las Vegas

$f(n)$ reached and ascertained with probability $> \epsilon$

PP,NP

Dynamic/Strict bounds

Make ϵ dynamic/null

Different classes

Complexity	Primitive Rec.	HO Prim. Rec.	Recursive

When is Probabilistic Choice Necessary?

Are all distributions deterministically representable?

~~**Finite Representation**~~

$$\cancel{\texttt{prob}\Big(P \rightsquigarrow k\Big) = P^*(k)} \in \mathbb{Q}$$

Functional Representation

$$\texttt{prob}\Big(P \rightsquigarrow k\Big) = \lim_{n\to\infty} P^*(n,k)$$

$$\text{s.t. } \sum_k \mathrm{Err}(P^*(n,k)) \leq \frac{1}{n}$$

Parametrization

For $P : \mathbb{N} \to \mathbb{N}$

Can we always perform a derandomization?

Monte Carlo

$f(n)$ reached with probability $> \frac{1}{2} + \epsilon$

Las Vegas

$f(n)$ reached and ascertained with probability $> \epsilon$

Dynamic/Strict bounds

Make ϵ dynamic/null

Different classes

Complexity **Primitive Rec.** **HO Prim. Rec.** **Recursive**

When is Probabilistic Choice Necessary?

Are all distributions deterministically representable?

Depends of Prob. Operators

Finite Representation

$$\texttt{prob}\left(P \rightsquigarrow k\right) = P^*(k) \;\in \mathbb{Q}$$

Functional Representation

$$\texttt{prob}\left(P \rightsquigarrow k\right) = \lim_{n\to\infty} P^*(n,k)$$

$$\text{s.t. } \sum_k \mathrm{Err}(P^*(n,k)) \le \frac{1}{n}$$

Parametrization

For $P : \mathbb{N} \to \mathbb{N}$

Can we always perform a derandomization?

Monte Carlo

$f(n)$ reached with probability $> \frac{1}{2} + \epsilon$

Las Vegas

$f(n)$ reached and ascertained with probability $> \epsilon$

Dynamic/Strict bounds

Make ϵ dynamic/null

Different classes

Complexity	Primitive Rec.	HO Prim. Rec.	Recursive

Gödel's System $\mathbb{T}$: A Language for HO Primitive Recursion

Gödel's System $\mathbb{T}$ (Call-by-Value)

$$M, N, L \ ::= \ x \mid \lambda x.M \mid M\ N \mid \mathbf{rec} \mid \mathbf{0} \mid \mathbf{S}$$

$$\mathbf{rec}\ M\ N\ \mathbf{0} \to M \qquad\qquad \mathbf{rec}\ M\ N\ (\mathbf{S}\boldsymbol{n}) \to N\ \boldsymbol{n}\ (\mathbf{rec}\ M\ N\ \boldsymbol{n})$$

$$\frac{}{\Gamma, x : A \vdash x : A} \qquad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \to B} \qquad \frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\ N : B}$$

$$\frac{}{\Gamma \vdash \mathbf{0} : \mathbb{N}} \qquad \frac{}{\Gamma \vdash \mathbf{S} : \mathbb{N} \to \mathbb{N}} \qquad \frac{}{\Gamma \vdash \mathbf{rec} : A \to (\mathbb{N} \to A \to A) \to \mathbb{N} \to A}$$

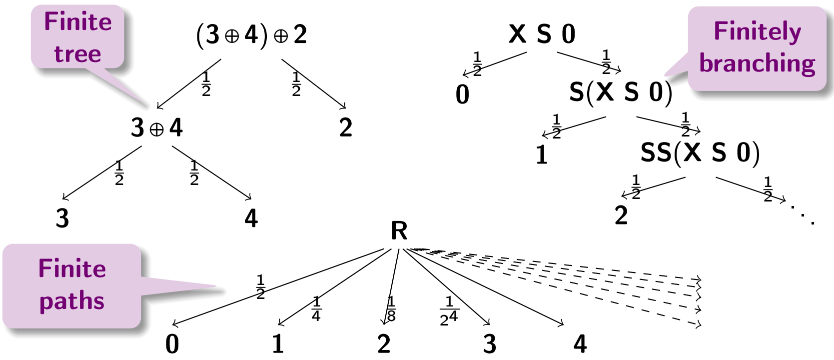
An Extremely Expressive System

- Corresponds to provably total functions in Peano arithmetic
- Encodes any monad (states, exceptions, continuations...)

Probabilistic Systems $\mathbb{T}$

Different Probabilistic Extensions for System $\mathbb{T}$

$$M, N, L ::= x \mid \lambda x.M \mid M\ N \mid \mathbf{rec} \mid \mathbf{0} \mid \mathbf{S} \mid M \oplus N \mid \mathbf{X} \mid \mathbf{R}$$



$\mathbb{T}^{\oplus,\mathbf{R},\mathbf{X}}$ is AST

$\mathbb{T}^{\oplus} \subset \mathbb{T}^{\mathbf{R}} = \mathbb{T}^{\mathbf{X}}$

Almost Sure Convergence

$\mathbb{T}^{\oplus,\mathbf{R},\mathbf{X}}$ is Almost Surely Terminating

$$\forall M \in \mathbb{T}^{\oplus,\mathbf{R},\mathbf{X}}, \qquad \texttt{Prob}(M \Downarrow) = 1$$

Reducibility

1) By induction on A, we define $\texttt{Red}_A \subseteq \{M \mid \vdash M : A\}$,
2) By induction on $\to$: $M \to N \in \texttt{Red}_A \;\Rightarrow\; M \in \texttt{Red}_A$,

2′) $\texttt{Red}_A$ is inhabited (ind. on A)

3) By induction on A: $\texttt{Red}_A \subseteq \texttt{ASC}$,
4) By induction on M: $\vdash M : A \;\Rightarrow\; M \in \texttt{Red}_A$,

Specificities for Probabilities

Item 3) becomes:

3) $\texttt{Red}_A$ are exactly the ASC terms that are evaluated into $[\![M]\!] \subseteq \texttt{Red}_A$.

We also need a technical lemma

0) The application is continuous:

$$[\![M \;\; N]\!] \;=\; \Big[\!\!\Big[[\![M]\!] \; [\![N]\!] \Big]\!\!\Big].$$

Finite Representation of $\mathbb{T}^{\oplus}$'s Distributions

$$\forall M \in \mathbb{T}^{\oplus}(\mathbb{N}), \quad \exists M^* \in \mathbb{T}(\mathbb{N} \to \mathbb{Q}), \quad \texttt{Prob}(M \to k) := (M^*\ k)$$

Using a Finite Tape $s : \texttt{Bool List}$

$$(N_1 \oplus N_2)^{\dagger} := \texttt{if hd}(s) \texttt{ then } s := tl(s)\,;\, N_1 \\ \texttt{else } s := tl(s)\,;\, N_2$$

State Passing Transformation

$$M^{\dagger} \rightsquigarrow \lambda s.M^{\ddagger}$$

Counting Occurrences

$$P(M \to k) := \frac{\#\left\{|s| = n \;\middle|\; M^{\ddagger} \to \boldsymbol{k}\right\}}{2^n}$$

for n sufficiently large.

$\mathbb{T}$-Computable
(simple recursion on s)

Exists since the execution of $M \in \mathbb{T}^{\oplus}$ is bounded

Parametrization: How do we calculate the bound n?

Feasible but more technical: a more complex monad (long version)

When is Probabilistic Choice Necessary?

Depends of Prob. Operators

Are all distributions deterministically representable?

Finite Representation

$$\mathtt{prob}\left(P \rightsquigarrow k\right) = P^*(k) \;\in \mathbb{Q}$$

Functional Representation

$$\mathtt{prob}\left(P \rightsquigarrow k\right) = \lim_{n\to\infty} P^*(n,k)$$

$$\text{s.t. } \sum_k \mathrm{Err}(P^*(n,k)) \leq \frac{1}{n}$$

Parametrization

For $P : \mathbb{N} \to \mathbb{N}$

Can we always perform a derandomization?

Monte Carlo

$f(n)$ reached with probability $> \frac{1}{2} + \epsilon$

Las Vegas

$f(n)$ reached and ascertained with probability $> \epsilon$

Dynamic/Strict bounds

Make ϵ dynamic/null

Different classes

Complexity	**Primitive Rec.**	**HO Prim. Rec.**	**Recursive**

Functional representation of $\mathbb{T}^{\mathbf{X}}$

Remark: Finite representations does not suffice

$\texttt{Prob}[\mathbf{X}\ (\mathbf{rec}\ \mathbf{0}\ (\lambda xy.\mathbf{0} \oplus \mathbf{SS}x))\ \mathbf{1}\ \to\ \mathbf{0}]$ is not rational

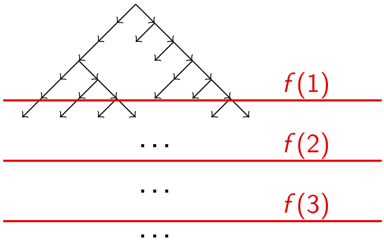
Objective: Functional representation of $\mathbb{T}^{\mathbf{X}}$ in $\mathbb{T}^{\oplus}$

$$\forall M \in \mathbb{T}^{\mathbf{X}}(\mathbb{N}), \quad \exists M^* \in \mathbb{T}^{\oplus}(\mathbb{N} \to \mathbb{N}), \qquad [\![M^*\ \ n]\!] \simeq_{\frac{1}{2^n}} [\![M]\!]$$

Naive idea: Counter

Stop M after $f(n)$ steps

$$\langle M,\ f(n)\rangle \xrightarrow{M \to M'} \langle M', f(n)-1\rangle$$
$$\ldots$$
$$\to \langle M'', \mathbf{0}\rangle$$
$$\to \mathbf{0}$$



Functional representation of $\mathbb{T}^{\mathbf{X}}$

Remark: Finite representations does not suffice

$\texttt{Prob}[\mathbf{X}\ (\mathbf{rec}\ \mathbf{0}\ (\lambda xy.\mathbf{0} \oplus \mathbf{SS}x))\ \mathbf{1}\ \to\ \mathbf{0}]$ is not rational

Objective: Functional representation of $\mathbb{T}^{\mathbf{X}}$ in $\mathbb{T}^{\oplus}$

$$\forall M \in \mathbb{T}^{\mathbf{X}}(\mathbb{N}), \quad \exists M^* \in \mathbb{T}^{\oplus}(\mathbb{N} \to \mathbb{N}), \qquad [\![M^*\ \ n]\!] \simeq_{\frac{1}{2^n}} [\![M]\!]$$

Naive idea: Counter

Stop M after $f(n)$ steps

$$\langle M,\ f(n)\rangle \xrightarrow{M \to M'} \langle M', f(n)-1\rangle$$

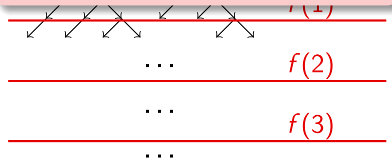
$$\dots$$

$$\to \langle M'', \mathbf{0}\rangle$$

$$\to \mathbf{0}$$

f has to be $\mathbb{T}$-definable!

May not be possible...

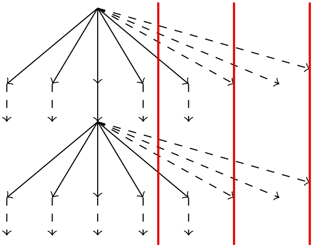


Functional representation of $\mathbb{T}^{\mathbf{R}}$ ($\simeq \mathbb{T}^{\mathbf{X}}$)

Better Idea: Truncating R

Limiting each occurrence of the operator **R** to $[0, ..., n \quad]$

$$\overline{\mathbf{R}} := \left\{ \begin{array}{ccc} 0 & \mapsto & \frac{1}{2} \\ & \cdots & \\ n & \mapsto & \frac{1}{2^{n+1}} \\ \mathtt{Err} & \mapsto & \frac{1}{2^{n+1}} \end{array} \right\}$$

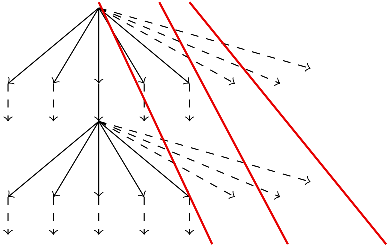


Functional representation of $\mathbb{T}^{\mathbf{R}}$ ($\simeq \mathbb{T}^{\mathbf{X}}$)

The Real Idea: Increasing Truncature

Limiting the mth occurrence of the operator $\mathbf{R}$ to $[0, ..., n*m]$

$$\overline{\mathbf{R}} := (m := m+1); \left\{ \begin{array}{ccc} 0 & \mapsto & \frac{1}{2} \\ & \cdots & \\ n*m & \mapsto & \frac{1}{2^{n*m+1}} \\ \mathtt{Err} & \mapsto & \frac{1}{2^{n*m+1}} \end{array} \right\}$$



Bounded Probability of Error

$$\mathtt{Prob}(M[\overline{\mathbf{R}}/\mathbf{R}] \to \mathtt{Err}) \quad \leq \quad 1 - \prod_{n \geq 0} (1 - \frac{1}{2^{m*n}}) \quad \leq \quad \frac{1}{n}$$

When is Probabilistic Choice Necessary?

Are all distributions deterministically representable?

Depends of Prob. Operators

Finite Representation

$$\texttt{prob}\left(P \rightsquigarrow k\right) = P^*(k) \in \mathbb{Q}$$

Functional Representation

$$\texttt{prob}\left(P \rightsquigarrow k\right) = \lim_{n\to\infty} P^*(n,k)$$

$$\text{s.t. } \sum_k \mathrm{Err}(P^*(n,k)) \leq \frac{1}{n}$$

Parametrization

For $P : \mathbb{N} \to \mathbb{N}$

Can we always perform a derandomization?

Monte Carlo

$f(n)$ reached with probability $> \frac{1}{2} + \epsilon$

Las Vegas

$f(n)$ reached and ascertained with probability $> \epsilon$

future work

Dynamic/Strict bounds

Make ϵ dynamic/null

Different classes

Complexity	Primitive Rec.	HO Prim. Rec.	Recursive

When is Probabilistic Choice Necessary?

Are all distributions deterministically representable?

~~Finite Representation~~

$$\mathtt{prob}\Big(P \rightsquigarrow k\Big) = P^*(k) \ \in \mathbb{Q}$$

Functional Representation

$$\mathtt{prob}\Big(P \rightsquigarrow k\Big) = \lim_{n\to\infty} P^*(n,k)$$

$$\text{s.t. } \sum_k \mathrm{Err}(P^*(n,k)) \leq \frac{1}{n}$$

Parametrization

For $P : \mathbb{N} \to \mathbb{N}$

Can we always perform a derandomization?

Monte Carlo

$f(n)$ reached with probability $> \frac{1}{2} + \epsilon$

Las Vegas

$f(n)$ reached and ascertained with probability $> \epsilon$

Dynamic/Strict bounds

Make ϵ dynamic/null

Different classes

Complexity **Primitive Rec.** **HO Prim. Rec.** **Recursive**

Functional Representation of Probabilistic Recursive functions

What is a functional representation?

Let M a probabilistic program that output an integer with probability 1.
We look for a recursive function $f : \mathbb{N} \to \mathbb{N} \to \mathbb{Q}$ such that:

$$\texttt{prob}(M \to k) = \lim_n f(k)(n) \qquad \left(1 - \sum_k f(k)(n)\right) \leq \frac{1}{n}$$

```
let f M k n :=
  let tab : Rational[] in
  let rec simul M p:=
      eval M with
        "return k" -> tab[k] += 1/(2^p);
        "if coin then L else N" -> {
                newThread{simul L (p+1)};
                newThread{simul N (p+1)};
              };
  in newthread{simul M 0};
  newThread{
    while ( sum tab < 1-1/n ) do skip;
    return tab[k];
  }
```

tab: dynamical approximation

Updating tab on terminating branches

Run probabilistic choices **in parallel**

Waiting for a reasonable approximation