Polynomial interpretation of stream programs.

Hugo Férée
Emmanuel Hainry Mathieu Hoyrup Romain Péchoux

INRIA Nancy - Grand Est, Nancy-Université, France

Overview

Complexity model

Stream language

Characterization of polynomial time functions

Other Results

Complexity model

Stream language

Characterization of polynomial time functions

Other Results

Context

Type 1 ($\mathbb{N} \to \mathbb{N}$)	Type 2 ($(\mathbb{N} \to \mathbb{N}) \to \mathbb{N} \to \mathbb{N}$)
Turing machines	Oracle Turing machines
polynomials	order-2 polynomials
Limited recursion on notation (Cobham)	Basic Feasible Functionals (Kapron & Cook)

Context

Type 1 ($\mathbb{N} \to \mathbb{N}$)	Type 2 ($(\mathbb{N} \to \mathbb{N}) \to \mathbb{N} \to \mathbb{N}$)
Turing machines	Oracle Turing machines
polynomials	order-2 polynomials
Limited recursion on notation (Cobham)	Basic Feasible Functionals (Kapron & Cook)

Definition (Order-2 polynomial)

$P := c \mid X_i \mid P + P \mid P \times P \mid Y_i\langle P\rangle$

Example

$$P(X, Y) = Y\langle X \times Y\langle X^2 + 1\rangle\rangle$$

$$P(2, x \to x^3) = (2 \times (2^2 + 1)^3)^3$$

Oracle Turing Machine

Definition (OTM)

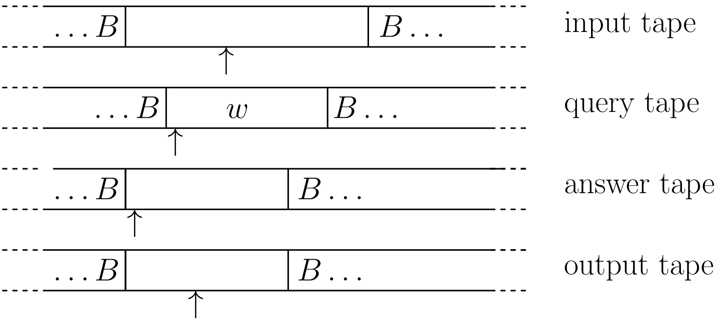

Figure: An OTM before oracle call

Oracle Turing Machine

Definition (OTM)

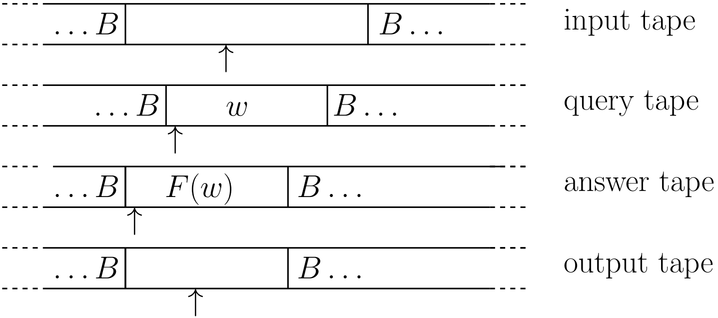

Figure: An OTM after oracle call

Definition (BFF)

- cost of the call of oracle f on input x: $|f(x)|$
- BFF functionals: cost bounded by $P(|x|, |f|)$

where basically, $\forall x, |f(x)| \leq |f|(|x|)$

Example (BFF functions)

- $x, f \mapsto g(x)$ $(g \in \mathcal{FP})$
- $x, f \mapsto f(x)$
- $x, f \mapsto f^n(x)$ (for a given $n \in \mathbb{N}$)
- $x, f \mapsto f^x(x)$ is not in BFF

Unary Oracle Turing Machine

Definition (UOTM)

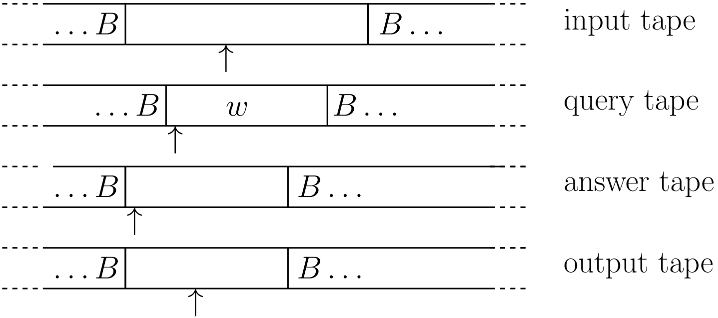

Figure: A UOTM before oracle call

Unary Oracle Turing Machine

Definition (UOTM)

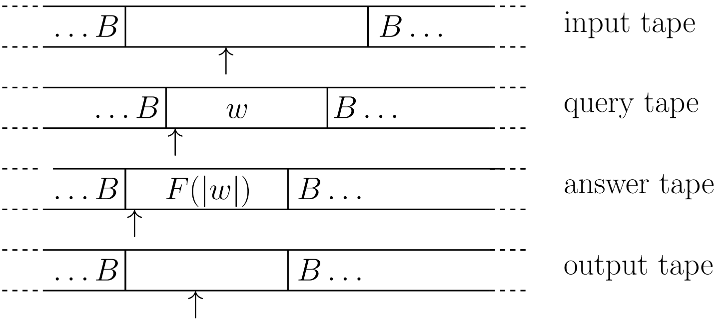

Figure: A UOTM after oracle call

Complexity

Definition (Size of a function)

$$\forall n \in \mathbb{N}, |F|(n) = \max_{k \leq n} |F(k)|$$

In particular, $|F(x)| \leq |F|(2^{|x|})$

Definition (UOTM-polynomial functional)

Same definition as BFF, but the oracle calls and the definition of the size have changed.

Example

$x, f \mapsto f(x)$ *is not UOTM-polynomial (cost: $\sim |f|(2^{|x|})$), but* $x, f \mapsto f(|x|)$ *is (cost: $\sim |f|(|x|)$).*

Complexity model

Stream language

Characterization of polynomial time functions

Other Results

- Functional language (Haskell like)
- Inductive data types
- co-inductive data types (streams): `[T] := T : [T]`

- Functional language (Haskell like)
- Inductive data types
- co-inductive data types (streams): `[T] := T : [T]`

$$\frac{(\mathtt{f}\ \mathtt{p}_1\ \ldots\ \mathtt{p}_n = \mathtt{e}) \in \mathcal{D} \qquad \sigma \in \mathfrak{S} \qquad \forall i \in \{1, n\},\ \sigma(\mathtt{p}_i) = \mathtt{e}_i}{\mathtt{f}\ \mathtt{e}_1\ \ldots\ \mathtt{e}_n \to \sigma(\mathtt{e})}\ (d)$$

$$\frac{\mathtt{e}_i \to \mathtt{e}'_i \qquad \mathtt{t} \in \mathcal{F} \cup \mathcal{C} \setminus \{:\}}{\mathtt{t}\ \mathtt{e}_1\ \ldots\ \mathtt{e}_i\ \ldots\ \mathtt{e}_n \to \mathtt{t}\ \mathtt{e}_1\ \ldots\ \mathtt{e}'_i\ \ldots\ \mathtt{e}_n}\ (t) \qquad \frac{\mathtt{e} \to \mathtt{e}'}{\mathtt{e} : \mathtt{e}_0 \to \mathtt{e}' : \mathtt{e}_0}\ (:)$$

Example

```
data nat := Z | S nat
data Pos := 0 Pos | 1 Pos | I
data Bnat := O | + Pos | - Pos

plus :: Znat -> Znat -> Znat
plus O x = x
plus x O = x
plus (+ x) (+ y) = ...
plus (+ x) (- y) = ...
...

nth :: [Tau] -> nat -> Tau
nth (h : t) Z = h
nth (h : t) (S n) = nth t n
```

Complexity model

Stream language

Characterization of polynomial time functions

Other Results

Definitions

Definition (Positive functionals)

$((\mathbb{N} \to \mathbb{N})^k \times \mathbb{N}^l) \to T$ with $k, l \in \mathbb{N}$ and $T \in \{\mathbb{N}, \mathbb{N} \to \mathbb{N}\}$

Definition (Monotonic positive functionals)

F is monotonic if $\forall i, \forall x_i > x_i',\ F(\dots, x_i, \dots) > F(\dots, x_i', \dots)$.

Definition (Interpretation of a program)

It is a mapping of each symbol function as a monotonic positive functional, whose type verifies:

- `t :  Tau` $\Rightarrow (\!|\texttt{t}|\!) : \mathbb{N}$
- `t :  [Tau]` $\Rightarrow (\!|\texttt{t}|\!) : \mathbb{N} \to \mathbb{N}$
- `t :  A -> B` $\Rightarrow (\!|\texttt{t}|\!) : T_A \to T_B$

Extended interpretation

- $(\!|\mathtt{x}|\!) = X$ if $\mathtt{x} : \mathtt{Tau}$.
- $(\!|\mathtt{y}|\!)(n) = Y\langle n \rangle$ if $\mathtt{y} : [\mathtt{Tau}]$

Extended interpretation

- $(\!|\mathtt{x}|\!) = X$ if $\mathtt{x}$: $\mathtt{Tau}$.
- $(\!|\mathtt{y}|\!)(n) = Y\langle n\rangle$ if $\mathtt{y}$: $[\mathtt{Tau}]$
- $(\!|\mathsf{c}|\!)(X_1, \ldots, X_n) = X_1 + \ldots X_n + 1$ if $\mathsf{c} \in \mathcal{C} \setminus \{:\}$ is of arity n
- $(\!|:|\!)(X, Y)(0) = X$
- $(\!|:|\!)(X, Y)(n+1) = 1 + X + Y\langle n\rangle$

Extended interpretation

- $(\!|\mathtt{x}|\!) = X$ if $\mathtt{x} : \mathtt{Tau}$.
- $(\!|\mathtt{y}|\!)(n) = Y\langle n \rangle$ if $\mathtt{y} : [\mathtt{Tau}]$
- $(\!|\mathsf{c}|\!)(X_1, \ldots, X_n) = X_1 + \ldots X_n + 1$ if $\mathsf{c} \in \mathcal{C} \setminus \{:\}$ is of arity n
- $(\!|:|\!)(X, Y)(0) = X$
- $(\!|:|\!)(X, Y)(n+1) = 1 + X + Y\langle n \rangle$
- $(\!|\mathtt{t}\ \mathtt{e_1}\ \ldots\ \mathtt{e_n}|\!) = (\!|\mathtt{t}|\!)((\!|\mathtt{e_1}|\!), \ldots, (\!|\mathtt{e_n}|\!))$

Extended interpretation

- $(\!|\mathtt{x}|\!) = X$ if $\mathtt{x} : \mathtt{Tau}$.
- $(\!|\mathtt{y}|\!)(n) = Y\langle n\rangle$ if $\mathtt{y} : [\mathtt{Tau}]$
- $(\!|\mathsf{c}|\!)(X_1, \ldots, X_n) = X_1 + \ldots X_n + 1$ if $\mathsf{c} \in \mathcal{C} \setminus \{:\}$ is of arity n
- $(\!|:|\!)(X, Y)(0) = X$
- $(\!|:|\!)(X, Y)(n+1) = 1 + X + Y\langle n\rangle$
- $(\!|\mathtt{t}\ \mathtt{e_1}\ \ldots\ \mathtt{e_n}|\!) = (\!|\mathtt{t}|\!)((\!|\mathtt{e_1}|\!), \ldots, (\!|\mathtt{e_n}|\!))$

Example

If $(\!|f|\!)(Y, X) = Y(X^2 + 1)$,
$(\!|\mathtt{S\ (f\ str\ (S\ Z))}|\!)$

Extended interpretation

- $(\!|\mathtt{x}|\!) = X$ if $\mathtt{x} : \mathtt{Tau}$.
- $(\!|\mathtt{y}|\!)(n) = Y\langle n \rangle$ if $\mathtt{y} : [\mathtt{Tau}]$
- $(\!|\mathsf{c}|\!)(X_1, \ldots, X_n) = X_1 + \ldots X_n + 1$ if $\mathsf{c} \in \mathcal{C} \setminus \{:\}$ is of arity n
- $(\!|:|\!)(X, Y)(0) = X$
- $(\!|:|\!)(X, Y)(n+1) = 1 + X + Y\langle n \rangle$
- $(\!|\mathtt{t}\ \mathtt{e_1}\ \ldots\ \mathtt{e_n}|\!) = (\!|\mathtt{t}|\!)((\!|\mathtt{e_1}|\!), \ldots, (\!|\mathtt{e_n}|\!))$

Example

If $(\!|f|\!)(Y, X) = Y(X^2 + 1)$,
$(\!|\mathtt{S\ (f\ str\ (S\ Z))}|\!) = 1 + (\!|\mathtt{f\ str\ (S\ Z)}|\!)$

Extended interpretation

- $(\!|\mathtt{x}|\!) = X$ if $\mathtt{x} : \mathtt{Tau}$.
- $(\!|\mathtt{y}|\!)(n) = Y\langle n\rangle$ if $\mathtt{y} : [\mathtt{Tau}]$
- $(\!|\mathsf{c}|\!)(X_1, \ldots, X_n) = X_1 + \ldots X_n + 1$ if $\mathsf{c} \in \mathcal{C} \setminus \{:\}$ is of arity n
- $(\!|:|\!)(X, Y)(0) = X$
- $(\!|:|\!)(X, Y)(n+1) = 1 + X + Y\langle n\rangle$
- $(\!|\mathtt{t}\ \mathtt{e}_1\ \ldots\ \mathtt{e}_\mathtt{n}|\!) = (\!|\mathtt{t}|\!)((\!|\mathtt{e}_1|\!), \ldots, (\!|\mathtt{e}_\mathtt{n}|\!))$

Example

If $(\!|f|\!)(Y, X) = Y(X^2 + 1)$,
$(\!|\mathtt{S}\ (\mathtt{f}\ \mathtt{str}\ (\mathtt{S}\ \mathtt{Z}))|\!) = 1 + (\!|\mathtt{f}\ \mathtt{str}\ (\mathtt{S}\ \mathtt{Z})|\!) = 1 + (\!|\mathtt{f}|\!)((\!|\mathtt{str}|\!), (\!|\mathtt{S}\ \mathtt{Z}|\!))$

Extended interpretation

- $(\!|\mathtt{x}|\!) = X$ if $\mathtt{x} : \mathtt{Tau}$.
- $(\!|\mathtt{y}|\!)(n) = Y\langle n\rangle$ if $\mathtt{y} : [\mathtt{Tau}]$
- $(\!|\mathsf{c}|\!)(X_1, \ldots, X_n) = X_1 + \ldots X_n + 1$ if $\mathsf{c} \in \mathcal{C} \setminus \{:\}$ is of arity n
- $(\!|:|\!)(X, Y)(0) = X$
- $(\!|:|\!)(X, Y)(n+1) = 1 + X + Y\langle n\rangle$
- $(\!|\mathtt{t}\ \mathtt{e}_1\ \ldots\ \mathtt{e}_\mathtt{n}|\!) = (\!|\mathtt{t}|\!)((\!|\mathtt{e}_1|\!), \ldots, (\!|\mathtt{e}_\mathtt{n}|\!))$

Example

If $(\!|f|\!)(Y, X) = Y(X^2 + 1)$,
$(\!|\mathtt{S}\ (\mathtt{f}\ \mathtt{str}\ (\mathtt{S}\ \mathtt{Z}))|\!) = 1 + (\!|\mathtt{f}\ \mathtt{str}\ (\mathtt{S}\ \mathtt{Z})|\!) = 1 + (\!|\mathtt{f}|\!)((\!|\mathtt{str}|\!), (\!|\mathtt{S}\ \mathtt{Z}|\!))$
$= 1 + (\!|\mathtt{f}|\!)(\mathtt{STR}, 2)$

Extended interpretation

- $(\!|\mathtt{x}|\!) = X$ if $\mathtt{x} : \mathtt{Tau}$.
- $(\!|\mathtt{y}|\!)(n) = Y\langle n\rangle$ if $\mathtt{y} : [\mathtt{Tau}]$
- $(\!|\mathrm{c}|\!)(X_1, \dots, X_n) = X_1 + \dots X_n + 1$ if $\mathrm{c} \in \mathcal{C} \setminus \{:\}$ is of arity n
- $(\!|:|\!)(X, Y)(0) = X$
- $(\!|:|\!)(X, Y)(n+1) = 1 + X + Y\langle n\rangle$
- $(\!|\mathtt{t}\ \mathtt{e}_1\ \dots\ \mathtt{e}_\mathtt{n}|\!) = (\!|\mathtt{t}|\!)((\!|\mathtt{e}_1|\!), \dots, (\!|\mathtt{e}_\mathtt{n}|\!))$

Example

If $(\!|f|\!)(Y, X) = Y(X^2 + 1)$,
$(\!|\mathtt{S}\ (\mathtt{f}\ \mathtt{str}\ (\mathtt{S}\ \mathtt{Z}))|\!) = 1 + (\!|\mathtt{f}\ \mathtt{str}\ (\mathtt{S}\ \mathtt{Z})|\!) = 1 + (\!|\mathtt{f}|\!)((\!|\mathtt{str}|\!), (\!|\mathtt{S}\ \mathtt{Z}|\!))$
$= 1 + (\!|\mathtt{f}|\!)(\mathtt{STR}, 2) = 1 + STR(2^2 + 1) = 1 + STR(5)$

Well-founded interpretations

Definition (Partial order over functionals)

$F > G$ if $\forall x_1 \ldots x_l \in \{\mathbb{N} \setminus \{0\}, \mathbb{N} \to^{\uparrow} \mathbb{N}\}$,
$F(x_1, \ldots, x_l) > G(x_1, \ldots, x_l)$

Definition (well-founded interpretation)

$\mathtt{f}\ \mathtt{p_1} \ldots \mathtt{p_n} = \mathtt{e} \in \mathcal{D} \Rightarrow (\!|\mathtt{f}\ \mathtt{p_1} \ldots \mathtt{p_n}|\!) > (\!|\mathtt{e}|\!)$

Well-founded interpretations

Definition (Partial order over functionals)

$F > G$ if $\forall x_1 \dots x_l \in \{\mathbb{N} \setminus \{0\}, \mathbb{N} \to^{\uparrow} \mathbb{N}\}$,
$F(x_1, \dots, x_l) > G(x_1, \dots, x_l)$

Definition (well-founded interpretation)

$\mathtt{f}\ \mathtt{p}_1 \dots \mathtt{p}_\mathtt{n} = \mathtt{e} \in \mathcal{D} \Rightarrow (\!|\mathtt{f}\ \mathtt{p}_1 \dots \mathtt{p}_\mathtt{n}|\!) > (\!|\mathtt{e}|\!)$

Example

$$(\!|nth|\!)(Y, N) = Y(N)$$

$$(\!|\mathtt{nth\ (h\ :\ t)\ Z}|\!) = (\!|\mathtt{h\ :\ t}|\!)(1) = (\!|h|\!) + 1 + (\!|t|\!)(0) > (\!|h|\!)$$

$$(\!|\mathtt{nth\ (h\ :\ t)\ (S\ n)}|\!) = 1 + (\!|h|\!) + (\!|t|\!)(\!|n|\!) > (\!|t|\!)(\!|n|\!) = (\!|\mathtt{nth\ t\ n}|\!)$$

Results

Lemma

$\mathtt{e} \to \mathtt{e}'$, *then* $(\!|\mathtt{e}|\!) > (\!|\mathtt{e}'|\!)$

Corollary

$\mathtt{e} \to^{\mathtt{n}} \mathtt{v}$, *then* $(\!|\mathtt{e}|\!) - (\!|\mathtt{v}|\!) \geq \mathtt{n}$

Corollary (Productivity)

If `e :: [Tau]`, *then* (`nth e n`) *can be evaluated in less than* $(\!|e|\!)(n+1)$ *steps.*

Theorem

A function is UOTM-polynomial $\Leftrightarrow$ *it is computed by a program with a well-founded polynomial interpretation.*

Complexity model

Stream language

Characterization of polynomial time functions

Other Results

BFF characterization

Definition (exp-poly)

$$EP := P \mid EP + EP \mid EP \times EP \mid Y\langle 2^{EP} \rangle$$

Theorem

A function is in BFF $\Leftrightarrow$ it is computed by a program with a well-founded exp-poly interpretation.

Polynomial time computable real functions

- $\mathbb{R} \sim [\mathbb{Q}]$
- Computable real functions (Weihrauch) $\sim$ some stream programs ($\mathbb{R} \to \mathbb{R} \sim$ [$\mathbb{Q}$]->[$\mathbb{Q}$])

Theorem

Polynomially computable real functions $\Leftrightarrow$ *some stream programs with well-founded polynomial interpretation.*

Conclusion

We have:

- a definition of polynomial time complexity for type-2 functions (and real functions)
- meaningful if seen as a stream program
- a characterization using program interpretations
- a similar result for *BFF* and real functions