

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

Context

Type 1 ($\mathbb{N} \rightarrow \mathbb{N}$)	Type 2 ($(\mathbb{N} \rightarrow \mathbb{N}) \rightarrow \mathbb{N} \rightarrow \mathbb{N}$)
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

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

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

Oracle Turing Machine

Definition (OTM)

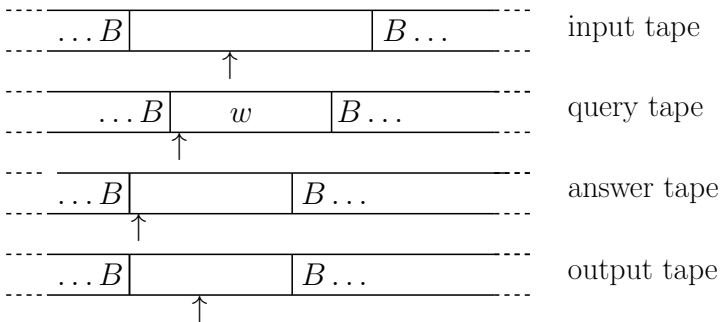


Figure: A UOTM before oracle call

Oracle Turing Machine

Definition (OTM)

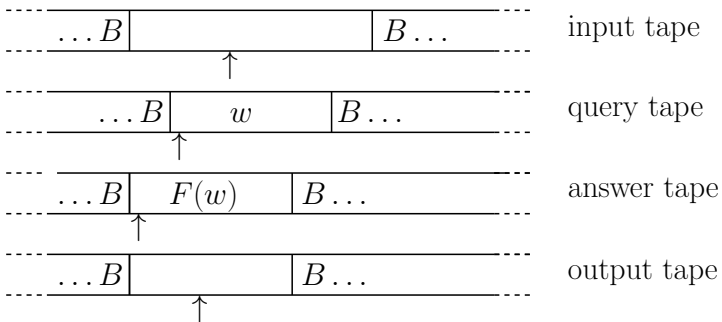


Figure: A UOTM after oracle call

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)

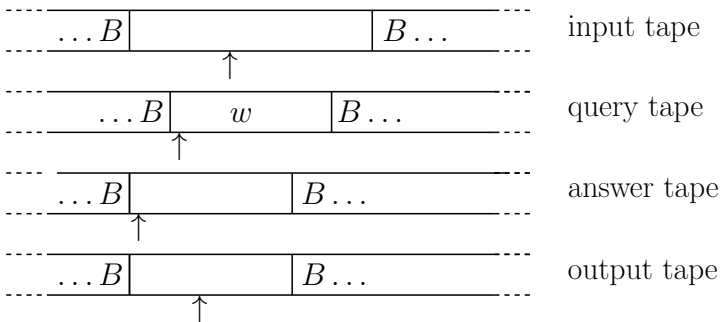


Figure: A UOTM before oracle call

Unary Oracle Turing Machine

Definition (UOTM)

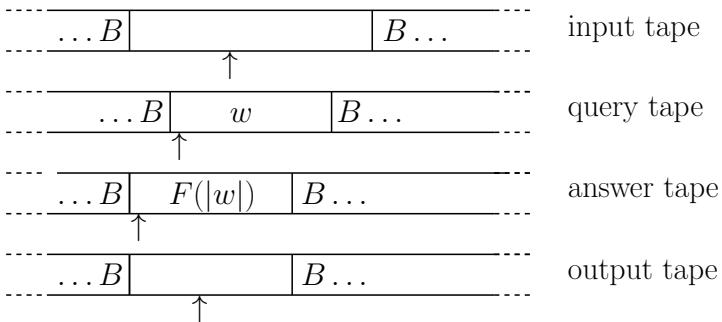


Figure: A UOTM after oracle call

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): $[T] := T : [T]$

$$\frac{(f p_1 \dots p_n = e) \in \mathcal{D} \quad \sigma \in \mathfrak{S} \quad \forall i \in \{1, n\}, \sigma(p_i) = e_i}{f e_1 \dots e_n \rightarrow \sigma(e)} \quad (d)$$

$$\frac{e_i \rightarrow e'_i \quad t \in \mathcal{FUC} \setminus \{:\}}{t e_1 \dots e_i \dots e_n \rightarrow t e_1 \dots e'_i \dots e_n} \quad (t) \qquad \frac{e \rightarrow e'}{e : e_0 \rightarrow e' : e_0} \quad (:)$$

Example

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

```
plus :: Znat -> Znat -> Znat
plus 0 x = x
plus x 0 = 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)

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

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:

- $t : \text{Tau} \Rightarrow \langle t \rangle : \mathbb{N}$
- $t : [\text{Tau}] \Rightarrow \langle t \rangle : \mathbb{N} \rightarrow \mathbb{N}$
- $t : A \rightarrow B \Rightarrow \langle t \rangle : T_A \rightarrow T_B$

Extended interpretation

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

Extended interpretation

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

Extended interpretation

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

Extended interpretation

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

Example

If $\langle f \rangle(Y, X) = Y(X^2 + 1)$,
 $\langle S \ (f \ \text{str} \ (S \ Z)) \rangle$

Extended interpretation

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

Example

$$\text{If } \langle f \rangle(Y, X) = Y(X^2 + 1),$$

$$\langle S \ (f \ \text{str} \ (S \ Z)) \rangle = 1 + \langle f \ \text{str} \ (S \ Z) \rangle$$

Extended interpretation

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

Example

If $\langle f \rangle(Y, X) = Y(X^2 + 1)$,

$\langle S \ (f \ \text{str} \ (S \ Z)) \rangle = 1 + \langle f \ \text{str} \ (S \ Z) \rangle = 1 + \langle f \rangle(\langle \text{str} \rangle, \langle S \ Z \rangle)$

Extended interpretation

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

Example

If $\langle f \rangle(Y, X) = Y(X^2 + 1)$,

$$\begin{aligned} \langle S \ (f \ \text{str} \ (S \ Z)) \rangle &= 1 + \langle f \ \text{str} \ (S \ Z) \rangle = 1 + \langle f \rangle(\langle \text{str} \rangle, \langle S \ Z \rangle) \\ &= 1 + \langle f \rangle(\text{STR}, 2) \end{aligned}$$

Extended interpretation

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

Example

If $\langle f \rangle(Y, X) = Y(X^2 + 1)$,

$$\begin{aligned} \langle S \ (f \ \text{str} \ (S \ Z)) \rangle &= 1 + \langle f \ \text{str} \ (S \ Z) \rangle = 1 + \langle f \rangle(\langle \text{str} \rangle, \langle S \ Z \rangle) \\ &= 1 + \langle f \rangle(\text{STR}, 2) = 1 + \text{STR}(2^2 + 1) = 1 + \text{STR}(5) \end{aligned}$$

Well-founded interpretations

Definition (Partial order over functionals)

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

Definition (well-founded interpretation)

$f \ p_1 \dots p_n = e \in \mathcal{D} \Rightarrow \langle f \ p_1 \dots p_n \rangle > \langle e \rangle$

Well-founded interpretations

Definition (Partial order over functionals)

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

Definition (well-founded interpretation)

$f \ p_1 \dots p_n = e \in \mathcal{D} \Rightarrow \langle f \ p_1 \dots p_n \rangle > \langle e \rangle$

Example

$$\langle nth \rangle(Y, N) = Y(N)$$

$$\langle nth \ (h : t) \ Z \rangle = \langle h : t \rangle(1) = \langle h \rangle + 1 + \langle t \rangle(0) > \langle h \rangle$$

$$\langle nth \ (h : t) \ (S \ n) \rangle = 1 + \langle h \rangle + \langle t \rangle(n) > \langle t \rangle(n) = \langle nth \ t \ n \rangle$$

Results

Lemma

$e \rightarrow e'$, then $\langle e \rangle > \langle e' \rangle$

Corollary

$e \rightarrow^n v$, then $\langle e \rangle - \langle v \rangle \geq n$

Corollary (Productivity)

If $e :: [\text{Tau}]$, then $(n\text{th } e \ n)$ can be evaluated in less than $\langle e \rangle(n + 1)$ 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 ($\mathbb{R} \rightarrow \mathbb{R} \sim [\mathbb{Q}] \rightarrow [\mathbb{Q}]$)

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* real functions