Characterizations of Polynomial Complexity Classes with a Better Intensionality

Romain Péchoux and Jean-Yves Marion

Carte project, Loria, Nancy

PPDP 2008

Motivations

- Resource control, resource certificates by static analysis
- Applications to Term Rewriting Systems / Functional programs
- Using:
  - Quasi-interpretation by Bonfante et al[2001] (inspired by polynomial interpretations Manna-Ness[1972] and Lankford[1979])
  - Sup-interpretation by Marion and Péchoux[2006]
  - Dependency pairs by Arts and Giesl[2000]
- Our concern is intensionality rather than extensionality

Syntax and semantics of First Order Language

A program is a quadruplet $\langle \mathcal{X}, \mathcal{C}, \mathcal{F}, \mathcal{R} \rangle$

Constructors: $\mathbf{c} \in \mathcal{C}$, functions: $\mathtt{f} \in \mathcal{F}$, variables: $x \in \mathcal{X}$.

$$
\begin{array}{llll}
\texttt{(Terms)} & \mathcal{T} \ni t & ::= & x \mid \mathbf{c}(t_1, \cdots, t_n) \mid \mathtt{f}(t_1, \cdots, t_n) \\
\texttt{(Patterns)} & \mathcal{P} \ni p & ::= & \mathbf{c}(p_1, \cdots, p_n) \mid x \\
\texttt{(Rules)} & \mathcal{R} \ni r & ::= & \mathtt{f}(p_1, \cdots, p_n) \to t \\
\texttt{(Values)} & \mathcal{V} \ni v & ::= & \mathbf{c}(v_1, \cdots, v_n)
\end{array}
$$

- The computational domain is the set of values $\mathcal{V}^* = \mathcal{V} \cup \{\mathbf{Err}\}$
- Define $[\![e]\!] = w$ iff $e \xrightarrow{*} w$ and $w \in \mathcal{V}^*$
- Linear and disjoint patterns (Confluence: Huet[1980])

Program example

Example (Unary logarithm)

$$\begin{aligned}
\mathtt{half}(\mathbf{0}) &\to \mathbf{0}\\
\mathtt{half}(\mathbf{S}(\mathbf{0})) &\to \mathbf{0}\\
\mathtt{half}(\mathbf{S}(\mathbf{S}(\mathrm{y}))) &\to \mathbf{S}(\mathtt{half}(\mathrm{y}))\\
\mathtt{log}(\mathbf{0}) &\to \mathbf{0}\\
\mathtt{log}(\mathbf{S}(\mathbf{0})) &\to \mathbf{0}\\
\mathtt{log}(\mathbf{S}(\mathbf{S}(\mathrm{y}))) &\to \mathbf{S}(\mathtt{log}(\mathbf{S}(\mathtt{half}(\mathrm{y}))))
\end{aligned}$$

Semantics:

- $[\![\mathtt{log}(\mathbf{S}^n(\mathbf{0}))]\!] = \mathbf{S}^{\lfloor \log(n) \rfloor}(\mathbf{0})$
- $[\![\mathtt{half}(\mathbf{S}^n(\mathbf{0}))]\!] = \mathbf{S}^{\lfloor n/2 \rfloor}(\mathbf{0})$ with $\mathbf{S}^n(\mathbf{0}) = \underbrace{\mathbf{S}(\ldots\mathbf{S}(\mathbf{0})\ldots)}_{n \text{ times } \mathbf{S}}$

Quasi-interpretations (QI)

Definition (Quasi-interpretation)

A program **p** admits a quasi-interpretation if there is a

- total: $\forall b$, $(\!|b|\!)$ is a function from $(\mathbb{R}^+)^n$ to $\mathbb{R}^+$,
- monotonic: $X_i \geq Y_i \Rightarrow (\!|b|\!)(\ldots, X_i, \ldots) \geq (\!|b|\!)(\ldots, Y_i, \ldots)$,
- and subterm: $(\!|b|\!)(X_1, \cdots, X_n) \geq X_i$

assignment $(\!|-|\!)$ such that for each rule $l \to r$:

$$(\!|l|\!) \geq (\!|r|\!)$$

Example of quasi-interpretation

Example (Quasi-interpretation of logarithm)

$$
\begin{aligned}
(\!|\mathtt{half}(\mathbf{0})|\!) &\geq (\!|\mathbf{0}|\!)\\
(\!|\mathtt{half}(\mathbf{S}(\mathbf{0}))|\!) &\geq (\!|\mathbf{0}|\!)\\
(\!|\mathtt{half}(\mathbf{S}(\mathbf{S}(\mathrm{y})))|\!) &\geq (\!|\mathbf{S}(\mathtt{half}(\mathrm{y}))|\!)\\
(\!|\mathtt{log}(\mathbf{0})|\!) &\geq (\!|\mathbf{0}|\!)\\
(\!|\mathtt{log}(\mathbf{S}(\mathbf{0}))|\!) &\geq (\!|\mathbf{0}|\!)\\
(\!|\mathtt{log}(\mathbf{S}(\mathbf{S}(\mathrm{y})))|\!) &\geq (\!|\mathbf{S}(\mathtt{log}(\mathbf{S}(\mathtt{half}(\mathrm{y}))))|\!)
\end{aligned}
$$

$$
\begin{aligned}
(\!|\mathbf{0}|\!) &= 0\\
(\!|\mathbf{S}|\!)(X) &= X+1\\
(\!|\mathtt{log}|\!)(X) &= (\!|\mathtt{half}|\!)(X) = X
\end{aligned}
$$

Example $(\!|l|\!) \geq (\!|r|\!)$

Example (Quasi-interpretation of logarithm)

$$\mathtt{half}(\mathbf{S}(\mathbf{S}(\mathtt{y}))) \to \mathbf{S}(\mathtt{half}(y))$$

$$\begin{aligned}
(\!|\mathtt{half}(\mathbf{S}(\mathbf{S}(\mathtt{y})))|\!) &= (\!|\mathtt{half}|\!)((\!|\mathbf{S}|\!)((\!|\mathbf{S}|\!)(Y))) \\
&= (\!|\mathtt{half}|\!)(Y+2) \\
&= Y+2 \\
&\geq Y+1 \\
&= (\!|\mathbf{S}(\mathtt{half}(y))|\!)
\end{aligned}
\qquad
\begin{aligned}
(\!|y|\!) &= Y \\
(\!|\mathbf{S}|\!)(X) &= X+1 \\
(\!|\mathtt{half}|\!)(X) &= X
\end{aligned}$$

Fundamental Lemma

Definition (Polynomial quasi-interpretation)

A quasi-interpretation is polynomial if $\forall b$ $(\!|b|\!)$ is a max-polynomial.

Definition (Additive quasi-interpretation)

A quasi-interpretation is additive if $\forall \mathbf{c} \in Cns$ of arity n:

- if $n > 0$ then $(\!|\mathbf{c}|\!)(X_1, \cdots, X_n) = \sum_{i=1}^{n} X_i + \alpha_{\mathbf{c}}$ with $\alpha_{\mathbf{c}} \geq 1$
- if $n = 0$ then $(\!|\mathbf{c}|\!) = 0$

Fundamental Lemma

If a program admits a polynomial and additive QI then there is a polynomial P s.t. $\forall b$ and $\forall v_1, \ldots, v_n \in Values$:

$$\text{if } [\![b(v_1, \ldots, v_n)]\!] \in \mathcal{V}, \text{ then } P(\max_{i=1,n}(|v_i|)) \geq |[\![b(v_1, \ldots, v_n)]\!]|$$

Characterizations of FPTIME and FPSPACE

Theorem (Bonfante, Marion and Moyen[2000,2001])

The set of functions computed by programs having an additive and polynomial QI and:

- *ordered by product $\prec_{rpo}$ is exactly FPTIME.*
- *ordered by product and lexicographic $\prec_{rpo}$ is exactly FPSPACE.*

Quasi-interpretations fail on natural algorithms

Example (A motivating example: Division)

$$
\begin{aligned}
\mathtt{minus}(\mathbf{0}, y) &\to \mathbf{0} \\
\mathtt{minus}(\mathbf{S}(x), \mathbf{0}) &\to \mathbf{S}(x) \\
\mathtt{minus}(\mathbf{S}(x), \mathbf{S}(y)) &\to \mathtt{minus}(x, y) \\
\mathrm{q}(\mathbf{0}, \mathbf{S}(y)) &\to \mathbf{0} \\
\mathrm{q}(\mathbf{S}(x), \mathbf{S}(y)) &\to \mathbf{S}(\mathrm{q}(\mathtt{minus}(x, y), \mathbf{S}(y)))
\end{aligned}
$$

$$
[\![\mathrm{q}(\mathbf{S}^n(\mathbf{0}), \mathbf{S}^m(\mathbf{0}))]\!] = \mathbf{S}^{\lceil n/m \rceil}(\mathbf{0})
$$

Is there a quasi-interpretation of division?

Answer: NO !

Example (Division)

Suppose that $(\!|-|\!)$ is an additive QI s.t. $(\!|\mathbf{S}|\!)(X) = X + k$.

$$
\begin{aligned}
(\!|\mathrm{q}(\mathbf{S}(x), \mathbf{S}(y))|\!) &\geq (\!|\mathbf{S}(\mathrm{q}(\mathtt{minus}(x, y), \mathbf{S}(y)))|\!) & \\
&\geq k + (\!|\mathrm{q}|\!)((\!|\mathtt{minus}|\!)(X, Y), Y + k) & (\!|\mathbf{S}|\!)(X) = X + k \\
&> (\!|\mathrm{q}|\!)(\max(X, Y), Y + k) & \text{Subterm property} \\
&\geq (\!|\mathrm{q}|\!)(X + k, Y + k) & \text{For } Y \geq X + k \\
&= (\!|\mathrm{q}(\mathbf{S}(x), \mathbf{S}(y))|\!) &
\end{aligned}
$$

Develop a tool with more intensionality:

- Partial instead of total assignments
- No more subterm property

Sup-interpretations (Marion and Péchoux[2006,2008])

Definition (Sup-interpretation)

A program admits a sup-interpretation if there is a partial assignment θ such that:

1. θ is monotonic.
2. $\forall v \in \mathcal{V}$, $\theta(v) \geq |v|$
3. $\forall b \in \text{dom}(\theta)$ of arity n and for each values $v_1, \ldots, v_n$, if $[\![b(v_1, \ldots, v_n)]\!] \in \mathcal{V}$, then:

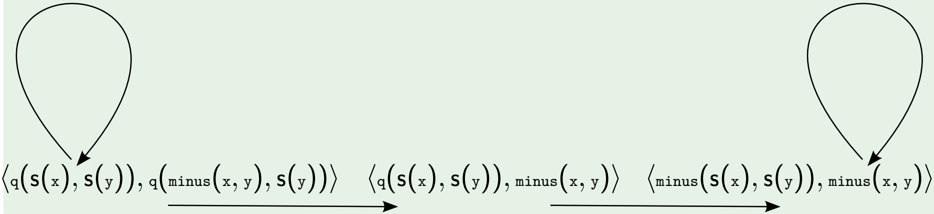
$$\theta(b(v_1, \ldots, v_n)) \geq \theta([\![b(v_1, \ldots, v_n)]\!])$$

Dependency pairs as a way to synthesize SI

Definition (Dependency pair and dependency pair graph)

- $\langle \mathtt{f}(p), \mathtt{g}(e) \rangle$ is a dependency pair if $\mathtt{f}(p) \rightarrow \mathtt{C}[\mathtt{g}(e)] \in \mathcal{R}$ and $\mathtt{g} \in Fct$
- The dependency pair graph $G = (V, E)$ is defined by:
  - V is the set of dependency pairs
  - $(\langle u, v \rangle, \langle w, z \rangle) \in E$ iff there is σ such that $v\sigma \xrightarrow{*} w\sigma$

Example (Dependency pair of logarithm)



Dependency pairs as a way to synthesize SI

Theorem (Dependency pair (Arts and Giesl[2000]))

A program is terminating if there is a reduction pair $(>, \geq)$ s.t.:

- *For each rule $l \to r$, $l \geq r$*
- *For each dependency pair $\langle s, t\rangle$, $s \geq t$*
- *For each cycle of the dependency pair graph, $\exists \langle s, t\rangle$ s.t. $s > t$*

Definition

If **p** terminates wrt the reduction pair reduction pair $(>, \geq)$, we say that the program is in $DP(\geq, >)$.

Definition (Polynomial space interpretation)

A program admits a polynomial space interpretation $(\!|-|\!)$ if $(\!|-|\!)$ is a monotonic, additive and polynomial assignment such that:

- For each rule $l \to r$, $(\!|l|\!) \geq (\!|r|\!)$
- For each dependency pair $\langle s, t\rangle$ s.t. $(\!|s|\!) \geq (\!|t|\!)$

Polynomial space interpretations

Theorem

Every polynomial space interpretation is a sup-interpretation

Example

$$(\!|\mathbf{0}|\!) = 0 \qquad (\!|\mathbf{S}|\!)(X) = X + 1$$
$$(\!|\mathtt{half}|\!)(X) = X/2 \qquad (\!|\mathsf{log}|\!)(X) = X$$

In particular:

$$(\!|\mathtt{half}(\mathbf{0})|\!) \geq (\!|\mathbf{0}|\!)$$
$$(\!|\mathtt{half}(\mathbf{S}(\mathbf{0}))|\!) \geq (\!|\mathbf{0}|\!)$$
$$(\!|\mathtt{half}(\mathbf{S}(\mathbf{S}(x)))|\!) \geq (\!|\mathbf{S}(\mathtt{half}(x))|\!)$$
$$(\!|\mathtt{half}(\mathbf{S}(\mathbf{S}(x)))|\!) \geq (\!|\mathtt{half}(x)|\!)$$

Some restrictions on space

Definition (Bounded Recursive Calls)

A program is in $BRC(\llparenthesis - \rrparenthesis)$ if for every dependency pair $(\mathtt{f}(p_1, \cdots, p_n), \mathtt{g}(e_1, \cdots, e_m))$ involved in a cycle of the DP graph, we have:

$$\sum_{j \in \{1,\dots,n\}} \llparenthesis p_j \rrparenthesis \geq \sum_{i \in \{1,\dots,m\}} \llparenthesis e_i \rrparenthesis$$

Definition ($DP(\textsc{space})$)

A program is in $DP(\textsc{space})$ if there is an additive, monotonic and max-polynomial assignment $\llparenthesis - \rrparenthesis$ and a constant $\delta > 0$ such that:

$$\mathbf{p} \in DP(\geq^{\llparenthesis - \rrparenthesis}, >_\delta^{\llparenthesis - \rrparenthesis}) \cap BRC(\llparenthesis - \rrparenthesis)$$

where $x >_\delta^{\llparenthesis - \rrparenthesis} y$ if $\llparenthesis x \rrparenthesis > \llparenthesis y \rrparenthesis + \delta$ (Lucas[2005])

Examples

Example (Bounded Recursive Calls)

Two dependency pairs are involved in cycles:

$$\langle \mathtt{minus}(\mathbf{S}(x),\mathbf{S}(y)) \,, \mathtt{minus}(x,y)\ \rangle : \ (\!|\mathbf{S}(x)|\!) + (\!|\mathbf{S}(y)|\!) \geq (\!|x|\!) + (\!|y|\!)$$
$$\langle \mathtt{q}(\mathbf{S}(x),\mathbf{S}(y)) \,, \mathtt{q}(\mathtt{minus}(x,y),\mathbf{S}(y))\ \rangle : \ (\!|\mathbf{S}(x)|\!) + (\!|\mathbf{S}(y)|\!) \geq (\!|\mathtt{minus}(x,y)|\!) + (\!|\mathbf{S}(y)|\!)$$

Example ($DP(\text{SPACE})$)

To show that $\mathbf{p} \in DP(\geq^{(\!|-|\!)}, >_\delta^{(\!|-|\!)}) \cap BRC((\!|-|\!))$, we have to find δ s.t.:

$$\langle \mathtt{minus}(\mathbf{S}(x),\mathbf{S}(y)) \,, \mathtt{minus}(x,y)\ \rangle : \ (\!|\mathtt{minus}(\mathbf{S}(x),\mathbf{S}(y))|\!) >_\delta (\!|\mathtt{minus}(x,y)|\!)$$
$$\langle \mathtt{q}(\mathbf{S}(x),\mathbf{S}(y)) \,, \mathtt{q}(\mathtt{minus}(x,y),\mathbf{S}(y))\ \rangle : \ (\!|\mathtt{q}(\mathbf{S}(x),\mathbf{S}(y))|\!) >_\delta (\!|\mathtt{q}(\mathtt{minus}(x,y),\mathbf{S}(y))|\!)$$
$$\langle \mathtt{q}(\mathbf{S}(x),\mathbf{S}(y)) \,, \mathtt{minus}(x,y)\ \rangle : \ (\!|\mathtt{q}(\mathbf{S}(x),\mathbf{S}(y))|\!) \geq (\!|\mathtt{minus}(x,y)|\!)$$

$(\!|\mathbf{S}|\!)(X) = X + 1$, $(\!|\mathtt{minus}|\!)(X, Y) = X$, $(\!|\mathtt{q}|\!)(X, Y) = X + Y$ and $\delta = 1$

Some restrictions on time

Definition (Neighborhood)

$N(l \to r)$=$\{(l,t)$, such that (l,t) is involved in a cycle of the SDP graph and there is a context $\mathrm{C}[\diamond]$ such that $r = \mathrm{C}[t]$ $\}$

Definition ($DP(\textsc{time})$)

A program $\mathbf{p}$ belongs to $DP(\textsc{time})$ if there is an additive, monotonic and max-polynomial assignment $(\!|-|\!)$ and a constant $\delta > 0$ such that:

- $\mathbf{p} \in DP(\geq^{(\!|-|\!)}, >_\delta^{(\!|-|\!)}) \cap BRC((\!|-|\!))$
- and, for each neighborhood $\{(l,t_1),\ldots,(l,t_n)\}$:

$$(\!|l|\!) >_\delta \sum_{i=1}^{n} (\!|t_i|\!)$$

Examples

Example (Neighborhood)

There are two neighborhoods:

$$N(\mathtt{minus}(\mathbf{S}(x),\mathbf{S}(y)) \rightarrow \mathbf{S}(\mathtt{minus}(x,y))) = \{\langle \mathtt{minus}(\mathbf{S}(x),\mathbf{S}(y)), \mathtt{minus}(x,y)\rangle\}$$
$$N(\mathtt{q}(\mathbf{S}(x),\mathbf{S}(y)) \rightarrow \mathbf{S}(\mathtt{q}(\mathtt{minus}(x,y),\mathbf{S}(y)))) = \{\langle \mathtt{q}(\mathbf{S}(x),\mathbf{S}(y)), \mathtt{q}(\mathtt{minus}(x,y),\mathbf{S}(y))\rangle\}$$

Example ($DP(\textsc{time})$)

We have already shown that $\mathbf{p} \in DP(\geq^{(\!|-|\!)}, >_1^{(\!|-|\!)}) \cap BRC((\!|-|\!))$
It remains to check that for the neighborhoods, we have:

$$(\!|\mathtt{minus}(\mathbf{S}(x),\mathbf{S}(y))|\!) \geq (\!|\mathtt{minus}(x,y)|\!)$$
$$(\!|\mathtt{q}(\mathbf{S}(x),\mathbf{S}(y))|\!) \geq (\!|\mathtt{q}(\mathtt{minus}(x,y),\mathbf{S}(y))|\!)$$

$(\!|\mathbf{S}|\!)(X) = X+1$, $(\!|\mathtt{minus}|\!)(X,Y) = X$, $(\!|\mathtt{q}|\!)(X,Y) = X+Y$

Conclusion

Theorem

- $DP(\textsc{time}) = \mathrm{FP}\textsc{time}$
- $DP(\textsc{space}) = \mathrm{FP}\textsc{space}$

We obtain a better intensionality (tight upper bounds)

- with non-subterm assignments
- and dependency pairs

We can extend the result to RPO characterizations:

Theorem

1. $DP(\precsim, \succ_{rpo}^{prod}) \cap QI_{poly}^{add}$ *is exactly* $\mathrm{FP}\textsc{time}$
2. $DP(\precsim, \succ_{rpo}) \cap QI_{poly}^{add}$ *is exactly* $\mathrm{FP}\textsc{space}$

whenever $(\precsim, \succ_{rpo})$ *is a reduction pair satisfying both* $\precsim \circ \succ_{rpo} \subseteq \succ_{rpo}$ *and* $\prec_{rpo} \circ \precsim \subseteq \succ_{rpo}$