Formalizing Termination Proofs under Polynomial Quasi-interpretations

Naohi Eguchi

Chiba University

July 5, 2015, LCC 2015, Kyoto, Japan

1Supported by Grants-in-Aid for JSPS fellows (No. 25·726)
Overview 1/2

Primitive-, Multiply Recursive Functions

(Peano) Arithmetic

Term Rewriting
Overview 1/2

Primitive-, Multiply Recursive Functions

- Parsons '70
- Hofbauer '92, Weiermann '95
- Buchholz '95

(Peano) Arithmetic

Term Rewriting
Overview 2/2

Poly-time-, Poly-space Functions

Bounded Arithmetic

Buss '86

Term Rewriting

Bonfante-Marion-Moyen '11, '01
Overview 2/2

Poly-time-, Poly-space Functions

Bounded Arithmetic

Bonfante-Marion-Moyen '11, '01

Term Rewriting

Buss '86

This work
First order functional programs (Term rewrite systems)

Multiset path orders (MPOs), Lexicographic path orders (LPOs)

Optimal formalizations of MPO-, LPO-termination proofs (Buchholz '95)

Polynomial quasi-interpretations (PQIs)

An optimal formalization of LPO-termination proofs under PQIs (This work)
First order functional programs: Syntax

### Syntax:

<table>
<thead>
<tr>
<th>Component</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>variable</td>
<td>$x$</td>
</tr>
<tr>
<td>signature (finite)</td>
<td>$\mathcal{F} := \mathcal{C} \cup \mathcal{D}$</td>
</tr>
<tr>
<td>constructor</td>
<td>$c$</td>
</tr>
<tr>
<td>defined symbol</td>
<td>$f$</td>
</tr>
<tr>
<td>term</td>
<td>$t := x \mid c(t_1, \ldots, t_k) \mid f(t_1, \ldots, t_k)$</td>
</tr>
<tr>
<td>constructor term</td>
<td>$s := x \mid c(s_1, \ldots, s_k)$</td>
</tr>
<tr>
<td>basic term</td>
<td>$u := f(s_1, \ldots, s_k)$</td>
</tr>
<tr>
<td>reduction rule</td>
<td>$u \rightarrow t$</td>
</tr>
</tbody>
</table>

- **Program** $\mathcal{R}$: finite set of reduction rules
- $\xrightarrow{i_{\mathcal{R}}}$: innermost reduction under $\mathcal{R}$
- $\xrightarrow{i_{\mathcal{R}}}^*$: reflexive and transitive closure $\xrightarrow{i_{\mathcal{R}}}$
- $t \xrightarrow{i_{\mathcal{R}}}^! s \Leftrightarrow t \xrightarrow{i_{\mathcal{R}}}^* s \in \text{NF}(\mathcal{R})$ (normal form under $\mathcal{R}$)
First order functional programs: Semantics

Semantics: \( R \) computes the function \( \| f \| : \mathcal{T}(C)^k \rightarrow \mathcal{T}(C) \quad (f \in \mathcal{D}) \) iff

\[
\forall s_1, \ldots, s_k \in \mathcal{T}(C), \exists! s \in \mathcal{T}(C) \text{ s.t. } f(s_1, \ldots, s_k) \xrightarrow{i!_R} s.
\]

Necessary:

1. \( R \): (innermost) terminating: \( \forall t \in \mathcal{B}(\mathcal{F}), \exists s \text{ s.t. } t \xrightarrow{i!_R} s \)
2. \( R \): confluent
3. \( R \): quasi-reducible (QR): any (closed) basic term is reducible

Termination criterion

\( R \): terminating if \( \exists \langle \mathcal{A}, \prec \rangle: \text{ well-founded, } \exists \langle \cdot \rangle : \mathcal{T}(\mathcal{F}) \rightarrow \mathcal{A} \text{ s.t.} \)

\[
(\forall l \rightarrow r \in \mathcal{R})(\forall \theta : \mathcal{V} \rightarrow \mathcal{T}(C))(\| r\theta \| \prec \| l\theta \|)
\]
1. First order functional programs (Term rewrite systems)

2. Multiset path orders (MPOs), Lexicographic path orders (LPOs)

3. Optimal formalizations of MPO-, LPO-termination proofs (Buchholz '95)

4. Polynomial quasi-interpretations (PQIs)

5. An optimal formalization of LPO-termination proofs under PQIs (This work)
This work is concerned with a more specific case:

∃ \textless_{rpo}: recursive path order s.t. \( (\forall l \rightarrow r \in \mathcal{R}) \ l \textgreater_{rpo} r \quad (\mathcal{R} \subseteq \textgreater_{rpo}) \)

**Definition (Recursive path orders with status)**

\( s \textless_{rpo} t := g(t_1, \ldots, t_l) \) iff

1. \( x \textless_{rpo} t_i \) for some \( i \in \{1, \ldots, l\} \), or
2. \( s = f(s_1, \ldots, s_k), \ rk(f) < rk(g) \) and \( s_1, \ldots, s_k \textless_{rpo} t \), or
3. \( s = g(s_1, \ldots, s_l) \) and \( (s_1, \ldots, s_l) \textless_{rpo}^\tau (t_1, \ldots, t_l) \), where \( \tau : \mathcal{F} \rightarrow \{\text{prod, mul, lex}\} \) is a status function.

**Definition (Multiset-, lexicographic path orders)**

1. \( \textless_{mpo}: \textless_{rpo} \) with \texttt{mul} status only
2. \( \textless_{lpo}: \textless_{rpo} \) with \texttt{lex} status only
First order functional programs (Term rewrite systems)

Multiset path orders (MPOs), Lexicographic path orders (LPOs)

Optimal formalizations of MPO-, LPO-termination proofs (Buchholz ’95)

Polynomial quasi-interpretations (PQIs)

An optimal formalization of LPO-termination proofs under PQIs (This work)
Formalizations of MPO-, LPO-termination proofs

Theorem (Buchholz ’95)

1. $\text{I} \Sigma_1 \vdash "R \subseteq_{\text{mpo}} \Rightarrow R \text{ is terminating}"
   (IΣ₁: Peano arithmetic with induction restricted to c.e. sets)
2. $\text{I} \Sigma_2 \vdash "R \subseteq_{\text{lpo}} \Rightarrow R \text{ is terminating}"
   (IΣ₂: induction restricted to “f is total” for some computable f)

Corollary

1. Computable by MPO-terminating programs $\Rightarrow$ primitive rec.
2. Computable by LPO-terminating programs $\Rightarrow$ multiply recursive

These results are optimal because:

1. Primitive rec. $\Rightarrow$ computable by MPO-terminating programs
2. Multiply rec. $\Rightarrow$ computable by LPO-terminating programs
1. First order functional programs (Term rewrite systems)

2. Multiset path orders (MPOs), Lexicographic path orders (LPOs)

3. Optimal formalizations of MPO-, LPO-termination proofs (Buchholz '95)

4. Polynomial quasi-interpretations (PQIs)

5. An optimal formalization of LPO-termination proofs under PQIs (This work)
Quasi-interpretations

Associate a quasi-interpretation $\langle f \rangle : N^k \to N$ for each $k$-ary $f \in F$:

$$m < n \Rightarrow \langle f \rangle(\cdots m \cdots) \leq \langle f \rangle(\cdots n \cdots)$$

(e.g. $m < n \Rightarrow \max(m,m') \leq \max(n,m')$)

Extend to $T(F)$:

$$\langle f(t_1,\ldots,t_k) \rangle := \langle f \rangle(\langle t_1 \rangle,\ldots,\langle t_k \rangle)$$

Definition

1. $R$ admits a quasi-interpretation $\langle \cdot \rangle$ if

$$(\forall l \to r \in R)(\forall \theta: V \to T(C))(\langle r\theta \rangle) \leq \langle l\theta \rangle.$$

2. $R$: LPO$^{\text{Poly}}(0)$-program if $R$: LPO-terminating & admits a (kind 0) polynomially-bounded quasi-interpretation (PQI)

Theorem (Bonfante-Marion-Moyen '01)

Computable by LPO$^{\text{Poly}}(0)$-programs $\iff$ polynomial-space computable
First order functional programs (Term rewrite systems)

Multiset path orders (MPOs), Lexicographic path orders (LPOs)

Optimal formalizations of MPO-, LPO-termination proofs (Buchholz ’95)

Polynomial quasi-interpretations (PQIs)

An optimal formalization of LPO-termination proofs under PQIs (This work)
Difficulty

Theorem (Buchholz ’95)
\[ \Sigma_2 \vdash "R \subseteq >_{lpo} \Rightarrow R \text{ is terminating}" \]

Lemma
\[ \Sigma_2 \vdash "R \subseteq >_{lpo} \Rightarrow \forall t \in T(F),\text{ the reduction tree } T \text{ rooted at } t \text{ is well-founded}" \]

- Problem: \( \text{size}(T) \approx 2^{\text{depth}(T)} \)
- Polynomial-space is not closed under \( m \mapsto 2^m \)
- The same argument does not yields the poly-space complexity
- Something smaller in size than reduction trees seems necessary
  \[ \Rightarrow \text{ Minimal function graph} \]
Minimal function graphs (Jones ’97, Marion ’03)

Minimal function graph $G_R(t) \subseteq B(\mathcal{F}) \times T(\mathcal{C})$ ($t \in B(\mathcal{F})$):

$$G_R(t) \subseteq \{\langle u, v \rangle \mid u \xrightarrow{R} v\} \& \exists s \in T(\mathcal{C}) \text{ s.t. } \langle t, s \rangle \in G_R(t)$$

How to construct minimal function graphs:

1. Let $t \in B(\mathcal{F})$
2. $\exists l \rightarrow r \in R, \exists \theta : \mathcal{V} \rightarrow T(\mathcal{C}) \text{ s.t. } t = l\theta$ (if $R$: quasi-reducible)
3. Let $u \triangleleft r\theta \& u \in B(\mathcal{F})$ ($u$ is a basic sub-term of $r\theta$)
4. Construction of $G_R(t)$ depends on $G_R(u)$
5. $u <_{lpo} l\theta = t$ (if $R \subseteq >_{lpo}$)
6. $$(\forall t \in B(\mathcal{F}))(\forall u <_{lpo} t)\exists G_R(u) \rightarrow \exists G_R(t)$$

Thus it suffices to deduce $T I_{\exists G_R}(<_{lpo})$:

$$\forall t \in B(\mathcal{F}))(\forall s <_{lpo} t)\exists G_R(s) \rightarrow \exists G_R(t) \rightarrow \forall t \in B(\mathcal{F})\exists G_R(t)$$

Suitable framework: weak enough so that $m \mapsto 2^m$ is not definable

- $U_2^1$: 2nd order Bounded arithmetic corresponding to PSPACE
Main result

$U^1_2$: axiomatized with $\varphi(0) \land \forall m (\varphi(\lfloor m/2 \rfloor) \rightarrow \varphi(m)) \rightarrow \forall m \varphi(m)$

($\varphi(\cdot)$: $\Sigma^{b,1}_1$-formula including $\exists G_R(\cdot)$)

Lemma

$U^1_2 \vdash "R: QR & R \subseteq >_lpo & R admits a PQI " \rightarrow TI_{\exists G_R}(<_lpo)$

Theorem

$U^1_2 \vdash "R: QR & LPO^{Poly(0)} " \rightarrow (\forall t \in B(\mathcal{F})) \exists G_R(t)$

By Buss’ theorem $\exists f$: poly-space s.t. $\forall t \in B(\mathcal{F}), t \xrightarrow{i_{\mathcal{R}}} f(t)$. Hence:

Corollary

Computationally by quasi-reducible LPO$^{Poly(0)}$-programs

$\Rightarrow$ polynomial-space computable
Summary

Polynomial-space Computable Functions

Bounded Arithmetic $U^1_2$

Term Rewriting $LPO^{Poly(0)}$

Buss '86

Bonfante-Marion-Moyen '01
Summary

Polynomial-space Computable Functions

Bounded Arithmetic $U_2^1$

Term Rewriting $LPO^{\text{Poly}(0)}$

Optimal termination proof for $LPO^{\text{Poly}(0)}$-programs in $U_2^1$
Future work?

\[ R: \text{MPO}^{\text{Poly}(0)}\text{-program if } R: \text{MPO-terminating (with prod status only)} & \text{admits a (kind 0) PQI} \]

**Theorem (Bonfante-Marion-Moyen ’11)**

*Computable by MPO^{\text{Poly}(0)}-programs \iff polynomial-time computable*

**Question**

\[ S_2^1 \vdash \text{“} R : \text{QR} & \text{MPO}^{\text{Poly}(0)} \text{”} \rightarrow (\forall t \in B(\mathcal{F})) \exists G_R(t) ? \]

---

*Formalizing Termination Proofs under Polynomial Quasi-interpretations*

Submitted to Workshop on Fixed Points in Computer Science

*Thank you for your attention!*