Functional Reachability

Luke Ong        Nikos Tzevelekos

Oxford University Computing Laboratory

AVOCS'09, Gregynog
The Problem

Reachability in HO functional languages

\[ M(\bar{x}) \]
The Problem

Reachability in HO functional languages
The Problem

Reachability in HO functional languages

\[ C : \text{prog} \]

\[ M(\overline{x}) \]
Functional Reachability

- Given a term $M$ of a HO functional language and a point $p$ inside $M$,
- is there a program context $C$ such that the computation of $C[M]$ reaches $p$?

Surprisingly, (Contextual) Reachability *per se* had not been studied in HO functional languages.
Relevant work

- Control Flow Analysis.
  - *Approximate at compile time the flow of control to happen at run time.*
  
  - Crucial element: *closures.*
  
  - Reynolds ('70), Jones ('80), Shivers ('90), ...
  - Malacaria & Hankin (late '90).

- CFA > Reach (more general)
  Reach > CFA (open vs closed world)

- Useless code detection, etc.
Examined language: PCF.

- lambda-calculus,
- Boolean base type,
- recursion at all types.

\[
\begin{align*}
A, B & ::= o \mid A \rightarrow B \\
M, N & ::= x \mid \lambda x. M \mid t \mid f \mid \text{if } M N_1 N_2 \mid Y_A
\end{align*}
\]
PCF

\[
A, B ::= o \mid A \rightarrow B
\]

\[
M, N ::= x \mid \lambda x. M \mid t \mid f \mid \text{if } M \ N_1 N_2 \mid Y_A
\]

\[
E ::= \_ \mid E M \mid \text{if } E N_1 N_2
\]

\[
(\lambda x. M) N \rightarrow M \{ N / x \}
\]

\[
\text{if } t \rightarrow \lambda xy.x , \ldots
\]

\[
Y M \rightarrow M (Y M)
\]
Notes on PCF

- Write \((A_1, \ldots, A_n, o)\) for \(A_1 \rightarrow \cdots A_n \cdots \rightarrow o\)
- Divergence definable: \(\perp := Y_0(\lambda x. x)\)
- *Finitary* restrictions (i.e. no rec.):

\[
\text{fPCF} \\
M, N ::= x | \lambda x. M | t | f | \text{if } M N_1 N_2
\]

\[
\text{fPCF}_\perp \\
M, N ::= x | \lambda x. M | t | f | \text{if } M N_1 N_2 | \perp
\]
Reachability (in PCF)

- Given a closed PCF-term $M:(A_1,\ldots,A_n,o)$ and a coloured subterm $L$ of $M$,
- are there closed PCF-terms $N_1,\ldots,N_n$ such that $MN_1\ldots N_n$ reduces to $E[L']$ with $L'$ coloured?
Reachability (in PCF)

• Given a closed PCF-term $M:(A_1,\ldots,A_n,o)$ and a coloured subterm $L$ of $M$,
• are there closed PCF-terms $N_1,\ldots,N_n$ such that $MN_1\ldots N_n$ reduces to $E[L']$ with $L'$ coloured?

We can make things even simpler …
PCF-with-error: PCF∗

Include an error constant: $o = \{t, f, *\}$

New rules: $E[*]$ reduces to $*$. 

*-Reachability:

- Given a closed PCF∗-term $M:(A_1,\ldots,A_n,o)$ with exactly one $*$,
- are there closed PCF-terms $N_1,\ldots,N_n$ such that $MN_1\ldots N_n$ reduces to $*$?
PCF-with-error: PCF*

Include an error constant: \( o = \{ t, f, * \} \)

New rules: \( E[*] \) reduces to *. 

Reachability \( \approx * \)-Reachability

*-Reachability:

- Given a closed PCF*-term \( M:(A_1,\ldots,A_n,o) \) with exactly one *,
- are there closed PCF-terms \( N_1,\ldots,N_n \) such that \( MN_1\ldots N_n \) reduces to *?
Reach template

• Several classes of problems:
  - Reachability
  - *-Reachability
Reach template

• Several classes of problems:
  - Reachability
  - \(\ast\)-Reachability, i.e. \(\ast\text{-REACH}[\text{PCF}^{1\ast},\text{PCF}]\)
Several classes of problems:

- Reachability

- \( \ast \)-Reachability, i.e. \( \ast \)-REACH[PCF\textsuperscript{1\ast},PCF]\n
- \( \ast \)-REACH[PCF\textsuperscript{1\ast},fPCF]\n
Reach template

• Several classes of problems:
  - Reachability
  - \(*\)-Reachability, i.e. \(*\)-REACH[PCF_{1*},PCF]
  - \(*\)-REACH[PCF_{1*},fPCF]
  - \(*\)-REACH[fPCF_{1*},fPCF]
Reach template

- Several classes of problems:
  - Reachability
  - *-Reachability, i.e. *-REACH[PCF^{1*},PCF]
  - *-REACH[PCF^{1*},fPCF]
  - *-REACH[fPCF^{1*},fPCF]
  - *-REACH[fPCF_{1*},fPCF]
Reach template

• Several classes of problems:
  - Reachability
  - \(*\)-Reachability, i.e. \(*\)-\text{REACH}[\text{PCF}^1*,\text{PCF}]
  - \(*\)-\text{REACH}[\text{PCF}^1*,\text{fPCF}]
  - \(*\)-\text{REACH}[\text{fPCF}^1*,\text{fPCF}]

UNDECIDABLE \(*\)-\text{REACH}[\text{fPCF}^1_\perp*,\text{fPCF}]
Reach template

- Several classes of problems:

  - Reachability
  - \(*\)-Reachability, i.e. \(*\)-REACH[PCF_{1*},PCF]
  - \(*\)-REACH[PCF_{1*},\text{fPCF}]
  - \(*\)-REACH[\text{fPCF}_{1*},\text{fPCF}]
  - \(*\)-REACH[\text{fPCF}_{1*},\text{fPCF}]

  UNDECIDABLE
Reach template

- Several classes of problems:

<table>
<thead>
<tr>
<th>Undecidable</th>
<th>Reachability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UNDECIDABLE</strong></td>
<td><strong>Reachability</strong></td>
</tr>
<tr>
<td><strong>UNDECIDABLE</strong></td>
<td>***-Reachability, i.e. <strong><em>-REACH[PCF^{1</em>},PCF]</strong></td>
</tr>
<tr>
<td><strong>UNDECIDABLE</strong></td>
<td><strong><em>-REACH[PCF^{1</em>},fPCF]</strong></td>
</tr>
<tr>
<td><em>-REACH[fPCF^{1</em>},fPCF]</td>
<td></td>
</tr>
<tr>
<td><strong>UNDECIDABLE</strong></td>
<td><strong><em>-REACH[fPCF^{1</em>},fPCF]</strong></td>
</tr>
<tr>
<td><strong>UNDECIDABLE</strong></td>
<td><em><em>t-REACH[fPCF^{1</em>},fPCF]</em>*</td>
</tr>
</tbody>
</table>
Our approach

- We examine $\nu$-REACH[fPCF$^{1*}$,fPCF] using:
  - Alternating Dependency Tree Automata
  - Alternating Tree Automata
Our approach

- We examine \( \nu\text{-REACH}[f\text{PCF}^1, f\text{PCF}] \) using:
  - Alternating Dependency Tree Automata
  - Alternating Tree Automata
- Given a term \( M \), the automaton runs on its computation tree (a souped-up syntax tree).

Stirling'09
Our approach

- We examine $\nu$-REACH[fPCF$^{1*}$,fPCF] using:
  - Alternating Dependency Tree Automata
  - Alternating Tree Automata
- Given a term $M$, the automaton runs on its computation tree (a souped-up syntax tree).
- The automaton assigns/checks profiles to the variables it encounters.
- Approach based on game semantics.

Stirling'09
Results

\[ \nu\text{-REACH}[fPCF^{1*}, fPCF] \rightarrow \text{ADTA-non-emptiness} \]

- Non-emptiness of ADTA's is undecidable.

\[ \nu\text{-REACH}[fPCF^{1*}, fPCF(n)] \rightarrow \text{ATA-non-emptiness} \]

- \( \nu\text{-REACH}[fPCF^{1*}, fPCF(n)] \) is decidable.
- \( \nu\text{-REACH}[fPCF^{1*}, fPCF] \) is decidable at order 3.
Conclusion

- A new kind of reachability problems.
- Some undecidability results.
- Some technology from game semantics.
- Characterisation by ATA's and ADTA's.
- Some relativised decidability results.
Conclusion

- A new kind of reachability problems.
- Some undecidability results.
- Some technology from game semantics.
- Characterisation by ATA's and ADTA's.
- Some relativised decidability results.

- Revisit (semantic) CFA?
- Conjecture: $*-\text{REACH}[\text{fPCF}^1,\text{fPCF}]$?
Conclusion

- A new kind of reachability problems.
- Some undecidability results.
- Some technology from game semantics.
- Characterisation by ATA's and ADTA's.
- Some relativised decidability results.

THANKS!

- Revisit (semantic) CFA?
- Conjecture: $\star$-REACH[fPCF$^{1\ast},\text{fPCF}$]?