Functional Reachability

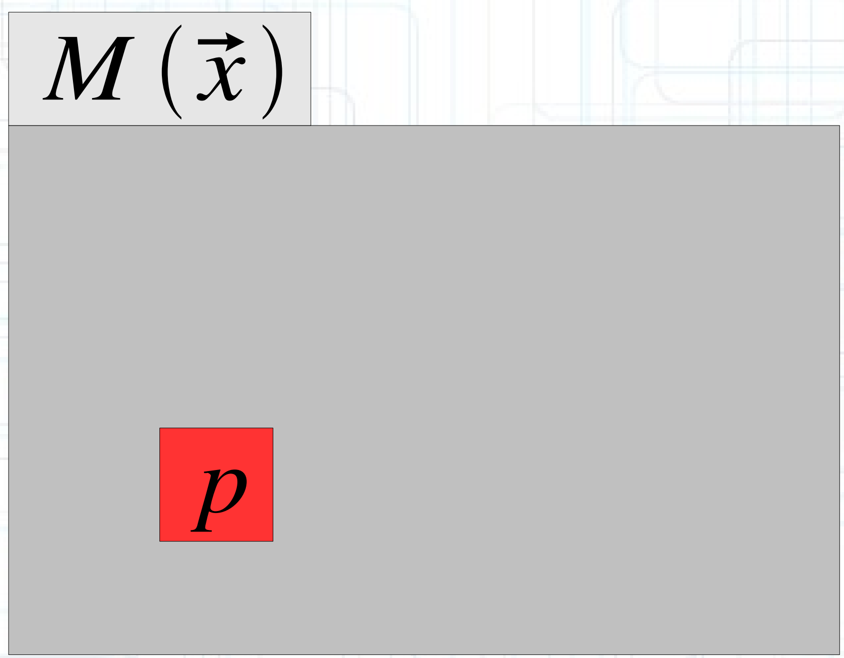
Luke Ong **Nikos Tzevelekos**

Oxford University Computing Laboratory

AVOCS'09, Gregynog

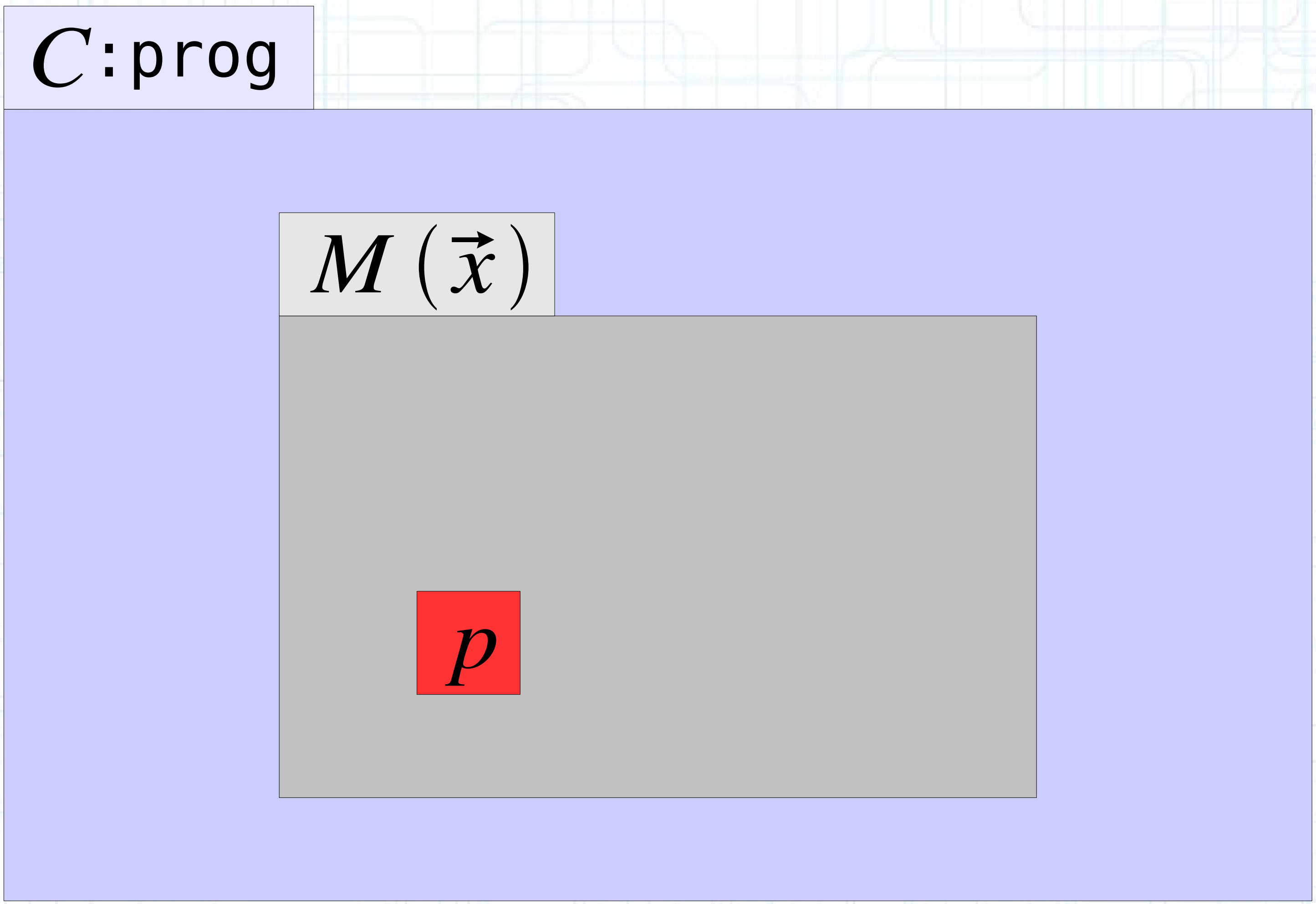
The Problem

Reachability in HO functional languages



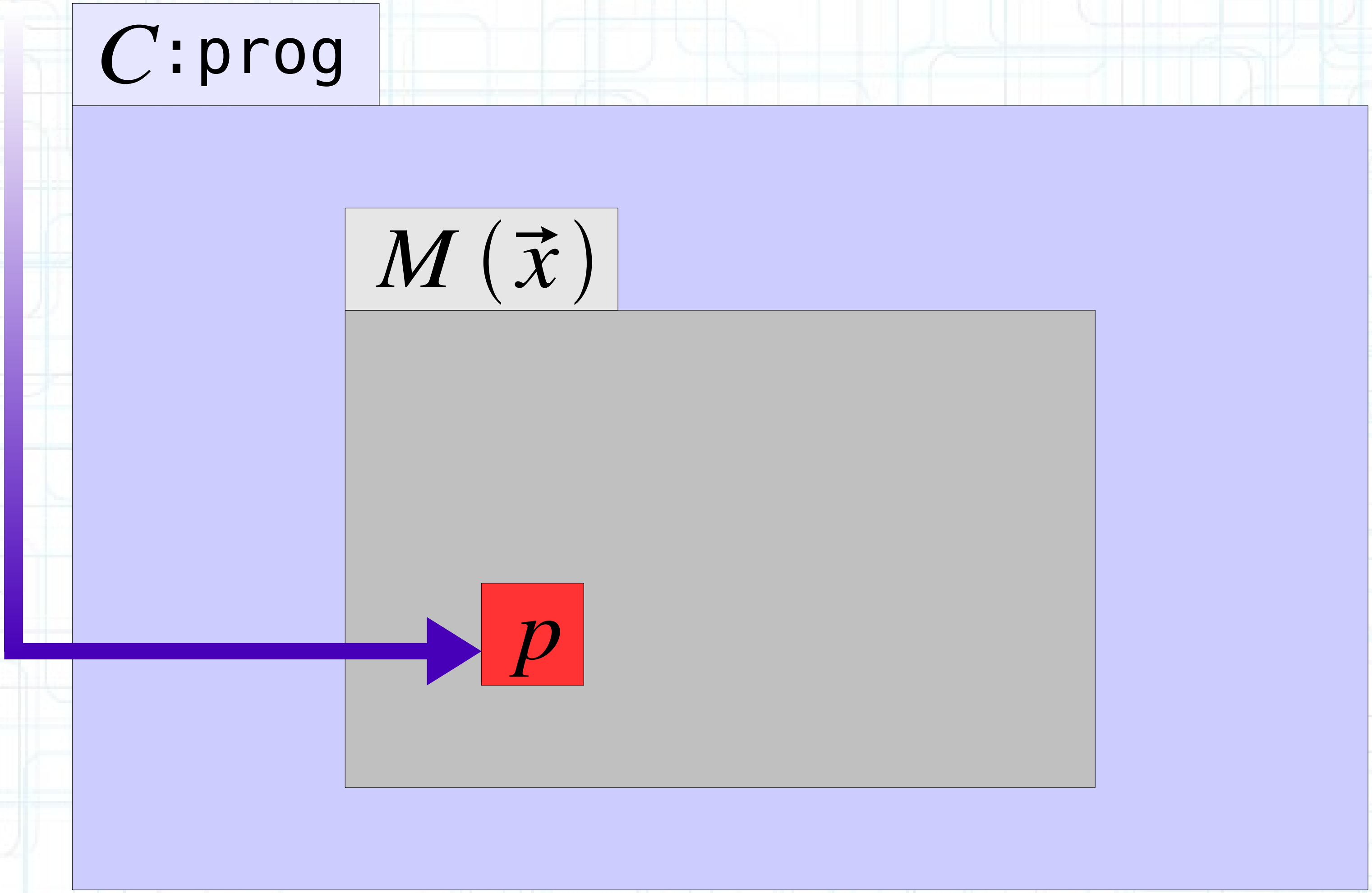
The Problem

Reachability in HO functional languages



The Problem

Reachability in HO functional languages



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.

PCF

Examined language: PCF.

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

$$A, B \ ::= o \mid A \to B$$

$$M, N \ ::= x \mid \lambda x. M \mid \mathrm{t} \mid \mathrm{f} \mid \mathrm{if}\, M\ N_1\, N_2 \mid \mathrm{Y}_A$$

PCF

$$A, B \ ::= o \mid A \to B$$

$$M, N \ ::= x \mid \lambda x.M \mid \mathrm{t} \mid \mathrm{f} \mid \mathrm{if}\, M\, N_1\, N_2 \mid \mathrm{Y}_A$$

$$E \ ::= [\_] \mid E\, M \mid \mathrm{if}\, E\, N_1\, N_2$$

$$(\lambda x.M)N \to M\{N/x\}$$

$$\mathrm{if}\,\mathrm{t} \to \lambda xy.x \ , \ldots$$

$$\mathrm{Y}\, M \to M(\mathrm{Y}\, M)$$

$$\frac{M \to N}{E[M] \to E[N]}$$

Notes on PCF

- Write *(A_1,…,A_n,o)* for $A_1 \to \cdots A_n \cdots \to o$
- Divergence definable: $\perp := \mathrm{Y}_0(\lambda x.\, x)$
- *Finitary* restrictions (i.e. no rec.):

fPCF

$$M, N \ ::= x \mid \lambda x.\, M \mid \mathrm{t} \mid \mathrm{f} \mid \mathrm{if}\, M\ N_1\, N_2$$

$\mathrm{fPCF}_\perp$

$$M, N \ ::= x \mid \lambda x.\, M \mid \mathrm{t} \mid \mathrm{f} \mid \mathrm{if}\, M\ N_1\, N_2 \mid \perp$$

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: $o = \{\mathrm{t}, \mathrm{f}, \star\}$

New rules: $E[\star]$ reduces to $\star$.

$\star$-Reachability:

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

PCF-with-error: PCF*

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

New rules: $E[\star]$ reduces to $\star$.

Reachability $\approx$ $\star$-Reachability

$\star$-Reachability:

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

PCF^{1*}

Reach template

- Several classes of problems:
  - Reachability
  - $\star$-Reachability

Reach template

- Several classes of problems:
  - Reachability
  - $\star$-Reachability, i.e. $\star$-REACH[PCF^{1*},PCF]

Reach template

- Several classes of problems:
  - Reachability
  - $\star$-Reachability, i.e. $\star$-REACH[PCF^{1*},PCF]
  - $\star$-REACH[PCF^{1*},fPCF]

Reach template

- Several classes of problems:
  - Reachability
  - $\star$-Reachability, i.e. $\star$-REACH[PCF^{1*},PCF]
  - $\star$-REACH[PCF^{1*},fPCF]
  - $\star$-REACH[fPCF^{1*},fPCF]

Reach template

- Several classes of problems:
  - Reachability
  - $\star$-Reachability, i.e. $\star$-REACH[PCF^{1*},PCF]
  - $\star$-REACH[PCF^{1*},fPCF]
  - $\star$-REACH[fPCF^{1*},fPCF]
  - $\star$-REACH[fPCF$_{\perp}^{1\star}$,fPCF]

Reach template

- Several classes of problems:
  - Reachability
  - $\star$-Reachability, i.e. $\star$-REACH[$\mathrm{PCF}^{1\star}$,PCF]
  - $\star$-REACH[$\mathrm{PCF}^{1\star}$,fPCF]
  - $\star$-REACH[$\mathrm{fPCF}^{1\star}$,fPCF]

UNDECIDABLE $\star$-REACH[$\mathrm{fPCF}_{\perp}^{1\star}$,fPCF]

Reach template

- Several classes of problems:

UNDECIDABLE – Reachability

UNDECIDABLE – $\star$-Reachability, i.e. $\star$-REACH[$\mathrm{PCF}^{1\star}$,PCF]

UNDECIDABLE – $\star$-REACH[$\mathrm{PCF}^{1\star}$,fPCF]

– $\star$-REACH[$\mathrm{fPCF}^{1\star}$,fPCF]

UNDECIDABLE – $\star$-REACH[$\mathrm{fPCF}_{\perp}^{1\star}$,fPCF]

Reach template

- Several classes of problems:
  - UNDECIDABLE Reachability
  - UNDECIDABLE $\star$-Reachability, i.e. $\star$-REACH[PCF^{1*},PCF]
  - UNDECIDABLE $\star$-REACH[PCF^{1*},fPCF]
  - $\star$-REACH[fPCF^{1*},fPCF]
  - UNDECIDABLE $\star$-REACH[$\mathrm{fPCF}_{\perp}^{1*}$,fPCF]
  - UNDECIDABLE t-REACH[fPCF^{1*},fPCF]

Our approach

- We examine ν-REACH[fPCF^{1*},fPCF] using:
  - Alternating Dependency Tree Automata
  - Alternating Tree Automata

Stirling'09

Our approach

- We examine ν-REACH[fPCF^{1*},fPCF] using:
  - Alternating Dependency Tree Automata
  - Alternating Tree Automata

Stirling'09

- Given a term *M*, the automaton runs on its *computation tree* (a souped-up syntax tree).

Our approach

- We examine ν-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

ν-REACH[fPCF^{1*},fPCF] $\longrightarrow$ ADTA-non-emptiness

- Non-emptiness of ADTA's is undecidable.

ν-REACH[fPCF^{1*},fPCF(n)] $\longrightarrow$ ATA-non-emptiness

- ν-REACH[fPCF^{1*},fPCF(n)] is decidable.
- ν-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: $\star$-REACH[fPCF^{1*},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*},fPCF] ?