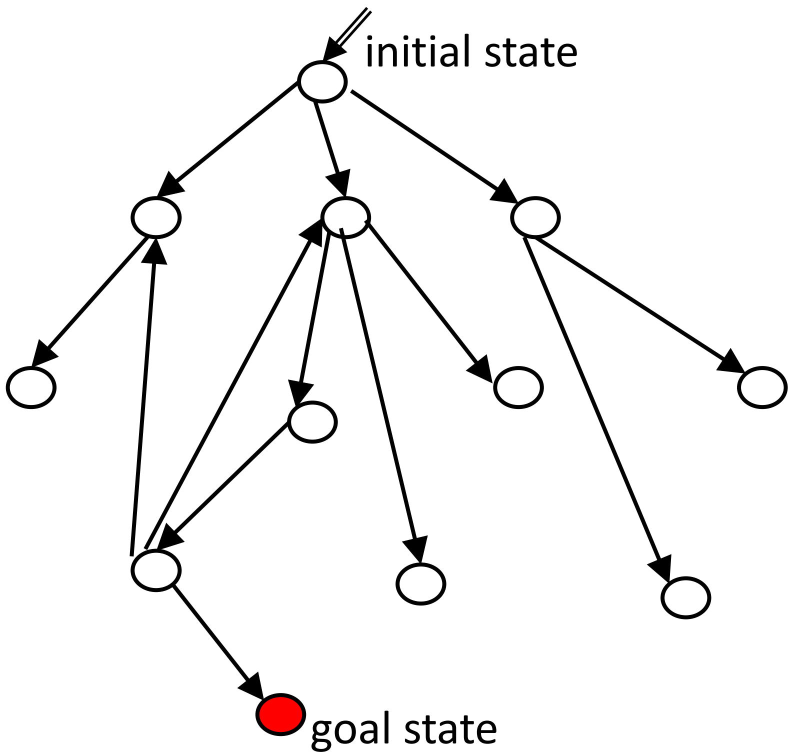
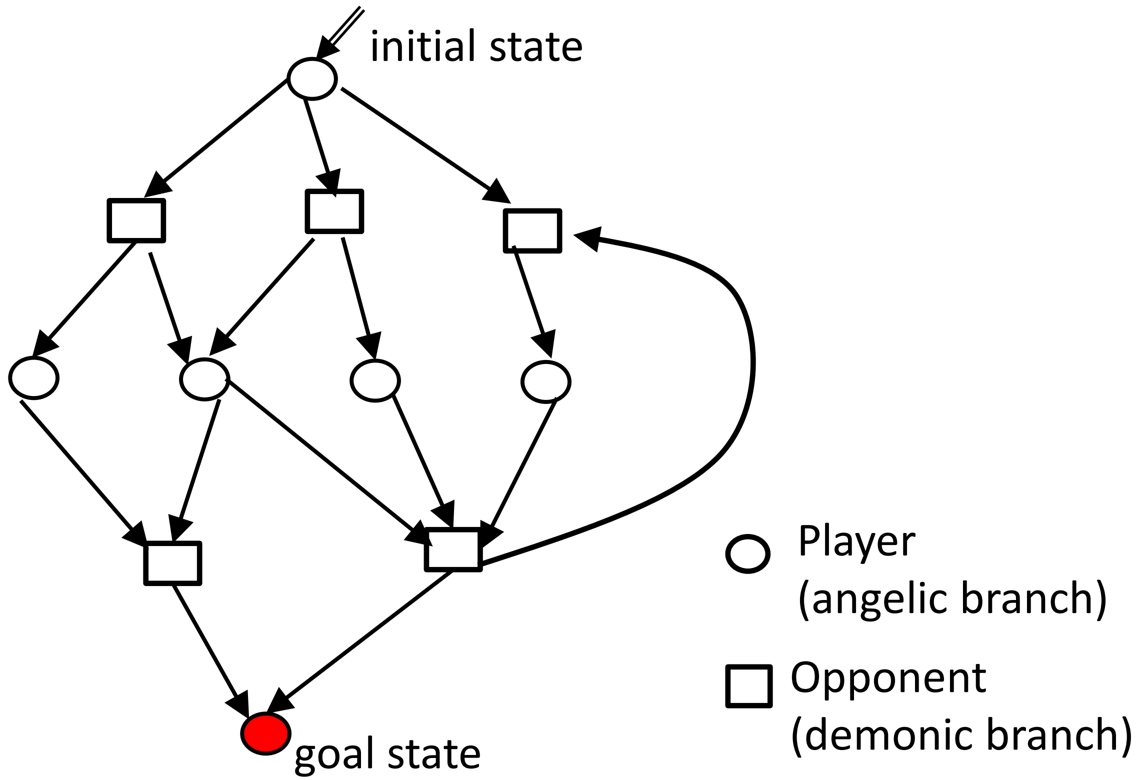
On Higher-Order Reachability Games vs May Reachability

Kazuyuki Asada
Tohoku University

Hiroyuki Katsura Naoki Kobayashi
The University of Tokyo

May Reachability vs Reachability Games

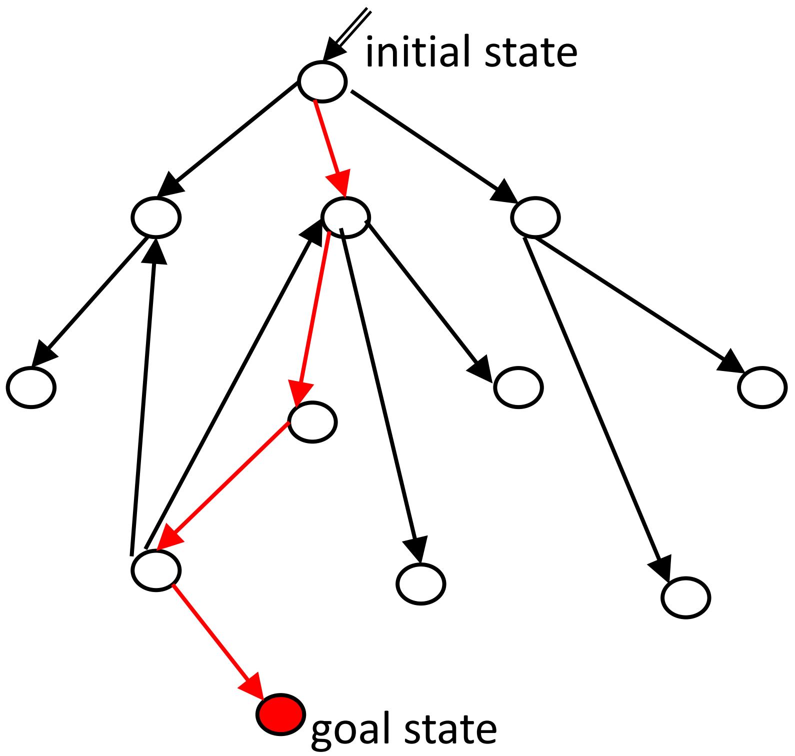




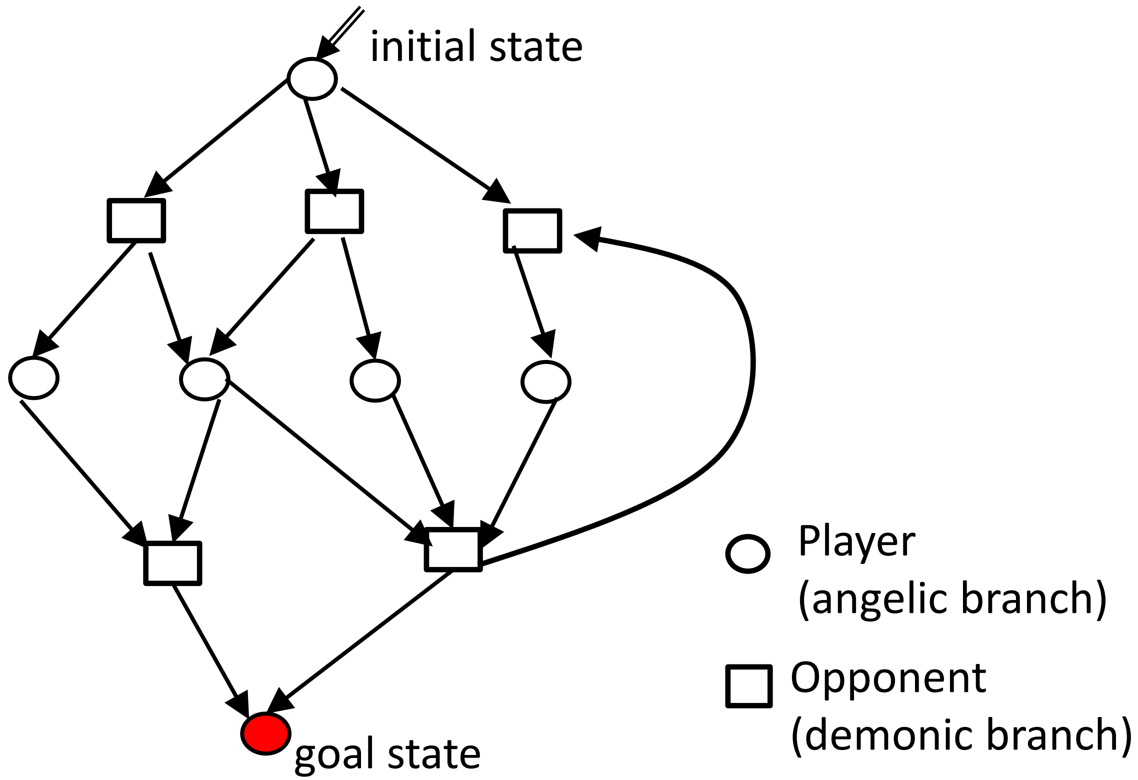
Does there exists a path to the goal state?

Can the goal state be reached
whatever move the opponent (□) chooses?

May Reachability vs Reachability Games

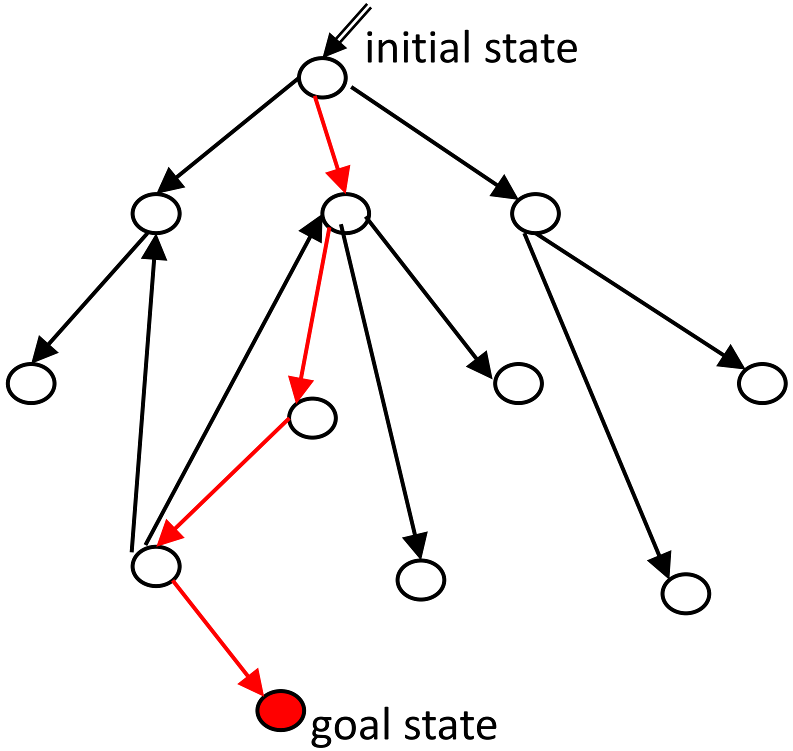


Does there exists a path to the goal state?

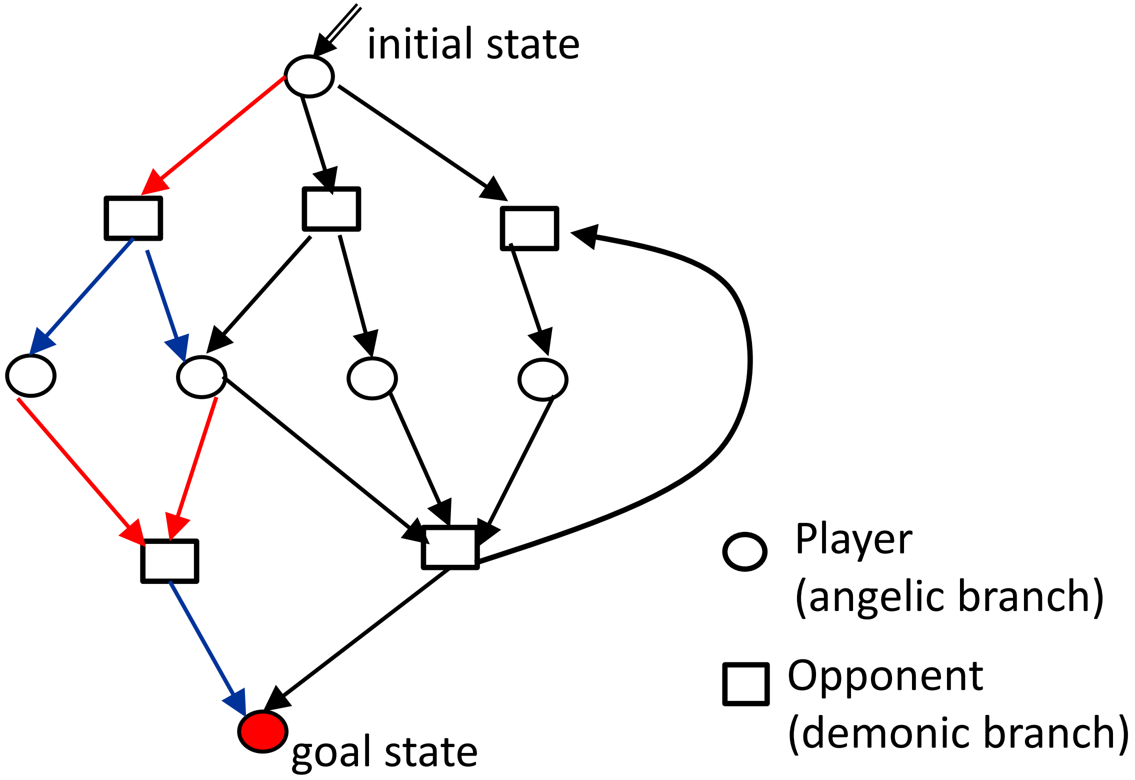


Can the goal state be reached
whatever move the opponent (□) chooses?

May Reachability vs Reachability Games

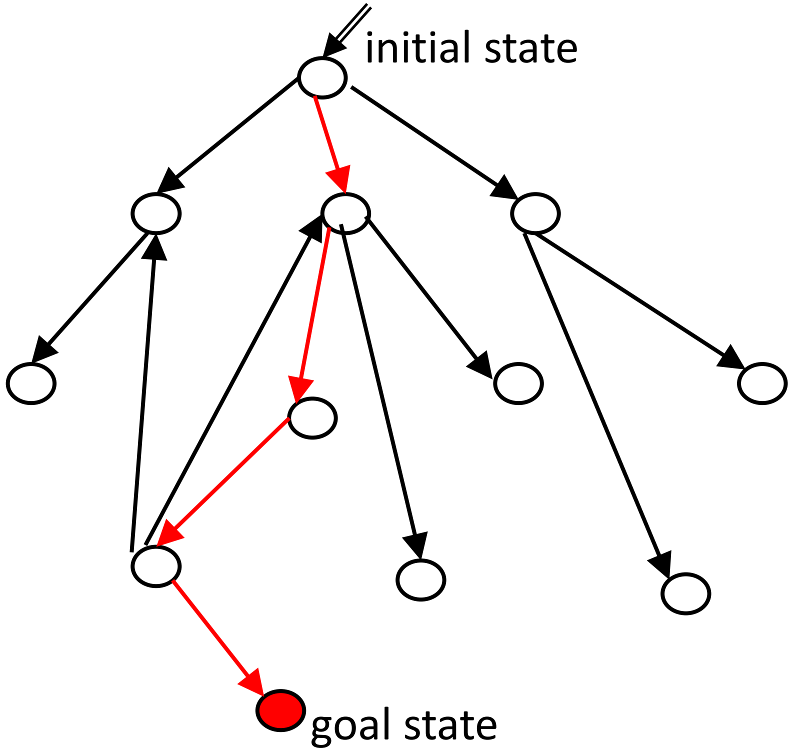


Does there exists a path to the goal state?



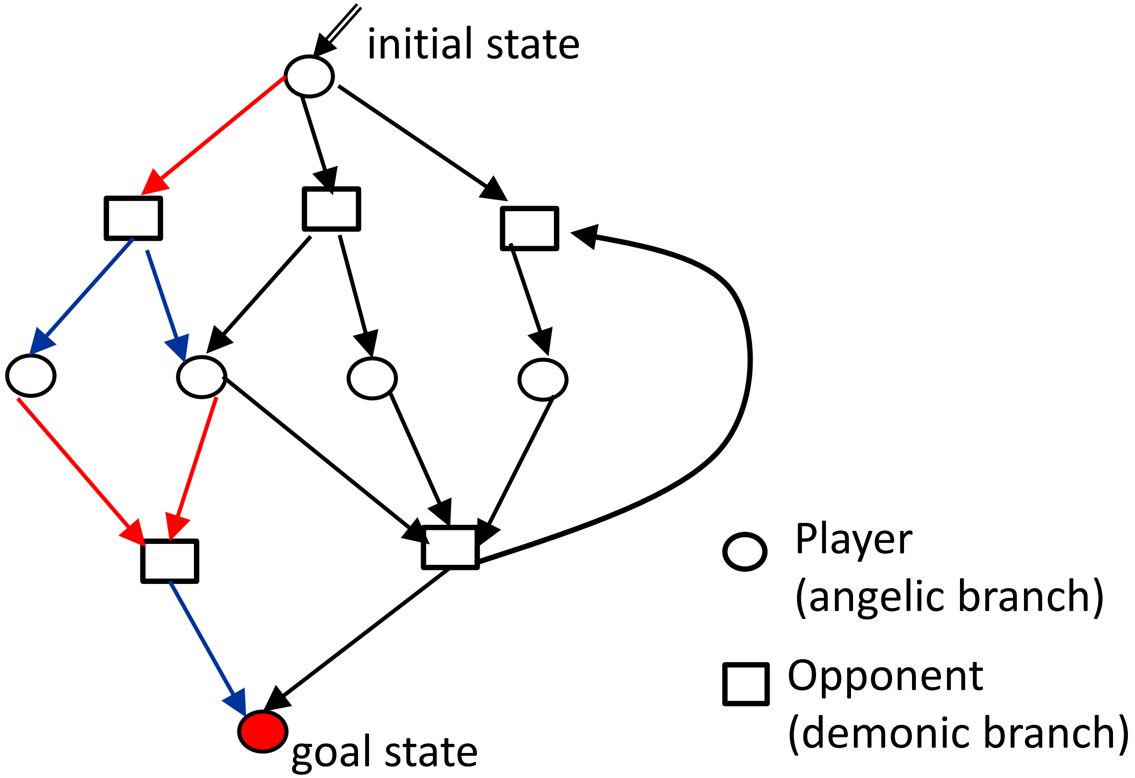
Can the goal state be reached whatever move the opponent (☐) chooses?

May Reachability vs Reachability Games



Does there exists a path to the goal state?

Does a program reach an error state?



Can the goal state be reached whatever move the opponent (☐) chooses?

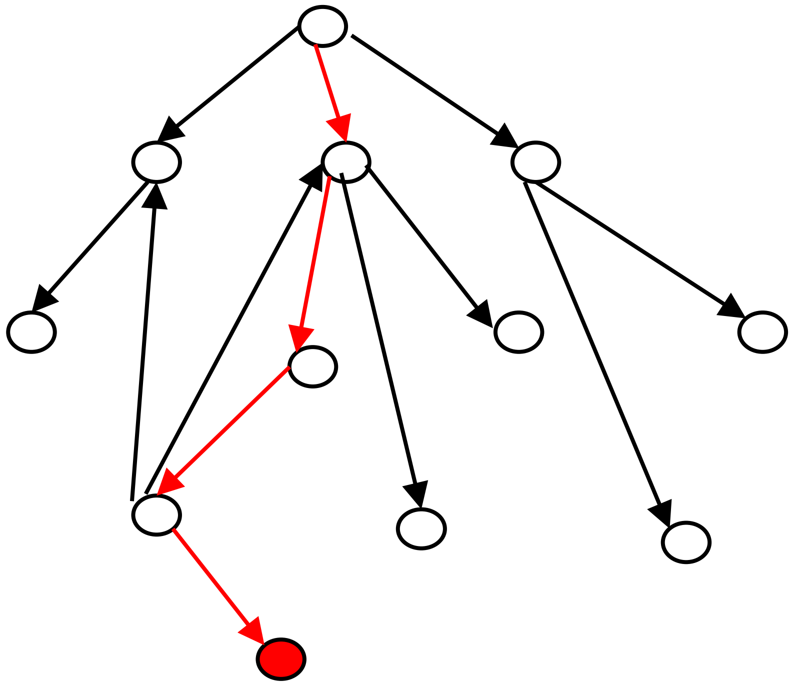
May a program reach an error state in the presence of angelic/demonic non-determinism?

Does a program always terminate?

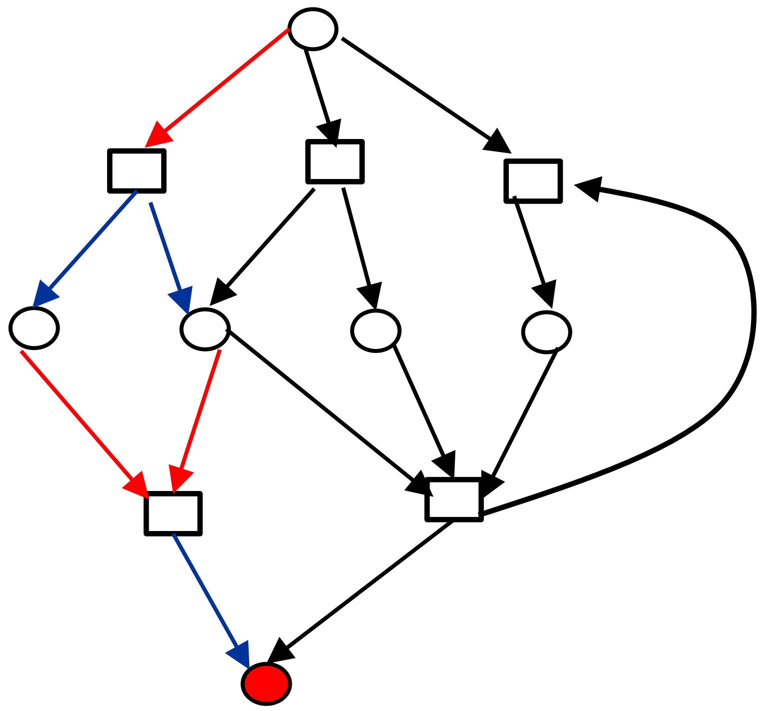
Our Result

For reachability games generated by higher-order call-by-name functional programs,
order-(n+1) may-reachability ≈ order-n reachability games

order-0: functions may take only integer arguments
order-(n+1): functions may take order-n functions



Does there exists a path to the goal state?



Can the goal state be reached whatever move the opponent (□) chooses?

Outline

- ♦ μHFL(Z) and higher-order reachability games
- ♦ From order-n reachability games to order-(n+1) may-reachability
- ♦ From order-(n+1) may-reachability to order-n reachability games
- ♦ Applications
- ♦ Related work and conclusion

μHFL(Z): higher-order logic with integers and least fixpoints

(HFL [Viswanathan&Viswanathan 04] – (ν, <a>, [a]) + integers)

φ ::= true | $\varphi_1 \wedge \varphi_2$ | $\varphi_1 \vee \varphi_2$ | X | $\mu X^{\kappa}.\varphi$ | $\lambda X^{\tau}.\,\varphi$ | $\varphi_1\,\varphi_2$
| φ e | $e_1 \leq e_2$

The least X s.t. X = φ

e ::= n | X | $e_1 + e_2$ | $e_1 \times e_2$

κ ::= o | $\tau \to \kappa$ τ ::= κ | int

order(o) = 0 order(int)= -1 order($\tau \to \kappa$) = max(1+order(τ), order(κ))
e.g. order(int$\to$ int$\to$ o) = 0, order((int $\to$ o) $\to$ o) = 1
order(φ) := the largest order(κ) such that $\mu X^{\kappa}.\phi$ occurs in φ

Example:

$(\mu Y^{int\to o}.\lambda x.\ P(x) \vee Y(x+1))0$

Y 0 where:
Y x $=_{\mu}$ P(x) $\vee$ Y(x+1)

$\equiv$ $(\lambda x.\ P(x) \vee (\mu Y.\lambda x.\ \ldots)(x+1))0$
$\equiv$ $P(0) \vee (\mu Y.\lambda x.\ P(x) \vee Y(x+1))\ 1$
$\equiv$ $P(0) \vee P(1) \vee \ldots$
$\equiv$ $\exists x \geq 0.\ P(x)$

Reachability games as μHFL(Z) formulas

```
let rec sum n k =
 if n≤0 then k 0
 else sum (n-1) λr.k(r+n)
in sum m (λr.assert(m≤ r))
```

May an assertion failure occur?

$$\begin{aligned}&\mathrm{Sum}\ m\ (\lambda r.\ m>r)\\ &\text{where}\\ &\ \mathrm{Sum}\ n\ k =_{\mu}\ (n\le 0 \wedge k\ 0) \vee\\ &\qquad\qquad\quad (n>0 \wedge \mathrm{Sum}\ (n-1)\ \lambda r.k(r+n))\end{aligned}$$

Is the formula valid? (Answer: No)

```
let rec f () =
 if flip() then
    if input() then () else f()
else f()
in f()
```

demonic branch

angelic branch

Does the program always terminate if an appropriate input is given from the environment?

$$\begin{aligned}&F\\ &\text{where}\\ &F =_{\mu} (\text{true} \vee F\ ) \wedge F\end{aligned}$$

Is the formula valid? (Answer: No)

Disjunctive μHFL(Z)

φ ::= true | $e_1 \leq e_2 \wedge \varphi$ | $\varphi_1 \vee \varphi_2$ | X | $\mu X^{\kappa}.\varphi$ | $\lambda X^{\tau}.\varphi$ | $\varphi_1\, \varphi_2$
| $\varphi\, e$ | $e_1 \leq e_2$

e ::= n | X | $e_1 + e_2$ | $e_1 \times e_2$

κ ::= o | $\tau \to \kappa$ τ ::= κ | int

Disjunctive

Sum m (λr. m>r)
where
Sum n k $=_\mu$ (n≤0 $\wedge$ k 0) $\vee$
(n>0 $\wedge$ Sum (n-1) λr.k(r+n))

Non-disjunctive

F
where
F $=_\mu$ (true $\vee$ F) $\wedge$ F

Main Result

There exist size- and semantics-preserving translations between
order-n closed μHFL(Z) formulas (i.e., order-n reachability games)
and
order-(n+1) closed disjunctive μHFL(Z) formulas (i.e., order-(n+1) may-reachability).

e.g.

order-0

$$\exists y.\ (\mu S.\ \lambda n.\lambda x.(n\leq 0 \wedge m=0) \vee (n>0 \wedge \exists r.S\ (n-1)\ r \wedge x=r+n))\ m\ y \wedge m>y$$

order-1 disjunctive

$$(\mu S.\ \lambda n.\lambda k.(n\leq 0 \wedge k\ 0) \vee (n>0 \wedge S\ (n-1)\ \lambda r.k(r+n))\ m\ (\lambda r.\ m>r)$$

$$\exists y.\ (\mu S.\ \lambda n.\lambda x.\lambda b.\ (n\leq 0 \wedge m=0) \vee (n>0 \wedge \exists r.S\ (n-1)\ r\ (x=r+n \wedge b))\ m\ y\ (m>y)$$

Outline

- μHFL(Z) and higher-order reachability games
- From order-n reachability games to order-(n+1) may-reachability
- From order-(n+1) may-reachability to order-n reachability games
- Applications
- Related work and conclusion

From order-n reachability games to order-(n+1) may-reachability

- Idea: translate a truth value b to $\lambda x.b \wedge x$

$[true] = \lambda x.x \quad [false] = \lambda x.false$

$[\varphi_1 \wedge \varphi_2] = \lambda x.[\varphi_1]([\varphi_2]x) \qquad [\varphi_1 \vee \varphi_2] = \lambda x.[\varphi_1]x \vee [\varphi_2]x$

$[X] = X \qquad [\mu X^{\kappa}.\varphi] = \mu X^{[\kappa]}.[\varphi] \qquad [\lambda X^{\tau}.\varphi] = \lambda X^{[\tau]}.[\varphi] \qquad \ldots$

$[e_1 \leq e_2] = \lambda x.\ e_1 \leq e_2 \wedge x$

$[Int] = Int \qquad [o] = o \to o \qquad [\tau \to \kappa] = [\tau] \to [\kappa]$

μHFL(Z):

$\varphi ::= true \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid X \mid \mu X^{\kappa}.\varphi \mid \lambda X^{\tau}.\varphi \mid \varphi_1\, \varphi_2 \mid \varphi\, e \mid e_1 \leq e_2$

Disjunctive μHFL(Z):

$\varphi ::= true \mid e_1 \leq e_2 \wedge \varphi \mid \varphi_1 \vee \varphi_2 \mid X \mid \mu X^{\kappa}.\varphi \mid \lambda X^{\tau}.\varphi \mid \varphi_1\, \varphi_2 \mid \varphi\, e \mid e_1 \leq e_2$

Outline

- μHFL(Z) and higher-order reachability games
- From order-n reachability games to order-(n+1) may-reachability
- From order-(n+1) may-reachability to order-n reachability games
  - From order-1 to order-0
  - General case
- Applications
- Related work and conclusion

From Order-1 May Rechability to Order-0 Rechability Game

- **Consider:**

$\varphi\ m\ p_1 \ldots p_k$

where: φ: int $\rightarrow$ (int $\rightarrow$ o)^k $\rightarrow$ o, m:int, p_i: int $\rightarrow$ o.

$\varphi\ m\ p_1 \ldots p_k \rightarrow^*$ true if

(1) $\varphi\ m\ (\lambda x.\text{false}) \ldots (\lambda x.\text{false}) \rightarrow^*$ true; or

(2) $\varphi\ m\ p_1 \ldots p_k \rightarrow^*\ p_i\ n \rightarrow^*$ true for some i, n.

Let $\varphi_0\ m \Leftrightarrow \varphi\ m\ (\lambda x.\text{false}) \ldots (\lambda x.\text{false})$

$\varphi_i\ m\ n \Leftrightarrow \varphi\ m\ p_1 \ldots p_k \rightarrow^*\ p_i\ n.$

Then $\varphi\ m\ p_1 \ldots p_k$ is equivalent to the order-0 formula:

$\varphi_0\ m \vee \exists n.\ (\varphi_1\ m\ n \wedge p_1\ n) \vee \ldots \vee \exists n.\ (\varphi_k\ m\ n \wedge p_k\ n)$

From Order-1 May Rechability to Order-0 Rechability Game

- **Example:** $\mathbf{sum}\ n\ (\lambda r.\ r<n)$ where:

  $$\mathrm{sum}\ x\ k =_\mu x<0 \vee (x=0 \wedge k\ 1) \vee (x>0 \wedge \mathrm{sum}\ (x-1)\ (\lambda r.k(r\times n)))$$

Equivalent order-0 formula:

$$\mathrm{sum}_0\ n \vee \exists r.(\mathrm{sum}_1\ x\ r \wedge r<n)$$

where:

condition for sum x k →* true (without using k)

$$\mathrm{sum}_0\ x =_\mu x<0 \vee (x>0 \wedge \mathrm{sum}_0\ (x-1))$$

$$\mathrm{sum}_1\ x\ y =_\mu (x=0 \wedge y=1) \vee (x>0 \wedge \exists r.\mathrm{sum}_1\ (x-1)\ r \wedge\ y= r\times n)$$

condition for sum x k →* k y

Transformation Relation (for the General Case)

$$\blacklozenge\ \Gamma; \underbrace{x_1, \ldots, x_k}_{\text{order-0 free variables}} \vdash \varphi : \tau \Rightarrow (\underbrace{\varphi_*, \varphi_0}_{\substack{\text{condition for}\\ \text{a predicate embedded}\\ \text{in a higher-order}\\ \text{argument to be reached}\\ \text{(e.g. condition for G (H p) q} \to^* \text{p n)}}}, \underbrace{\varphi_1, \ldots, \varphi_k}_{\substack{\text{condition for}\\ x_i \text{ to be reached}}}, \underbrace{\varphi_{k+1}, \ldots, \varphi_{k+m}}_{\substack{\text{condition for}\\ \text{j-th order-0 argument}\\ \text{to be reached (j=1,...,m)}}})$$

$$\frac{\begin{array}{c}\mathtt{decomp}(\tau) = (\epsilon, m-1, p) \\ \mathcal{K}; \widetilde{x}_{1,\ldots,k} \vdash_{\Theta} \varphi : (\mathtt{Int}^M \to \star) \to \tau \rightsquigarrow (\varphi_*, \varphi_0, \ldots, \varphi_{k+m}) \\ \mathcal{K}; \widetilde{x}_{1,\ldots,k} \vdash_{\Theta} \psi : \mathtt{Int}^M \to \star \rightsquigarrow (\psi_*, \psi_0, \ldots, \psi_k) \\ \xi_j = \lambda \widetilde{z}_{1,\ldots,p}.\lambda \widetilde{w}_{1,\ldots,M}.\varphi_j\, \widetilde{z}\, \widetilde{w} \vee \exists \widetilde{u}_{1,\ldots,M}.(\varphi_{k+1}\, \widetilde{z}\, \widetilde{u}_{1,\ldots,M} \wedge \psi_j\, \widetilde{u}_{1,\ldots,M}\, \widetilde{w}_{1,\ldots,M})\end{array}}{\mathcal{K}; \widetilde{x}_{1,\ldots,k} \vdash_{\Theta} \varphi\,\psi : \tau \rightsquigarrow (\xi_*, \xi_0, \ldots, \xi_k, \varphi_{k+2}, \ldots, \varphi_{k+m})}$$

(TR-APPG)

Outline

- ♦ μHFL(Z) and higher-order reachability games
- ♦ From order-n reachability games to order-(n+1) may-reachability
- ♦ From order-(n+1) may-reachability to order-n reachability games
- ♦ Applications
- ♦ Related work and conclusion

Applications

- **From order-n reachability games to order-(n+1) may reachability**

  Improve the efficiency of νHFL(Z) Solver ReTHFL [Katsura+, APLAS 2020]

Input	ReTHFL	ReTHFL+i.s.	ReTHFL+ tr.
fixpoint_nonterm	11.579	0.054	0.102
unfoldr_nonterm	timeout	unknown	4.22
indirect_e	16.832	0.035	0.066
alternate	unknown	unknown	unknown
fib_CPS_nonterm	timeout	0.047	0.075
foldr_nonterm	8.447	unknown	0.122
passing_cond	116.423	unknown	0.444
indirectHO_e	11.582	0.044	0.073
inf_closure	timeout	20.171	9.080
loopHO	timeout	0.026	0.121

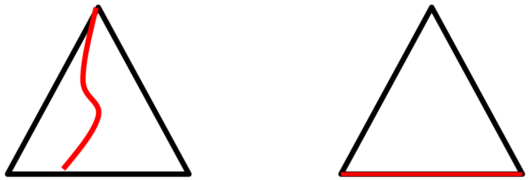
After the translation from reachability games to may-reachability

- **From order-(n+1) may-reachability to reachability games**

  Helps us to avoid a limitation caused by the incompleteness of ReTHFL.

Related Work

- **Order-(n+1) Word Languages = Order-n Frontier Languages**
  (special case: context-free languages = frontier languages of regular tree grammars)
  - for safe grammars [Damm 1982]
  - for unsafe grammars [Asada&K, FSCD20]



- **Order-n fixpoint characterization of order-(n+1) probabilistic higher-order recursive programs** [K+, LICS19]
- **n-EXPTIME completeness of disjunctive properties of order-(n+1) HORS** [K&Ong, ICALP09]

Conclusion

- We have shown:

  Order-(n+1) may reachability $\approx$ Order-n reachability games

  through fixpoint logic μHFL(Z)

- Applications to νHFL(Z) solvers
  (higher-order extension of CHC solvers,
  which serve as common backend for higher-order program verification)