関数型言語の到達可能性を検証する篩型システム

佐藤 聡太, 松下 祐介, 末永 幸平, 五十嵐 淳　京都大学大学院情報学研究科

背景

- どんな選択でも (demonic choice)
- エラー値に行かない (partial)

	手続き型言語	関数型言語	
安全性	Hoare Logic [Hoare '69]	篩型システム F* [Swamy+ '16] など	Relatively Complete Refinement type system [Unno+ '17]
非安全性	Incorrectness Logic [O'Hearn '19] 全射性を保証 Sufficient Incorrectness Logic(SIL) [Ascari+ '23] 到達可能性を保証	**本研究** **篩型システムで到達可能性を保証**	

検査の成功がバグの存在を保証

- うまく選択すると (angelic choice)
- 無限ループせず値に行き着く (total)

本研究

対象言語 『名前呼びλ計算』＋『非決定的分岐 $\oplus$』＋『再帰』

例

$(\lambda x\,.\,x + x)\ (1 \oplus 2) \rightsquigarrow (1 \oplus 2) + (1 \oplus 2) \rightsquigarrow 3$

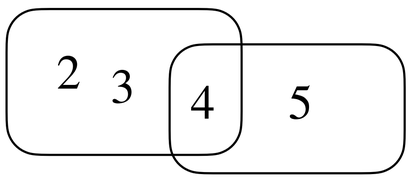
$\text{let rec}\ f\ x\ =\ x \oplus f(x+1)\ \text{in}\ f\ 0 \rightsquigarrow f\ 100 \rightsquigarrow 100$

型

$$\tau ::= \{v : \text{int} \mid \phi\} \quad | \quad \tau_1 \wedge \tau_2 \quad | \quad (x : \tau_1) \to \tau_2$$

依存関数型

$(\lambda x\,.\,x + x)\ (1 \oplus 2)$



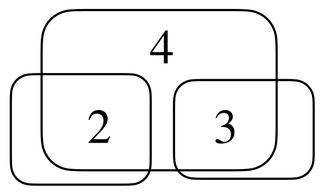
$\{v : \text{int} \mid 4 \le v \le 5\}$

$\vdash (\lambda x\,.\,x + x)\ (1 \oplus 2) : \{v : \text{int} \mid 4 \le v \le 5\}$

述語 ϕ を満たす値に到達可能な項につく篩型

τ_1 と τ_2 両方を満たす項につく交差型

$(\lambda x\,.\,x + x)\ (1 \oplus 2)$



$\{v : \text{int} \mid v = 2\}\ \{v : \text{int} \mid v = 3\}$

$\vdash (\lambda x\,.\,x + x)\ (1 \oplus 2) : \{v : \text{int} \mid v = 2\} \wedge \{v : \text{int} \mid v = 3\}$

型付け規則

うまく選択すると τ 型がつく

$$\frac{\Gamma \vdash e_i : \tau}{\Gamma \vdash e_1 \oplus e_2 : \tau}$$

$$\frac{\Gamma \vdash e' : \tau \quad \Gamma \vDash e \rightsquigarrow e'}{\Gamma \vdash e : \tau}$$

Loop Unrolling 再帰関数の展開に使う

$$\frac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x\,.\,e : (x : \tau_1) \to \tau_2}$$

安全性の型システムと同じ規則

$$\frac{\Gamma \vdash e_1 : (x : \tau_1) \to \tau_2 \qquad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1\ e_2 : \tau_2[e_2/x]}$$

関数型の引数や型環境 $(x : \tau)$ の意味は『任意の τ 型の項 e で x を置換すると』

型判断例

xは1でも2でもよい

$x : \{v : \text{int} \mid v = 1 \vee v = 2\} \vdash x + (1 \oplus 2) : \{v : \text{int} \mid v = 3\}$

xは1と2 両方に到達可能

$x : \{v : \text{int} \mid v = 1\} \wedge \{v : \text{int} \mid v = 2\} \vdash x + x : \{v : \text{int} \mid v = 3\}$

3に到達可能

$\vdash \text{let rec}\ f\ x\ =\ x \oplus f(x+1)\ \text{in}\ f : (x : \text{int}) \to \bigwedge_{i \ge 0} \{v : \text{int} \mid v = x + i\}$

x 以上の任意の値に到達可能

型システムの正当性

予想(鋭意証明中)

$$\Gamma \vdash e : \tau \implies \forall s \in [\![\Gamma]\!]\,.\,[\![s(\tau)]\!](\{v \mid s(e) \rightsquigarrow v\})$$

系として $\Gamma \vdash e : \{v : \text{int} \mid \phi\} \implies \forall s \in [\![\Gamma]\!]\,.\,\{w \mid s(e) \rightsquigarrow w\} \cap \{v \mid s(\phi) \rightsquigarrow \top\} \neq \emptyset$

c.f. SIL の3つ組 $\langle\!\langle P \rangle\!\rangle\ C\ \langle\!\langle Q \rangle\!\rangle$ は $\forall s \in P\,.\,[\![C]\!](s) \cap Q \neq \emptyset$

想定される応用例

$\vdash^{\text{安全}} e : \{v : \text{int} \mid \phi\}$ の型検査に失敗したら

$\vdash^{\text{到達可能}} e : \{v : \text{int} \mid \neg\phi\}$ の型検査でバグを発見

目下の課題

自動型検査にむけてソルバーをどう用いるか

例えば $\Gamma \vdash n : \{v : \text{int} \mid \phi\}$ は

どの理論の論理式に帰着できる？