関数型言語のためのHyper Hoare Typeにむけて

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　手続き型言語の(非)安全性の論理

Hoare Logic(HL) [Hoare '69] 安全性を保証

Incorrectness Logic (IL) [O'Hearn '19]

全射性を保証, 偽陽性のないバグ発見

例: $[\mathrm{isSorted}(a)]\ b := \mathrm{shuffle}(a)\ [\mathrm{sort}(b) = a]$

shuffle関数は全ての置換をカバー

Sufficient Incorrectness Logic(SIL) [Ascari+ '23]

到達可能性を保証, 偽陽性のないバグ発見

関数型言語上で複数論理を統合

- Covering All the Bases [Zhou+ '23]
  関数型言語でHLに加え全射的(IL的)篩型が扱える
  全射的篩型は事後条件/basetypeのみ
- Relatively Complete Refinement Type System [Unno+ '17]
  関数型言語で HL / SIL を統一的に扱える

手続き型言語上でHL/IL/SILを統合した Hyper Hoare Logic(HHL) [Dardinier+ '23]

プログラムの状態の集合の集合を扱う　$\{\mathbb{P}\}\ C\ \{\mathbb{Q}\} \iff \forall S \in \mathbb{P}.\ C(S) \in \mathbb{Q}$

各変数から値への割り当て

『状態の集合』の集合

状態の集合

HHLの判断例　プログラム C を $x := x + 1$として

✅ $\{\{x \mapsto 1, x \mapsto 2\}, \{x \mapsto 4\}\}\ C\ \{\{x \mapsto 2, x \mapsto 3\}, \{x \mapsto 5\}, \{x \mapsto 7, x \mapsto 8\}\}$

✅ $\{\{\{1 \le x \le 2\}, \{x = 4\}\}\}\ C\ \{\{\{2 \le x \le 3\}, \{x = 5\}, \{7 \le x \le 8\}\}\}$

❌ $\{\{\{x = 1 \vee x = 2\}\}\}\ C\ \{\{\{x = 2\}, \{x = 3\}\}\}$　✅ $\{\{\{x = v\} \mid v\ \%\ 2 = 0\}\}\ C\ \{\{\{x = v\} \mid v\ \%\ 2 = 1\}\}$

HHLで HL / IL / SIL を表現

HL の $\{P\}\ C\ \{Q\}$ をHHLで　$\cdots$　$\{\{S \mid S \subseteq P\}\}\ C\ \{\{S \mid S \subseteq Q\}\}$

IL の $[P]\ C\ [Q]$ をHHLで　$\cdots$　$\{\{S \mid S \supseteq P\}\}\ C\ \{\{S \mid S \supseteq Q\}\}$

SIL の $\langle\!\langle P \rangle\!\rangle\ C\ \langle\!\langle Q \rangle\!\rangle$をHHLで　$\cdots$　$\{\{S \mid S \cap P \neq \varnothing\}\}\ C\ \{\{S \mid S \cap Q \neq \varnothing\}\}$

本研究の目標：関数型言語上でHL/IL/SILを統合したい

HyperType $\mathbb{t}$ で値の集合の集合を表現した型システム

値の集合、すなわち型

$$f : \mathbb{t}_1 \to \mathbb{t}_2 \iff \forall S \in [\![\mathbb{t}_1]\!].\ f(S) \in [\![\mathbb{t}_2]\!]$$

困難：ILに基づく関数型に対する導出規則が不明

例：関数 $\lambda n.(\lambda i.\ n\text{の}\ i\ \text{bit目})$ が $[0, 2^k)$ から『$(0, \cdots, 0) \sim (1, \cdots, 1)$ の 2^k 種類の関数』への全射である

HyperTypeとしては $\lambda n.(\lambda i.\ n\text{の}\ i\ \text{bit目}) : \{0, \cdots, 2^k - 1\}^{\uparrow} \to \left(\{0, \cdots, k-1\}^{\downarrow} \to \{0, 1\}^{\downarrow}\right)^{\uparrow}$を導出したい

$k = 3$ のとき

0	1	2	3
4	5	6	7

$\to$

$(0,1,2) \mapsto (0,0,0)$
$\vdots$
$(0,1,2) \mapsto (1,1,1)$

型(値の集合) τ に対して

$\tau^{\downarrow} ::= \{S \mid S \subseteq \tau\}$　(HL的近似)

$\tau^{\uparrow} ::= \{S \mid S \supseteq \tau\}$　(IL的近似)

$(\mathbb{t}_1 \to \mathbb{t}_2)^{\downarrow}$ には通常の λ 導入/除去規則が成立

現在想定している型判断

型環境　$\Gamma ::= x_i : \mathbb{t}, \cdots$

型判断　$\Gamma \vdash e : \mathbb{t} \iff \forall \sigma^2 \in [\![\Gamma]\!].\{\sigma(e) \mid \sigma \in \sigma^2\} \in [\![\mathbb{t}]\!]$

$[\![\Gamma]\!]$ は付値の集合の集合

各 $x_i : \mathbb{t}_i$ から $\tau_i \in \mathbb{t}_i$ を任意に選んでつくる
付値の集合 $\sigma^2 = [[x_i : \tau_i, \cdots]] = \{\sigma \mid \forall i.\ \sigma(x_i) \in \tau_i\}$

解決法求む！　???には何がくるべき？

$$\frac{n : [0, 2^k)^{\uparrow}, i : ??? \vdash n\text{の}\ i\ \text{bit目} : ???}{n : [0, 2^k)^{\uparrow} \vdash \lambda i.\ n\text{の}\ i\ \text{bit目} : \left([0, k)^{\downarrow} \to \{0, 1\}^{\downarrow}\right)^{\uparrow}}$$

$n : [0, 2^k)^{\uparrow}, i : [0, k)^{\downarrow}$　は不適 ❌　なぜならnを制限した

$n : \{1, 2, 4, \cdots, 2^{k-1}\}^{\uparrow}, i : [0, k)^{\downarrow}$ は不成立になってほしいが

$[\![\Gamma]\!]\,(n\text{の}\ i\text{bit目})$が同じ冪集合$\{\{0, 1\}\}$に評価されてしまう