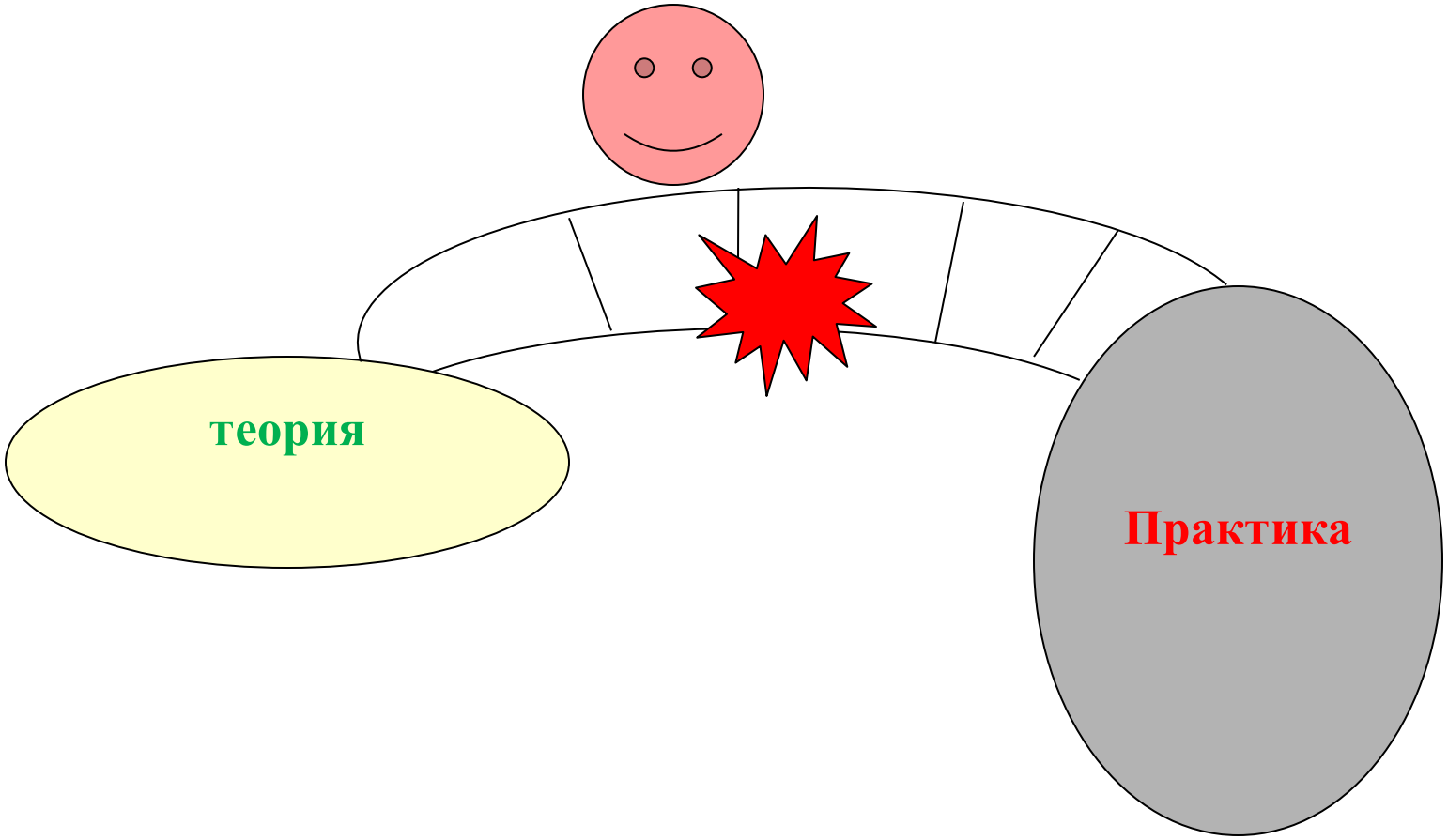
18 Февраля 2010

Инсерционное моделирование и верификация программ

Лекция 1

Исчисление Хоара

Мост между теорией и практикой



A program verifier

- automatically checks that a program conforms to its specification
- serves as an essential tool for research into the science of programming.
- proposed in 1969
- still a Grand Challenge for Computing research

T.Hoare
2006

A Program Verifier

One can dream of routinely using a verifying compiler as an everyday tool. In the context of this idea our work has been extremely modest and must be considered as a small first step. We only hope that, indeed, this has been a first step of a progression which will allow this dream to come to fruition.

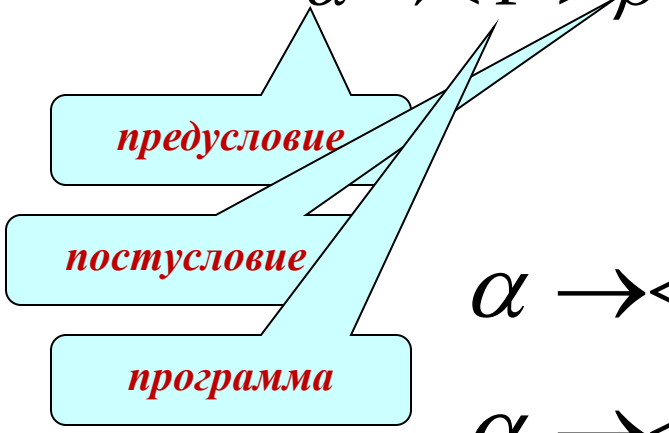
A Program Verifier
Thesis by James C. King
Carnegie Institute of Technology
September 1969

Логика Хора-Флойда

Формулы:

$$\alpha \to [P]\beta$$

$$\alpha \to < P > \beta$$



Частичная корректность программ

(если предусловие и программа останавливается, то постусловие)

$$\{\alpha\}P\{\beta\}$$

Полная корректность программ

(если предусловие, то программа останавливается и постусловие)

$$\alpha \to < P > \beta \Leftrightarrow$$

$$\alpha \to < P > 1 \wedge$$

$$\alpha \to [P]\beta$$

Все это формулы темпоральной динамической логики

Hoare 1969 структурные программы,
Floyd 1967 программы с goto

Структурные программы

Базовые операторы

$$x := y$$

$$(x_1 := y_1, \ldots, x_n := y_n)$$

синтаксис

- **Именующие выражения**
- **Алгебраические выражения (арифметические, булевские, …)**
- **Вызовы программ (функций)**
- **Типы данных, многосортные алгебраические системы**

Основные композиции (синтаксические конструкции)

$$(P;Q), if\,(u,P,Q), while(u,P)$$

Семантика Хоаровских троек

$$[[\alpha \to [P]\beta]] : D^R \to \{0,1\}$$

$$[[\alpha \to [P]\beta]](s) =$$
$$= [[\alpha]](s) \wedge [[P]](s) \neq \perp \to [[\beta]]([[P]](s))$$

$$[[\alpha \to < P > \beta]](s) =$$
$$= [[\alpha]](s) \to [[P]](s) \neq \perp \wedge [[\beta]]([[P]](s))$$

Исчисление Хора

$$\frac{\alpha \to [P]\gamma, \gamma \to [Q]\beta}{\alpha \to [PQ]\beta}$$

$$\frac{\alpha \wedge \gamma \to [P]\beta, \alpha \wedge \bar{\gamma} \to [Q]\beta}{\alpha \to [\mathbf{if}(\gamma, P, Q)]\beta}$$

$$\frac{\alpha \to \delta, \delta \wedge \gamma \to [P]\delta, \delta \wedge \bar{\gamma} \to \beta}{\alpha \to [\mathbf{while}(\gamma, P)]\beta}$$

$$\frac{\alpha \to \beta(t_1, t_2, \ldots)}{\alpha \to [(x_1 := t_1, x_2 := t_2, \ldots)]\beta(x_1, x_2, \ldots)}$$

Интерпретируется на семантической модели императивного структурного программирования

Для доказательства частичной корректности нужно найти инварианты циклов

John Reynolds
Separation Logic
Marktoberdorf

Программы с указателями

Пример

```
s:=0;
for j:=1 .. n do(
    s:=s+a(j)
);
```

```
s:=0;
j:=1;
while (j<=n,
    s:=s+a(j);
    j:=j+1
);
```

$$\frac{\alpha \to [P]\gamma, \gamma \to [Q]\beta}{\alpha \to [PQ]\beta}$$

$$\frac{\alpha \wedge \gamma \to [P]\beta, \alpha \wedge \bar{\gamma} \to [Q]\beta}{\alpha \to [\mathbf{if}(\gamma, P, Q)]\beta}$$

$$\frac{\alpha \to \delta, \delta \wedge \bar{\gamma} \to [P]\delta, \delta \wedge \gamma \to \beta}{\alpha \to [\mathbf{while}(\gamma, P)]\beta}$$

$$\frac{\alpha \to \beta(t_1, t_2, \ldots)}{\alpha \to [(x_1 := t_1, x_2 := t_2, \ldots)]\beta(x_1, x_2, \ldots)}$$

Спецификация:

$$1 \to < P > \beta$$

$$\beta = (s = \sum_{k=1}^{n} a[k])$$

Инвариант цикла

$$\delta = (s = \sum_{k=1}^{j-1} a[k])$$

$$1 \to [P]\beta \Leftrightarrow$$
$$[s := 0; P']\beta$$
$$[s := 0](s = 0), (s = 0) \to [j := 1; P'']\beta$$
$$s = 0 \to [j := 1](s = 0 \wedge j = 1),$$
$$(s = 0 \wedge j = 1) \to \text{while } (j <= n, Q)\beta$$

$$\alpha = (s = 0 \wedge j = 1)$$

$$\alpha \to \delta, \delta \wedge j <= n \to [Q]\delta, \delta \wedge j > n \to \beta$$

Не получается

```
s:=0;
j:=1;
while (j<=n,
    s:=s+a(j);
    j:=j+1
);
```

$$1 \rightarrow < P > s = \sum_{k=1}^{n} a[k]$$

Настоящий инвариант

$$\delta = (s = \sum_{k=1}^{j-1} a[k]) \wedge (j <= n+1)$$

$$\alpha \rightarrow \delta, \delta \wedge j <= n \rightarrow [Q]\delta, \delta \wedge j > n \rightarrow \beta$$

Обоснования и применения

Правила логики Хоара <=> высказывания динамической логики

$$\frac{\alpha \to [P]\gamma, \gamma \to [Q]\beta}{\alpha \to [PQ]\beta} \qquad (\alpha \to [P]\gamma) \wedge (\gamma \to [Q]\beta) \to (\alpha \to [PQ])\beta$$

Пропозициональная динамическая логика

Применяя правила в обратном порядке, Хоаровскую тройку можно редуцировать к формуле логики первого порядка!

Полнота доказана для целочисленной арифметики
(с использованием Геделевской нумерации)

```
s:=0;
j:=1;
while (j<=n,
    s:=s+a(j);
    j:=j+1
);
```

$$1 \rightarrow < P > s = \sum_{k=1}^{n} a[k]$$

$$\delta = (s = \sum_{k=1}^{j-1} a[k]) \wedge (j <= n+1)$$

$$\alpha \rightarrow \delta$$

$$s = 0 \wedge j = 1 \rightarrow (s = \sum_{k=1}^{j-1} a[k]) \wedge (j <= n+1)$$

$$\delta \wedge j <= n \rightarrow [Q]\delta$$

$$(s = \sum_{k=1}^{j-1} a[k]) \wedge (j <= n+1) \wedge (j <= n) \rightarrow [$$

$$s := s + a[j];$$

$$j := j + 1$$

$$](s = \sum_{k=1}^{j-1} a[k]) \wedge (j <= n+1)$$

$$\delta \wedge j > n \rightarrow \beta$$

$$(s = \sum_{k=1}^{j-1} a[k]) \wedge (j <= n+1) \wedge j > n \rightarrow (s = \sum_{k=1}^{n} a[k])$$

Задача

Построить программу поиска минимального и максимального элементов одномерного массива

Специфицировать

Доказать правильность