

Логика программ

H1; H2; ... , Hn
C

А.Хоар выбрал простейший язык программирования с целыми:

x := E
S1; S2
if B then S1 else S2 fi
while B do S od

- оператор присваивания
- последовательность операторов
- условный оператор
- оператор цикла

Формулы аксиоматической теории – тройки {P} S {Q},

где: S – программа,
P и Q – предикаты.

- Нелогические аксиомы (дополнение к аксиомам исчисления предикатов):

- аксиома присваивания $\{P_{x \leftarrow E}\} x := E \{P\}$ (или $\{P(x/E)\} x := E \{P(x)\}$),
- аксиомы арифметики для целых,
- аксиомы прикладной области (например, определение НОД).

Пример "нелогических" аксиом:

A1: $(\forall x) \text{НОД}(x, x) = x;$
A2: $(\forall x, y) [(x > y) \Rightarrow \text{НОД}(x, y) = \text{НОД}(x-y, y)].$

20

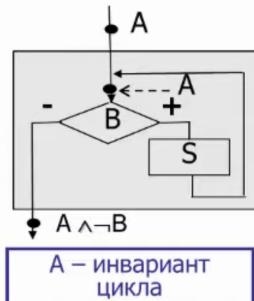
Аксиомы и правила вывода программной логики Хоара

1. Аксиомы исчисления предикатов
2. Аксиомы арифметики
3. Аксиома присваивания: $\{P(x/E)\} x := E \{P(x)\}$

Язык:

x := E
S1; S2
if B then S1 else S2 fi
while B do S od

Оператор цикла



Правила вывода:

Правило следствия: $P \Rightarrow P_1; \{P_1\} S \{Q_1\}; Q_1 \Rightarrow Q \quad \boxed{\{P\} S \{Q\}}$

Композиция: $\{P\} S_1 \{P_1\}; \{P_1\} S_2 \{Q\} \quad \boxed{\{P\} S_1; S_2 \{Q\}}$

Цикл: $A - \text{инвариант цикла} \quad \boxed{\{A \& B\} S \{A\}} \quad \{A\} \text{while } B \text{ do } S \text{ od } \{A \wedge \neg B\}$

21

Формальное доказательство на основе аксиоматической теории программ

- Пример вывода в аксиоматической теории

Prog::

begin

S₁: X := Y - X;
S₂: Y := Y - X;
S₃: X := Y + X;
end

Prog переставляет X и Y?

Хотим доказать:

$\{I\} [S_1; S_2; S_3] \{R\}$

где

I = {X=a \wedge Y=b}

R = {X=b \wedge Y=a}

Prog::

begin

I = {X=a \wedge Y=b}
S₁: X := Y - X;
F1 = {Y=b \wedge Y-X=a}
S₂: Y := Y - X;
F2 = {Y+X=b \wedge Y=a}
S₃: X := Y + X;
R = {X=b \wedge Y=a}
end

Хотим доказать:

$\{I\} [S_1; S_2; S_3] \{R\}$

где

I = {X=a \wedge Y=b}

R = {X=b \wedge Y=a}

Аксиома присваивания:

$\{P(x/E)\} x := E \{P(x)\}$

X/E – подстановка E вместо всех
вхождений x в утверждении P

$\{P\} S_1 \{Q_1\}, \{Q_1\} S_2 \{Q\}$

$\{P\} S_1; S_2 \{Q\}$

Доказательство:

1. $\{I\} S_1 \{F1\}$ – аксиома ($I = \{X=a \wedge Y=b\}$, $S_1 = [X := Y - X]$, $F1 = \{Y=b \wedge Y-X=a\}$).
2. $\{F1\} S_2 \{F2\}$ – аксиома ($F1 = \{Y=b \wedge Y-X=a\}$, $S_2 = [Y := Y - X]$, $F2 = \{Y+X=b \wedge Y=a\}$).
3. $\{I\} S_1; S_2 \{F2\}$ – правило вывода для последовательности операторов из 1, 2.
4. $\{F2\} S_3 \{R\}$ – аксиома ($F2 = \{Y+X=b \wedge Y=a\}$, $S_3 = [X := Y + X]$, $R = \{X=b \wedge Y=a\}$).
5. $\{I\} S_1; S_2; S_3 \{R\}$ – правило вывода для последовательности операторов из 3, 4.

25