ВЕРИФИКАЦИЯ ПРОГРАММ

ДВС

Лектор - С.А. Ивановский

Лекция 6

0. Задача о большинстве
1. Об индивидуальных заданиях
2. О возможностях метода Хоара (Соотношение между хоаровскими инвариантами цикла и индуктивными утверждениями Флойда)

Об индивидуальных заданиях

...

О возможностях метода Хоара

Абрамов С.А. Элементы анализа программ. Частичные функции на множестве состояний. – М.: Наука. Гл. ред. физ.-мат. лит., 1986.

Рассматриваются примеры циклических программ, некоторые свойства которых являются «труднодоказуемыми» с позиций метода Хоора. Большинство этих программ укладывается в схему

$$\textbf{while } \zeta(a) \textbf{ do } b := g(b);\ a := f(a) \textbf{ od},$$

где f — монотонно убывающая, а g — монотонно возрастающая, в смысле некоторого отношения порядка, функции. Эта схема подсказана доказательством теоремы Ламе: там последовательность значений переменной a — это последовательность остатков, а последовательность значений переменной b — последовательность чисел Фибоначчи, начиная со второго.

Преамбула

Из Лекции 2.2.(сл.31-34)

Аннотирование цикла и понимание аннотаций

Цикл рекомендуется оформлять следующим образом:

```
//@ Pred Q: предусловие
//@ inv P: инвариант
//@ bound t: ограничивающая функция
//@         (вариант цикла)
while (B) {
   S
}
//@ Post R: постусловие
```

Здесь Q – предусловие, а R – постусловие цикла, и выполняются соотношения $Q \rightarrow P$, $!B \ \& \ P \rightarrow R$.

Из Лекции 2.2.(сл.31-34)

Список условий для проверки (аннотированного) цикла

1) показать, что P – истинно до выполнения цикла, т. е. $Q \rightarrow P$

2) показать, что тело цикла имеет свойство $\{B \,\&\, P\}\ S\ \{P\}$, т. е. – инвариант;

3) показать, что $!B \,\&\, P \rightarrow R$;

4) показать, что $P \,\&\, B \rightarrow (t > 0)$;

5) показать, что

$$\{P \,\&\, B\}\ \ t1 = t;\ \ \ S;\ \{0 \le t < t1\},$$

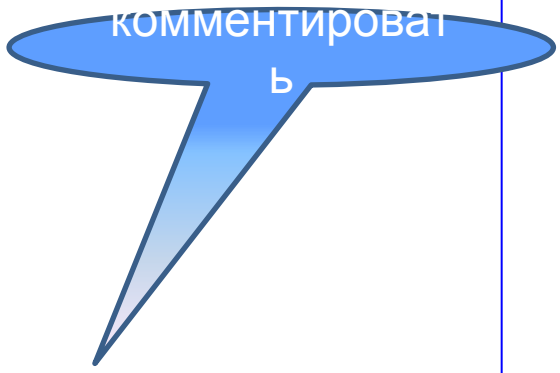
т. е. t уменьшается на каждом шаге цикла.

инвариант

ограничивающая функция

Из Лекции 2.2.(сл.31-34)

```
Пример:  int i, n;
         //@ n > 0
         i = 1;
         //@ inv P: (0 < i ≤ n)
         //@ bound t: n - i
         while (2*i <= n) i = 2*i ;
         //@ post: ( 0<i ≤ n < 2*i)
```



Проверим 5 указанных ранее условий.

1) Очевидно $\{(n > 0)\ \&\ (i = 1)\} \rightarrow \text{inv}$.

2) Проверим свойство $\{B\ \&\ \text{inv}\}\ i = 2*i\ ;\ \{\text{inv}\}$.

Очевидно $(B\ \&\ \text{inv}) \equiv \{(2*i \le n)\ \&\ (0 < i \le n)\}$.

Для оператора присваивания имеем:

$\{\text{предусловие}\}\ i = 2*i\ ;\ \{0<i \le n\}$.

предусловие $\equiv (0 < 2*i \le n)$ следует из $(B\ \&\ \text{inv})$

3) Утверждение $!B$ есть $(2*i > n)$. Отсюда очевидно, что $(!B \ \& \ \text{inv}) \equiv \text{post}$

$(2*i > n) \ \& \ (0 < i \le n) \equiv (\ 0 < i \le n < 2*i)$

4) $t = n - i > 0$ при $0 < 2*i \le n$.

5) Проверим свойство

$\{0 < 2*i \le n\}\ t1 = n - i;\ \ i = 2*i;\ \ \{0 \le t < t1\}$.

Действительно,

$\{\ \mathbf{wp}\ \}\ t1 = n - i;\ \ i = 2*i;\ \{0 \le n - i < t1\}$

$\mathbf{wp} \equiv (\ 0 \le n - 2*i < n - i\ )$

$(0 < 2*i \le n) \rightarrow \mathbf{wp}$

Из Лекции 2.2.(сл.31-34)

Проверка завершена

О переменных-призраках

```
int i, n;
//@ n > 0
i = 1;  // int j = 0;
//@ inv P: (0 < i ≤ n)
//@ bound t: n - i
while (2*i <= n) i = 2*i ; // j = j + 1;
//@ post: ( 0<i ≤ n < 2*i) & (i=2^j) & (j>=0)
```

Альтернатива: см. след. слайд

Альтернатива – использование кванторов

```
int i, n;
//@ n > 0
i = 1;
//@ inv P: (0 < i ≤ n)
//@ bound t: n - i
while (2*i <= n) i = 2*i ;
//@ post: ( 0<i ≤ n < 2*i) & (∃j>=0:i=2^j)
```

! Комментарии об усилении постусловия и т.п.

Соотношение между хоаровскими инвариантами цикла и индуктивными утверждениями Флойда

См. файлы .docx