26 Февраля 2009

Инсерционное моделирование 1

Лекция 2

Метод Флойда

http://apsystem.org.ua/lectures.html

Метод Флойда

Модель программы:

Транзиционная система (агент)
погруженная в среду данных
Для параллельных и объектно-ориентированных программ (систем) :
множество агентов в коммуникационной
среде многоуровневой памяти

Действия программы:

пара < условие > → <оператор >

Состояние среды:

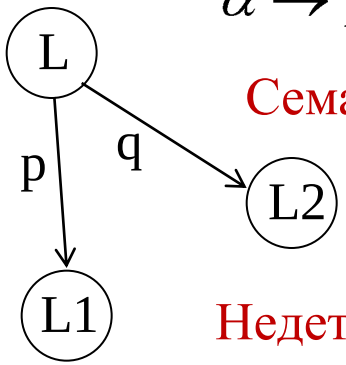
состояние памяти (конкретная модель)
формула, определяющая множество
состояний (символьная модель)

Дополнение: 2008 3 курс/Лекция 1 2-Транзиционные системы

Пример программы

Семантика условного оператора

$$\alpha \to p \Leftrightarrow \mathbf{if}(\alpha, p, \bot)$$



Семантика ветвления

(p;goto L1) + (q;gotoL2)

Недетерминированный выбор

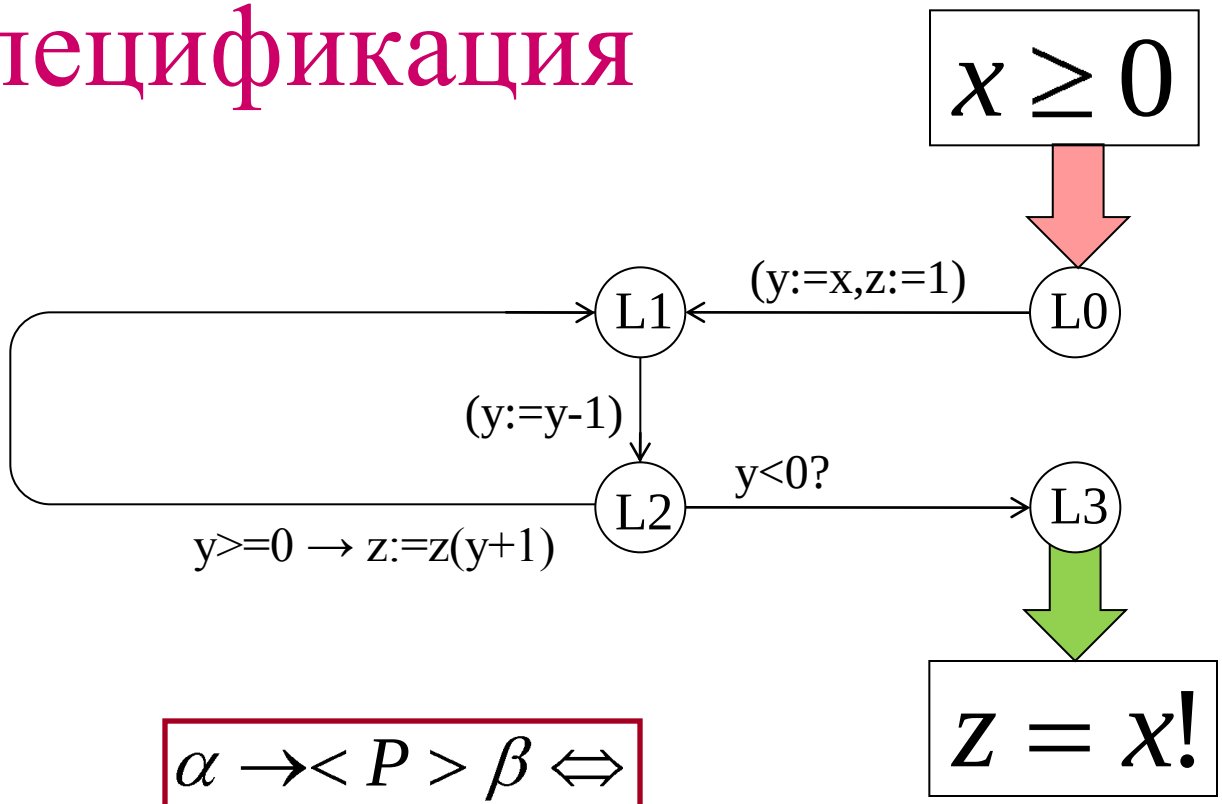
Программа с goto:

```
L0: y:=x;
    z:=1;
L1: y:=y-1;
L2: if y>=0
    then z:=z*(y+1)
    else  go to L3;
    go to L1
L3: stop
```

В структурном виде:

```
L0: y:=x;
    z:=1;
L1: y:=y-1;
    while y>=0 do
        z:=z*(y+1);
        L1: y:=y-1
    end;
L3: stop
```

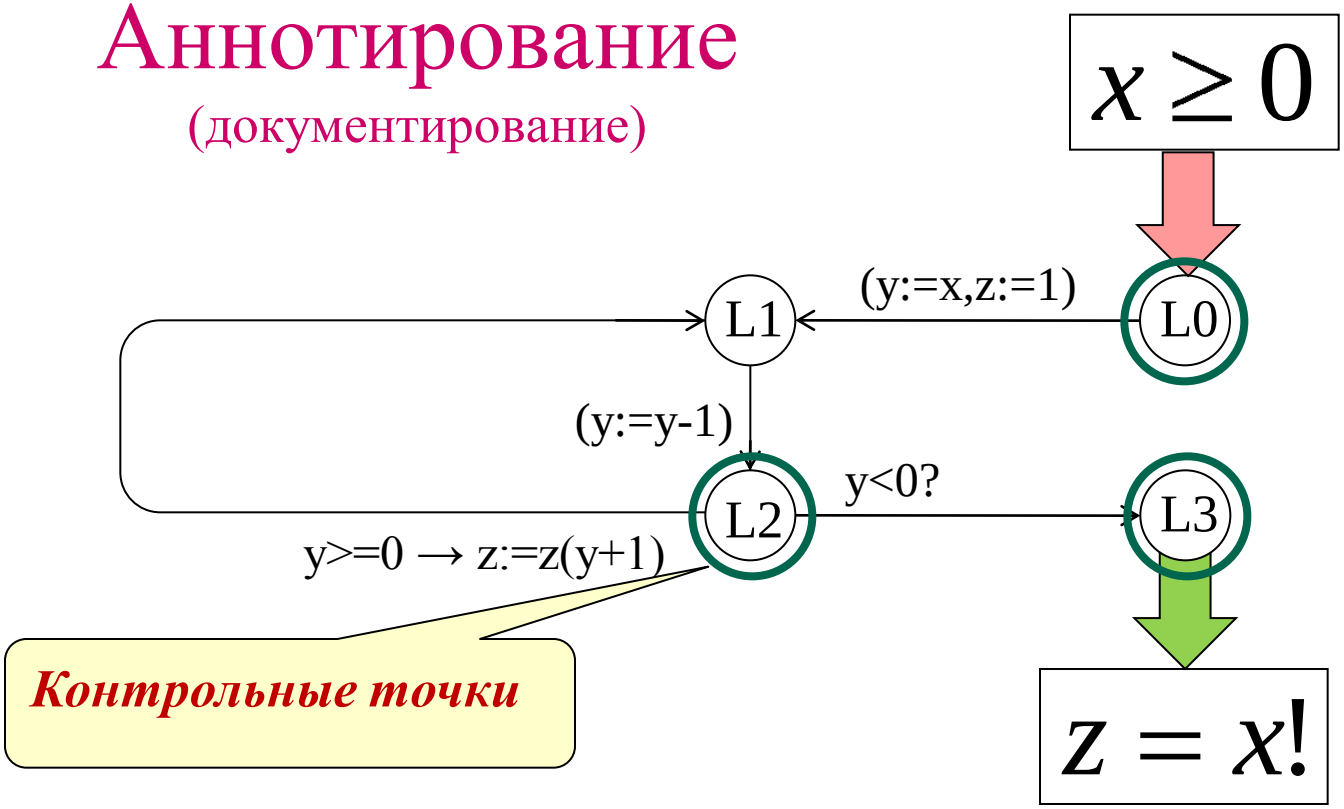
Спецификация



$$\alpha \rightarrow < P > \beta \Leftrightarrow$$
$$\alpha \rightarrow < P > 1 \wedge$$
$$\alpha \rightarrow [P]\beta$$

Аннотирование

(документирование)



Контрольные точки

аннотации

$$L0 : x \geq 0$$

$$L2 : -1 \leq y < x \wedge x! = z(y+1)!$$

$$L3 : z = x!$$

Главная идея программы или догадка?

```
L0:assertion:x>=0;
      y:=x;
      z:=1;
L1: y:=y-1;
L2: assertion: -1<=y<x/\x!=z*(y+1)!;
      if y>=0
      then z:=z*(y+1)
      else  go to L3;
      go to L1
L3: assertion: z=x!
      stop
```

Аннотации удобно также вставлять в текст программы, выделяя их специальным символом, Например, **assertion**: x<y

```
L0: assertion: x>=0;
      y:=x;
      z:=1;
L1: y:=y-1;
      assertion: -1<=y<x/\x!=z*(y+1)!;
      while y>=0 do
         assertion: -1<=y<x/\x!=z*(y+1)!;
         z:=z*(y+1);
         L1: y:=y-1
      end;
L3: assertion: z=x!;
      stop
```

Верифицирующие условия

Для каждой пары контрольных точек *a* и *b* аннотированных условиями φ и ψ, соответственно, построим все пути из *a* в *b* (контрольные пути)

$$\pi : a = a_0 \xrightarrow{q_1} a_1 \xrightarrow{q_2} a_2 \ldots a_{m-1} \xrightarrow{q_m} a_m = b$$

$$q_i = u_i \rightarrow p_i, i = 1,\ldots, m > 0$$

Условие корректности для пути π:

$$C_\pi = \varphi \rightarrow [q_1 q_2 \ldots q_m]\psi$$

$$a / \varphi, b / \psi$$

Теорема (Флойд)

Все верифицирующие условия верны=>
программа частично корректна

Начальное состояние

Заключительное состояние

$$\pi : a = a_0 \xrightarrow{q_1} a_1 \xrightarrow{q_2} a_2 \ldots a_{m-1} \xrightarrow{q_m} a_m = b \Leftrightarrow$$

$$a \xrightarrow{\pi} b \Leftrightarrow a = c_1 / \phi_1 \xrightarrow{\pi_1} c_2 / \phi_2 \xrightarrow{\pi_2} c_3 / \phi_3 \ldots \xrightarrow{\pi_{n-1}} c_n / \phi_n = b$$

Контрольные точки

Проверка верифицирующих условий

$$\pi : a = a_0 \xrightarrow{q_1} a_1 \xrightarrow{q_2} a_2 \ldots a_{m-1} \xrightarrow{q_m} a_m = b$$
$$q_i = u_i \to p_i, i = 1,\ldots,m > 0$$

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

$$[p;(u \to q)]\beta \Leftrightarrow [p]u \wedge [pq]\beta \qquad \frac{\alpha \wedge \gamma \to [P]\beta}{\alpha \to [\mathbf{if}(\gamma, P, \bot)]\beta} \qquad [pq]\beta \Leftrightarrow [p][q]\beta$$

$$C_\pi = \varphi \to [q_1 q_2 \ldots q_m]\psi \Leftrightarrow$$
$$\Leftrightarrow \varphi \to [u_1 \to p_1][q_2 \ldots q_m]\psi \Leftrightarrow$$
$$\Leftrightarrow \varphi \wedge u_1 \to [p_1]u_2 \wedge [p_2 \ldots q_m]\psi \Leftrightarrow$$
$$\Leftrightarrow \varphi \wedge u_1 \wedge [p_1]u_2 \to [p_1 p_2 q_3 \ldots q_m]\psi \Leftrightarrow$$
$$\Leftrightarrow \varphi \wedge u_1 \wedge [p_1]u_2 \wedge [p_1 p_2]u_3 \wedge \ldots \wedge [p_1 p_2 \ldots p_{m-1}]u_m \to [p_1 p_2 \ldots p_m]\psi$$

Композиция присваиваний

$$P = (x_1 := t_1(x_1, x_2, \ldots), x_2 := t_2(x_1, x_2, \ldots), \ldots)$$

$$P' = (x_1 := t'_1(x_1, x_2, \ldots), x_2 := t'_2(x_1, x_2, \ldots), \ldots)$$

$$(P;Q) = (x_1 := t'_1(t_1, t_2, \ldots), x_2 := t'_2(t_1, t_2, \ldots), \ldots)$$

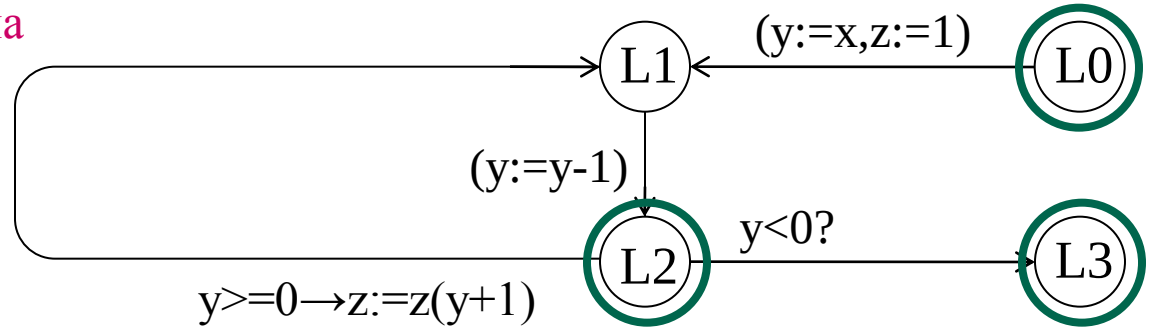
$$(P;P')(s) = P'(P(s)) \Rightarrow ((P;P')(s))(x_i) = t'_i(t_1, t_2, \ldots)$$

Верификация факториала
(частичная корректность)

$L0 : x \geq 0$

$L2 : -1 \leq y < x \wedge x! = z(y+1)!$

$L3 : z = x!$



$$C_{02} : x \geq 0 \rightarrow [y := x-1, z := 1](-1 \leq y < x \wedge x! = z(y+1)!) \Leftrightarrow$$
$$x \geq 0 \rightarrow (-1 \leq x-1 < x \wedge x! = (x-1+1)!) \Leftrightarrow \textbf{true}$$

$$C_{22} : (-1 \leq y < x \wedge x! = z(y+1)!) \wedge y \geq 0 \rightarrow$$
$$[y := y-1, z := z*(y+1)](-1 \leq y < x \wedge x! = z(y+1)!) \Leftrightarrow$$
$$(-1 \leq y < x \wedge x! = z(y+1)!) \wedge y \geq 0 \rightarrow (-1 \leq y-1 < x \wedge x! = z(y+1)y!)$$

proof

let $(-1 \leq y < x \wedge x! = z(y+1)!) \wedge y \geq 0$

$x! = z(y+1)! = z(y!(y+1)) = z(y+1)y!$

by definition of factorial : $0! = 1, (y+1)! = y!(y+1)$

$$C_{23} : (-1 \leq y < x \wedge x! = z(y+1)!) \wedge y < 0 \rightarrow z = x!$$

Завершимость факториала

$$P = C_{02} C_{22}^{*} C_{23}$$

При каждом прохождении цикла y убывает => станет < 0