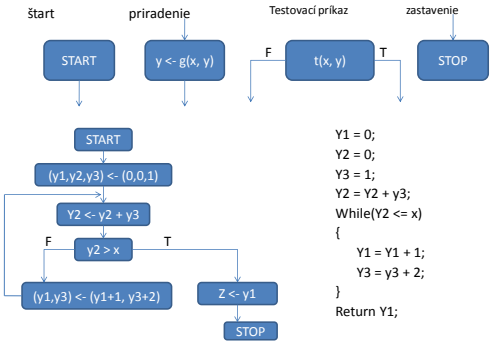
Verifikácia programov

Verifikácia programov

- Opis správania sa programu:
  - Vstupný predikát(Θ): opisuje prvky, ktoré môžu byť vstupné hodnoty
  - Vystupný predikát(Ψ): opisuje podmienky, ktoré musia spĺňať výstupé premenné v okamihu skončenia programu
- Opis správania sa programu: správnosť (korektnosť, correctness)
  - program sa zastaví
  - Je splnený výstupný predikát
- Premenné:
  - **Vstupné**: vstupný vektor x = (x1, x2,...,xn)
  - **Výstupné**: výstupný vektor z = (z1, z2,...,zm)
  - **Programové**: programový vektor y = (y1, y2,...,yk)

Jazyk vývojových diagramov



Verifikácia programov

- Každý program sa dá zapísať vývojovým diagramom
- Príkaz START sa môže nachádzať len raz
- Každý príkaz sa nachádza na ceste START – STOP
- Program sa môže vykonať, ak je zadaná hodnota vstupného vektora
- Program sa končí dosiahnutím príkazu STOP (výstupnému vektoru sa priradí hodnota)

Správnosť programu

1. Program P sa vzhľadom na Θ zastaví, ak sa P skončí pre všetky vstupné hodnoty x také, pre ktoré je Θ(x) pravda
2. Program P je čiastočne správny vzhľadom k Θ a Ψ, ak pre každú hodnotu x, pre ktorú je Θ(x) pravda a pre ktorú sa P skončí, je Ψ(x, P(x)) pravda
   ∀x (P skončí pre x ∧ Θ(x) ⇒ Ψ(x, P(x)))
3. Program P je správny vzhľadom k Θ a Ψ, ak pre každú hodnotu x, pre ktorú je Θ(x), sa P skončí a Ψ(x, P(x)) pravda
   ∀x (Θ(x) ⇒ P skončí pre x ∧ Ψ(x, P(x)))

Verifikovať program = dokázať jeho (úplnú) správnosť

Správnosť programu podľa Hoara

- induktívny výraz
  - { p(x, y)} B {q(x,y)}
  - p, q – predikáty
  - B – segment programu
  - napr.
    - { p(x, g(x,y))} y <- g(x,y) {p(x,y)}
- dôkaz čiastočnej správnosti programu P podľa Hoara – odvodenie induktívneho výrazu
- {Θ(x)} P {Ψ(x, z)}

Hoarove verifikačné pravidlá

1. Axioma priradenia:
   { p(x, g(x,y))} y <- g(x,y) {p(x,y)}
2. Pravidlá podmienených príkazov

$$\frac{\{p \wedge t\}\ B1\ \{q\} \wedge \{p \wedge !t\}\ B2\ \{q\}}{\{p\}\ \text{IF t then B1 else B2}\ \{q\}}$$

$$\frac{\{p \wedge t\}\ B\ \{q\} \wedge\ \{p \wedge\ !t\}\ \text{subset q}}{\{p\}\ \text{IF t then B}\ \{q\}}$$

7

Hoarove verifikačné pravidlá

3. Pravidlo cyklu

$$\frac{\{p \wedge t\}\ B\ \{p\}}{\{p\}\ \text{WHILE t DO B}\ \{p \wedge !t\}}$$

4. Pravidlo sekvencie

$$\frac{\{p\}\ B1\ \{q\} \wedge \{q\}\ B2\ \{r\}}{\{p\}\ B1\ ;\ B2\ \{r\}}$$

8

Hoarove verifikačné pravidlá

5. Pravidlá dôsledku

$$\frac{p \text{ subset } q \wedge \{q\}\ B\ \{r\}}{\{p\}\ B\ \{r\}}$$

$$\frac{\{p\}\ B\ \{q\} \wedge q \text{ subset } r}{\{p\}\ B\ \{r\}}$$

9