# ZÁKLADY MATEMATICKEJ TEÓRIE PROGRAMOV

Časť 2.4: Správnosť programov – konštrukcia správnych programov

Igor Prívara
**Inštitút informatiky a štatistiky**

FMFI UK Bratislava, Katedra informatiky

# Základy teórie programovania

**Programové schémy** – abstrakcia programov

- základné pojmy, vlastnosti programových schém
- rozhodnuteľnosť vlastností programových schém
- porovnávanie tried programových schém

**Správnosť programov** – vzhľadom na špecifikácie

- Floydova metóda a Hoareova metóda
- indukčné techniky použité pri dokazovaní správnosti
- **(systematická) konštrukcia správnych programov**
- dokazovanie správnosti rekurzívnych programov

**Sémantika programov** – formálny význam programov

- princípy operačnej, denotačnej a axiomatickej sémantiky
- algebraická štruktúra sémantických domén
- formálna definícia denotačného a operačného významu imperatívnych a rekurzívnych programov
- porovnanie denotačného a operačného významu programov

**Typy a sémantika** – využitie typov pri definícii sémantiky

# Vývoj správnych programov

**Cieľ (úloha)** – $\{p\}\ P^?\ \{q\}$

- skonštruovať program $P$, ktorý je čiastočne správny vzhľadom na danú vstupnú podmienku $p$ a danú výstupnú podmienku $q$.
- konštrukcia programu spolu s dôkazom jeho správnosti

**Vývojový krok** – na základe axióm a inferenčných pravidiel $\mathcal{H}$

- návrh riešenia na základe dostupných jazykových konštrukcií
- redukcia problému na podproblémy
- predpoklady pre zvolené riešenie

**Priradenie** – *návrh riešenia:* $P \equiv x := s$
*redukcia na podproblémy:* vyriešené
*predpoklad:* $p \Rightarrow q[x/s]$

**Kompozícia** – *návrh riešenia:* $P \equiv P_1; P_2$
*redukcia na podproblémy:* $\{p\}\ P_1^?\ \{r\} \quad \{r\}\ P_2^?\ \{q\}$
*predpoklad:* stanoviť "medzipodmienku" $r$

**Vetvenie** – *návrh riešenia:* $P \equiv$ **if** $b$ **then** $P_1$ **else** $P_2$ **fi**
*redukcia na podproblémy:* $\{p\&b\}\ P_1^?\ \{q\} \quad \{p\&\neg b\}\ P_2^?\ \{q\}$
*predpoklad:* stanoviť podmienku vetvenia $b$

**Iterácia** – *návrh riešenia:* $P \equiv$ **while** $b$ **do** $P_1$ **od**
*redukcia na podproblémy:* $\{r\&b\}\ P_1^?\ \{r\}$
*predpoklad:* stanoviť podmienku $b$ a invariant $r$: $p \Rightarrow r$ a $p\&\neg b \Rightarrow q$

# Príklad konštrukcie správneho programu

**Neformálne zadanie** – navrhnúť program, ktorý "pivotizuje" dané pole $A$ vzhľadom na hodnotu–pivota $x$, ktorý sa v danom poli (zaručene) vyskytuje, a nájsť také dva indexy $j < i$, že všetky prvky naľavo od $i$ budú menšie alebo rovné prvkom na pravej strane od $j$.

**Formálne špecifikácie** – vstupná a výstupná podmienka

- $p \equiv \exists k\ \{1 \leq k \leq n\ \&\ A[k] = x\}$,
- $q \equiv j < i\ \ \&\ \ \forall p, q\ \{1 \leq p < i\ \&\ j < q \leq n\ \Rightarrow\ A[p] \leq A[q]\}$.

**Invariant** – $I_i\ \&\ I_j$

- $I_i \equiv\ \forall p\ \{1 \leq p < i\ \Rightarrow\ A[p] \leq x\}$
- $I_j \equiv\ \forall q\ \{j < q \leq n\ \Rightarrow\ A[q] \geq x\}$

**Riešenie** – výsledný čiastočne správny program

**begin** $\{\exists k\ \{1 \leq k \leq n\ \&\ A[k] = x\}\}$
  $[i, j] := [1, n]$
  **while** $i \leq j$ **do** $\{I_i\ \&\ I_j$
    **while** $A[i] < x$ **do** $[i] := [i + 1]$ **od**
    **while** $A[j] > x$ **do** $[j] := [j - 1]$ **od**
    **if** $i \leq j$ **then** $[A[i], A[j]] := [A[j], A[i]]$
      $[i, j] := [i + 1, j - 1]$
    **fi**
  **od**
**end** $\{j < i\ \ \&\ \ \forall p, q\ \{1 \leq p < i\ \&\ j < q \leq n\ \Rightarrow\ A[p] \leq A[q]\}\}$

# Konštrukcia správneho programu – 2

1. *problém:* $\{p\}\, P\, \{q\}$
   *návrh riešenia:* $P \equiv P_1; P_2$
   $P_1 \equiv \langle$inicializuj premenné $i, j\rangle$
   $P_2 \equiv \langle$prezri pole zdola cez $i$, zhora cez $j$ a rob príslušné úpravy$\rangle$
   *dekompozícia na podproblémy:* $\{p\}\, P_1\, \{r\} \quad \{r\}\, P_2\, \{q\}$
   *heuristika:* $r \equiv I_i \& I_j$
   $I_i \equiv\ \forall p\ \{1 \leq p < i\ \Rightarrow\ A[p] \leq x\}$
   $I_j \equiv\ \forall q\ \{j < q \leq n\ \Rightarrow\ A[q] \geq x\}$

2. *problém:* $\{p\}\, P_1\, \{r\}$
   *návrh riešenia:* $P_1 \equiv [i, j] := [1, n]$
   *dekompozícia na podproblémy:* vyriešené
   *treba dokázať:* $p \Rightarrow I_1 \& I_n$ ($I_1 \& I_n$ triviálne platí)

3. *problém:* $\{r\}\, P_2\, \{q\}$
   *návrh riešenia:* $P_2 \equiv$ **while** $b$ **do** $P_{21}$ **od**
   $P_{21} \equiv \langle$znižuj $i$, zvyšuj $j$ a manipuluj pole$\rangle$
   *dekompozícia na podproblémy:* $\{p_1 \& b\}\, P_{21}\, \{p_1\}$
   *heuristika:* $p_1 \equiv r \quad b \equiv i \leq j$
   *treba dokázať:* $r \Rightarrow p_1 \quad (r \Rightarrow r)$
   $p_1 \& \neg b \Rightarrow q \quad (I_i \,\&\, I_j \,\&\, i > j \Rightarrow q)$

# Konštrukcia správneho programu – 3

1. *problém:* $\{p_1 \& b\}\ P_{21}\ \{p_1\}$
   *návrh riešenia:* $P_{21} \equiv\ P_{211}; P_{212}; P_{213}$
   $P_{211} \equiv \langle$nájdi $i$ na potenciálnu výmenu$\rangle$
   $P_{212} \equiv \langle$nájdi $j$ na potenciálnu výmenu$\rangle$
   $P_{213} \equiv \langle$vymeň prvky na nájdených $i, j$ indexoch$\rangle$
   *dekompozícia na podproblémy:*
   $\{p_1 \& b\}\ P_{211}\ \{p_2\}$ $\{p_2\}\ P_{212}\ \{p_3\}$ $\{p_3\}\ P_{213}\ \{p_1\}$
   *heuristika:* $p_2 \equiv I_i \,\&\, I_j \,\&\, A[i] \geq x$
   $p_3 \equiv I_i \,\&\, I_j \,\&\, A[i] \geq x \geq A[j]$

2. *problém:* $\{p_1 \& b\}\ P_{211}\ \{p_2\}$
   *návrh riešenia:* $P_{211} \equiv$ **while** $b_1$ **do** $P_{2111}$ **od**
   $P_{2111} \equiv \langle$inkrementuj $i\rangle$
   *dekompozícia na podproblémy:* $\{p_1 \& b_1\}\ P_{2111}\ \{p_1\}$
   *heuristika:* $b_1 \equiv A[i] < x$
   *treba dokázať:* $p_1 \& b \Rightarrow p_1 \quad (I_i \,\&\, I_j \,\&\, i \leq j \Rightarrow I_i \,\&\, I_j)$
   $p_1 \& \neg b_1 \Rightarrow p_2 \quad (I_i \,\&\, I_j \,\&\, A[i] \geq x \Rightarrow I_i \,\&\, I_j \,\&\, A[i] \geq x)$

3. *problém:* $\{p_1 \& b_1\}\ P_{2111}\ \{p_1\}$
   *návrh riešenia:* $P_{2111} \equiv [i] := [i+1]$
   *dekompozícia na podproblémy:* vyriešené
   *treba dokázať:* $p_1 \& b_1 \Rightarrow p_1[i/i+1]$
   $(I_i \,\&\, I_j \,\&\, A[i] < x \Rightarrow I_{i+1} \,\&\, I_j)$

# Konątrukcia správneho programu – 4

1. *problém:* $\{p_2 \& b\}\ P_{212}\ \{p_3\}$
   *návrh riešenia:* $P_{212} \equiv$ **while** $b_2$ **do** $P_{2121}$ **od**
   $P_{2121} \equiv \langle$dekrementuj $j\rangle$
   *dekompozícia na podproblémy:* $\{p_2 \& b_2\}\ P_{2121}\ \{p_2\}$
   *heuristika:* $b_2 \equiv A[j] > x$
   *treba dokázať:* $p_2 \& \neg b_2 \Rightarrow p_3$
   $(I_i \,\&\, I_j \,\&\, A[i] \geq x \,\&\, A[j] \leq x \Rightarrow I_i \,\&\, I_j \,\&\, A[i] \geq x \geq A[j])$

2. *problém:* $\{p_2 \& b_2\}\ P_{2121}\ \{p_2\}$
   *návrh riešenia:* $P_{2121} \equiv [j] := [j-1]$
   *dekompozícia na podproblémy:* vyriešené
   *treba dokázať:* $p_2 \& b_2 \Rightarrow p_2[j/j-1]$
   $(I_i \,\&\, I_j \,\&\, A[i] \geq x \,\&\, A[j] > x \Rightarrow I_i \,\&\, I_{j-1} \,\&\, A[i] \geq x)$

3. *problém:* $\{p_3\}\ P_{213}\ \{p_1\}$
   *návrh riešenia:* $P_{213} \equiv$ **if** $b_3$ **then** $P_{2131}$ **fi**
   $P_{2131} \equiv \langle$vymeň prvky a zabezpeč posuny $i$ a $j\rangle$
   *dekompozícia na podproblémy:* $\{p_3 \& b_3\}\ P_{2131}\ \{p_1\}$
   *heuristika:* $b_3 \equiv b$

# Konštrukcia správneho programu – 5

1. *problém:* $\{p_3 \& b\}\ P_{2131}\ \{p_1\}$
   *návrh riešenia:* $P_{2131} \equiv P_{21311}; P_{21312}$
   $P_{21311} \equiv \langle$zabezpeč výmenu $i$ a $j\rangle$
   $P_{21312} \equiv \langle$zabezpeč posuny $i$ a $j\rangle$
   *dekompozícia na podproblémy:*
   $\{p_3 \& b\}\ P_{21311}\ \{p_4\} \quad \{p_4\}\ P_{21312}\ \{p_1\}$
   *heuristika:* $p_4 \equiv I_i \,\&\, I_j \,\&\, A[i] \leq x \leq A[j]$

2. *problém:* $\{p_3 \& b\}\ P_{21311}\ \{p_4\}$
   *návrh riešenia:* $P_{21311} \equiv [A[i], A[j]] := [A[j], A[i]]$
   *dekompozícia na podproblémy:* vyriešené
   *treba dokázať:* $p_3 \& b \Rightarrow p_4[A[i]/A[j], A[j]/A[i]]$
   $(I_i \,\&\, I_j \,\&\, A[i] \geq x \geq A[j] \,\&\, i \leq j \Rightarrow I_i \,\&\, I_j \,\&\, A[i] \leq x \leq A[j])$

3. *problém:* $\{p_4\}\ P_{21312}\ \{p_1\}$
   *návrh riešenia:* $P_{21312} \equiv [i, j] := [i + 1, j - 1]$
   *dekompozícia na podproblémy:* vyriešené
   *treba dokázať:* $p_4 \Rightarrow p_1[i/i + 1, j/j - 1]$
   $(I_i \,\&\, I_j \,\&\, A[i] \leq x \leq A[j] \Rightarrow I_{i+1} \,\&\, I_{j-1})$