Úvod

Nech nasledujúci program vypočíta celočíselnú $\sqrt{x}$:

1. y := 1
2. if $y^2 > x$ then STOP[y – 1]
3. y := y + 1
4. goto 2.

Úlohou je dokázať správnosť programu, inými slovami: ukázať, že program naozaj vypočíta $\sqrt{x}$.

V matematike nie je možné si uvedenú úlohu jednoducho nevšimnúť s konštatovaním, že to „intuitívne vidieť“ a ani v programovaní to nie je vždy možné, lebo nie vždy sú programy takéto jednoduché a môže ísť o kritický program, napr. v jadrovej oblasti.

Tu nevystačia matematické vedomosti s programátorskými vedomosťami. Nato vznikol vedný odbor, ktorý sa zaoberá touto problematiku, nazýva sa m a t e m a t i c k á t e ó r i a p r o g r a m o v.

Program – vo všeobecnosti veľmi široký pojem, v tejto práci sa pojmom „program“ myslí algoritmus doplnený o určitú schopnosť typickú pre počítače, napr. čítanie a zápis do súboru.

1 Formalizácia

U čitateľa sa predpokladajú všeobecné vedomosti matematiky, predovšetkým predikátový počet. Na programátorskej úrovni sa očakáva znalosť významu jednoduchého programu, napr. programu uvedeného vyššie. V prípade zavedenia nových príkazov bude ich význam vysvetlený.

Nasledujúci text je časťou novej, okolo 50 ročnej vednej disciplíny nazývanej matematická teória programov. Nutné je dobre si uvedomiť význam všetkých troch slov. Čo je teória, a čo program (ako bol ten uvedený v Úvode), je iste intuitívne jasné, dôležité je uvedomiť si, že ide o m a t e m a t i c k ú teóriu.

Na dôkaz správnosti programov sa totiž budú používať matematické symbolické zápisy *predikátového počtu* a jeho pravidlá. Okrem toho jadrom dôkazu je *matematická indukcia*.

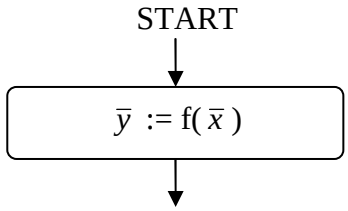
1.1 Program a vývojový diagram

Definícia: Programom rozumieme postupnosť príkazov, začínajúcu vždy príkazom START.

Navyše bude program vyjadrený *vývojovým diagramom*, a každý príkaz musí ležať na niektorej ceste z príkazu START do jedného z príkazov STOP.

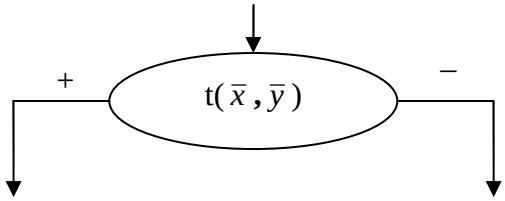
Základné príkazy zobrazené vo vývojových diagramoch sú:

1. príkaz START:



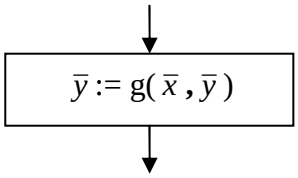
f je funkcia z D $\bar{x}$ do D $\bar{y}$

2. podmienkový príkaz:



t je predikát nad D $\bar{x}$ × D $\bar{y}$

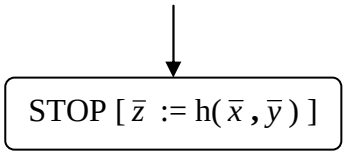
3. priradenie:



g je funkcia z $D_{\bar{x}} \times D_{\bar{y}}$ do $D_{\bar{y}}$

priradenie je paralelné, t.j. všetky priradenia naraz (nie postupne)

4. príkaz STOP:

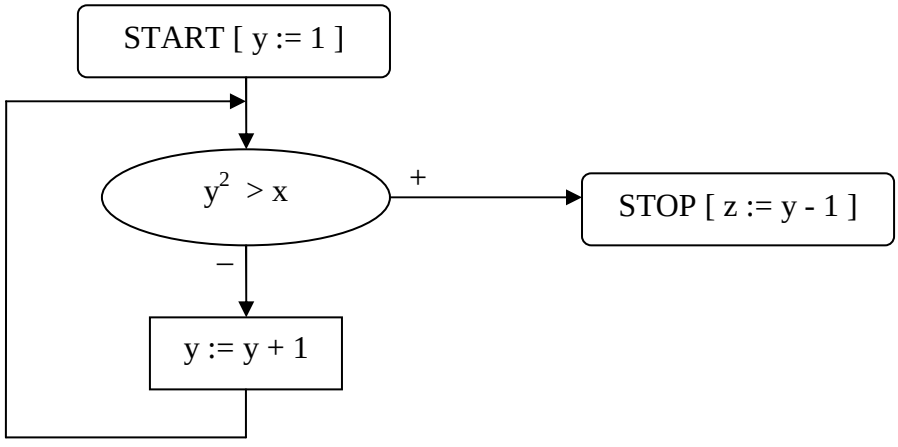


h je funkcia z $D_{\bar{x}} \times D_{\bar{y}}$ do $D_{\bar{z}}$

Pričom označujeme:

- $\bar{x}$ - vstupné premenné (nikdy sa nemenia)
- $\bar{y}$ - pracovné premenné (menia sa v priebehu výpočtu)
- $\bar{z}$ - výstupné premenné (výsledok)

Príklad: Vývojový diagram programu na výpočet $\sqrt{x}$ z Úvodu.



1.2 Špecifikácia programu

Špecifikácia programu, inými slovami vstupná a výstupná podmienka, je popísanie čo je správny program.

V matematickej teórii programov uvádzame špecifikáciu predikátom **φ** nad oborom vstupných premenných $D_{\bar{x}}$ a predikátom **ψ** nad oborom vstupno-výstupných premenných $D_{\bar{x}}$, $D_{\bar{z}}$.

V našom príklade z Úvodu je program správny, ak vypočíta celočíselnú druhú odmocninu x:

- vstupná podmienka:

$$\varphi(x) = x \geq 0$$

- výstupná podmienka:

$$\psi(x,z) = z^2 \leq x < (z+1)^2$$

1.3 Rozdelenie programu

V prípade veľmi jednoduchého programu sa priamo zo vstupnej podmienky podľa príslušných príkazov programu dokáže výstupná podmienka, inak sa program musí rozdeliť na menšie časti, z ktorých sa každá dokazuje osobitne. Body, v ktorých sa program rozdelí, nazývame deliace body programu.

Predstavme si výpočet programu s deliacimi bodmi $A_1, A_2, \ldots, A_k$ postupnosťou hodnôt pracovných premenných v týchto deliacich bodoch:

START: $\bar{y}_0 = f(\bar{x})$

$\bar{y}_1$

$\bar{y}_2$

$\bar{y}_3$

...

$\bar{y}_n$

STOP: $z = h(\bar{x}, \bar{y}_n)$

pričom výpočet môže niektorým deliacim bodom prechádzať viackrát.

Dôkaz správnosti je nasledujúci:

Ak platí vstupná podmienka $\varphi(\bar{x})$, tak po vykonaní prvých príkazov, (keď sa výpočet nachádza v nasledujúcom deliacom bode A) platí iná podmienka, predikát $p_A(\bar{x}, \bar{y})$.

Po vykonaní ďalšieho bloku príkazov (keď sa výpočet dostane do nasledujúceho deliaceho bodu B), platí iná podmienka, predikát $p_B(\bar{x}, \bar{y})$, atď.

V poslednom deliacom bode (označme ho D) pred príkazom STOP platí podmienka $p_D(\bar{x}, \bar{y})$. Na záver treba ukázať, že platnosť tejto poslednej podmienky $p_D(\bar{x}, \bar{y})$ implikuje po vykonaní posledných príkazov platnosť $\psi(\bar{x}, \bar{z})$, a teda program je správny.

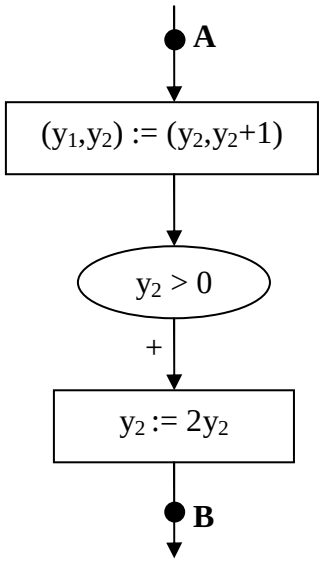
Tu si uvedomme dve skutočnosti:

- stále nemáme mechanizmus na formálne zachytenie zmien hodnôt pracovných premenných, ku ktorému dochádza prechodom z jedného deliaceho bodu do nasledujúceho
- v prípade cyklu sa deliace body môžu opakovať (napr. môže platiť A = B, program prejde z B opäť do B), samotný cyklus sa môže opakovať nekonečne (program neskončí), alebo sa opakuje n - krát, n je prirodzené číslo. Čitateľ zbehlý v matematických dôkazoch vidí neomylne príležitosť na matematickú indukciu.

1.4 Spätná substitúcia

Mechanizmus spätnej substitúcie, ktorý je jedným z možných prístupov k zaznamenaniu zmien hodnôt premenných počas prechodu z jedného deliaceho bodu do druhého, je najlepšie pochopiť vyskúšaním na viacerých príkladoch. Tu iba popíšeme postup.

Nasleduje výsek programu, ktorý obsahuje cestu z jedného deliaceho bodu do druhého:



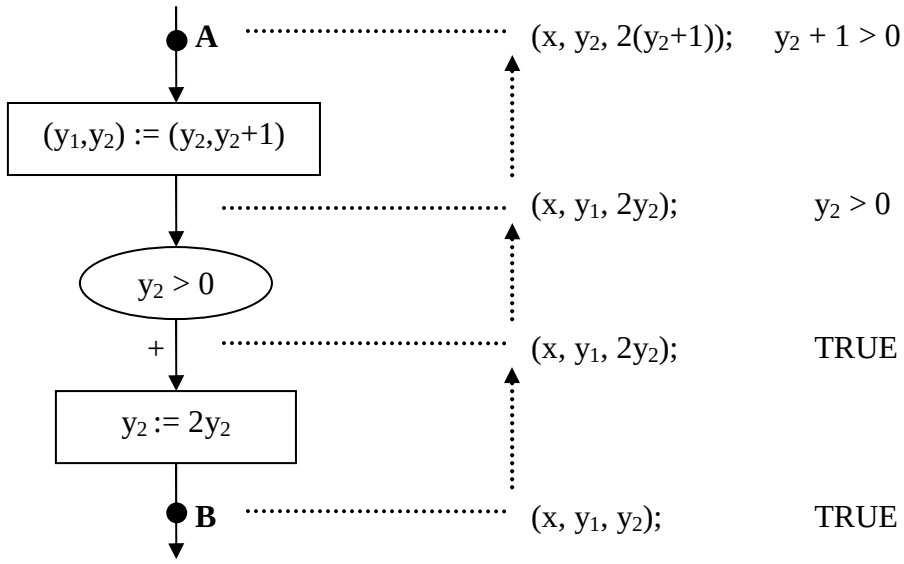
Nech má na začiatku trojica vstupných a výstupných premenných hodnoty (x,y_1,y_2) a podmienka hodnotu TRUE.

Prechádzajme programom spätne (odtiaľ názov spätná substitúcia) z bodu B do A a

- pri každom príkaze priradenia, substituujme v našej trojici a tiež v podmienke(nezabúdať!) premenné z ľavej strany priradenia za zodpovedajúce hodnoty z pravej strany priradenia

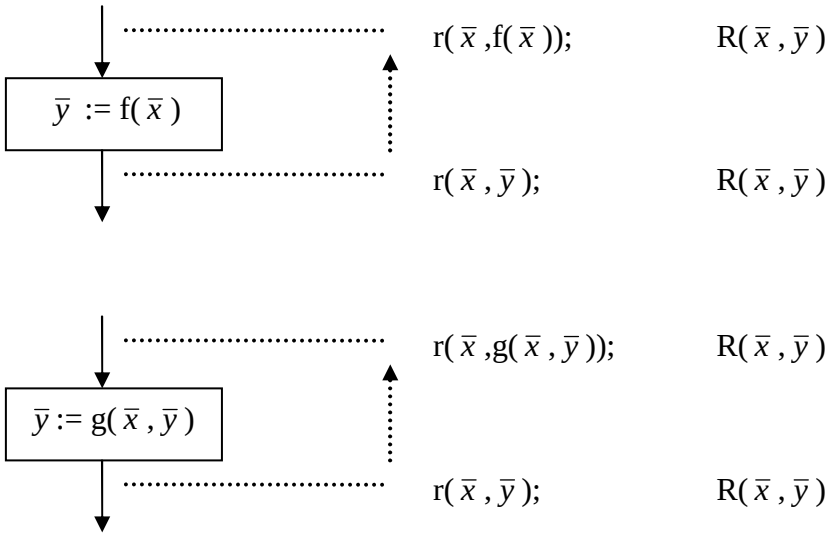
- pri každom podmienkovom príkaze $t(x,y_1,y_2)$, ktorý nasleduje „+“ ho jednoducho priraďme k doterajšej podmienke, t.j. ak súčasná podmienka je p, nová podmienka bude $p \wedge t(x,y_1,y_2)$; ak nasleduje „–“ priradíme jeho negáciu, nová podmienka by teda bola $p \wedge \neg t(x,y_1,y_2)$

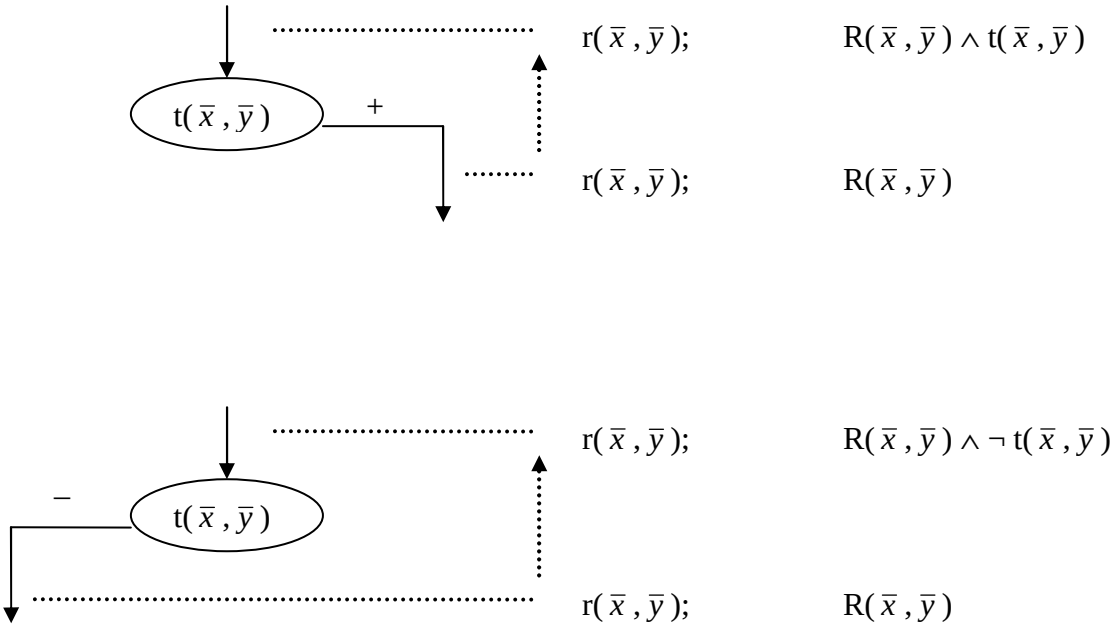
Teda:



Nové hodnoty premenných po prechode z A do B budeme označovať $r_{AB}(\bar{x}, \bar{y})$ a novú podmienku $R_{AB}(\bar{x}, \bar{y})$. Uvedomme si, že ak R_{AB} je predikát nad $D_{\bar{x}} \times D_{\bar{y}}$, r_{AB} je funkcia z $D_{\bar{x}} \times D_{\bar{y}}$ do $D_{\bar{y}}$.

Všeobecne:





1.5 Matematická indukcia

Teraz sa dostávame k jadru dôkazu spočívajúcom v matematickej indukcii. Aplikuje sa na cykly v programe, princíp je klasickým princípom matematickej indukcie:

*Ak pre všetky k ∈ **N** z platnosti tvrdenia pre k, vyplýva platnosť tvrdenia pre k+1, stačí ukázať platnosť tvrdenia pre 0, potom tvrdenie platí pre všetky n ∈ **N**.*

Samozrejme, nemusí byť platnosť tvrdenia práve od 0, môže byť dokázané pre ľubovoľné

a ∈ ***N***, *potom* tvrdenie platí pre všetky n ∈ ***N***, n ≥ a, ale pre program ide práve o to, aby podmienka platila už pri vstupe do cyklu. Teda matematická indukcia prispôsobená potrebám programu:

Označme $p_B(\bar{x}, \bar{y})$ predikát, ktorý platí vždy, keď výpočet prechádza deliacim bodom B. Nazýva sa tiež induktívna podmienka alebo invariant[1] bodu B.

Nech β je cesta z deliaceho bodu B opäť do B a $p_B(\bar{x}, \bar{y})$ invariant bodu B.

*Ak pre všetky k ∈ **N** z platnosti* $p_B(\bar{x}, \bar{y}) \wedge R_\beta(\bar{x}, \bar{y})$ *vyplýva platnosť* $p_B(\bar{x}, r_\beta(\bar{x}, \bar{y}))$*, stačí ukázať platnosť* $p_B(\bar{x}, \bar{y})$ *v B pri vstupe do cyklu programu, potom* $p_B(\bar{x}, \bar{y})$ *platí v B aj po ľubovoľnom počte opakovaní cyklu.*

Indukčný krok znamená dokázať podmienku $p_B(\bar{x}, \bar{y}) \wedge R_\beta(\bar{x}, \bar{y}) \Rightarrow p_B(\bar{x}, r_\beta(\bar{x}, \bar{y}))$ nazývanú verifikačná podmienka, totiž ak dokážeme platnosť verifikačných podmienok, dokázali sme správnosť celého programu (verifikovali sme ho).

[1] Predikát p_B platí vždy pri prechode bodom B, nezávisle na počte opakovaní cyklu - odtiaľ názov *invariant*

1.6 Induktívne podmienky

Vo všeobecnosti otázka čo aj čiastočnej správnosti programu je nerozhodnuteľný problém. Dôvodom je, že my musíme počítaču, ktorý by overil verifikačné podmienky, dať na vstup invarianty[1] k deliacim bodom a na zostrojenie invariantov deliacich bodov algoritmický postup neexistuje. Sú oblasti matematickej teórie programov venujúce sa praktickým postupom zostrojovania induktívnych podmienok, vo všeobecnosti je ale zostrojenie induktívnych podmienok nerozhodnuteľný problém.

Návod ako nájsť induktívne podmienky, je pochopiť vnútornú logiku programu, najmä v ktorej pracovnej premennej je čo „zapamätávané".

Induktívnu podmienku k deliacemu bodu B sme označili $p_B(\bar{x}, \bar{y})$. Charakterizuje vzťah medzi premennými v tomto bode, vždy keď výpočet prechádza týmto bodom, $p_B(\bar{x}, \bar{y})$ je predikát pre priebežné hodnoty $\bar{x}, \bar{y}$.[2]

Príklad: V našom programe z Úvodu na výpočet celočíselnej odmocniny je použitá premenná y na zapamätanie doteraz testovanej hodnoty (od 0, po každom prechode o 1 zvýšenej, až po výsledok+1), ktorej druhá mocnina, ak má cyklus bežať, musí byť menšia alebo rovná x, v deliacom bode B teda bude vždy platiť $(y-1)^2 \leq x$. Vidieť, že je to vhodný predikát aj vzhľadom k výstupnej podmienke, ktorú dokázať je cieľom.

1.7 Problém ukončenia

Na rozdiel od matematiky je v teórii programovania pri matematickej indukcii jedna vlastnosť neželaná – nekonečný cyklus.

Matematik použije matematickú indukciu práve na dokázanie tvrdenia pre nekonečne veľa prirodzených čísel, programátor si nielenže neželá, aby cyklus bežal nekonečne, ale všetky cykly v programe, ktorý je správny, musia skončiť a navyše, ako je snahou každého dobrého programátora, po čo najmenšom počte opakovaní. Nie je tomu ani 10 rokov, keď boli programovacie nástroje na takej úrovni, že nekonečný cyklus spôsobil pád celého programovacieho nástroja (väčšinou bez uloženia), alebo celého systému. Dnes samozrejme väčšina programovacích nástrojov najprv zmeny uloží, potom program spustí, s prípadným nekonečným cyklom sa vysporiada sama bez nutnosti reštartovať sa alebo používať nejaké „kilovanie" procesu a kombináciu CTRL+ALT+DEL, napriek tomu nekonečný cyklus je v programovaní veľmi nežiaduci jav.

Ukázali sme už postup dôkazu, že po ľubovoľnom počte opakovaní cyklu bude platiť istá podmienka. Teraz nasleduje druhá a posledná časť dôkazu, a to ukázať, že cyklus skončí. Princíp je nasledovný:

Nech máme premennú, ktorej hodnotu vieme zmerať v určitom bode cyklu. Dokážeme, že po každom otočení cyklu je hodnota v tomto bode menšia a okrem toho, že táto premenná nadobúda len hodnoty z čiastočne usporiadanej množiny, v ktorej neexistuje nekonečná klesajúca postupnosť. Potom cyklus zjavne musí skončiť.

[1] Opäť pripomíname, že pojmy ‚invariant' a ‚induktívna podmienka' tu majú ten istý význam

[2] V priebehu výpočtu sa menia iba hodnoty $\bar{y}$

Definícia: Množina W s čiastočným usporiadaním $\prec$, v ktorej neexistuje nekonečná klesajúca postupnosť ... $\prec a_2 \prec a_1 \prec a_0$ sa nazýva dobre založená množina a označuje $(W, \prec)$.

Vhodnou voľbou je množina prirodzených čísel **N**, ale využiť možno ľubovoľnú takto dobre založenú množinu.

Zvolí sa teda dobre založená množina W, deliace body všetkých cyklov programu a ku každému deliacemu bodu i funkcia u_i taká, že

$$(\forall \bar{x})(\forall \bar{y})(u_i(\bar{x}, \bar{y}) \in W)$$

Ak sa podarí ukázať, že pre každú cestu α z deliaceho bodu i do nasledujúceho bodu v cykle j platí

$$(\forall \bar{x})(\forall \bar{y})[\varphi(\bar{x}) \wedge R_\alpha(\bar{x}, \bar{y}) \Rightarrow (u_i(\bar{x}, \bar{y}) \succ u_i(\bar{x}, r_\alpha(\bar{x}, \bar{y})))]$$

tak program končí vzhľadom k $\varphi(\bar{x})$.

V teórii by bolo všetko v poriadku, ibaže v praxi sa ukazuje, že takéto silné podmienky sa málokedy podarí dokázať, presnejšie, nájsť vhodné funkcie u_i. Riešenie sa ponúka už pri pohľade na induktívne podmienky, ktoré rovnako platia v deliacich bodoch, prečo teda dokazovať podmienky pre $(\forall \bar{x})$ a $(\forall \bar{y})$, keď $\bar{x}$ a $\bar{y}$ v deliacom bode môže nadobúdať len obmedzené hodnoty?

Zvolí sa preto vhodná množina deliacich bodov tak, aby preťali všetky cykly programu, ku každému deliacemu bodu i sa priradí vhodná induktívna podmienka $q_i(\bar{x}, \bar{y})$, dokáže sa jej platnosť po každom prechode cyklom a tvrdenie o klesajúcej hodnote $u_i(\bar{x}, \bar{y})$ sa tak zredukuje na tie $\bar{x}, \bar{y}$, pre ktoré $q_i(\bar{x}, \bar{y})$ je pravdivé.

Presný postup spolu s Floydovou vetou o Metóde dobre založených množín bude popísaný v kap. 2.2.

T e r m i n o l o g i c k á p o z n á m k a: V literatúre sa miesto ukončenie používa niekde termín *zastavenie* programu. Nezmyselný program môže obsahovať ako mŕtve cykly, tak aj slepé cesty, v ktorých zastaví, ale neukončí, nakoľko ukončenie znamená vrátiť nejaký výstup, no v slepej ceste sa program len „zasekne“, nevráti žiadne výstupné hodnoty. Vzhľadom k tomu, ako bol tu definovaný program, je správny pojem *ukončenie* programu, nakoľko sme definovali, že každý príkaz leží na niektorej ceste zo START do STOP, teda každé zastavenie programu znamená vrátenie výstupu $\bar{z}$.

1.8 Vstupno-výstupné operácie

Potrebujeme previesť do symbolov predikátového počtu vstupno-výstupné operácie, presnejšie čítanie a zo súboru.

Definícia: Súbor f, nastavený na čítanie je postupnosť $f = f_1 f_2 ... fn$, kde f_i je prvok súboru, dĺžka súboru f je n; a F je pozícia čítacej hlavy, na začiatku F = 1.

Definícia: EOF(f, F) = (F > n), kde n = dĺžka(f) a F je pozícia hlavy súboru f ,

Je to teda funkcia, ktorá vráti boolovskú hodnotu TRUE, ak je čítacia hlava na konci súboru, inak vráti boolovskú hodnotu FALSE.

2 Dôkaz správnosti Floydovou metódou

2.1 Čiastočná správnosť metódou induktívnych podmienok - Floyd

Nasledujúca metóda dokazuje čiastočnú správnosť programu, t.j. ak program zastaví, výsledok je správny (t.j. výstupný predikát pravdivý).

Postup:

1. k r o k : D e l i a c e b o d y

   Rozdeliť program vhodnými deliacimi bodmi. Pridať jeden deliaci bod hneď za príkaz START a takisto bezprostredne pred každý príkaz STOP.

2. k r o k : I n d u k t í v n e p o d m i e n k y

   Každému deliacemu bodu X priradiť vhodnú induktívnu podmienku $p_X(\bar{x}, \bar{y})$.
   Prvému deliacemu bodu za príkazom START je priradený vstupný predikát $\varphi(\bar{x})$ a každému pred príkazom STOP výstupný predikát $\psi(\bar{x}, \bar{y})$.

3. k r o k : V e r i f i k a č n é p o d m i e n k y

   Zostrojiť verifikačnú podmienky pre každú možnú cestu z bodu X do nasledujúceho bodu Y, t.j. podmienku

$$p_X(\bar{x}, \bar{y}) \wedge R_{XY}(\bar{x}, \bar{y}) \Rightarrow p_Y(\bar{x}, r_{XY}(\bar{x}, \bar{y}))$$

Veta: (dôkaz správnosti programu metódou induktívnych podmienok - Floyd)

Nech P je program špecifikovaný vstupným predikátom $\varphi(\bar{x})$ a výstupným predikátom $\psi(\bar{x}, \bar{y})$. Zostrojme postupne:

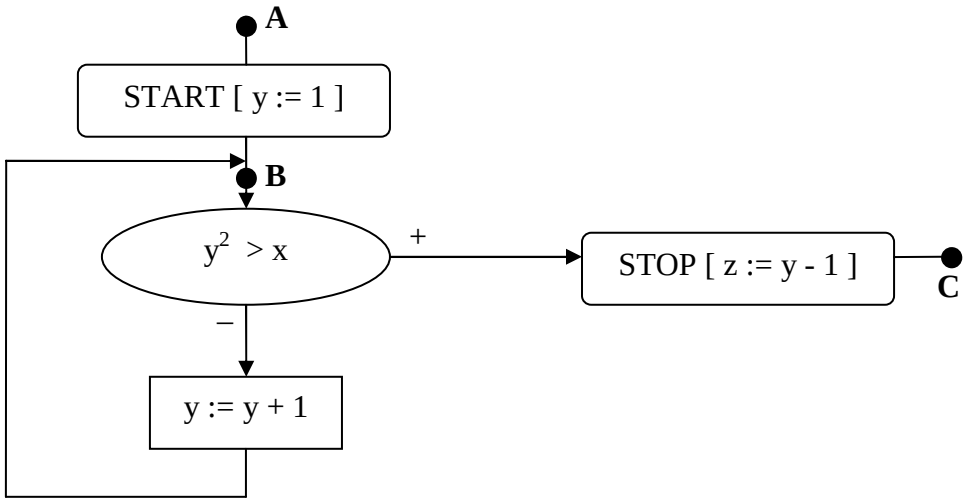
1.) deliace bodu každému cyklu programu

2.) vhodné induktívne podmienky každému deliacemu bodu

3.) verifikačné podmienky pre každú cestu z deliaceho bodu do nasledujúceho deliaceho bodu

Ak sú všetky verifikačné podmienky pravdivé, je program P čiastočne správny vzhľadom k φ a ψ.

Príklad (celočíselnej odmocniny x z úvodu):



Krok 1: Deliace body: A, B, C

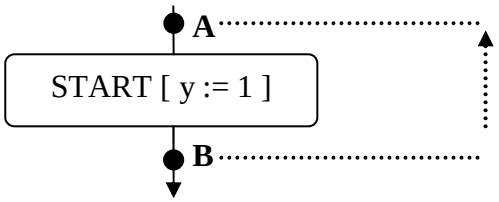
Krok 2: Induktívne podmienky:

- A: $\varphi(x) = x \geq 0$
- B: $p_B(x,y) = (y-1)^2 \leq x$
- C: $\psi(x,z) = z^2 \leq x < (z+1)^2$

Krok 3: Verifikačné podmienky:

- cesta α (z bodu A do B):

  spätná substitúcia:



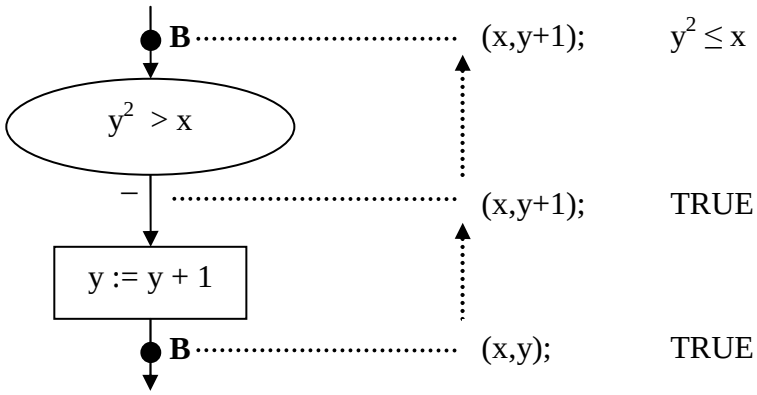
(x,1); TRUE

(x,y); TRUE

verifikačná podmienka: $\varphi(x) \Rightarrow p_B(x,1)$

- cesta β (cyklom z bodu B do B):

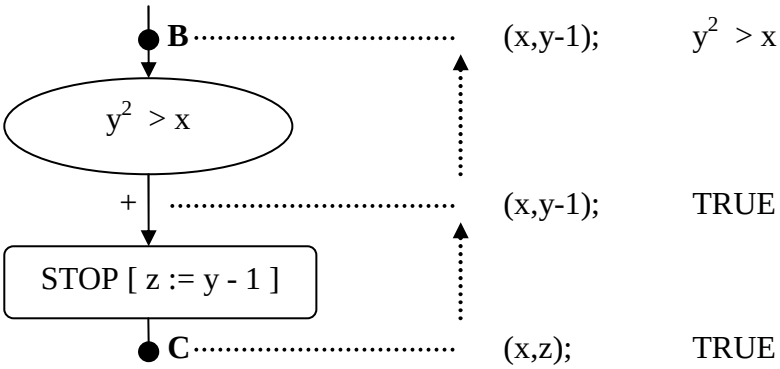
  spätná substitúcia:



  verifikačná podmienka: $p_B(x,y) \wedge y^2 \leq x \Rightarrow p_B(x,y+1)$

- cesta γ (z bodu B do C):

  spätná substitúcia:



  verifikačná podmienka: $p_B(x,y) \wedge y^2 > x \Rightarrow \psi(x,y-1)$

Overenie pravdivosti verifikačných podmienok:

Pre cestu α:

$$0 \leq x \Rightarrow 0 \leq x$$

$$0 \leq x \Rightarrow 0^2 \leq x$$

$$0 \leq x \Rightarrow (1-1)^2 \leq x$$

$$\varphi(x) \Rightarrow p_B(x,1)$$

Pre cestu β:

$$y^2 \le x \Rightarrow y^2 \le x$$

$$y^2 \le x \Rightarrow (y + 1 - 1)^2 \le x$$

$$(y-1)^2 \le x \wedge y^2 \le x \Rightarrow (y + 1 - 1)^2 \le x$$

$$p_B(x,y) \wedge y^2 \le x \Rightarrow p_B(x,y+1)$$

Pre cestu γ:

$$(y-1)^2 \le x \wedge y^2 > x \Rightarrow (y-1)^2 \le x < y^2$$

$$(y-1)^2 \le x \wedge y^2 > x \Rightarrow (y-1)^2 \le x < (y - 1 + 1)^2$$

$$p_B(x,y) \wedge y^2 > x \Rightarrow \psi(x,y-1)$$

Pretože všetky verifikačné podmienky sú pravdivé, program je čiastočne správny vzhľadom k daným vstupným, výstupným podmienkam.

2.2 Ukončenie metódou dobre založených množín - Floyd

K dôkazu úplnej správnosti programu, treba ešte ukázať, že program skončí pre všetky vstupy spĺňajúce vstupnú podmienku. Princíp dôkazu je popísaný v kap. 1.7.

Postup je nasledovný:

Krok 1: Voľba vhodných deliacich bodov tak, aby sa v každom cykle nachádzal aspoň jeden a voľba dobre založenej množiny $(W, \prec)$.

Krok 2: Ku každému deliacemu bodu i zvoliť „dobrý“ predikát $q_i(\bar{x}, \bar{y})$, t.j. taký, že platí

- pre každú cestu α z bodu START do nasledujúceho deliaceho bodu i platí

$$\varphi(\bar{x}) \wedge R_\alpha(\bar{x}) \Rightarrow q_i(\bar{x}, r_\alpha(\bar{x}))$$

- pre každú cestu z bodu i do nasledujúceho bodu j platí

$$q_i(\bar{x}, \bar{y}) \wedge R_\alpha(\bar{x}, \bar{y}) \Rightarrow q_i(\bar{x}, r_\alpha(\bar{x}, \bar{y}))$$

Krok 3: Ku každému deliacemu bodu i zvoliť „dobrú“ čiastočnú funkciu $u_i(\bar{x}, \bar{y})$ z $D_{\bar{x}} \times D_{\bar{y}}$ do W, t.j. takú, že platí

$$(\forall \bar{x})(\forall \bar{y})[q_i(\bar{x}, \bar{y}) \Rightarrow u_i(\bar{x}, \bar{y}) \in W]$$

Krok 4: Dokázať *podmienky ukončenia* ku každej ceste α z deliaceho bodu i do nasledujúceho deliaceho bodu j takej, že celá leží v niektorom cykle; tieto podmienky majú tvar:

$$(\forall \bar{x})(\forall \bar{y})[q_i(\bar{x}, \bar{y}) \wedge R_\alpha(\bar{x}, \bar{y}) \Rightarrow u_i(\bar{x}, \bar{y}) \succ u_j(\bar{x}, r_\alpha(\bar{x}, \bar{y}))]$$

<u>Veta</u>: (Metóda dobre založených množín - Floyd)

Nech P je program špecifikovaný vstupným predikátom $\varphi(\bar{x})$. Zostrojme postupne:

1.) deliace bodu všetkých cyklov programu a dobre založenú množinu $(W, \prec)$

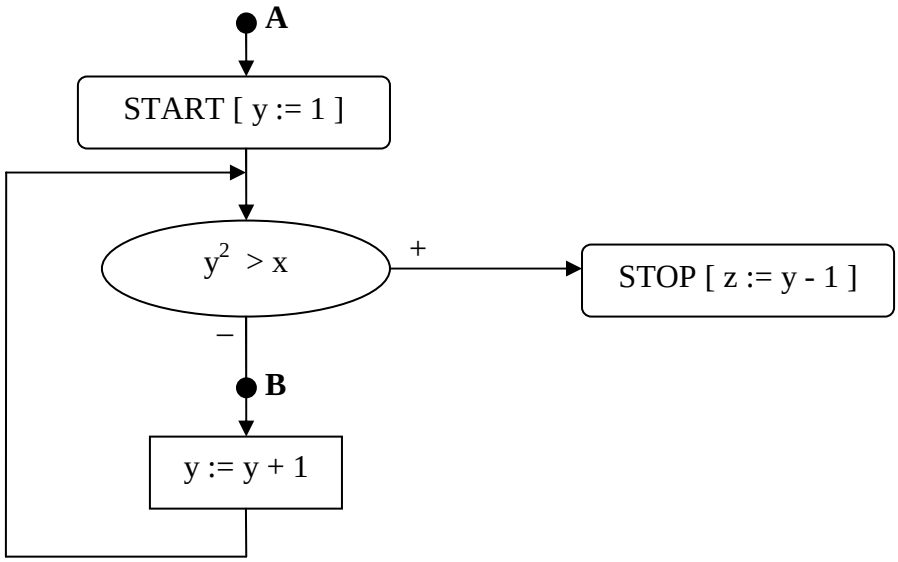
2.) ku každému deliacemu bodu „dobrý“ predikát

3.) ku každému deliacemu bodu „dobrú“ funkciu

4.) ku každej ceste z bodu i do nasledujúceho bodu j ležiacej v cykle podmienku ukončenia

Ak sú všetky podmienky ukončenia pravdivé, program P končí vzhľadom k φ.

<u>Príklad</u> (celočíselnej odmocniny x z úvodu):

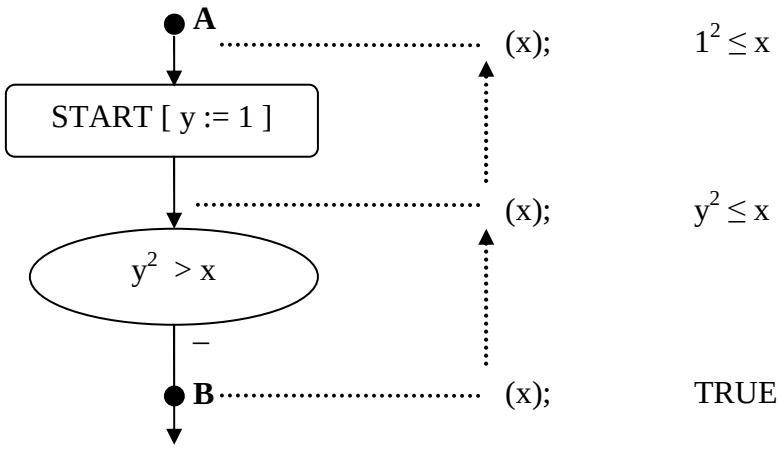


Krok 1: Deliace body: B. Dobre založená množina: množina prirodzených čísel **N** s prirodzeným usporiadaním <, t.j. (**N**,<).

Krok 2: $q_B(x,y) = y \geq 1$

Overíme, že q_B je dobrý predikát.

Spätná substitúcia pre cestu AB:



t.j. $R_{AB}(x) = 1 \le x$, $r_{AB}(x) = x$

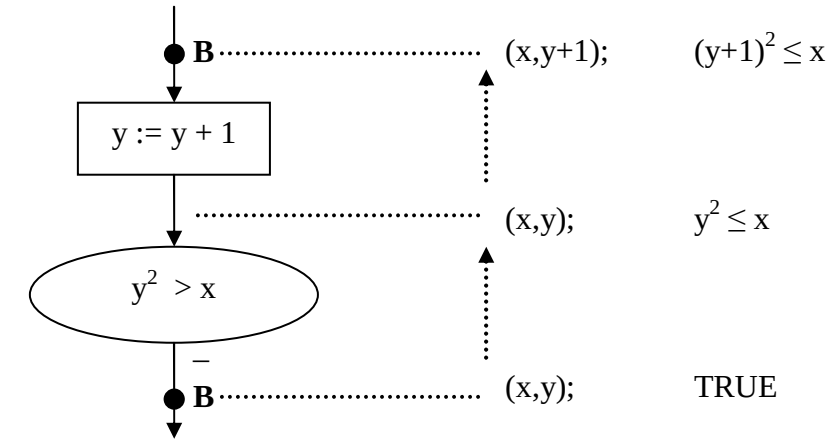
a platí

$$x \ge 1 \Rightarrow x \ge 1$$

$$x \ge 0 \wedge 1 \le x \Rightarrow x \ge 1$$

t.j. $\varphi(x) \wedge R_\alpha(x) \Rightarrow q_i(x, r_\alpha(x))$

Spätná substitúcia pre cestu BB:



t.j. $R_{BB}(x,y) = (y+1)^2 \le x$, $r_{BB}(x,y) = y+1$

a platí

$$y \ge 1 \Rightarrow y+1 \ge 1$$

$$y \ge 1 \wedge (y+1)^2 \le x \Rightarrow y+1 \ge 1$$

t.j. $q_B(x,y) \wedge R_{BB}(x,y) \Rightarrow q_B(x, r_{BB}(x,y))$

Teda $q_B(x,y)$ je dobrý predikát.

Krok 3: $u_B(x,y) = x - y^2$

Overiť, že u_B je dobrá funkcia, je triviálne, nakoľko pracujeme nad oborom prirodzených čísel, obyčajne sa ale táto skutočnosť v $\varphi(\bar{x})$ explicitne neuvádza, preto:

$$q_B(x,y) \Rightarrow u_B(x,y) \in \mathbf{N}$$

Krok 4: jediná cesta cyklu z bodu B do B:

Máme:

$R_{BB}(x,y) = (y+1)^2 \leq x$

$r_{BB}(x,y) = y+1$

podmienka ukončenia:

$$y \geq 1 \wedge (y+1)^2 \leq x \Rightarrow x - y^2 > x - (y+1)^2$$

Ukážme, že je pravdivá:

$$y \geq 1 \Rightarrow y^2 < (y+1)^2 \Rightarrow -y^2 > -(y+1)^2 \Rightarrow x - y^2 > x - (y+1)^2$$

$$y \geq 1 \Rightarrow x - y^2 > x - (y+1)^2$$

$$y \geq 1 \wedge (y+1)^2 \leq x \Rightarrow x - y^2 > x - (y+1)^2$$

$$\text{t.j. } q_B(x,y) \wedge R_{BB}(x,y) \Rightarrow u_B(x,y) > u_B(x,r_{BB}(x,y))$$

Všetky podmienky ukončenia sú pravdivé, preto podľa uvedenej vety program končí vzhľadom na $\varphi(x)$.

3 Vyriešený príklad

Zostrojiť a dokázať správnosť programu, ktorý na vstupe dostane súbor obsahujúci postupnosť reálnych čísel ukončený EOF. Dĺžka súboru nie je vstupnou informáciou. Výstupom programu je číslo, ktoré udáva počet maxím, za ktorými sa hneď nachádza minimum.

3.1 Špecifikácia

Vstupná podm.:

$$\varphi(f, F) = \omega(f, F) \wedge n \geq 2 \wedge F = 1$$

Výstupná podm.:

$$\psi(f, z, F) = \omega(f, F) \wedge F = n + 1 \wedge$$
$$(\exists mn)[1 \leq mn \leq n \wedge (\forall i)(1 \leq i \leq n \Rightarrow f_i \geq f_{mn})] \wedge$$
$$(\exists mx)[1 \leq mx \leq n \wedge (\forall i)(1 \leq i < n \Rightarrow f_i \leq f_{mx})] \wedge$$
$$(\exists z_1)(\exists z_2)...(\exists z_z)\ [(\forall i)(1 \leq i \leq z \Rightarrow (1 \leq z_i < n \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$$
$$\wedge (\forall j)((1 \leq j < n \wedge j \notin \{z_1,z_2,...,z_z\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$$

kde

$$\omega(f, F) = (\forall i)(1 \leq i \leq n \Rightarrow f_i \in R) \wedge f = (f_1 f_2 f_3 ... f_n) \wedge n \in N \wedge F \in N$$

Uvedomme si, že už pri špecifikovaní programu, pri zostrojovaní vstupných a výstupných podmienok, myslíme na dôkaz správnosti.

Výstupná podmienka totiž mohla byť definovaná napr. nasledovne:

$$\psi(f, z, F) = \omega(f, F) \wedge F = n + 1 \wedge$$
$$(\exists z_1)(\exists z_2)...(\exists z_z)[(\forall i)(1 \leq i \leq z \Rightarrow 1 \leq z_i < n \wedge (\forall j)(\ 1 \leq j \leq n \Rightarrow f_j \leq f_{zi} \wedge F_j \geq f_{zi+1}))$$
$$\wedge (\forall i)(1 \leq i \leq n \wedge i \notin \{z_1,z_2,...,z_z\} \Rightarrow (\exists j)(\ 1 \leq j \leq n \wedge (f_j > f_i \wedge f_j < f_{i+1})))]$$

Navyše sa zdá byť táto definícia úspornejšia. Prečo sme teda výstupnú podmienku definovali tak ako sme ju definovali?

Myslime na dôkaz implikácií tvaru

$$A_1 \wedge A_2 \wedge ... \wedge A_n \Rightarrow B_1 \wedge B_2 \wedge ... \wedge B_m$$

v ktorom budú všetky verifikačné podmienky uvedeného programu.

Dôkaz takejto implikácie sa ľahšie zostrojuje a je názornejší v prípade, že členy konjunkcie sú čo najjednoduchšie formuly. Často bude

$$A_i \Leftrightarrow B_j$$

alebo

$$A_i \wedge A_j \Rightarrow B_k$$

príp. A_i bude rovnosť zhodných termov.

Z tohto dôvodu sme zvolili radšej výstupný predikát z piatimi jednoduchšími formulami v konjunkcii ako úspornejší predikát z tromi formulami, ale s jednou veľmi zložitou.

3.2 Program

Najjednoduchší postup, ktorý nás obyčajne napadne prvý, je nájsť najprv minimum a maximum a potom počet maxím, za ktorými sa hneď nachádza minimum. Ilustrujeme aj tento postup, ale kompletný dôkaz prevedieme na inom, ktorý vráti výsledok po jedinom prečítaní vstupného súboru.

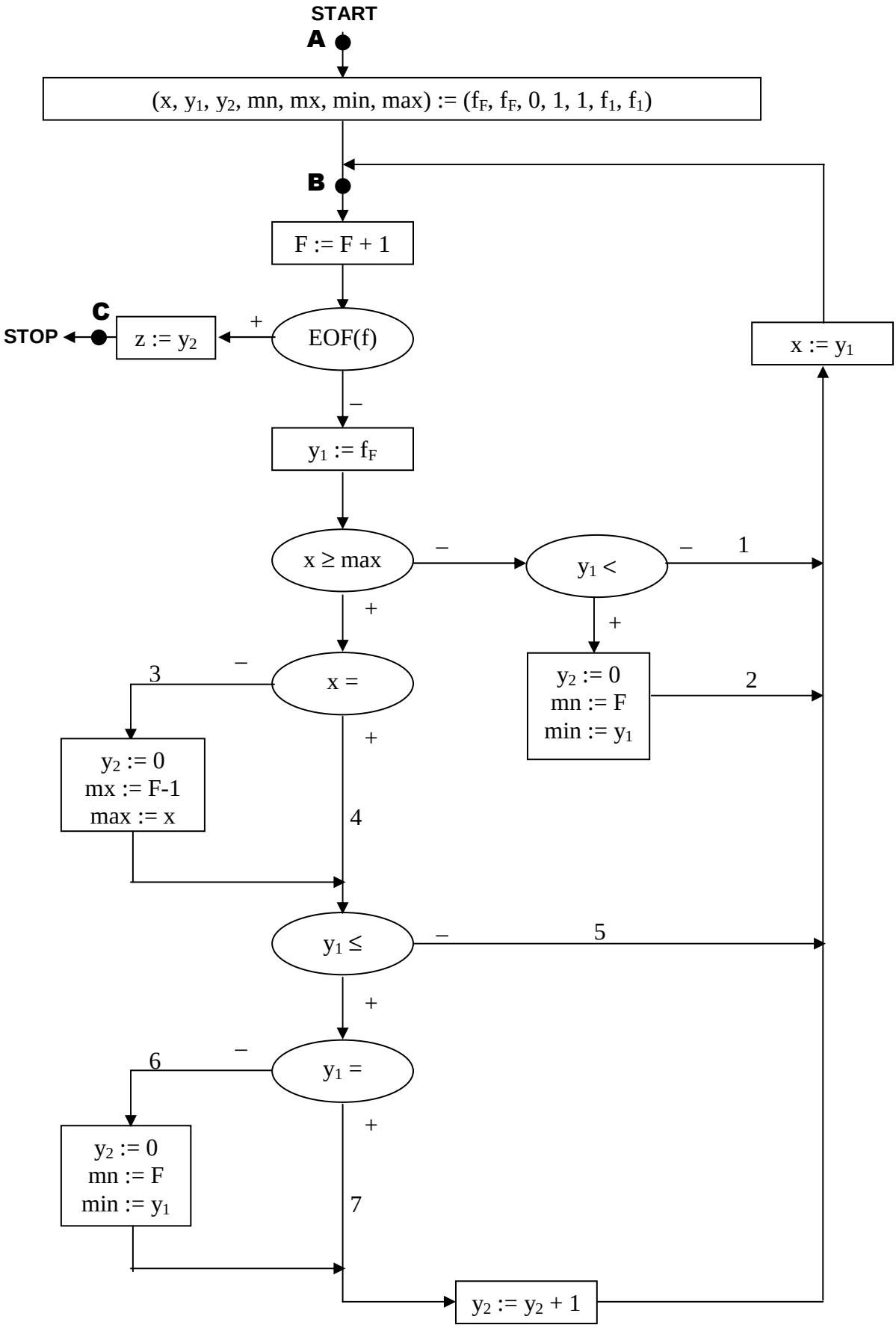
Možné sú aj ďalšie prístupy, napríklad najprv nájsť minimum, potom maximum a potom počet maxím, za ktorými sa hneď nachádza minimum. My vyberieme tieto dva prístupy:

1. Na dva prechody: v prvom nájsť minimum aj maximum, v druhom počet maxím, za ktorými sa hneď nachádza minimum
2. Na jeden prechod vrátiť hneď počet maxím, za ktorými sa hneď nachádza minimum

Kompletný dôkaz správnosti ukážeme v 1. postupe.

Na záver porovnáme obidva prístupy a to ako z hľadiska efektívnosti programu a programovania, tak, a to najmä, z hľadiska obtiažnosti dôkazu správnosti

3.3 Prvý prístup



P o z n á m k a (návod ako čítať dôkaz):

Dokazujú sa vždy implikácie tvaru $A_1 \wedge A_2 \wedge ... \wedge A_n \Rightarrow B_1 \wedge B_2 \wedge ... \wedge B_m$,

t.j. obidve strany sú vždy konjunkcie určitých formulí, preto dôkaz prebieha v krokoch, v každom sa dokáže vždy jedna formula B_i. Nedokazujeme tie formule B_i, ktoré

- ✓ sú rovnosťou dvoch zhodných termov, t.j. majú tvar $t(\bar{x}, \bar{y}) = t(\bar{x}, \bar{y})$, tieto triv. platia
- ✓ patria medzi predpoklady, t.j. $(\exists j)(1 \leq j \leq n \wedge A_j = B_i)$

3.3.1 Čiastočná správnosť

K r o k 1: Deliace body: A, B, C

K r o k 2: Induktívne podmienky k deliacim bodom:

A – vstupná podm. $\varphi(f, F)$

B – $p_B(f,x,y_1,y_2,mn,mx,min,max,F) = \omega(f, F) \wedge F \leq n \wedge$

$max = f_{mx} \wedge min = f_{mn} \wedge x=f_F \wedge y_1=f_F \wedge$

$1 \leq mx \leq F \wedge (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge$

$1 \leq mn \leq F \wedge (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn}) \wedge$

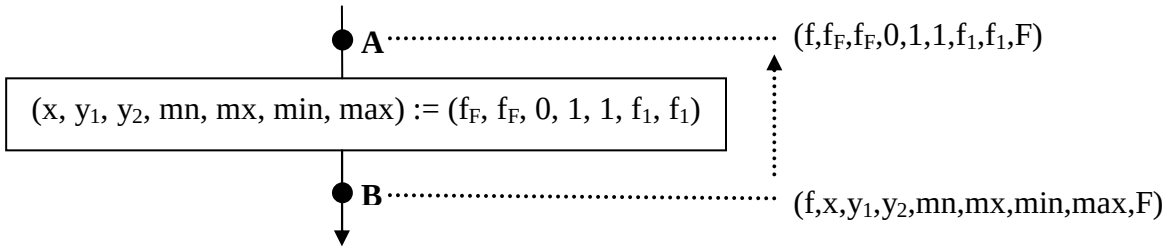
$(\exists z_1)(\exists z_2)...(\exists z_{y2})\ [(\forall i)(1 \leq i \leq y_2 \Rightarrow (1 \leq z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn})) \wedge$

$(\forall j)((1 \leq j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$

C – výstupná podm. $\psi(f, z, F)$

K r o k 3: Verifikačné podmienky:

- cesta α (z bodu A do B):



verifikačná podmienka: $\varphi(f, F) \Rightarrow p_B(f,f_F,f_F,0,1,1,f_1,f_1,F)$

Pretože platí:

1.) $F = 1 \wedge n \geq 2 \Rightarrow F \leq n$

2.) $F = 1 \Rightarrow 1 \leq F$

3.) $F = 1 \Rightarrow (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_1)$, nakoľko formula $1 \leq i < 1$ je vždy nepravda

4.) $F = 1 \Rightarrow (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_1)$, nakoľko $f_1 \geq f_1$

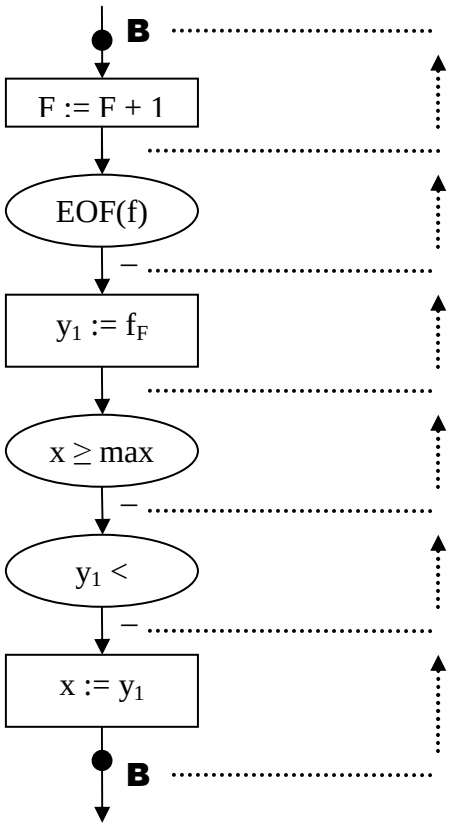
platí aj:

$\omega(f, F) \wedge n \geq 2 \wedge F = 1 \Rightarrow \omega(f, F) \wedge F \leq n \wedge f_1 = f_1 \wedge f_1 = f_1 \wedge f_F = f_F \wedge f_F = f_F \wedge$

$1 \leq 1 \leq F \wedge (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_1) \wedge 1 \leq 1 \leq F \wedge (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_1)$

t.j. verifikačná podmienka.

- cesta β_1 (z bodu B do B hranou 1):



$(f,f_{F+1},f_{F+1},y_2,mn,mx,min,max,F+1)$
$f_{F+1} \geq min \wedge x < max \wedge F + 1 \leq n$

$(f,f_F,f_F,y_2,mn,mx,min,max,F)$
$f_F \geq min \wedge x < max \wedge F \leq n$

$(f,f_F,f_F,y_2,mn,mx,min,max,F);$
$f_F \geq min \wedge x < max$

$(f,y_1,y_1,y_2,mn,mx,min,max,F);$
$y_1 \geq min \wedge x < max$

$(f,y_1,y_1,y_2,mn,mx,min,max,F);$ $y_1 \geq min$

$(f,y_1,y_1,y_2,mn,mx,min,max,F);$ TRUE

$(f,x,y_1,y_2,mn,mx,min,max,F);$ TRUE

verifikačná podmienka:

$p_B(f,x,y_1,y_2,mn,mx,min,max,F) \wedge f_{F+1} \geq min \wedge x < max \wedge F + 1 \leq n$

$\Rightarrow p_B(f,f_{F+1},f_{F+1},y_2,mn,mx,min,max,F+1)$

Pretože platí:

1.) $1 \leq mx \leq F \Rightarrow 1 \leq mx \leq F+1$

2.) $1 \leq mn \leq F \Rightarrow 1 \leq mn \leq F+1$

3.) $(\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge x < max \wedge x = f_F \wedge max = f_{mx}$

$\Rightarrow (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge f_F < f_{mx} \Rightarrow (\forall i)(1 \leq i < F+1 \Rightarrow f_i \leq f_{mx})$

4.) $(\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn}) \wedge f_{F+1} \geq min \wedge min = f_{mn}$

$\Rightarrow (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn}) \wedge f_{F+1} \geq f_{mn} \Rightarrow (\forall i)(1 \leq i \leq F+1 \Rightarrow f_i \geq f_{mn})$

5.) $(\exists z_1)(\exists z_2)...(\exists z_{y2})\ [(\forall i)(1 \leq i \leq y2 \Rightarrow (1 \leq z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \leq j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$,

nech sa $z_1,z_2...,z_{y2}$ nezmení,

a pretože platí $1 \leq z_i < F \Rightarrow 1 \leq z_i < F+1$

a tiež $x < max \wedge x = f_F \wedge max = f_{mx} \Rightarrow f_F < f_{mx} \Rightarrow f_F \neq f_{mx}$

teda $(\exists z_1)(\exists z_2)... (\exists z_{y2})\ [(\forall i)(1 \leq i \leq y2 \Rightarrow (1 \leq z_i < F+1 \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \leq j < F+1 \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$

platí aj:

$\omega(f, F) \wedge F \leq n \wedge max = f_{mx} \wedge min = f_{mn} \wedge x = f_F \wedge y_1 = f_F \wedge$

$1 \leq mx \leq F \wedge (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge 1 \leq mn \leq F \wedge (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn})$

$\wedge (\exists z_1)(\exists z_2)...(\exists z_{y2})\ [(\forall i)(1 \leq i \leq y_2 \Rightarrow (1 \leq z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \leq j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$

$\wedge f_{F+1} \geq min \wedge x < max \wedge F + 1 \leq n$

$\Rightarrow$

$\omega(f, F) \wedge F+1 \leq n \wedge max = f_{mx} \wedge min = f_{mn} \wedge f_{F+1}=f_{F+1} \wedge f_{F+1}=f_{F+1}$

$\wedge 1 \leq mx \leq F+1 \wedge (\forall i)(1 \leq i < F+1 \Rightarrow f_i \leq f_{mx})$

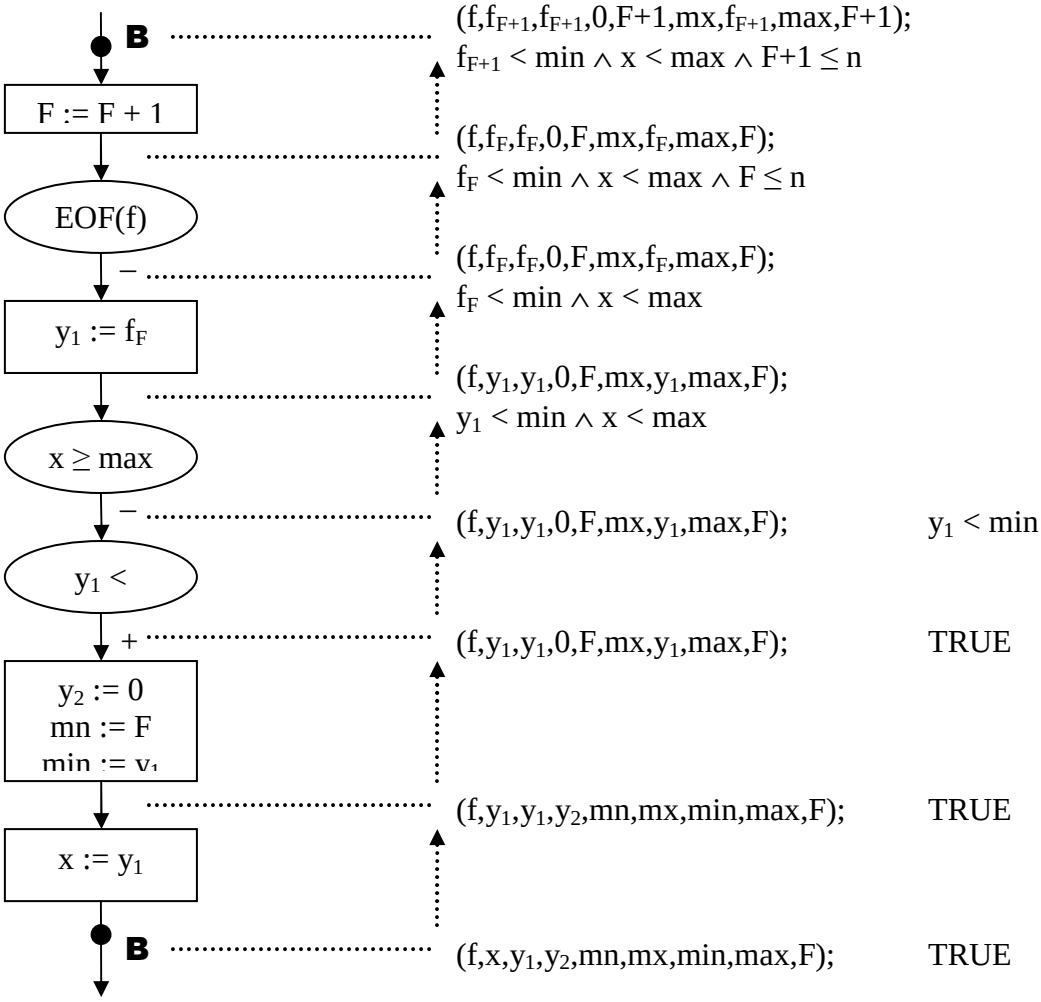
$\wedge 1 \leq mn \leq F+1 \wedge (\forall i)(1 \leq i \leq F+1 \Rightarrow f_i \geq f_{mn})$

$\wedge (\exists z_1)(\exists z_2)...(\exists z_{y2})\ [(\forall i)(1 \leq i \leq y_2 \Rightarrow (1 \leq z_i < F+1 \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \leq j < F+1 \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$

a to je verifikačná podmienka

- cesta β_2 (z B do B hranou 2):



verifikačná podmienka:

$p_B(f,x,y_1,y_2,mn,mx,min,max,F) \wedge f_{F+1} < min \wedge x < max \wedge F + 1 \le n$

$\Rightarrow\ p_B(f,f_{F+1},f_{F+1},0,F+1,mx,f_{F+1},max,F+1)$

Pretože platí:

1.) $1 \le mx \le F \ \Rightarrow\ 1 \le mx \le F+1$

2.) $1 \le mn \le F \ \Rightarrow\ 1 \le F$

3.) $(\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge x < max \wedge x = f_F \wedge max = f_{mx}$

$\Rightarrow\ (\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge f_F < f_{mx} \ \Rightarrow\ (\forall i)(1 \le i < F+1 \Rightarrow f_i \le f_{mx})$

4.) $(\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn}) \wedge f_{F+1} < min \wedge min = f_{mn}$

$\Rightarrow (\forall i)(1 \le i \le F \Rightarrow f_i > f_{mn}) \wedge f_{mn} > f_{F+1} \wedge f_{F+1} \ge f_{F+1}$

$\Rightarrow (\forall i)(1 \le i \le F+1 \Rightarrow f_i \ge f_{F+1})$

platí aj:

$\omega(f, F) \wedge F \leq n \wedge max = f_{mx} \wedge min = f_{mn} \wedge x = f_F \wedge y_1 = f_F \wedge$

$1 \leq mx \leq F \wedge (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge 1 \leq mn \leq F \wedge (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn})$

$\Rightarrow$

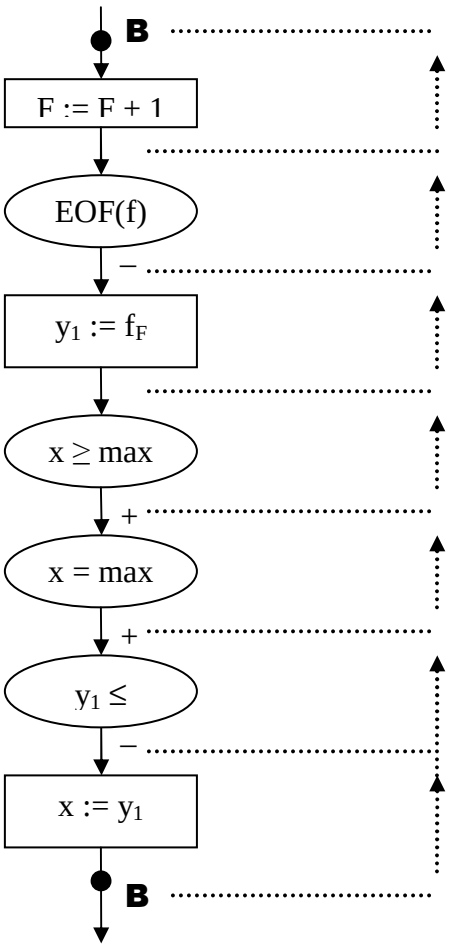
$\omega(f, F) \wedge F+1 \leq n \wedge max = f_{mx} \wedge f_{F+1} = f_{F+1} \wedge f_{F+1}=f_{F+1} \wedge f_{F+1}=f_{F+1}$

$\wedge 1 \leq mx \leq F+1 \wedge (\forall i)(1 \leq i < F+1 \Rightarrow f_i \leq f_{mx})$

$\wedge 1 \leq F+1 \leq F+1 \wedge (\forall i)(1 \leq i \leq F+1 \Rightarrow f_i \geq f_{F+1})$

a to je verifikačná podmienka.

- cesta β_{45} (z B do B hranami 4 a 5):



$(f,f_{F+1},f_{F+1},y_2,mn,mx,min,max,F+1);$
$f_{F+1} > min \wedge x = max \wedge x \geq max \wedge F+1 \leq n$

$(f,f_F,f_F,y_2,mn,mx,min,max,F);$
$f_F > min \wedge x = max \wedge x \geq max \wedge F \leq n$

$(f,f_F,f_F,y_2,mn,mx,min,max,F);$
$f_F > min \wedge x = max \wedge x \geq max$

$(f,y_1,y_1,y_2,mn,mx,min,max,F);$
$y_1 > min \wedge x = max \wedge x \geq max$

$(f,y_1,y_1,y_2,mn,mx,min,max,F);$
$y_1 > min \wedge x = max$

$(f,y_1,y_1,y_2,mn,mx,min,max,F);$ $y_1 > min$

$(f,y_1,y_1,y_2,mn,mx,min,max,F);$ TRUE

$(f,x,y_1,y_2,mn,mx,min,max,F);$ TRUE

verifikačná podmienka:

$p_B(f,x,y_1,y_2,mn,mx,min,max,F) \wedge f_{F+1} > min \wedge x = max \wedge x \geq max \wedge F + 1 \leq n$

$\Rightarrow p_B(f,f_{F+1},f_{F+1},y_2,mn,mx,min,max,F+1)$

Pretože platí:

1.) $1 \leq mx \leq F \Rightarrow 1 \leq mx < F+1$

2.) $1 \leq mn \leq F \Rightarrow 1 \leq mn \leq F+1$

3.) $(\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge x = max \wedge x = f_F \wedge max = f_{mx}$

$\Rightarrow\ (\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge f_F = f_{mx}\ \Rightarrow\ (\forall i)(1 \le i < F+1 \Rightarrow f_i \le f_{mx})$

4.) $(\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn}) \wedge f_{F+1} > min \wedge min = f_{mn}$

$\Rightarrow (\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn}) \wedge f_{F+1} > f_{mn}\ \Rightarrow\ (\forall i)(1 \le i \le F+1 \Rightarrow f_i \ge f_{mn})$

5.) $(\exists z_1)(\exists z_2)...(\exists z_{y2})\ [(\forall i)(1 \le i \le y2 \Rightarrow (1 \le z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \le j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \ne f_{mx} \vee f_{j+1} \ne f_{mn}))]$,

nech sa $z_1,z_2...,z_{y2}$ nezmení,

a pretože $1 \le z_i < F\ \Rightarrow\ 1 \le z_i < F+1$

a tiež $f_{F+1} > min \wedge min = f_{mn}\ \Rightarrow\ f_{F+1} > f_{mn}\ \Rightarrow\ f_{F+1} \ne f_{mn}$

teda $(\exists z_1)(\exists z_2)...(\exists z_{y2})\ [(\forall i)(1 \le i \le y2 \Rightarrow (1 \le z_i < F+1 \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \le j < F+1 \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \ne f_{mx} \vee f_{j+1} \ne f_{mn}))]$

platí aj:

$\omega(f, F) \wedge F \le n \wedge max = f_{mx} \wedge min = f_{mn} \wedge x = f_F \wedge y_1 = f_F \wedge$

$1 \le mx \le F \wedge (\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge 1 \le mn \le F \wedge (\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn})$

$\wedge (\exists z_1)(\exists z_2)...(\exists z_{y2})[(\forall i)(1 \le i \le y_2 \Rightarrow (1 \le z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \le j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \ne f_{mx} \vee f_{j+1} \ne f_{mn}))]$

$\wedge f_{F+1} > min \wedge x = max \wedge x \ge max \wedge F + 1 \le n$

$\Rightarrow$

$\omega(f, F) \wedge F+1 \le n \wedge max = f_{mx} \wedge min = f_{mn} \wedge f_{F+1}=f_{F+1} \wedge f_{F+1}=f_{F+1}$

$\wedge\ 1 \le mx \le F+1 \wedge (\forall i)(1 \le i < F+1 \Rightarrow f_i \le f_{mx})$

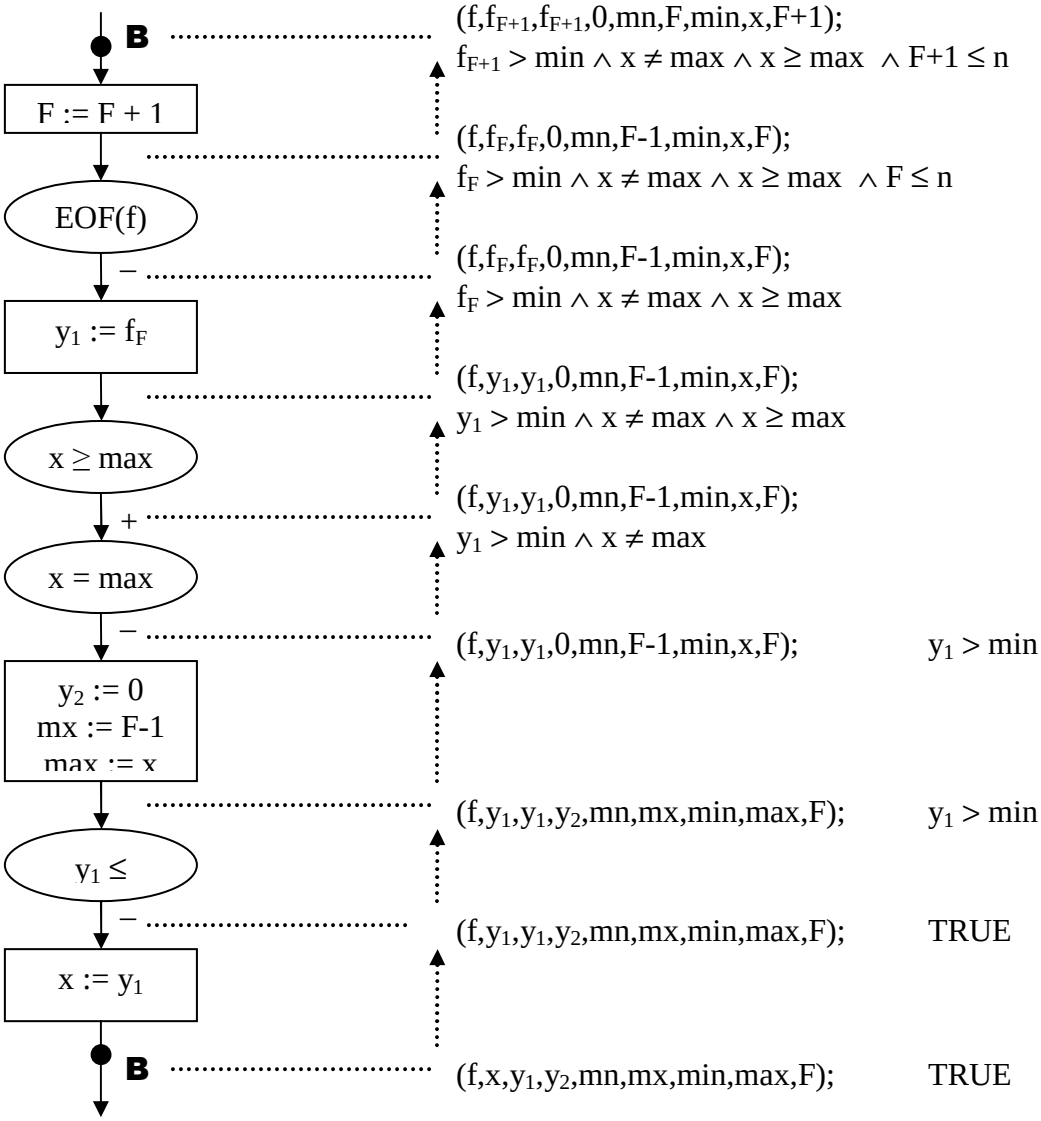
$\wedge\ 1 \le mn \le F+1 \wedge (\forall i)(1 \le i \le F+1 \Rightarrow f_i \ge f_{mn})$

$\wedge (\exists z_1)(\exists z_2)...(\exists z_{y2})[(\forall i)(1 \le i \le y_2 \Rightarrow (1 \le z_i < F+1 \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \le j < F+1 \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \ne f_{mx} \vee f_{j+1} \ne f_{mn}))]$

a to je verifikačná podmienka.

- cesta β_{35} (z B do B hranami 3 a 5):



verifikačná podmienka:

$p_B(f,x,y_1,y_2,mn,mx,min,max,F) \wedge f_{F+1} > min \wedge x \neq max \wedge x \geq max \wedge F+1 \leq n$

$\Rightarrow p_B(f,f_{F+1},f_{F+1},0,mn,F,min,x,F+1)$

Pretože platí:

1.) $1 \leq mx \leq F \Rightarrow 1 \leq F$

2.) $1 \leq mn \leq F \Rightarrow 1 \leq mn \leq F+1$

3.) $(\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge x \geq max \wedge x = f_F \wedge max = f_{mx}$

$\Rightarrow (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge f_{mx} \leq f_F \wedge f_F \leq f_F \Rightarrow (\forall i)(1 \leq i < F+1 \Rightarrow f_i \leq f_F)$

4.) $(\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn}) \wedge f_{F+1} > min \wedge min = f_{mn}$

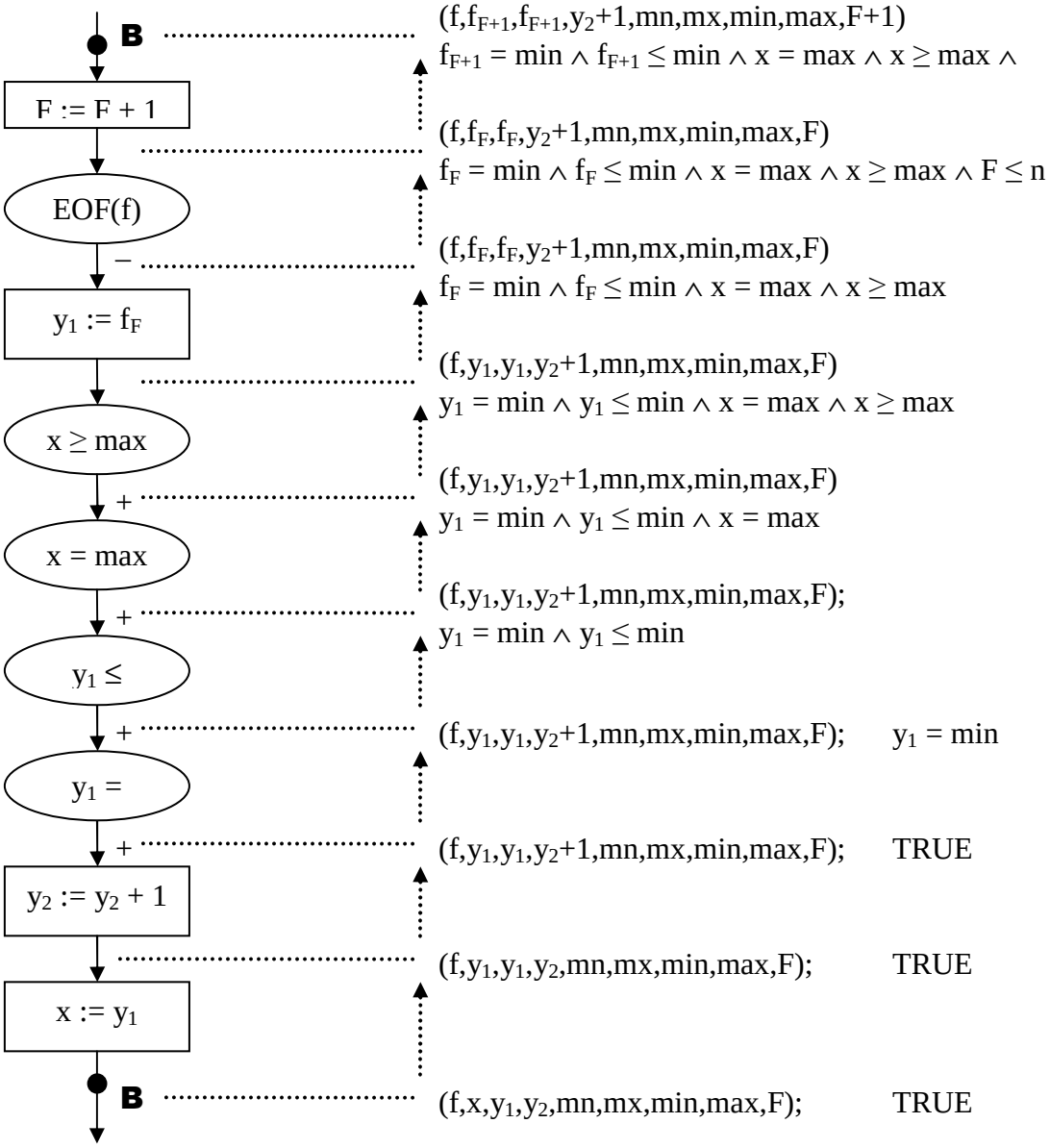
$$\Rightarrow (\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn}) \wedge f_{F+1} > f_{mn} \;\Rightarrow\; (\forall i)(1 \le i \le F+1 \Rightarrow f_i \ge f_{mn})$$

platí aj:

$$\omega(f, F) \wedge F \le n \wedge max = f_{mx} \wedge min = f_{mn} \wedge x = f_F \wedge y_1 = f_F \wedge$$
$$1 \le mx \le F \wedge (\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge 1 \le mn \le F \wedge (\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn})$$
$$\Rightarrow$$
$$\omega(f, F) \wedge F+1 \le n \wedge x = f_F \wedge min = f_{mn} \wedge f_{F+1}=f_{F+1} \wedge f_{F+1}=f_{F+1}$$
$$\wedge\ 1 \le F \le F+1 \wedge (\forall i)(1 \le i < F+1 \Rightarrow f_i \le f_F)$$
$$\wedge\ 1 \le mn \le F+1 \wedge (\forall i)(1 \le i \le F+1 \Rightarrow f_i \ge f_{mn})$$

a teda platí verifikačná podmienka

- cesta β_{47} (z B do B hranami 4 a 7):



verifikačná podmienka:

$p_B(f,x,y_1,y_2,mn,mx,min,max,F)$

$\wedge\ f_{F+1} = min \wedge f_{F+1} \leq min \wedge x = max \wedge x \geq max \wedge F+1 \leq n$

$\Rightarrow\ p_B(f,f_{F+1},f_{F+1},y_2+1,mn,mx,min,max,F+1)$

Pretože platí:

1.) $1 \leq mx \leq F\ \Rightarrow\ 1 \leq mx < F+1$

2.) $1 \leq mn \leq F\ \Rightarrow\ 1 \leq mn \leq F+1$

3.) $(\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge x = max \wedge x = f_F \wedge max = f_{mx}$

$\Rightarrow\ (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge f_F = f_{mx}\ \Rightarrow\ (\forall i)(1 \leq i < F+1 \Rightarrow f_i \leq f_{mx})$

4.) $(\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn}) \wedge f_{F+1} = min \wedge min = f_{mn}$

$\Rightarrow (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn}) \wedge f_{F+1} = f_{mn}\ \Rightarrow\ (\forall i)(1 \leq i \leq F+1 \Rightarrow f_i \geq f_{mn})$

5.) $(\exists z_1)(\exists z_2)...(\exists z_{y2})\ [(\forall i)(1 \leq i \leq y2 \Rightarrow (1 \leq z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge\ (\forall j)((1 \leq j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$,

nech sa $z_1,z_2...,z_{y2}$ nezmení a položme $z_{y2+1} = F$

máme: $1 \leq z_i < F\ \Rightarrow\ 1 \leq z_i < F+1$

$1 \leq mx \leq F\ \Rightarrow\ 1 \leq F\ \Rightarrow\ 1 \leq z_{y2+1}$

$F < F+1\ \Rightarrow\ z_{y2+1} < F+1$

$x = max \wedge x = f_F \wedge max = f_{mx}\ \Rightarrow\ f_F = f_{mx}\ \Rightarrow\ f_{zy2+1} = f_{mx}$

$f_{F+1} = min \wedge min = f_{mn}\ \Rightarrow\ f_{F+1} = f_{mn}\ \Rightarrow\ f_{zy2+1+1} = f_{mn}$

spolu: $1 \leq z_{y2+1} < F+1 \wedge f_{zy2+1} = f_{mx} \wedge f_{zy2+1+1} = f_{mn}$

a tiež: $(\forall j)((1 \leq j < F+1 \wedge j \notin \{z_1, z_2, \dots, z_{y2}, F\})$

$\Rightarrow 1 \leq j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\} \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))$

teda $(\exists z_1)(\exists z_2)...(\exists z_{y2})(\exists z_{y2+1})\ [(\forall i)(1 \leq i \leq y_2+1 \Rightarrow (1 \leq z_i < F+1 \wedge f_{zi}=f_{mx} \wedge f_{zi+1}=f_{mn}))$

$\wedge\ (\forall j)((1 \leq j < F+1 \wedge j \notin \{z_1,z_2,...,z_{y2},z_{y2+1}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$

platí aj:

$\omega(f, F) \wedge F \leq\ n \wedge max = f_{mx} \wedge min = f_{mn} \wedge x = f_F \wedge y_1 = f_F \wedge$

$1 \leq mx \leq F \wedge (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge 1 \leq mn \leq F \wedge (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn})$

$\wedge\ (\exists z_1)(\exists z_2)...\ (\exists z_{y2})\ [(\forall i)(1 \leq i \leq y_2 \Rightarrow (1 \leq z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge\ (\forall j)((1 \leq j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$

$\wedge\ f_{F+1} = min \wedge f_{F+1} \leq min \wedge x = max \wedge x \geq max \wedge F+1 \leq n$

$\Rightarrow$

$\omega(f, F) \wedge F+1 \leq\ n \wedge max = f_{mx} \wedge min = f_{mn} \wedge f_{F+1}=f_{F+1} \wedge f_{F+1}=f_{F+1}$

$\wedge\ 1 \le mx \le F+1 \wedge (\forall i)(1 \le i < F+1 \Rightarrow f_i \le f_{mx})$

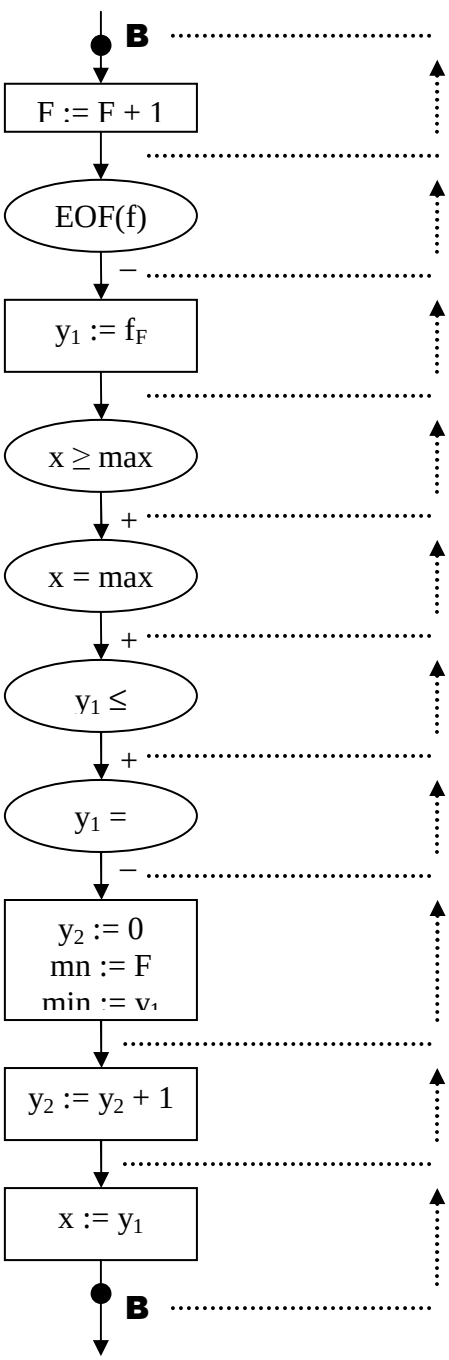
$\wedge\ 1 \le mn \le F+1 \wedge (\forall i)(1 \le i \le F+1 \Rightarrow f_i \ge f_{mn})$

$\wedge\ (\exists z_1)(\exists z_2)...(\exists z_{y2})(\exists z_{y2+1})\ [(\forall i)(1 \le i \le y_2+1 \Rightarrow (1 \le z_i < F+1 \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge\ (\forall j)((1 \le j < F+1 \wedge j \notin \{z_1,z_2,...,z_{y2},z_{y2+1}\}) \Rightarrow (f_j \ne f_{mx} \vee f_{j+1} \ne f_{mn}))]$

a to je verifikačná podmienka

- cesta β_{46} (z B do B hranami 4 a 6):



(f,f_{F+1},f_{F+1},1,F+1,mx,f_{F+1},max,F+1);
$f_{F+1} \ne min \wedge f_{F+1} \le min \wedge x = max \wedge x \ge max \wedge$

(f,f_F,f_F,1,F,mx,f_F,max,F);
$f_F \ne min \wedge f_F \le min \wedge x = max \wedge x \ge max \wedge F \le n$

(f,f_F,f_F,1,F,mx,f_F,max,F);
$f_F \ne min \wedge f_F \le min \wedge x = max \wedge x \ge max$

(f,y_1,y_1,1,F,mx,y_1,max,F);
$y_1 \ne min \wedge y_1 \le min \wedge x = max \wedge x \ge max$

(f,y_1,y_1,1,F,mx,y_1,max,F);
$y_1 \ne min \wedge y_1 \le min \wedge x = max$

(f,y_1,y_1,1,F,mx,y_1,max,F);
$y_1 \ne min \wedge y_1 \le min$

(f,y_1,y_1,1,F,mx,y_1,max,F); $y_1 \ne min$

(f,y_1,y_1,0+1,F,mx,y_1,max,F); TRUE

(f,y_1,y_1,y_2+1,mn,mx,min,max,F); TRUE

(f,y_1,y_1,y_2,mn,mx,min,max,F); TRUE

(f,x,y_1,y_2,mn,mx,min,max,F); TRUE

verifikačná podmienka:

$p_B(f,x,y_1,y_2,mn,mx,min,max,F)$

$\wedge\ f_{F+1} \neq min \wedge f_{F+1} \leq min \wedge x = max \wedge x \geq max \wedge F+1 \leq n$

$\Rightarrow\ p_B(f,f_{F+1},f_{F+1},1,F+1,mx,f_{F+1},max,F+1)$

Pretože platí:

1.) $1 \leq mx \leq F \ \Rightarrow\ 1 \leq mx < F+1$

2.) $(\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge x = max \wedge x = f_F \wedge max = f_{mx}$

$\Rightarrow\ (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge f_F = f_{mx}\ \Rightarrow\ (\forall i)(1 \leq i < F+1 \Rightarrow f_i \leq f_{mx})$

3.) $(\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn}) \wedge min = f_{mn} \wedge min \geq f_{F+1}$

$\Rightarrow\ (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn}) \wedge f_{mn} \geq f_{F+1}\ \Rightarrow\ (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{F+1})$

4.) $(\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{F+1}) \wedge f_{F+1} \geq f_{F+1}\ \Rightarrow\ (\forall i)(1 \leq i \leq F+1 \Rightarrow f_i \geq f_{F+1})$

5.) položme $z_1 = F$

máme: $1 \leq mx \leq F\ \Rightarrow\ 1 \leq F$

$x = max \wedge x = f_F \wedge max = f_{mx}\ \Rightarrow\ f_F = f_{mx}$

$(\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn})\ \Rightarrow\ (\forall j)(1 \leq j < F+1 \Rightarrow f_j \geq f_{mn})$

$(\forall j)(1 \leq j < F+1 \Rightarrow f_j \geq f_{mn}) \wedge f_{F+1} \neq min \wedge f_{F+1} \leq min \wedge min = f_{mn}$

$\Rightarrow\ (\forall j)(1 \leq j < F+1 \Rightarrow f_j \geq f_{mn}) \wedge f_{mn} > f_{F+1}$

$\Rightarrow\ (\forall j)(1 \leq j < F+1 \Rightarrow f_j \geq f_{F+1})$

$\Rightarrow\ (\forall j)(1 \leq j < F \Rightarrow f_{j+1} \geq f_{F+1})$

$\Rightarrow\ (\forall j)(1 \leq j < F+1 \wedge j \notin \{F\} \Rightarrow f_{j+1} \geq f_{F+1})$

spolu: $[(\forall i)(1 \leq i \leq 1 \Rightarrow (1 \leq F < F+1 \wedge f_F=f_{mx} \wedge f_{F+1}=f_{F+1}))$

$\wedge (\forall j)((1 \leq j < F+1 \wedge j \notin \{F\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{F+1}))]$

teda $(\exists z_1)\ [(\forall i)(1 \leq i \leq 1 \Rightarrow (1 \leq z_i < F+1 \wedge f_{zi}=f_{mx} \wedge f_{zi+1}=f_{F+1}))$

$\wedge (\forall j)((1 \leq j < F+1 \wedge j \notin \{z_1\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{F+1}))]$

platí aj:

$\omega(f, F) \wedge F \leq n \wedge max = f_{mx} \wedge min = f_{mn} \wedge x = f_F \wedge y_1 = f_F \wedge$

$1 \leq mx \leq F \wedge (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge 1 \leq mn \leq F \wedge (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn})$

$\wedge (\exists z_1)(\exists z_2)... (\exists z_{y2})\ [(\forall i)(1 \leq i \leq y_2 \Rightarrow (1 \leq z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \leq j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$

$\wedge f_{F+1} \neq min \wedge f_{F+1} \leq min \wedge x = max \wedge x \geq max \wedge F+1 \leq n$

$\Rightarrow$

$\omega(f, F) \wedge F+1 \leq n \wedge max = f_{mx} \wedge f_{F+1} = f_{F+1} \wedge f_{F+1}=f_{F+1} \wedge f_{F+1}=f_{F+1}$

$\wedge\ 1 \le mx \le F+1 \wedge (\forall i)(1 \le i < F+1 \Rightarrow f_i \le f_{mx})$

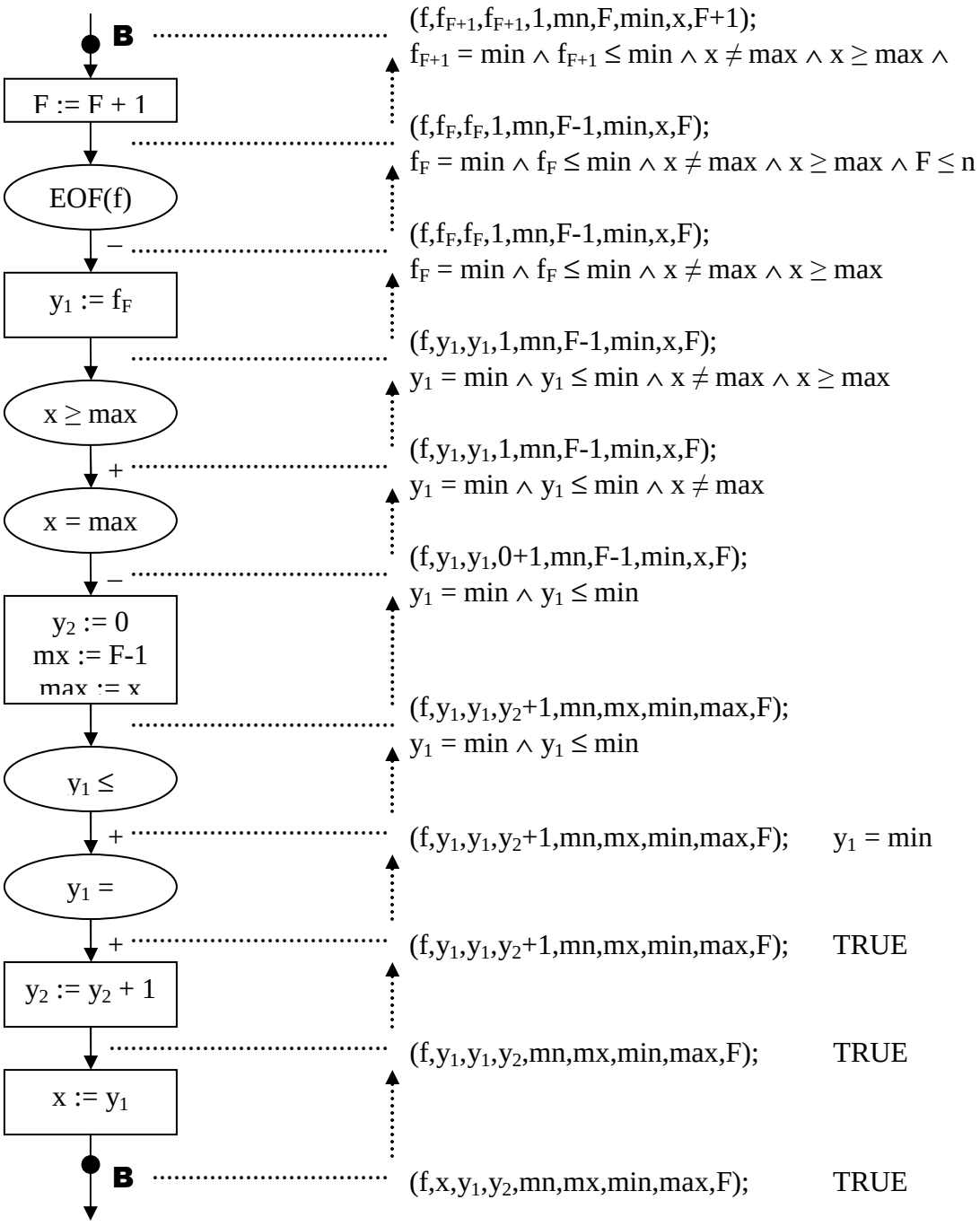
$\wedge\ 1 \le F+1 \le F+1 \wedge (\forall i)(1 \le i \le F+1 \Rightarrow f_i \ge f_{F+1})$

$\wedge\ (\exists z_1)\ [(\forall i)(1 \le i \le 1 \Rightarrow (1 \le z_i < F+1 \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{F+1}))$

$\wedge\ (\forall j)((1 \le j < F+1 \wedge j \notin \{z_1\}) \Rightarrow (f_j \ne f_{mx} \vee f_{j+1} \ne f_{F+1}))]$

a to je verifikačná podmienka.

- cesta β_{37} (z B do B hranami 3 a 7):



verifikačná podmienka:

$p_B(f,x,y_1,y_2,mn,mx,min,max,F)$

$\wedge\ f_{F+1} = min \wedge f_{F+1} \le min \wedge x \ne max \wedge x \ge max \wedge F+1 \le n$

$\Rightarrow\ p_B(f,f_{F+1},f_{F+1},1,mn,F,min,x,F+1)$

Pretože platí:

1.) $1 \le mx \le F \ \Rightarrow\ 1 \le F$

2.) $1 \le mn \le F \ \Rightarrow\ 1 \le mn \le F+1$

3.) $(\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge x \ge max \wedge x = f_F \wedge max = f_{mx}$

$\Rightarrow\ (\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge f_{mx} \le f_F \ \Rightarrow\ (\forall i)(1 \le i < F \Rightarrow f_i \le f_F)$

$(\forall i)(1 \le i < F \Rightarrow f_i \le f_F) \wedge f_F \le f_F \ \Rightarrow\ (\forall i)(1 \le i < F+1 \Rightarrow f_i \le f_F)$

4.) $(\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn}) \ \wedge f_{F+1} = min \wedge min = f_{mn}$

$\Rightarrow\ (\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn}) \ \wedge f_{F+1} = f_{mn} \ \Rightarrow\ (\forall i)(1 \le i \le F+1 \Rightarrow f_i \ge f_{mn})$

5.) položme $z_1 = F$

máme: $1 \le mx \le F \ \Rightarrow\ 1 \le F$

$f_{F+1} = min \wedge min = f_{mn} \Rightarrow\ f_{F+1} = f_{mn}$

$(\forall j)(1 \le j < F \Rightarrow f_j \le f_{mx}) \wedge x \ne max \wedge x \ge max$

$\Rightarrow\ (\forall j)(1 \le j < F \Rightarrow f_j \le f_{mx}) \wedge x > max$

$(\forall j)(1 \le j < F \Rightarrow f_j \le f_{mx}) \wedge x > max \wedge x = f_F \wedge max = f_{mx}$

$\Rightarrow\ (\forall j)(1 \le j < F \Rightarrow f_j \le f_{mx}) \wedge f_{mx} < f_F$

$\Rightarrow\ (\forall j)(1 \le j < F \Rightarrow f_j < f_F)$

$\Rightarrow\ (\forall j)(1 \le j < F \Rightarrow f_j \ne f_F)$

$\Rightarrow\ (\forall j)(1 \le j < F+1 \wedge j \ne F \ \Rightarrow f_j \ne f_F)$

$\Rightarrow\ (\forall j)(1 \le j < F+1 \wedge j \ne F \ \Rightarrow (f_j \ne f_F \vee f_{j+1} \ne f_{mn}))$

spolu: $[1 \le F < F+1 \wedge f_F = f_F \wedge f_{F+1} = f_{mn}))$

$\wedge (\forall j)((1 \le j < F+1 \wedge j \notin \{F\}) \Rightarrow (f_j \ne f_F \vee f_{j+1} \ne f_{mn}))]$

teda $(\exists z_1)\ [1 \le z_1 < F+1 \wedge f_{z1} = f_F \wedge f_{z1+1} = f_{mn}))$

$\wedge (\forall j)((1 \le j < F+1 \wedge j \notin \{z_1\}) \Rightarrow (f_j \ne f_F \vee f_{j+1} \ne f_{mn}))]$

platí aj:

$\omega(f, F) \wedge F \le n \wedge max = f_{mx} \wedge min = f_{mn} \wedge x = f_F \wedge y_1 = f_F \wedge$

$1 \le mx \le F \wedge (\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge 1 \le mn \le F \wedge (\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn})$

$\wedge (\exists z_1)(\exists z_2)... (\exists z_{y2})\ [(\forall i)(1 \le i \le y_2 \Rightarrow (1 \le z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \le j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \ne f_{mx} \vee f_{j+1} \ne f_{mn}))]$

$\wedge f_{F+1} = \min \wedge f_{F+1} \leq \min \wedge x \neq \max \wedge x \geq \max \wedge F+1 \leq n$

$\Rightarrow$

$\omega(f, F) \wedge F+1 \leq n \wedge x = f_F \wedge \min = f_{mn} \wedge f_{F+1}=f_{F+1} \wedge f_{F+1}=f_{F+1}$

$\wedge 1 \leq F \leq F+1 \wedge (\forall i)(1 \leq i < F+1 \Rightarrow f_i \leq f_F)$

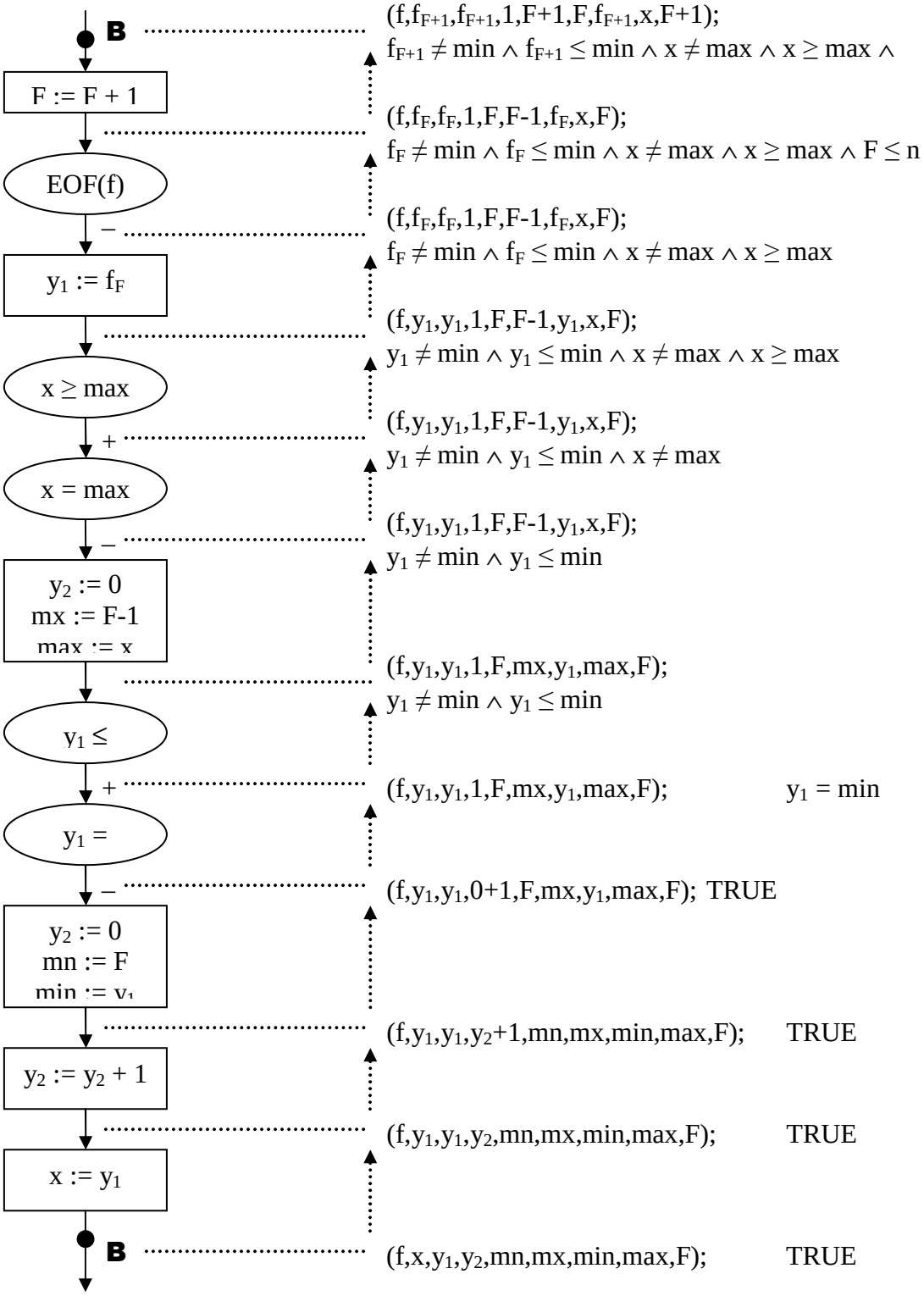
$\wedge 1 \leq mn \leq F+1 \wedge (\forall i)(1 \leq i \leq F+1 \Rightarrow f_i \geq f_{mn})$

$\wedge (\exists z_1)\ [(\forall i)(1 \leq i \leq 1 \Rightarrow (1 \leq z_i < F+1 \wedge f_{zi}=f_{mx} \wedge f_{zi+1}=f_{F+1}))$

$\wedge (\forall j)((1 \leq j < F+1 \wedge j \notin \{z_1\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{F+1}))]$

a to je verifikačná podmienka

- cesta β_{36} (z B do B hranami 3 a 6):



verifikačná podmienka:

$p_B(f,x,y_1,y_2,mn,mx,min,max,F)$

$\wedge\ f_{F+1} \neq \min \wedge f_{F+1} \leq \min \wedge x \neq \max \wedge x \geq \max \wedge F+1 \leq n$

$\Rightarrow\ p_B(f,f_{F+1},f_{F+1},1,F+1,F,f_{F+1},x,F+1)$

Pretože platí:

1.) $1 \leq mx \leq F\ \Rightarrow\ 1 \leq F$

2.) $1 \leq F\ \Rightarrow\ 1 \leq F+1$

3.) $(\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge x \geq \max \wedge x = f_F \wedge \max = f_{mx}$

$\Rightarrow\ (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge f_{mx} \leq f_F\ \Rightarrow\ (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_F)$

$(\forall i)(1 \leq i < F \Rightarrow f_i \leq f_F) \wedge f_F \leq f_F\ \Rightarrow\ (\forall i)(1 \leq i < F+1 \Rightarrow f_i \leq f_F)$

4.) $(\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn})\ \wedge f_{F+1} \leq \min \wedge \min = f_{mn}$

$\Rightarrow\ (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn})\ \wedge f_{mn} \geq f_{F+1}\ \Rightarrow\ (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{F+1})$

$(\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{F+1}) \wedge f_{F+1} = f_{F+1}\ \Rightarrow\ (\forall i)(1 \leq i \leq F+1 \Rightarrow f_i \geq f_{F+1})$

5.) položme $z_1 = F$

máme: $1 \leq mx \leq F\ \Rightarrow\ 1 \leq F$

$(\forall j)(1 \leq j < F \Rightarrow f_j \leq f_{mx}) \wedge x \neq \max \wedge x \geq \max$

$\Rightarrow\ (\forall j)(1 \leq j < F \Rightarrow f_j \leq f_{mx}) \wedge x > \max$

$(\forall j)(1 \leq j < F \Rightarrow f_j \leq f_{mx}) \wedge x > \max \wedge x = f_F \wedge \max = f_{mx}$

$\Rightarrow\ (\forall j)(1 \leq j < F \Rightarrow f_j \leq f_{mx}) \wedge f_{mx} < f_F$

$\Rightarrow\ (\forall j)(1 \leq j < F \Rightarrow f_j < f_F)$

$\Rightarrow\ (\forall j)(1 \leq j < F \Rightarrow f_j \neq f_F)$

$\Rightarrow\ (\forall j)(1 \leq j < F+1 \wedge j \neq F \Rightarrow f_j \neq f_F)$

$\Rightarrow\ (\forall j)(1 \leq j < F+1 \wedge j \neq F \Rightarrow (f_j \neq f_F \vee f_{j+1} \neq f_{F+1}))$

spolu: $[1 \leq F < F+1 \wedge f_F=f_F \wedge f_{F+1}=f_{F+1}))$

$\wedge (\forall j)((1 \leq j < F+1 \wedge j \notin \{F\}) \Rightarrow (f_j \neq f_F \vee f_{j+1} \neq f_{F+1}))]$

teda $(\exists z_1)\ [1 \leq z_1 < F+1 \wedge f_{z1} = f_F \wedge f_{z1+1} = f_{F+1}))$

$\wedge (\forall j)((1 \leq j < F+1 \wedge j \notin \{z_1\}) \Rightarrow (f_j \neq f_F \vee f_{j+1} \neq f_{F+1}))]$

platí aj:

$\omega(f, F) \wedge F \leq\ n \wedge \max = f_{mx} \wedge \min = f_{mn} \wedge x = f_F \wedge y_1 = f_F \wedge$

$1 \leq mx \leq F \wedge (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx}) \wedge 1 \leq mn \leq F \wedge (\forall i)(1 \leq i \leq F \Rightarrow f_i \geq f_{mn})$

$\wedge (\exists z_1)(\exists z_2)... (\exists z_{y2})\ [(\forall i)(1 \leq i \leq y_2 \Rightarrow (1 \leq z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge (\forall j)((1 \leq j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$

$\wedge f_{F+1} \neq \min \wedge f_{F+1} \leq \min \wedge x \neq \max \wedge x \geq \max \wedge F+1 \leq n$

$\Rightarrow$

$\omega(f, F) \wedge F+1 \leq\ n \wedge x = f_F \wedge f_{F+1} = f_{F+1} \wedge f_{F+1}=f_{F+1} \wedge f_{F+1}=f_{F+1}$

$\wedge\ 1 \leq F \leq F+1 \wedge (\forall i)(1 \leq i < F+1 \Rightarrow f_i \leq f_F)$

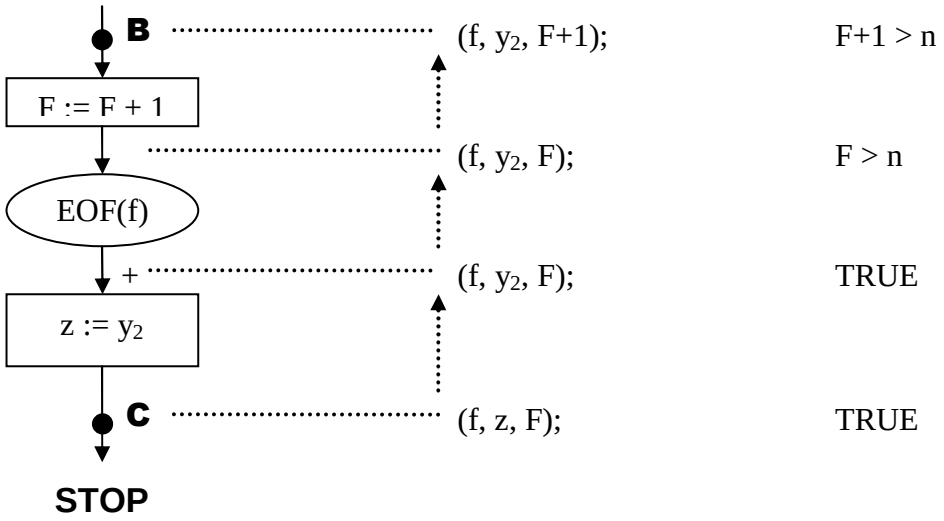
$\wedge\ 1 \le F+1 \le F+1 \wedge (\forall i)(1 \le i \le F+1 \Rightarrow f_i \ge f_{F+1})$

$\wedge\ (\exists z_1)\ [(\forall i)(1 \le i \le 1 \Rightarrow (1 \le z_i < F+1 \wedge f_{zi} = f_F \wedge f_{zi+1} = f_{F+1})) \wedge$

$(\forall j)((1 \le j < F+1 \wedge j \notin \{z_1\}) \Rightarrow (f_j \ne f_F \vee f_{j+1} \ne f_{F+1}))]$

a to je verifikačná podmienka

- cesta γ (z bodu B do C):



verifikačná podmienka:

$p_B(f,x,y_1,y_2,mn,mx,min,max,F) \wedge F+1 > n \ \Rightarrow\ \psi\ (f,y_2,F+1)$

Pretože platí:

1.) $F \le\ n \wedge F+1 > n \wedge n \in N \wedge F \in N \ \Rightarrow\ F = n \ \Rightarrow\ F+1 = n+1$

2.) za nový index mx vo výstupnej podmienke položme pôvodné mx, podobne pre mn, a pretože F = n, môžeme substituovať n na miesto F

platí aj:

$\omega(f, F) \wedge F \le\ n \wedge max = f_{mx} \wedge min = f_{mn} \wedge x = f_F \wedge y_1 = f_F \wedge$

$1 \le mx \le F \wedge (\forall i)(1 \le i < F \Rightarrow f_i \le f_{mx}) \wedge 1 \le mn \le F \wedge (\forall i)(1 \le i \le F \Rightarrow f_i \ge f_{mn})$

$\wedge\ (\exists z_1)(\exists z_2)... (\exists z_{y2})\ [(\forall i)(1 \le i \le y_2 \Rightarrow (1 \le z_i < F \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge\ (\forall j)((1 \le j < F \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \ne f_{mx} \vee f_{j+1} \ne f_{mn}))]$

$\wedge\ F+1 > n$

$\Rightarrow$

$\omega(f, F) \wedge F+1 = n+1 \wedge (\exists mx)[1 \le mx \le n \wedge (\forall i)(1 \le i < n \Rightarrow f_i \le f_{mx})]$

$\wedge\ (\exists mn)[1 \le mn \le n \wedge (\forall i)(1 \le i \le n \Rightarrow f_i \ge f_{mn})]$

$\wedge\ (\exists z_1)(\exists z_2)...(\exists z_{y2})\ [(\forall i)(1 \le i \le y_2 \Rightarrow (1 \le z_i < n \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn}))$

$\wedge\ (\forall j)((1 \le j < n \wedge j \notin \{z_1,z_2,...,z_{y2}\}) \Rightarrow (f_j \ne f_{mx} \vee f_{j+1} \ne f_{mn}))]$

a to je verifikačná podmienka.

Ukázali sme platnosť všetkých verifikačných podmienok, podľa Floydovej vety je teda program čiastočne správny vzhľadom k $\varphi(f, F)$ a $\psi(f, z, F)$.

3.3.2 Ukončenie

K r o k 1: Deliaci bod: B, dobre založená množina bude množina prirodzených čísel **N** s prirodzeným usporiadaním <

K r o k 2: $B - q_B(f, F) = F \leq n$

Ukážme, že q_B je "dobrý" predikát:

Nech α je cesta z príkazu START do bodu B.

$$n \geq 2 \wedge F = 1 \Rightarrow F \leq n$$

$$\omega(f, F) \wedge n \geq 2 \wedge F = 1 \Rightarrow F \leq n$$

$$\varphi(f, F) \wedge R_\alpha(f, F) \Rightarrow q_B(f, r_\alpha(f, F))$$

Nech β je cesta z bodu B do B ľubovoľnou z možných ciest. Vidíme, že:

$R_\beta(f, ..., F) = A \wedge F+1 \leq n$, kde A sú ďalšie členy konjunkcie

$r_\beta(f, ..., F) = (f, ..., F+1)$

t.j.

$$F+1 \leq n \Rightarrow F+1 \leq n$$

$$F \leq n \wedge A \wedge F+1 \leq n \Rightarrow F+1 \leq n$$

$$q_i(f, ..., F) \wedge R_\alpha(f, ..., F) \Rightarrow q_i(f, r_\alpha(f, ..., F+1))$$

K r o k 3: $B - u_B(f, F) = n - F$

Ukážeme, že u_B je "dobrá" funkcia:

Máme:

$R_\beta(f, ..., F) = A \wedge F+1 \leq n$

$r_\beta(f, ..., F) = (f, ..., F+1)$

teda:

$$F \leq n \Rightarrow n - F \in \mathbf{N}$$

$$q_B(f, ..., F) \Rightarrow u_B(f, ..., F) \in \mathbf{N}$$

K r o k 4: Podmienky ukončenia:

Nech β je cesta z bodu B do B ľubovoľnou z možných ciest. Vidíme, že:

$R_\beta(f, ..., F) = A \wedge F+1 \leq n$, kde A sú zvyšné členy konjunkcie

$r_\beta(f, ..., F) = (f, ..., F+1)$

Ak $n \in \mathbf{Z}$, $F \in \mathbf{Z}$ platí:

$$1 > 0$$

$$n - F + 1 > n - F$$

$$n - F > n - F - 1$$

$$n - F > n - (F + 1)$$

preto aj

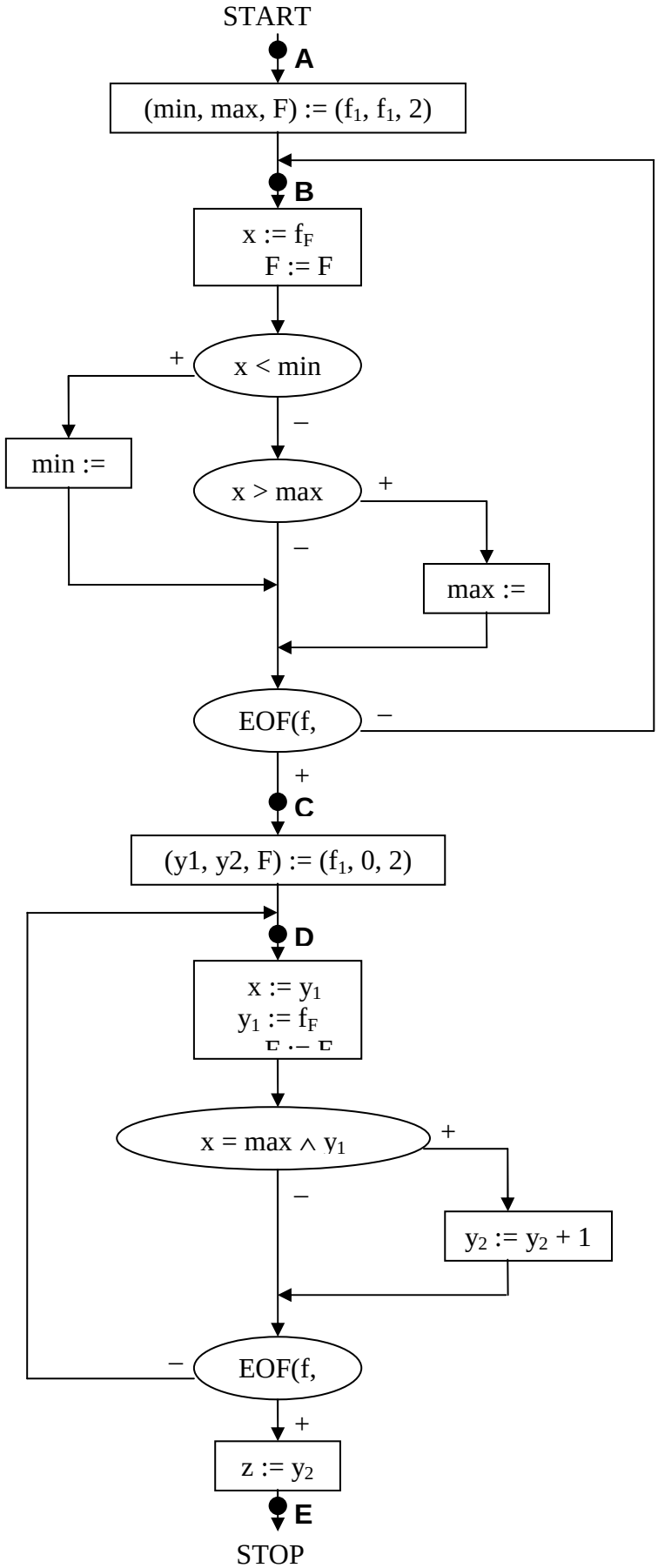
$$F \leq n \wedge A \wedge F + 1 \leq n \Rightarrow n - F > n - (F + 1)$$

$$q_B(f, ..., F) \wedge A \wedge F+1 \leq n \Rightarrow u_B(f, ..., F) > u_B(f, ..., F+1)$$

$$\text{t.j. } q_B(f, ..., F) \wedge R_\beta(f, ..., F) \Rightarrow u_B(f, ..., F) > u_B(f, r_\beta(f, ..., F))$$

Pretože podmienky ukončenia sú pravdivé, podľa vety Floydovej uvedenej v X.Y vety o metóde dobre založených množín, program končí vzhľadom k $\varphi(f, F)$.

3.4 Druhý prístup



K r o k 1: Deliace body: A, B, C, D, E

K r o k 2: Induktívne podmienky k deliacim bodom:

A: vstupná podm. $\varphi(f, F)$

B: $p_B(f, x, min, max, F) = \omega(f, F) \wedge F \leq n \wedge$

$(\exists mn)[1 \leq mn < F \wedge (\forall i)(1 \leq i < F \Rightarrow f_i \geq f_{mn})] \wedge$

$(\exists mx)[1 \leq mx < F \wedge (\forall i)(1 \leq i < F \Rightarrow f_i \leq f_{mx})]$

C: $p_C(f, x, min, max, F) = \omega(f, F) \wedge F = n + 1 \wedge$

$(\exists mn)[1 \leq mn \leq n \wedge (\forall i)(1 \leq i \leq n \Rightarrow f_i \geq f_{mn})] \wedge$

$(\exists mx)[1 \leq mx \leq n \wedge (\forall i)(1 \leq i \leq n \Rightarrow f_i \leq f_{mx})]$

D: $pD(f, x, min, max, F) = \omega(f, F) \wedge F \leq n \wedge$

$(\exists mn)[1 \leq mn \leq n \wedge (\forall i)(1 \leq i \leq n \Rightarrow f_i \geq f_{mn})] \wedge$

$(\exists mx)[1 \leq mx \leq n \wedge (\forall i)(1 \leq i \leq n \Rightarrow f_i \leq f_{mx})] \wedge$

$(\exists z_1)(\exists z_2)...(\exists z_{y2})\ [(\forall i)(1 \leq i \leq y_2 \Rightarrow (1 \leq z_i < F\text{-}1 \wedge f_{zi} = f_{mx} \wedge f_{zi+1} = f_{mn})) \wedge$

$(\forall j)((1 \leq j < F\text{-}1 \wedge j \notin \{z_1, z_2, ..., z_{y2}\}) \Rightarrow (f_j \neq f_{mx} \vee f_{j+1} \neq f_{mn}))]$

E: výstupná podm. $\psi(f, z)$

3.5 Porovnanie oboch postupov

1. p r í s t u p:

Výhody:

- ✓ menší počet čítaní zo súboru (prechádzame ním len raz)
- ✓ menší celkový počet vykonaných príkazov vo výpočte
- ✓ použiteľný aj v prípade, že vstup (nemusí ísť vždy len o súbor) je možné čítať len raz

Nevýhody:

- ✓ menej prehľadný
- ✓ náročnejší na pochopenie človekom
- ✓ náročnejší vzhľadom k navrhnutiu
- ✓ veľa možných vetvení v programe
- ✓ náročnejší dôkaz čiastočnej správnosti

2. p r í s t u p:

Výhody:

- ✓ prehľadnejší a názornejší ľudskému pohľadu
- ✓ jednoduchý a rýchly návrh
- ✓ šetrí čas programátora
- ✓ menej možných ciest vo výpočte
- ✓ jednoduchší a prehľadnejší dôkaz čiastočnej správnosti

Nevýhody:

- ✓ väčší počet čítaní zo súboru
- ✓ väčší celkový počet vykonaných príkazov vo výpočte
- ✓ nutné čítať súbor dvakrát
- ✓ nepoužiteľný v prípade, že vstup je možné čítať len raz

Aký prístup zvoliť, je takmer vždy kompromisom. Okrem prípadov ako napr. hľadať minimum a maximum dvoma prechodmi – v prvom minimum a v druhom maximum, takýto prístup je väčšinou hneď možné odmietnuť, nakoľko ním nezískame nič, ale strácame čas dvojnásobným počtom vstupno-výstupných operácií. Voliť medzi tu uvedenými dvomi postupmi je už zložitejšie. Napr. ak máme k dispozícii výkonné počítače a rýchle vstupno-výstupné operácie, ale chýbajú nám ľudské zdroje (programátori), zvolíme druhý prístup, v minulosti pri obmedzených zdrojoch by sme volili skôr prvý prístup. Najjednoduchšia voľba je v prípade, ak môžme vstupom prejsť len raz, vtedy je možný iba prvý prístup.

Z hľadiska dôkazu správnosti je náročnejší prístup „v jednom prechode všetko“, preto sme aj tu detailne dokazovali správnosť práve takéhoto programu, aby bol ukázaný ten náročnejší dôkaz.

Záver

Ukázali sme postup dokazovania správnosti programov metódou induktívnych podmienok. Zároveň sme ilustrovali tento postup na zložitejšom príklade, ktorý by mal stačiť k úplnému pochopeniu matematického dôkazu správnosti programu.

Už iba uveďme odpoveď na najčastejšiu námietku, či nejde o zbytočný formalizmus. Odpoveď je, že na chápanie významu takéhoto dokazovania je potrebné matematické videnie. S matematickým myslením sa dá nielen ľahko nahliadnuť nevyhnutnosť podobných dôkazov, ale aj ľahko chápať celý dôkaz a takisto postup programov, ktoré sú na dokazovanie navrhnuté. Nakoniec ako v iných oblastiach matematiky platí, že bez pochopenia dôkazu nie je možné porozumieť celej problematike, takisto pochopenie dôkazov programov pomáha porozumieť priebehu výpočtu a návrhu programov.

Zoznam použitej literatúry

[1] Manna, Z. *Matematická teorie programů*. Praha: SNTL Nakladatelství technické literatury, 1981.

[2] Rogers, R. *Mathematical Logic and Formalized Theories.* Amsterdam: North-Holland Publ. Comp. Inc. 1971.

[3] Trachtenbrot, B. A. *Algoritmy a strojové riešenie úloh.* Praha: NČSAV. 1963.