

## 10 Důkazové postupy pro algoritmy

Nyní si ukážeme, jak formální deklarativní jazyk z Lekce 9 využít k formálně přesným induktivním důkazům vybraných algoritmů. Dá se říci, že tato lekce je „vrcholem“ v naší snaze o matematické dokazování algoritmů v informatice.

$f(3)$	$\mapsto$	if 3 then 3 * f(3 - 1) else 1 fi	$\mapsto$	3 * f(3 - 1)	$\mapsto$
$3 * f(2)$	$\mapsto$	3 * (if 2 then 2 * f(2 - 1) else 1 fi)	$\mapsto$	3 * (2 * f(2 - 1))	$\mapsto$
$3 * (2 * f(1))$	$\mapsto$	3 * (2 * (if 1 then 1 * f(1 - 1) else 1 fi))	$\mapsto$	3 * (2 * (1 * f(1 - 1)))	$\mapsto$
$3 * (2 * (1 * f(0)))$	$\mapsto$	3 * (2 * (1 * (if 0 then 0 * f(0 - 1) else 1 fi)))	$\mapsto$	3 * (2 * (1 * 1))	$\mapsto$
$3 * (2 * 1)$	$\mapsto$	3 * 2	$\mapsto$	6	

□

### Stručný přehled lekce

- \* Důkaz indukcí s „fixací parametrů“.
- \* Důkaz indukcí vzhledem k součtu parametrů.
- \* Důkaz indukcí se „zesílením tvrzení“.

## 10.1 Technika „fixace parametru“

**Příklad 10.1.** Uvažme deklaraci  $\Delta$  obsahující pouze rovnici

$$g(x, y) = \text{if } x \text{ then } y + g(x - 1, y) \text{ else } 0 \text{ fi.}$$

**Věta.** Pro každé  $m, n \in \mathbb{N}$  platí  $g(\mathbf{m}, \mathbf{n}) \mapsto^* \mathbf{z}$ , kde  $\mathbf{z} \equiv m \cdot n$ .  $\square$

**Důkaz:** Budiž  $n \in \mathbb{N}$  libovolné ale pro další úvahy **pevné**. Dokážeme, že pro každé  $m \in \mathbb{N}$  platí  $g(\mathbf{m}, \mathbf{n}) \mapsto^* \mathbf{z}$ , kde  $\mathbf{z} \equiv m \cdot n$ , indukcí vzhledem k  $m$ .  $\square$

- **Báze**  $m = 0$ . Platí  $g(\mathbf{0}, \mathbf{n}) \mapsto \text{if } \mathbf{0} \text{ then } \mathbf{n} + g(\mathbf{0} - 1, \mathbf{n}) \text{ else } \mathbf{0} \text{ fi} \mapsto \mathbf{0}$ .  $\square$
- **Indukční krok.** Necht'  $m + 1 \equiv \mathbf{k}$ . Pak

$$g(\mathbf{k}, \mathbf{n}) \mapsto \text{if } \mathbf{k} \text{ then } \mathbf{n} + g(\mathbf{k} - 1, \mathbf{n}) \text{ else } \mathbf{0} \text{ fi} \mapsto \mathbf{n} + g(\mathbf{k} - 1, \mathbf{n}) \mapsto \mathbf{n} + g(\mathbf{w}, \mathbf{n}),$$

kde je  $\mathbf{w} \equiv m$ . Podle I.P. platí  $g(\mathbf{w}, \mathbf{n}) \mapsto^* \mathbf{u}$  pro  $\mathbf{u} \equiv m \cdot n$ . Dále  $\mathbf{n} + g(\mathbf{w}, \mathbf{n}) \mapsto^* \mathbf{n} + \mathbf{u} \mapsto \mathbf{v}$ , kde  $\mathbf{v} \equiv n + (m \cdot n) = (m + 1) \cdot n = \mathbf{k} \cdot n$ , a tím jsme dohromady hotovi s důkazem  $g(\mathbf{k}, \mathbf{n}) \mapsto^* \mathbf{v}$ .  $\square$

## 10.2 Technika „indukce k součtu parametrů“

**Příklad 10.2.** Uvažme deklaraci  $\Delta$  obsahující pouze rovnici

$$g(x, y) = \text{if } x \text{ then (if } y \text{ then } g(x - 1, y) + g(x, y - 1) \text{ else } 0 \text{ fi) else } 0 \text{ fi}.$$

**Věta.** Pro každé  $m, n \in \mathbb{N}$  platí  $g(\mathbf{m}, \mathbf{n}) \mapsto^* 0$ .  $\square$

Tvrzení této věty **přímo nelze** dokázat indukcí vzhledem k  $m$ , ani indukcí vzhledem k  $n$ , neboť u žádného z  $m, n$  nemáme zaručeno, že se vždy zmenší.  $\square$  Důkaz lze ovšem postavit na faktu, že se vždy zmenší **alespoň jeden** z  $m, n$ , neboli se vždy zmenší **součet**  $m$  a  $n$ . To znamená, že výše uvedené tvrzení nejprve přeformulujeme do následující (matematicky ekvivalentní) podoby:

**Věta.** Pro každé  $i \in \mathbb{N}$  platí, že jestliže  $i = m + n$  pro kterákoliv  $m, n \in \mathbb{N}$ , pak  $g(\mathbf{m}, \mathbf{n}) \mapsto^* 0$ .  $\square$

**Důkaz** indukcí vzhledem k  $i$ : **Báze**  $i = 0$  znamená, že  $0 = m + n$  pro  $m, n \in \mathbb{N}$ , neboli  $m = n = 0$ . Dokazujeme tedy, že  $g(\mathbf{0}, \mathbf{0}) \mapsto^* 0$ . Platí

$$g(\mathbf{0}, \mathbf{0}) \mapsto \text{if } 0 \text{ then (if } 0 \text{ then } g(\mathbf{0} - \mathbf{1}, \mathbf{0}) + g(\mathbf{0}, \mathbf{0} - \mathbf{1}) \text{ else } 0 \text{ fi) else } 0 \text{ fi} \mapsto 0.$$

**Indukční krok.** Necht'  $i+1 = m+n$ , kde  $m, n \in \mathbb{N}$ . Nyní rozlišíme tři možnosti (z nichž první dvě jsou svým způsobem jen rozšířeními předchozí báze indukce):

- Pro  $m = 0$  platí

$$g(\mathbf{0}, \mathbf{n}) \mapsto \text{if } \mathbf{0} \text{ then (if } \mathbf{n} \text{ then } g(\mathbf{0} - \mathbf{1}, \mathbf{n}) + g(\mathbf{0}, \mathbf{n} - \mathbf{1}) \text{ else } \mathbf{0} \text{ fi) else } \mathbf{0} \text{ fi} \mapsto \mathbf{0}. \square$$

- Pro  $m > 0, n = 0$  platí

$$\begin{aligned} g(\mathbf{m}, \mathbf{0}) &\mapsto \text{if } \mathbf{m} \text{ then (if } \mathbf{0} \text{ then } g(\mathbf{m} - \mathbf{1}, \mathbf{0}) + g(\mathbf{m}, \mathbf{0} - \mathbf{1}) \text{ else } \mathbf{0} \text{ fi) else } \mathbf{0} \text{ fi} \mapsto \\ &\mapsto \text{if } \mathbf{0} \text{ then } g(\mathbf{m} - \mathbf{1}, \mathbf{0}) + g(\mathbf{m}, \mathbf{0} - \mathbf{1}) \text{ else } \mathbf{0} \text{ fi} \mapsto \mathbf{0}. \square \end{aligned}$$

- Pro  $m > 0, n > 0$  platí

$$\begin{aligned} g(\mathbf{m}, \mathbf{n}) &\mapsto \text{if } \mathbf{m} \text{ then (if } \mathbf{n} \text{ then } g(\mathbf{m} - \mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \text{ else } \mathbf{0} \text{ fi) else } \mathbf{0} \text{ fi} \mapsto \\ &\mapsto \text{if } \mathbf{n} \text{ then } g(\mathbf{m} - \mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \text{ else } \mathbf{0} \text{ fi} \mapsto g(\mathbf{m} - \mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \square \end{aligned}$$

Podle I.P. platí  $g(\mathbf{m} - \mathbf{1}, \mathbf{n}) \mapsto^* \mathbf{0}$  a současně  $g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \mapsto^* \mathbf{0}$ , proto

$$g(\mathbf{m} - \mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \mapsto^* \mathbf{0} + g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \mapsto^* \mathbf{0} + \mathbf{0} \mapsto \mathbf{0}.$$

Tím jsme s důkazem matematickou indukcí hotovi. □

## Zajímavější verze

**Příklad 10.3.** Uvažme deklaraci  $\Delta$  obsahující pouze rovnici

$$g(x, y) = \text{if } x \text{ then (if } y \text{ then } g(x - 1, y) + g(x, y - 1) \text{ else } \mathbf{1} \text{ fi) else } \mathbf{1} \text{ fi. } \square$$

**Věta.** Pro každé  $m, n \in \mathbb{N}$  platí  $g(\mathbf{m}, \mathbf{n}) \mapsto^* \mathbf{k}$ , kde  $k = \binom{m+n}{m}$  (kombinační číslo).

Toto tvrzení opět budeme dokazovat indukcí vzhledem k  $i = m + n$ .  $\square$

Vzpoměňte si nejprve na známý *Pascalův trojúhelník* kombinačních čísel, který je definovaný rekurentním vztahem

$$\binom{a+1}{b+1} = \binom{a}{b+1} + \binom{a}{b}.$$

Nepřipomíná to trochu naši deklaraci? Je však třeba správně „nastavit“ význam parametrů  $a, b$ .  $\square$

**Důkaz** indukcí vzhledem k  $i$ : **Báze**  $i = 0$  znamená, že  $0 = m + n$  pro  $m, n \in \mathbb{N}$ , neboli  $m = n = 0$ . Dokazujeme tedy, že  $g(\mathbf{0}, \mathbf{0}) \mapsto^* \mathbf{1}$ . Platí

$$g(\mathbf{0}, \mathbf{0}) \mapsto \text{if } \mathbf{0} \text{ then (if } \mathbf{0} \text{ then } g(\mathbf{0} - \mathbf{1}, \mathbf{0}) + g(\mathbf{0}, \mathbf{0} - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi) else } \mathbf{1} \text{ fi} \mapsto \mathbf{1}.$$

**Indukční krok.** Necht'  $i + 1 = m + n$ , kde  $m, n \in \mathbb{N}$ . Opět rozlišíme stejné tři možnosti:

- Pro  $m = 0$  platí

$$g(\mathbf{0}, \mathbf{n}) \mapsto \text{if } \mathbf{0} \text{ then (if } \mathbf{n} \text{ then } g(\mathbf{0} - \mathbf{1}, \mathbf{n}) + g(\mathbf{0}, \mathbf{n} - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi) else } \mathbf{1} \text{ fi} \mapsto \mathbf{1}. \square$$

- Pro  $m > 0, n = 0$  platí

$$\begin{aligned} g(\mathbf{m}, \mathbf{0}) &\mapsto \text{if } \mathbf{m} \text{ then (if } \mathbf{0} \text{ then } g(\mathbf{m} - \mathbf{1}, \mathbf{0}) + g(\mathbf{m}, \mathbf{0} - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi) else } \mathbf{1} \text{ fi} \mapsto \\ &\mapsto \text{if } \mathbf{0} \text{ then } g(\mathbf{m} - \mathbf{1}, \mathbf{0}) + g(\mathbf{m}, \mathbf{0} - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi} \mapsto \mathbf{1}. \square \end{aligned}$$

- Pro  $m > 0, n > 0$  platí

$$\begin{aligned} g(\mathbf{m}, \mathbf{n}) &\mapsto \text{if } \mathbf{m} \text{ then (if } \mathbf{n} \text{ then } g(\mathbf{m} - \mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi) else } \mathbf{1} \text{ fi} \mapsto \\ &\mapsto \text{if } \mathbf{n} \text{ then } g(\mathbf{m} - \mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi} \mapsto g(\mathbf{m} - \mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \square \end{aligned}$$

Podle I.P. platí  $g(\mathbf{m} - \mathbf{1}, \mathbf{n}) \mapsto^* \mathbf{k}_1$ , kde  $\mathbf{k}_1 \equiv \binom{m+n-1}{m-1}$ , a současně  $g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \mapsto^* \mathbf{k}_2$ , kde  $\mathbf{k}_2 \equiv \binom{m+n-1}{m}$ .  $\square$  Přitom z Pascalova trojúhelníka plyne

$$\binom{m+n-1}{m-1} + \binom{m+n-1}{m} = \binom{m+n-1+1}{m} = \binom{m+n}{m},$$

a proto

$$g(\mathbf{m} - \mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n} - \mathbf{1}) \mapsto^* \mathbf{k}_1 + \mathbf{k}_2 \mapsto^* \mathbf{k} \equiv \binom{m+n}{m}. \quad \square$$

## 10.3 Technika „zesílení dokazovaného tvrzení“

**Příklad 10.4.** Uvažme deklaraci  $\Delta$  obsahující tyto rovnice:

$$f(x) = \text{if } x \text{ then } h(x) \text{ else } \mathbf{1} \text{ fi}$$

$$h(x) = \text{if } x \text{ then } f(x - \mathbf{1}) + h(x - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi}$$

**Věta.** Pro každé  $n \in \mathbb{N}$  platí  $f(\mathbf{n}) \mapsto^* \mathbf{m}$ , kde  $m = 2^n$ .

Požadované tvrzení bohužel **nelze přímo** dokázat indukcí podle  $n$ .  $\square$  Řešením je přeformulování dokazovaného tvrzení do **silnější** podoby, kterou již indukcí dokázat lze:

**Věta.** Pro každé  $n \in \mathbb{N}$  platí  $f(\mathbf{n}) \mapsto^* \mathbf{m}$  a  $h(\mathbf{n}) \mapsto^* \mathbf{m}$ , kde  $m = 2^n$ .  $\square$

**Důkaz**, již poměrně snadno indukcí vzhledem k  $n$ :

- **Báze**  $n = 0$ . Platí

$$f(\mathbf{0}) \mapsto \text{if } \mathbf{0} \text{ then } h(\mathbf{0}) \text{ else } \mathbf{1} \text{ fi} \mapsto \mathbf{1},$$

$$h(\mathbf{0}) \mapsto \text{if } \mathbf{0} \text{ then } f(\mathbf{0} - \mathbf{1}) + h(\mathbf{0} - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi} \mapsto \mathbf{1}.$$

- Indukční krok: Nechť  $n + 1 \equiv \mathbf{k}$ , pak platí

$$f(\mathbf{k}) \mapsto \text{if } \mathbf{k} \text{ then } h(\mathbf{k}) \text{ else } \mathbf{1} \text{ fi} \mapsto h(\mathbf{k}) \mapsto$$

$$\mapsto \text{if } \mathbf{k} \text{ then } f(\mathbf{k} - \mathbf{1}) + h(\mathbf{k} - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi} \mapsto f(\mathbf{k} - \mathbf{1}) + h(\mathbf{k} - \mathbf{1}) \mapsto f(\mathbf{w}) + h(\mathbf{k} - \mathbf{1}),$$

kde  $\mathbf{w} \equiv k - 1 = n$ . Podle I.P. platí  $f(\mathbf{w}) \mapsto^* \mathbf{m}$ , kde  $m = 2^n$ .  $\square$  Zároveň také (naše „zesílení“) platí i  $h(\mathbf{w}) \mapsto^* \mathbf{m}$ , a proto

$$f(\mathbf{w}) + h(\mathbf{k} - \mathbf{1}) \mapsto^* \mathbf{m} + h(\mathbf{k} - \mathbf{1}) \mapsto^* \mathbf{m} + h(\mathbf{w}) \mapsto^* \mathbf{m} + \mathbf{m} \mapsto \mathbf{q},$$

kde  $q = m + m = 2m = 2 \cdot 2^n = 2^{n+1} = 2^k$ . Proto tranzitivně  $f(\mathbf{k}) \mapsto \mathbf{q}$  a první část našeho tvrzení platí i pro  $n + 1 \equiv \mathbf{k}$ .  $\square$

Podobně je třeba ještě dokončit druhou část tvrzení.

$$h(\mathbf{k}) \mapsto \text{if } \mathbf{k} \text{ then } f(\mathbf{k} - \mathbf{1}) + h(\mathbf{k} - \mathbf{1}) \text{ else } \mathbf{1} \text{ fi} \mapsto$$

$$f(\mathbf{k} - \mathbf{1}) + h(\mathbf{k} - \mathbf{1}) \mapsto^* f(\mathbf{w}) + h(\mathbf{k} - \mathbf{1}),$$

kde  $\mathbf{w} \equiv k - 1 = n$ . Podle I.P. platí  $f(\mathbf{w}) \mapsto^* \mathbf{m}$ , kde  $m = 2^n$ , a také  $h(\mathbf{w}) \mapsto^* \mathbf{m}$ , a proto

$$f(\mathbf{w}) + h(\mathbf{w}) \mapsto^* \mathbf{m} + \mathbf{m} \mapsto \mathbf{q},$$

kde  $q = m + m = 2 \cdot 2^n = 2^{n+1} = 2^k$ . Proto  $h(\mathbf{k}) \mapsto \mathbf{q}$  a i druhá část našeho tvrzení platí pro  $n + 1 \equiv \mathbf{k}$ .  $\square$



## 10.4 Dva „klasické“ algoritmy

### Euklidův algoritmus

**Věta 10.5.** Uvažme deklaraci  $\Delta$  obsahující pouze rovnici

$g(x, y) = \text{if } x - y \text{ then } g(x - y, y) \text{ else (if } y - x \text{ then } g(x, y - x) \text{ else } x \text{ fi) fi}$

Pak pro každé nenulové  $m, n \in \mathbb{N}$  platí  $g(m, n) \mapsto^* z$ , kde  $z$  je největší společný dělitel čísel  $m, n$ .  $\square$

**Důkaz** indukcí k  $i = m + n$ .

(Tj. dokazujeme následující tvrzení: Pro každé  $i \geq 2$  platí, že jestliže  $i \geq m + n$ , kde  $m, n \in \mathbb{N}$ ,  $m, n > 0$ , pak  $z$  je největší společný dělitel čísel  $m, n$ .)  $\square$

V bázi pro  $i = 2$  je  $m, n = 1$  a platí

$g(1, 1) \mapsto \text{if } 1 - 1 \text{ then } g(1 - 1, 1) \text{ else (if } 1 - 1 \text{ then } g(1, 1 - 1) \text{ else } 1 \text{ fi) fi} \mapsto$   
 $\mapsto \text{if } 0 \text{ then } g(1 - 1, 1) \text{ else (if } 1 - 1 \text{ then } g(1, 1 - 1) \text{ else } 1 \text{ fi) fi} \mapsto$   
 $\mapsto \text{if } 1 - 1 \text{ then } g(1, 1 - 1) \text{ else } 1 \text{ fi} \mapsto \text{if } 0 \text{ then } g(1, 1 - 1) \text{ else } 1 \text{ fi} \mapsto 1.$

**Indukční krok.** Necht'  $i + 1 = m + n$  kde  $m, n \in \mathbb{N}$ . Probereme tři možnosti:

- $m = n$ . Pak

$g(m, n) \mapsto$  if  $m - n$  then  $g(m - n, n)$  else (if  $n - m$  then  $g(m, n - m)$  else  $m$  fi) fi  $\mapsto$   
if  $0$  then  $g(m - n, n)$  else (if  $n - m$  then  $g(m, n - m)$  else  $m$  fi) fi  $\mapsto$   
if  $n - m$  then  $g(m, n - m)$  else  $m$  fi  $\mapsto$  if  $0$  then  $g(m, n - m)$  else  $m$  fi  $\mapsto m$ .

- $m < n$ . Pak

$g(m, n) \mapsto$  if  $m - n$  then  $g(m - n, n)$  else (if  $n - m$  then  $g(m, n - m)$  else  $m$  fi) fi  $\mapsto$   
if  $0$  then  $g(m - n, n)$  else (if  $n - m$  then  $g(m, n - m)$  else  $m$  fi) fi  $\mapsto$   
if  $n - m$  then  $g(m, n - m)$  else  $m$  fi  $\mapsto$  if  $z$  then  $g(m, n - m)$  else  $m$  fi  $\mapsto$   
 $g(m, n - m) \mapsto g(m, k)$ ,

kde  $k \equiv n - m$ .  $\square$  Platí  $m + k = m + (n - m) = n \leq i$ , takže podle I.P. také platí  $g(m, k) \mapsto^* z$ , kde  $z$  je největší společný dělitel čísel  $m$  a  $n - m$ .  
Ověříme, že  $z$  je největší společný dělitel čísel  $m$  a  $n$ .

- \* Jelikož číslo  $z$  dělí čísla  $m$  a  $n - m$ , dělí i jejich součet  $(n - m) + m = n$ . Celkem  $z$  je společným dělitelem  $m$  a  $n$ .  $\square$
- \* Buď  $d$  nějaký společný dělitel čísel  $m$  a  $n$ . Pak  $d$  dělí také rozdíl  $n - m$ . Tedy  $d$  je společný dělitel čísel  $m$  a  $n - m$ . Jelikož  $z$  je **největší** společný dělitel čísel  $m$  a  $n - m$ , nutně  $d$  dělí  $z$  a závěr platí.

- $m > n$ . Pak

$$g(\mathbf{m}, \mathbf{n}) \mapsto^* g(\mathbf{m} - \mathbf{n}, \mathbf{n}) \mapsto g(\mathbf{k}, \mathbf{n}),$$

kde  $\mathbf{k} \equiv m - n$ . Podle I.P. platí  $g(\mathbf{k}, \mathbf{n}) \mapsto^* \mathbf{z}$ , kde  $z$  je největší společný dělitel čísel  $m - n$  a  $n$ . Podobně jako výše ověříme, že  $z$  je také největší společný dělitel čísel  $m$  a  $n$ . □

□

**Poznámka:** Jak byste výše uvedený zápis Euklidova algoritmu vylepšili, aby správně „počítal“ největšího společného dělitele i v případech, že  $m = 0$  nebo  $n = 0$ ?  
Co v takových případech selže při současném zápise?

## Inkrementace dekadického zápisu

**Příklad 10.6.** Mějme přirozené číslo  $m$  dekadicky zapsané pomocí číslic  $(c_{k-1}c_{k-2} \dots c_1c_0)_{10}$  (kde zleva se implicitně vyplňují nuly). Pak dekadický zápis čísla  $m' = m + 1$  získáme takto:  $\square$

### Algoritmus . Inkrementace.

```
k ← počet číslic m;  
p ← 1;  
foreach i ← 0, 1, ..., k - 1, k do  
    c'_i ← (c_i + p) mod 10;  
    if c'_i ≠ 0 then p ← 0;  
done
```

Zapišme tento kód formální deklarací našeho jazyka.  $\square$

Řešení:

- Jelikož nyní nejsou k dispozici proměnné typu pole, „pomůžeme si“ funkčním zápisem číslic  $g(i)$  a  $g'(i)$  místo  $c_i, c'_i$ .  $\square$
- Cyklus `foreach` nahradíme rekurzí (běžný postup).
- Nakonec „trikově“ nahradíme proměnnou  $p$ , která vyjadřuje *přenos* do  $i$ -tého řádu, zavedením nové funkce  $p(i)$ , což výrazně zjednoduší zápis deklarace.  $\square$

Celá **formální deklaráce**  $\Delta$  bude vypadat například následovně:

$$g'(i) = (g(i) + p(i)) \bmod 10$$

$$p(i) = \text{if } i \text{ then (if } g'(i-1) \text{ then } 0 \text{ else } p(i-1) \text{ fi) else } 1 \text{ fi}$$

$$g(0) = c_0, g(1) = c_1, \dots, g(k-1) = c_{k-1} \quad \square$$

Všimněte si zvláštního posledního řádku, kde jsou rovnice deklarující konstantní hodnoty jednotlivých číslic vstupního čísla  $m$ .

(Proč to tak je zapsáno?)

**Věta.** Pro každé  $i \in \mathbb{N}$  platí, že  $g'(i)$  udává dekadickou číslici  $i$ -tého řádu zprava čísla  $m+1$ , kde  $m$  má dekadický zápis po číslicích  $(c_{k-1} \dots c_1 c_0)_{10}$ .  $\square$

Dokažte si tvrzení sami za domácí úkol (diskutujte na IS).

Je potřeba použít matematickou indukci se zesíleným předpokladem, který se bude vhodně vyjadřovat i o významu hodnoty  $p(i)$  („přenos“).

Pochopitelně je třeba pro úplnou správnost řešení ještě rozepsat operaci „modulo“ pomocí povolených aritmetických operací, což si také za úkol vyzkoušejte.  $\square$