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.

$$
\begin{array}{lcllcllcl}
f(\mathbf{3}) & \mapsto & \textbf{if } \mathbf{3} \textbf{ then } \mathbf{3} * f(\mathbf{3}-\mathbf{1}) \textbf{ else } \mathbf{1} & \mapsto & \mathbf{3} * f(\mathbf{3}-\mathbf{1}) & \mapsto \\
\mathbf{3} * f(\mathbf{2}) & \mapsto & \mathbf{3} * (\textbf{if } \mathbf{2} \textbf{ then } \mathbf{2} * f(\mathbf{2}-\mathbf{1}) \textbf{ else } \mathbf{1}) & \mapsto & \mathbf{3} * (\mathbf{2} * f(\mathbf{2}-\mathbf{1})) & \mapsto \\
\mathbf{3} * (\mathbf{2} * f(\mathbf{1})) & \mapsto & \mathbf{3} * (\mathbf{2} * (\textbf{if } \mathbf{1} \textbf{ then } \mathbf{1} * f(\mathbf{1}-\mathbf{1}) \textbf{ else } \mathbf{1})) & \mapsto & \mathbf{3}*(\mathbf{2}*(\mathbf{1}* f(\mathbf{1}-\mathbf{1}))) & \mapsto \\
\mathbf{3}*(\mathbf{2}*(\mathbf{1}*f(\mathbf{0}))) & \mapsto & \mathbf{3}*(\mathbf{2}*(\mathbf{1}*(\textbf{if } \mathbf{0} \textbf{ then } \mathbf{0} * f(\mathbf{0}-\mathbf{1}) \textbf{ else } \mathbf{1}))) & \mapsto & \mathbf{3} * (\mathbf{2} * (\mathbf{1} * \mathbf{1})) & \mapsto \\
\mathbf{3} * (\mathbf{2} * \mathbf{1}) & \mapsto & \mathbf{3} * \mathbf{2} & \mapsto & \mathbf{6} &
\end{array}
$$

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.

$$
\begin{array}{llllll}
f(3) & \mapsto & \textbf{if 3 then } 3*f(3-1) \textbf{ else } 1 & \mapsto & 3*f(3-1) & \mapsto \\
3*f(2) & \mapsto & 3*(\textbf{if 2 then } 2*f(2-1) \textbf{ else } 1) & \mapsto & 3*(2*f(2-1)) & \mapsto \\
3*(2*f(1)) & \mapsto & 3*(2*(\textbf{if 1 then } 1*f(1-1) \textbf{ else } 1)) & \mapsto & 3*(2*(1*f(1-1))) & \mapsto \\
3*(2*(1*f(0))) & \mapsto & 3*(2*(1*(\textbf{if 0 then } 0*f(0-1) \textbf{ else } 1))) & \mapsto & 3*(2*(1*1)) & \mapsto \\
3*(2*1) & \mapsto & 3*2 & \mapsto & 6 &
\end{array}
$$

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 Δ obsahující pouze rovnici*

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

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

10.1 Technika „fixace parametru“

Příklad 10.1. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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

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.

10.1 Technika „fixace parametru“

Příklad 10.1. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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

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.

- Báze $m = 0$. Platí $g(\mathbf{0}, \mathbf{n}) \mapsto \textbf{if } \mathbf{0} \textbf{ then } \mathbf{n} + g(\mathbf{0} - \mathbf{1}, \mathbf{n}) \textbf{ else } \mathbf{0} \mapsto \mathbf{0}$.

10.1 Technika „fixace parametru“

Příklad 10.1. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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

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.

- Báze $m = 0$. Platí $g(\mathbf{0},\mathbf{n}) \mapsto \textbf{if } \mathbf{0} \textbf{ then } \mathbf{n} + g(\mathbf{0}-\mathbf{1},\mathbf{n}) \textbf{ else } \mathbf{0} \mapsto \mathbf{0}$.
- Indukční krok. Nechť $m + 1 \equiv \mathbf{k}$. Pak

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

  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 $\mathbf{v} \equiv n + (m \cdot n) = (m+1) \cdot n = k \cdot n$, a tím jsme dohromady hotovi s důkazem $g(\mathbf{k},\mathbf{n}) \mapsto^* \mathbf{v}$.

□

10.2 Technika „indukce k součtu parametrů“

Příklad 10.2. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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

10.2 Technika „indukce k součtu parametrů“

Příklad 10.2. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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

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.

10.2 Technika „indukce k součtu parametrů“

Příklad 10.2. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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

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

10.2 Technika „indukce k součtu parametrů“

Příklad 10.2. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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

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

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 $g(\mathbf{0},\mathbf{0}) \mapsto^* \mathbf{0}$. Platí

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

Indukční krok. Nechť $i+1 = m+n$, 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

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

Indukční krok. Nechť $i+1 = m+n$, 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

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

- Pro $m > 0, n = 0$ platí

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

Indukční krok. Nechť $i+1 = m+n$, 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

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

- Pro $m > 0, n = 0$ platí

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

- Pro $m > 0, n > 0$ platí

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

Indukční krok. Nechť $i+1 = m+n$, 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

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

- Pro $m > 0, n = 0$ platí

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

- Pro $m > 0, n > 0$ platí

  $$g(\mathbf{m}, \mathbf{n}) \mapsto \textbf{if } \mathbf{m} \textbf{ then } (\textbf{if } \mathbf{n} \textbf{ then } g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1}) \textbf{ else } \mathbf{0}) \textbf{ else } \mathbf{0} \mapsto$$
  $$\mapsto \textbf{if } \mathbf{n} \textbf{ then } g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1}) \textbf{ else } \mathbf{0} \mapsto g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1})\,.$$

  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 Δ obsahující pouze rovnici*

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

Zajímavější verze

Příklad 10.3. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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 $i = m + n$.

Zajímavější verze

Příklad 10.3. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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 $i = m + n$.

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.

Zajímavější verze

Příklad 10.3. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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 $i = m+n$.

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.

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

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

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

- Pro $m = 0$ platí

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

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

- Pro $m = 0$ platí

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

- Pro $m > 0, n = 0$ platí

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

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

- Pro $m = 0$ platí

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

- Pro $m > 0, n = 0$ platí

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

- Pro $m > 0, n > 0$ platí

  $g(\mathbf{m}, \mathbf{n}) \mapsto$ **if m then** $(\mathbf{if\ n\ then}\ g(\mathbf{m-1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n-1})\ \mathbf{else}\ 1)\ \mathbf{else}\ 1 \mapsto$
  $\mapsto$ **if n then** $g(\mathbf{m-1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n-1})$ **else** $1 \mapsto g(\mathbf{m-1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n-1})$.

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

- Pro $m = 0$ platí

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

- Pro $m > 0, n = 0$ platí

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

- Pro $m > 0, n > 0$ platí

  $g(\mathbf{m}, \mathbf{n}) \mapsto$ **if m then** (**if n then** $g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1})$ **else 1**) **else 1** $\mapsto$
  $\mapsto$ **if n then** $g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1})$ **else 1** $\mapsto g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1})$.

  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 $\mathbf{k_2} \equiv \binom{m+n-1}{m}$.

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

- Pro $m = 0$ platí

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

- Pro $m > 0, n = 0$ platí

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

- Pro $m > 0, n > 0$ platí

  $g(\mathbf{m}, \mathbf{n}) \mapsto$ **if m then (if n then** $g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1})$ **else 1) else 1** $\mapsto$
  $\mapsto$ **if n then** $g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1})$ **else 1** $\mapsto g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1})$.

  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 $\mathbf{k_2} \equiv \binom{m+n-1}{m}$. 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

  $$g(\mathbf{m}-\mathbf{1}, \mathbf{n}) + g(\mathbf{m}, \mathbf{n}-\mathbf{1}) \mapsto^* \mathbf{k_1} + \mathbf{k_2} \mapsto^* \mathbf{k} \equiv \binom{m+n}{m}.$$

□

10.3 Technika „zesílení dokazovaného tvrzení“

Příklad 10.4. *Uvažme deklaraci Δ obsahující tyto rovnice:*

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

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.

10.3 Technika „zesílení dokazovaného tvrzení“

Příklad 10.4. *Uvažme deklaraci Δ obsahující tyto rovnice:*

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

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. 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 $m = 2^n$.

10.3 Technika „zesílení dokazovaného tvrzení“

Příklad 10.4. *Uvažme deklaraci Δ obsahující tyto rovnice:*

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

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. 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 $m = 2^n$.

Důkaz, již poměrně snadno indukcí vzhledem k n:

- Báze $n = 0$. Platí

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

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

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

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

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

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

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

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

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

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

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 $n+1 \equiv \mathbf{k}$.

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

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

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

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

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

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 $n+1 \equiv \mathbf{k}$.
Podobně je třeba ještě dokončit druhou část tvrzení.

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

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

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 $n+1 \equiv \mathbf{k}$.

□

10.4 Dva „klasické“ algoritmy

Euklidův algoritmus

Věta 10.5. *Uvažme deklaraci Δ obsahující pouze rovnici*

$$g(x,y) = \textbf{if } x-y \textbf{ then } g(x-y,y) \textbf{ else } (\textbf{if } y-x \textbf{ then } g(x,y-x) \textbf{ else } x)\,.$$

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

10.4 Dva „klasické“ algoritmy

Euklidův algoritmus

Věta 10.5. *Uvažme deklaraci Δ obsahující pouze rovnici*

$$g(x,y) = \textbf{if } x-y \textbf{ then } g(x-y,y) \textbf{ else } (\textbf{if } y-x \textbf{ then } g(x,y-x) \textbf{ else } x)\,.$$

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

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

10.4 Dva „klasické“ algoritmy

Euklidův algoritmus

Věta 10.5. *Uvažme deklaraci Δ obsahující pouze rovnici*

$$g(x,y) = \textbf{if } x-y \textbf{ then } g(x-y,y) \textbf{ else } (\textbf{if } y-x \textbf{ then } g(x,y-x) \textbf{ else } x)\,.$$

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

Důkaz indukcí k $i = m+n$.
(Tj. dokazujeme následující tvrzení: Pro každé $i \geq 2$ platí, že jestliže $i = m+n$, kde $m,n \in \mathbb{N}$, $m,n > 0$, pak z je největší společný dělitel čísel m,n.)
V bázi pro $i = 2$ je $m,n = 1$ a platí

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

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

- $m = n$. Pak

  $g(\mathbf{m}, \mathbf{n}) \mapsto$ **if** $\mathbf{m} - \mathbf{n}$ **then** $g(\mathbf{m} - \mathbf{n}, \mathbf{n})$ **else** (**if** $\mathbf{n} - \mathbf{m}$ **then** $g(\mathbf{m}, \mathbf{n} - \mathbf{m})$ **else** $\mathbf{m}$)
  if $\mathbf{0}$ **then** $g(\mathbf{m} - \mathbf{n}, \mathbf{n})$ **else** (**if** $\mathbf{n} - \mathbf{m}$ **then** $g(\mathbf{m}, \mathbf{n} - \mathbf{m})$ **else** $\mathbf{m}$) $\mapsto$
  if $\mathbf{n} - \mathbf{m}$ **then** $g(\mathbf{m}, \mathbf{n} - \mathbf{m})$ **else** $\mathbf{m} \mapsto$ **if** $\mathbf{0}$ **then** $g(\mathbf{m}, \mathbf{n} - \mathbf{m})$ **else** $\mathbf{m} \mapsto \mathbf{m}$.

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

- $m = n$. Pak

  $g(\mathbf{m},\mathbf{n}) \mapsto$ **if** $\mathbf{m}-\mathbf{n}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$)
  if $\mathbf{0}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$) $\mapsto$
  if $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto$ **if** $\mathbf{0}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto \mathbf{m}$.

- $m < n$. Pak

  $g(\mathbf{m},\mathbf{n}) \mapsto$ **if** $\mathbf{m}-\mathbf{n}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$)
  if $\mathbf{0}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$) $\mapsto$
  if $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto$ **if** $\mathbf{z}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto$
  $g(\mathbf{m},\mathbf{n}-\mathbf{m}) \mapsto g(\mathbf{m},\mathbf{k})$,

  kde $\mathbf{k} \equiv n - m$.

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

- $m = n$. Pak

  $g(\mathbf{m},\mathbf{n}) \mapsto$ **if** $\mathbf{m}-\mathbf{n}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$)
  if $\mathbf{0}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$) $\mapsto$
  if $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto$ **if** $\mathbf{0}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto \mathbf{m}$.

- $m < n$. Pak

  $g(\mathbf{m},\mathbf{n}) \mapsto$ **if** $\mathbf{m}-\mathbf{n}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$)
  if $\mathbf{0}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$) $\mapsto$
  if $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto$ **if** $\mathbf{z}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto$
  $g(\mathbf{m},\mathbf{n}-\mathbf{m}) \mapsto g(\mathbf{m},\mathbf{k})$,

  kde $\mathbf{k} \equiv n-m$. Platí $m+k = m+(n-m) = n \leq i$, takže podle I.P. také platí $g(\mathbf{m},\mathbf{k}) \mapsto^* \mathbf{z}$, 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.

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

- $m = n$. Pak

  $g(\mathbf{m},\mathbf{n}) \mapsto$ **if** $\mathbf{m}-\mathbf{n}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$)
  if $\mathbf{0}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$) $\mapsto$
  if $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto$ **if** $\mathbf{0}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto \mathbf{m}$.

- $m < n$. Pak

  $g(\mathbf{m},\mathbf{n}) \mapsto$ **if** $\mathbf{m}-\mathbf{n}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$)
  if $\mathbf{0}$ **then** $g(\mathbf{m}-\mathbf{n},\mathbf{n})$ **else** (**if** $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m}$) $\mapsto$
  if $\mathbf{n}-\mathbf{m}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto$ **if** $\mathbf{z}$ **then** $g(\mathbf{m},\mathbf{n}-\mathbf{m})$ **else** $\mathbf{m} \mapsto$
  $g(\mathbf{m},\mathbf{n}-\mathbf{m}) \mapsto g(\mathbf{m},\mathbf{k})$,

  kde $\mathbf{k} \equiv n-m$. Platí $m+k = m+(n-m) = n \leq i$, takže podle I.P. také platí $g(\mathbf{m},\mathbf{k}) \mapsto^* \mathbf{z}$, 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.
  * 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.

□

- $m > n$. 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* $(c_{k-1}c_{k-2}\ldots c_1c_0)_{10}$ *(kde zleva se implicitně vyplňují nuly). Pak dekadický zápis čísla* $m' = m + 1$ *získáme takto:*

Inkrementace dekadického zápisu

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

Algoritmus . **Inkrementace.**

```
k ← počet číslic m;
p ← 1;
for 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.

Inkrementace dekadického zápisu

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

Algoritmus . **Inkrementace.**

```
k ← počet číslic m;
p ← 1;
for 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.

Řešení:

- Jelikož nyní nejsou k dispozici proměnné typu pole, „pomůžeme si“ funkčním zápisem číslic $g(i)$ a $g'(i)$ místo c_i, c'_i.

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:*

Algoritmus . **Inkrementace.**

```
k ← počet číslic m;
p ← 1;
for 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.

Řešení:

- Jelikož nyní nejsou k dispozici proměnné typu pole, „pomůžeme si“ funkčním zápisem číslic $g(i)$ a $g'(i)$ místo c_i, c'_i.
- Cyklus `for` 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.

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:*

Algoritmus . **Inkrementace.**

```
k ← počet číslic m;
p ← 1;
for 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.

Řešení:

- Jelikož nyní nejsou k dispozici proměnné typu pole, „pomůžeme si“ funkčním zápisem číslic $g(i)$ a $g'(i)$ místo c_i, c'_i.
- Cyklus `for` 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.

Celá formální deklarace Δ bude vypadat například následovně:

$$g'(i) = \big(g(i) + p(i)\big) \bmod \mathbf{10}$$
$$p(i) = \textbf{if } i \textbf{ then } \big(\textbf{if } g'(i-1) \textbf{ then } \mathbf{0} \textbf{ else } \mathbf{1}\big) \textbf{ else } \mathbf{1}$$
$$g(\mathbf{0}) = \mathbf{c_0},\ g(\mathbf{1}) = \mathbf{c_1},\ \ldots\ g(\mathbf{k-1}) = \mathbf{c_{k-1}}$$

Celá formální deklarace Δ bude vypadat například následovně:

$$g'(i) = \big(g(i) + p(i)\big) \bmod \mathbf{10}$$
$$p(i) = \textbf{if } i \textbf{ then } \big(\textbf{if } g'(i-1) \textbf{ then } \mathbf{0} \textbf{ else } \mathbf{1}\big) \textbf{ else } \mathbf{1}$$
$$g(\mathbf{0}) = \mathbf{c_0},\ g(\mathbf{1}) = \mathbf{c_1},\ \ldots\ g(\mathbf{k-1}) = \mathbf{c_{k-1}}$$

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 $(c_{k-1} \ldots c_1 c_0)_{10}$.

Celá formální deklarace Δ bude vypadat například následovně:

$$g'(i) = \big(g(i) + p(i)\big) \bmod \mathbf{10}$$
$$p(i) = \textbf{if } i \textbf{ then } \big(\textbf{if } g'(i-1) \textbf{ then } \mathbf{0} \textbf{ else } \mathbf{1}\big) \textbf{ else } \mathbf{1}$$
$$g(\mathbf{0}) = \mathbf{c_0},\ g(\mathbf{1}) = \mathbf{c_1},\ \ldots\ g(\mathbf{k-1}) = \mathbf{c_{k-1}}$$

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 $(c_{k-1} \ldots c_1 c_0)_{10}$.

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. □