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.

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*

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

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

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 $g(\mathbf{0},\mathbf{n}) \ \mapsto \ \text{if } \mathbf{0} \text{ then } \mathbf{n} + g(\mathbf{0}-\mathbf{1},\mathbf{n}) \text{ else } \mathbf{0} \text{ fi} \ \mapsto \ \mathbf{0}$.□
- Indukční krok. Nechť $m+1 \equiv \mathbf{k}$. Pak

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

  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*

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

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

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

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

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

- Pro $m > 0, n = 0$ platí

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

- Pro $m > 0, n > 0$ platí

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

  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*

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

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

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

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

- Pro $m > 0, n = 0$ platí

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

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

- Pro $m > 0, n > 0$ platí

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

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

  Podle I.P. platí $g(\mathbf{m}-\mathbf{1},\mathbf{n}) \mapsto^* \mathbf{k_1}$, kde $\mathbf{k_1} \equiv \binom{m-1+n}{m-1}$, 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

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

$\square$

10.3 Technika „zesílení dokazovaného tvrzení“

Příklad 10.4. *Uvažme deklaraci Δ 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. □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

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

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

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

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

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

Podobně je třeba ještě dokončit druhou část tvrzení.

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

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

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

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

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

□

10.4 Dva dobře známé školní algoritmy

Číslice dekadického zápisu

Příklad 10.5. *Mějme přirozené číslo m. Jednotlivé číslice i-tého řádu jeho dekadického zápisu získáme deklarací*

$$c(m,i) = \text{if } i \text{ then } c(m \div \mathbf{10}, i - \mathbf{1}) \text{ else } m - \mathbf{10} * (m \div \mathbf{10}) \text{ fi}\,. \ \square$$

Dokažte:

Věta. Pro každá $m, i \in \mathbb{N}$ platí $c(\mathbf{m},\mathbf{i}) \mapsto^* \mathbf{s}$, kde $\mathbf{s}$ je číslice řádu i (počítáno od nultého zprava) v dekadickém zápise čísla $\mathbf{m}$, nebo $\mathbf{s} \equiv \mathbf{0}$ v případě, že dekadický zápis čísla $\mathbf{m}$ má méně než $i+1$ číslic. $\square$

Důkaz: Použijeme techniku fixace parametru m při indukci podle i.

- Báze $i = 0$. Platí

$$c(\mathbf{m},\mathbf{0}) \mapsto^* \mathbf{m} - \mathbf{10} * (\mathbf{m} \div \mathbf{10}) \mapsto^* \mathbf{t}, \text{ kde } t = m \bmod 10\,.$$

V tomto výsledku $\bmod$ znamená známou funkci modulo definovanou vztahem $x = \lfloor x/y \rfloor \cdot y + (x \bmod y)$. Tudíž t je poslední číslicí dekadického zápisu m.

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

$$c(\mathbf{m},\mathbf{j}) \mapsto \text{if } \mathbf{j} \text{ then } c(\mathbf{m} \div \mathbf{10}, \mathbf{j}-\mathbf{1}) \text{ else } \mathbf{m} - \mathbf{10} * (\mathbf{m} \div \mathbf{10}) \text{ fi} \mapsto$$
$$\mapsto c(\mathbf{m} \div \mathbf{10}, \mathbf{j}-\mathbf{1}) \mapsto^* c(\mathbf{p},\mathbf{w}),$$

kde $\mathbf{p} \equiv \lfloor m/10 \rfloor$ a $\mathbf{w} \equiv j-1 = i$. □Podle I.P. platí $c(\mathbf{p},\mathbf{w}) \mapsto^* \mathbf{t}$ a t je číslice i-tého řádu dekadického zápisu čísla p. Jelikož $m = 10p + (m \bmod 10)$ a násobení deseti v dekadické soustavě znamená posun číslic v zápise „o jedno doleva“, je t zároveň číslice $i+1 = j$-tého řádu dekadického zápisu čísla m. To je přesně co bylo třeba dokázat.

□

Euklidův algoritmus

Věta 10.6. *Uvažme deklaraci Δ obsahující pouze rovnici*

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

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 $i \geq m+n$, 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

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

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

- $m=n$. Pak

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

- $m<n$. Pak

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

  kde $\mathbf{k}\equiv n-m$. □Platí $m+k=m+(n-m)=n\le i$, 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. $\square$

$\square$

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?