# 1-AIN-121 Diskrétna matematika (1)

## Zimný semester 2023/24

## 8. prednáška

Ján Komara

# Obsah prednášky

# Matematické dôkazy

## Základné druhy matematických dôkazov

- Leibnizovo pravidlo
  - Leibnizovo pravidlo pre rovnosť
  - Leibnizovo pravidlo pre ekvivalenciu
- Dôkaz implikácie
  - Priamy dôkaz
  - Nepriamy dôkaz
  - Dôkaz sporom
- Dôkaz rozborom prípadov
- Dôkaz myslenou konštrukciou
- Dôkaz indukciou
  - Matematická indukcia
  - Silná matematická indukcia
  - Úplna matematická indukcia
  - Indukcia s mierou

# Matematická indukcia

## Princíp matematickej indukcie

### Definícia

Pre každú formulu $\varphi[x]$, princíp matematickej indukcie podľa premennej $x$ pre formulu $\varphi$ je nasledujúce tvrdenie:

$$\varphi[0] \land \forall x(\varphi[x] \to \varphi[x+1]) \to \forall x \varphi[x].$$

Indukčná formula $\varphi$ môže obsahovať okrem indukčnej premennej $x$ aj iné voľné premenné ako parametre.

- Formula $\varphi[0]$ sa nazýva báza (základný krok) indukcie.
- Formula $\forall x(\varphi[x] \to \varphi[x+1])$ nazýva indukčný krok.
  - Formula $\varphi[x]$ sa nazýva indukčný predpoklad.
  - Formula $\varphi[x+1]$ sa nazýva záver indukčného kroku.

## Fibonacciho postupnosť

Je to postupnosť prirodzených čísel $f_n$ definovaná vzťahom:

$$f_0 = 0$$
$$f_1 = 1$$
$$f_{n+2} = f_{n+1} + f_n.$$

| n | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_n$ | 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | ... |

# Matematická indukcia

Verifikácia iteratívneho programu (while cyklus)

## Výpočet

Výpočtová postupnosť pre $f_5$:

$$f_5 = f_4 + f_3 = f_3 + f_2 + f_3 = f_2 + f_1 + f_2 + f_3 =$$

$$f_1 + f_0 + f_1 + f_2 + f_3 = 1 + f_0 + f_1 + f_2 + f_3 =$$

$$1 + 0 + f_1 + f_2 + f_3 = 1 + f_1 + f_2 + f_3 = 1 + 1 + f_2 + f_3 =$$

$$2 + f_2 + f_3 = 2 + (f_1 + f_0) + f_3 = 2 + (1 + f_0) + f_3 =$$

$$2 + (1 + 0) + f_3 = 2 + 1 + f_3 = 3 + f_3 = 3 + (f_2 + f_1) =$$

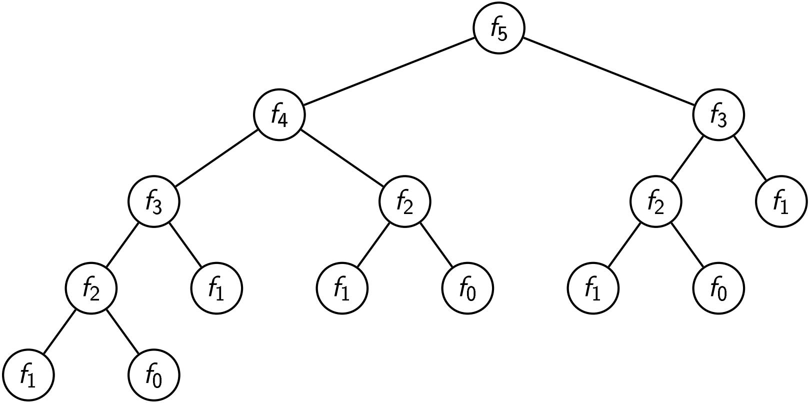
$$3 + (f_1 + f_0 + f_1) = 3 + (1 + f_0 + f_1) = 3 + (1 + 0 + f_1) =$$

$$3 + (1 + f_1) = 3 + (1 + 1) = 3 + 2 = 5.$$

# Matematická indukcia

## Verifikácia iteratívneho programu (while cyklus)

### Výpočtový strom



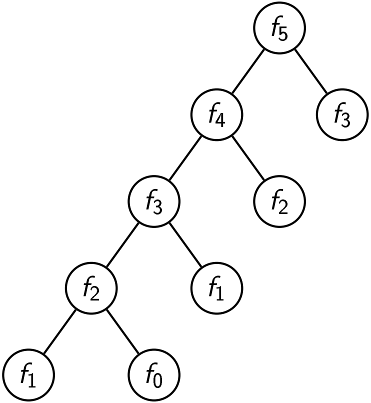
## Efektívny výpočet Fibonacciho postupnosti

Pythonovský program, ktorý počíta $f_n$:

```
def f(n):
    if n == 0:
        return(0)
    else:
        n = n-1
        a, b = 1, 0
        while n != 0:
            n, a, b = n-1, a+b, a
        return(a)
```

Počet krokov výpočtu je lineárny vzhľadom k vstupu $n$.

## Výpočtový strom



## Verifikácia programu

- Tvrdíme, že program počíta $f_n$.
- Stačí ukázať, že nasledujúci podprogram počíta $f_{n+1}$:

```
a, b = 1, 0
while n != 0:
    n, a, b = n-1, a+b, a
return(a)
```

# Matematická indukcia

## Verifikácia iteratívneho programu (while cyklus)

### Ako to dokázať?

Výstup tejto časti programu

```
while n != 0:
    n, a, b = n-1, a+b, a
return(a)
```

závisí od hodnôt premenných $n$, $a$ a $b$. Označme si ho $g(n, a, b)$. Stačí teda dokázať túto rovnosť:

$$g(n, 1, 0) = f_{n+1}.$$

Pri dôkaze využijeme, že platí

$$g(0, a, b) = a$$
$$g(n+1, a, b) = g(n, a+b, a).$$

## Iterácia deklaratívne

Uvažujme ternárnu funkciu $g$ definovanú primitívnou rekurziou so substitúciou v oboch parametroch:

$$\begin{aligned} g(0, a, b) &= a \\ g(n+1, a, b) &= g(n, a+b, a). \end{aligned}$$

Tvrdíme, že platí rovnosť

$$g(n, 1, 0) = f_{n+1}.$$

## Dôkaz

Dokážeme to matematickou indukciou podľa $n$.

# Matematická indukcia

## Verifikácia iteratívneho programu (while cyklus)

### Báza indukcie

Pre $n = 0$ tvrdenie platí, pretože

$$g(0, 1, 0) = 1 = f_1 = f_{0+1}.$$

### Indukčný krok

Predpokladajme, že tvrdenie platí pre $n$:

$$g(n, 1, 0) = f_{n+1}. \tag{IP}$$

To je indukčný predpoklad. Dokážeme, že platí aj pre $n + 1$:

$$g(n + 1, 1, 0) = g(n, 1 + 0, 1) = g(n, 1, 1) = \textbf{?}.$$

**Nedokázali sme to!**

## Iterácia deklaratívne

Uvažujme ternárnu funkciu $g$ definovanú primitívnou rekurziou so substitúciou v oboch parametroch:

$$\begin{aligned} g(0, a, b) &= a \\ g(n+1, a, b) &= g(n, a+b, a). \end{aligned}$$

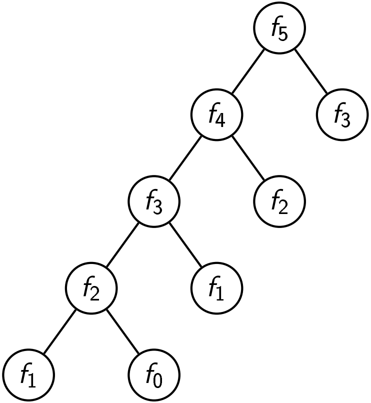
Tvrdíme, že platí rovnosť

$$g(n, 1, 0) = f_{n+1}.$$

# Matematická indukcia

## Verifikácia iteratívneho programu (while cyklus)

### Výpočtový strom



# Matematická indukcia

## Verifikácia iteratívneho programu (while cyklus)

### Lema

Pre každé prirodzené číslo $n$ a $k$ platí

$$g(n, f_{k+1}, f_k) = f_{n+1+k}.$$

### Dôkaz

Dokážeme to matematickou indukciou podľa $n$.

### Báza indukcie

Pre $n = 0$ tvrdenie platí, pretože

$$g(0, f_{k+1}, f_k) = f_{k+1} = f_{0+1+k}.$$

## Indukčný krok

Predpokladajme, že tvrdenie platí pre $n$:

$$g(n, f_{k+1}, f_k) = f_{n+1+k}. \tag{IP}$$

To je indukčný predpoklad. Dokážeme, že platí aj pre $n+1$:

$$g(n+1, f_{k+1}, f_k) = f_{n+1+1+k}.$$

Postupnými úpravami dostaneme

$$g(n+1, f_{k+1}, f_k) = g(n, f_{k+1} + f_k, f_{k+1}) = g(n, f_{k+2}, f_{k+1}) = \textbf{?}.$$

**Nedokázali sme to!**

# Matematická indukcia

## Verifikácia iteratívneho programu (while cyklus)

### Lema

Pre každé prirodzené číslo $n$ platí

$$\forall k \, g(n, f_{k+1}, f_k) = f_{n+1+k}.$$

### Dôkaz

Dokážeme to matematickou indukciou podľa $n$.

### Báza indukcie

Pre $n = 0$ tvrdenie platí, pretože

$$g(0, f_{k+1}, f_k) = f_{k+1} = f_{0+1+k}$$

pre ľubovolné číslo $k$.

# Matematická indukcia

## Verifikácia iteratívneho programu (while cyklus)

### Indukčný krok

Predpokladajme, že tvrdenie platí pre $n$:

$$\forall k\, g(n, f_{k+1}, f_k) = f_{n+1+k}. \tag{IP}$$

To je indukčný predpoklad. Dokážeme, že platí aj pre $n+1$:

$$\forall k\, g(n+1, f_{k+1}, f_k) = f_{n+1+1+k}.$$

Zvoľme si ľubovolné číslo $k$. Postupnými úpravami dostaneme

$$\begin{aligned} g(n+1, f_{k+1}, f_k) = g(n, f_{k+1} + f_k, f_{k+1}) &= g(n, f_{k+2}, f_{k+1}) \\ &\overset{\text{IP}}{=} f_{n+1+k+1} = f_{n+1+1+k}. \end{aligned}$$

Všimnime si, že sme IP použili s parametrom $k+1$ a nie s $k$!

## Dôkaz korektnosti programu

V predchádzajúcej leme sme dokázali, že rovnosť

$$g(n, f_{k+1}, f_k) = f_{n+1+k} \tag{1}$$

platí pre každé prirodzené číslo $n$ a $k$. Teraz už môžeme dokázať požadovanú identitu

$$g(n, 1, 0) = f_{n+1},$$

ktorá tvrdí, že naša efektívna implementácia Fibonacciho postupnosti je korektná. Postupnými úpravami dostaneme

$$g(n, 1, 0) = g(n, f_1, f_0) \overset{(1)}{=} f_{n+1+0} = f_{n+1}.$$

# Matematická indukcia

## Verifikácia iteratívneho programu (while cyklus)

$$f_0 = 0 \qquad f_1 = 1 \qquad f_{n+2} = f_{n+1} + f_n$$

### Imperatívny program

Efektívny výpočet postupnosti $f_n$ v paradigme imperatívneho programovania:

```
def f(n):
    if n == 0:
        return(0)
    else:
        n = n-1
        a, b = 1, 0
        while n != 0:
            n, a, b = n-1, a+b, a
        return(a)
```

## Deklaratívny program

Efektívny výpočet postupnosti $f_n$ v paradigme deklaratívneho programovania:

$$\begin{aligned} g(0, a, b) &= a \\ g(n+1, a, b) &= g(n, a+b, a) \end{aligned}$$

$$\begin{aligned} f_0 &= 0 \\ f_{n+1} &= g(n, 1, 0). \end{aligned}$$

Program pre $g$ má tvar *chvostovej* rekurzie. Optimalizujúci kompilátor nahradí takúto rekurziu jednoduchým skokom; nevyžaduje sa použitie všeobecnéhop mechanizmu pre volanie funkcie. Vznikne tak program podobný imperatívnemu cyklu.

## Definícia

Pre každú formulu $\varphi[x]$, princíp úplnej matematickej indukcie podľa premennej $x$ pre formulu $\varphi$ je nasledujúce tvrdenie:

$$\forall x\,(\forall y(y < x \to \varphi[y]) \to \varphi[x]) \to \forall x \varphi[x].$$

Indukčná formula $\varphi$ môže obsahovať okrem indukčnej premennej $x$ aj iné volné premenné ako parametre.

- Formula $\forall x\,(\forall y(y < x \to \varphi[y]) \to \varphi[x])$ sa nazýva indukčný krok.
  - Formula $\forall y(y < x \to \varphi[y])$ sa nazýva indukčný predpoklad.
  - Formula $\varphi[x]$ sa nazýva záver indukčného kroku.

Notačná konvencia:

$$\forall x\,(\forall y < x\,\varphi[y] \to \varphi[x]) \to \forall x \varphi[x].$$

# Úplna matematická indukcia

## Princíp úplnej matematickej indukcie

### Veta

*Princíp úplnej matematickej indukcie je platný logický princíp nad oborom prirodzených čísel.*

### Dôkaz

Predpokladajme, že formula $\phi[x]$ je *progresívna*:

$$\forall x \big(\forall y < x \, \phi[y] \to \varphi[x]\big). \tag{1}$$

Chceme ukázať, že $\varphi[x]$ platí pre každé prirodzené číslo $x$.

Najprv dokážeme túto pomocnú vlastnosť:

$$\forall n \forall z < n \, \phi[z]. \tag{2}$$

Dokážeme ju (obyčajnou) matematickou indukciou podľa $n$.

- V základnom kroku netreba nič dokazovať.

# Úplna matematická indukcia

## Princíp úplnej matematickej indukcie

- V indukčnom kroku predpokladajme, že platí
$$\forall y < n\, \phi[y]. \tag{IP}$$
Vyberme ľubovolné $z < n + 1$ a uvažujme dva prípady.
  - Ak $z < n$ potom $\phi[z]$ plynie z IP.
  - Ak $z = n$ potom z (1) pre $x$ rovné $z$ dostaneme
  $$\forall y < n\, \phi[y] \to \phi[z].$$
  Teraz stačí aplikovať IP a dostaneme, že $\phi[z]$ platí.

Tým sme dokázali pomocnú vlastnosť (2).

Nech $x$ je ľubovolné prirodzené číslo. Platnosť $\phi[x]$ plynie okamžite z (2); stačí tam totiž položiť $n$ rovné $x + 1$ and $z$ rovné $x$.

# Úplna matematická indukcia

## Vzorový príklad

### Poznámka

Na nasledujúcom probléme ilustrujeme princíp úplnej matematickej indukcie.

### Označenie

- $x \mid y$, ak prirodzené číslo $x$ delí prirodzené číslo $y$.
- $Pr(x)$, ak prirodzené číslo $x$ je prvočíslo.

### Veta

$$\forall x(x > 1 \to \exists p(Pr(p) \wedge p \mid x)).$$

### Dôkaz

Tvrdenie dokážeme úplnou matematickou indukciou.

# Úplna matematická indukcia

Vzorový príklad

## Indukčný krok

Predpokladajme, že tvrdenie platí pre každé $y < x$:

$$\forall y < x(y > 1 \rightarrow \exists p(Pr(p) \wedge p \mid y)). \qquad \text{(IP)}$$

To je indukčný predpoklad. Dokážeme, že platí aj pre $x$:

$$x > 1 \rightarrow \exists p(Pr(p) \wedge p \mid x)$$

Nech $x > 1$. Uvažujeme dva prípady.

- Číslo $x$ je prvočíslo. Stačí položiť $p$ rovné $x$.
- Číslo $x$ je zložené číslo. Vtedy $x$ sa dá zapísať v tvare $x = yz$, kde $y$ je číslo spĺňajúce nerovnosť $1 < y < x$. Z induktívneho predpokladu dostaneme, že existuje prvočíslo $p$, ktoré delí y. Potom $p$ delí aj $x$. Našli sme tak prvočíselného deliteľa čísla $x$.

# Indukcia s mierou

## Princíp indukcie s mierou

### Označenie

$$\vec{x} \equiv x_1, \ldots, x_n.$$

### Definícia

Pre každú formulu $\varphi[\vec{x}]$, princíp indukcie s mierou $\mu[\vec{x}]$ pre formulu $\varphi$ je nasledujúce tvrdenie:

$$\forall \vec{x}\,(\forall \vec{y}(\mu[\vec{y}] < \mu[\vec{x}] \to \varphi[\vec{y}]) \to \varphi[\vec{x}]) \to \forall \vec{x} \varphi[\vec{x}].$$

Indukčná formula $\varphi$ môže obsahovať okrem indukčných premenných $\vec{x}$ aj iné volné premenné ako parametre.

- Formula $\forall \vec{x}\,(\forall \vec{y}(\mu[\vec{y}] < \mu[\vec{x}] \to \varphi[\vec{y}]) \to \varphi[\vec{x}])$ sa nazýva indukčný krok.
  - Formula $\forall \vec{y}(\mu[\vec{y}] < \mu[\vec{x}] \to \varphi[\vec{y}])$ sa nazýva indukčný predpoklad.
  - Formula $\varphi[\vec{x}]$ sa nazýva záver indukčného kroku.

### Veta

*Princíp indukcie s mierou je platný logický princíp nad oborom prirodzených čísel.*

### Dôkaz

Predpokladajme, že formula $\phi[x]$ je *progresívna*:

$$\forall\vec{x}\,(\forall\vec{y}(\mu[\vec{y}] < \mu[\vec{x}] \to \varphi[\vec{y}]) \to \varphi[\vec{x}])\,. \tag{1}$$

Chceme ukázať, že $\varphi[\vec{x}]$ platí pre všetky prirodzené čísla $\vec{x}$.

Najprv dokážeme túto pomocnú vlastnosť:

$$\forall n \forall\vec{z}(\mu[\vec{z}] < n \to \phi[\vec{z}]). \tag{2}$$

Dokážeme ju (obyčajnou) matematickou indukciou podľa $n$.

- V základnom kroku netreba nič dokazovať.

# Indukcia s mierou

## Princíp indukcie s mierou

- V indukčnom kroku predpokladajme, že platí

  $$\forall \vec{y}(\mu[\vec{y}] < n \to \phi[\vec{y}]). \tag{IP}$$

  Vyberme ľubovolné $\vec{z}$: $\mu[\vec{z}] < n + 1$ a uvažujme dva prípady.
  - Ak $\mu[\vec{z}] < n$ potom $\phi[\vec{z}]$ plynie z IP.
  - Ak $\mu[\vec{z}] = n$ potom z (1) pre $\vec{x}$ rovné $\vec{z}$ dostaneme

    $$\forall \vec{y}(\mu[\vec{y}] < n \to \varphi[\vec{y}]) \to \varphi[\vec{z}].$$

    Teraz stačí aplikovať IP a dostaneme, že $\phi[\vec{z}]$ platí.

  Tým sme dokázali pomocnú vlastnosť (2).

Nech $\vec{x}$ sú ľubovolné prirodzené čísla. Platnosť $\phi[\vec{x}]$ plynie okamžite z (2); stačí tam totiž položiť $n$ rovné $\mu[\vec{x}] + 1$ and $\vec{z}$ rovné $\vec{x}$.

# Indukcia s mierou

## Verifikácia iteratívneho programu (for cyklus)

### Príklad

Uvažujme postupnosť prirodzených čísel $f_n$ definovanú vzťahom:

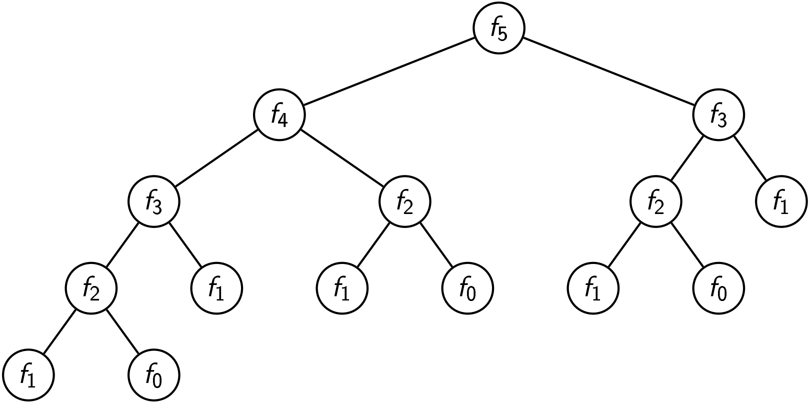
$$f_0 = 0$$
$$f_1 = 1$$
$$f_{n+2} = f_{n+1} + f_n + n.$$

| n | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_n$ | 0 | 1 | 1 | 3 | 6 | 12 | 22 | 39 | 67 | 113 | 188 | ... |

# Indukcia s mierou

## Verifikácia iteratívneho programu (for cyklus)

### Výpočtový strom



## Efektívny výpočet postupnosti

Pythonovský program, ktorý počíta $f_n$:

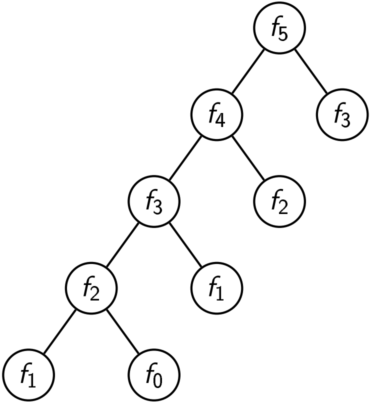
```
def f(n):
    if n == 0:
        return(0)
    else:
        n = n-1
        a, b = 1, 0
        for i in range(0, n):
            a, b = a+b+i, a
        return(a)
```

Počet krokov výpočtu je lineárny vzhľadom k vstupu $n$.

# Indukcia s mierou

## Verifikácia iteratívneho programu (for cyklus)

### Výpočtový strom



## Verifikácia programu

- Tvrdíme, že program počíta $f_n$.
- Stačí ukázať, že nasledujúci podprogram počíta $f_{n+1}$:

```
a, b = 1, 0
for i in range(0, n):
    a, b = a+b+i, a
return(a)
```

# Indukcia s mierou



## Ako to dokázať?

Uvažujme takéto zobecnenie predošlého *for* cyklu

```
for i in range(m, n):
    a, b = a+b+i, a
return(a)
```

Výstup tohoto programu závisí od od hodnôt premenných $m$, $n$, $a$ a $b$. Označme si ho $g(m, n, a, b)$. Stačí teda dokázať túto rovnosť:

$$g(0, n, 1, 0) = f_{n+1}.$$

Pri dôkaze využijeme, že platí

$$m \geq n \to g(m, n, a, b) = a$$
$$m < n \to g(m, n, a, b) = g(m+1, n, a+b+m, a).$$

# Indukcia s mierou

## Verifikácia iteratívneho programu (for cyklus)

### Modifikované odčítanie

$$x \dot{-} y = \begin{cases} x - y & \text{ak } x \geq y, \\ 0 & \text{ak } x \leq y. \end{cases}$$

### Iterácia deklaratívne

Uvažujme kvartérnu funkciu $g$ definovanú rekurzívne predpisom

$$g(i, n, a, b) = \begin{cases} a & \text{ak } i \geq n, \\ g(i+1, n, a+b+i, a) & \text{ak } i < n. \end{cases}.$$

Je to korektná rekurzívna definícia s mierou $n \dot{-} i$; platí totiž

$$i < n \to n \dot{-} (i+1) < n \dot{-} i.$$

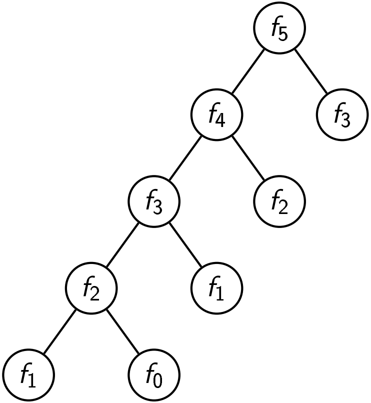
Tvrdíme, že platí rovnosť

$$g(0, n, 1, 0) = f_{n+1}.$$

# Indukcia s mierou

## Verifikácia iteratívneho programu (for cyklus)

### Výpočtový strom



# Indukcia s mierou

## Verifikácia iteratívneho programu (for cyklus)

### Lema

Pre každé prirodzené čísla $i$ a $n$ platí

$$i \leq n \to g(i, n, f_{i+1}, f_i) = f_{n+1}. \tag{1}$$

### Dôkaz korektnosti programu

Teraz už môžeme dokázať požadovanú identitu

$$g(0, n, 1, 0) = g(0, n, f_1, f_0) \stackrel{(1)}{=} f_{n+1}.$$

# Indukcia s mierou

## Verifikácia iteratívneho programu (for cyklus)

### Dôkaz lemy

Tvrdenie dokážeme indukciou s mierou $n \dot{-} i$. Nech $i$ a $n$ sú ľubovolné čísla také, že platí

$$\forall j \forall m \, (m \dot{-} j < n \dot{-} i \to j \leq m \to g(j, m, f_{j+1}, f_j) = f_{m+1}) \,. \quad \text{(IP)}$$

Predpokladajme ďalej, že $i \leq n$. Uvažujme dva prípady.

- Nech $i = n$. Z definície funkcie $g$ okamžite dostaneme, že

$$g(n, n, f_{n+1}, f_n) = f_{n+1} \,.$$

- Nech $i < n$. Odtiaľ $i < i + 1 \leq n$ a preto

$$\begin{aligned} g(i, n, f_{i+1}, f_i) &= g(i+1, n, f_{i+1} + f_i + i, f_{i+1}) \\ &= g(i+1, n, f_{i+2}, f_{i+1}) \stackrel{\text{IP}}{=} f_{n+1} \,. \end{aligned}$$

# Indukcia s mierou

## Verifikácia iteratívneho programu (for cyklus)

$$f_0 = 0 \qquad f_1 = 1 \qquad f_{n+2} = f_{n+1} + f_n + n$$

### Imperatívny program

Efektívny výpočet postupnosti $f_n$ v paradigme imperatívneho programovania:

```
def f(n):
    if n == 0:
        return(0)
    else:
        n = n-1
        a, b = 1, 0
        for i in range(0, n):
            a, b = a+b+i, a
        return(a)
```

## Deklaratívny program

Efektívny výpočet postupnosti $f_n$ v paradigme deklaratívneho programovania:

$$
\begin{aligned}
g(i, n, a, b) &= a \leftarrow i \geq n \\
g(i, n, a, b) &= g(n, a + b + i, a) \leftarrow i < n
\end{aligned}
$$

$$
\begin{aligned}
f_0 &= 0 \\
f_{n+1} &= g(0, n, 1, 0).
\end{aligned}
$$

Program pre $g$ má tvar *chvostovej* rekurzie. Optimalizujúci kompilátor nahradí takúto rekurziu jednoduchým skokom; nevyžaduje sa použitie všeobecnéhop mechanizmu pre volanie funkcie. Vznikne tak program podobný imperatívnemu cyklu.

# Záver

## Organizácia predmetu

- Konzultácie
  - Dnes o 14.30, m. I-16.
  - V piatok o 12.00, m. I-16 alebo online.
- 3. domáca úloha
  - Zadanie nájdete na webe predmetu.
  - Riešenie odovzdať do MOODLE najneskôr v pondelok 13. novembra.

# Záver

## Otázky

- Ak máte otázku, tak zdvihnite ruku.

# Koniec prednášky