Diskrétní struktury 1

Indukce a rekurze

Radim Bělohlávek

KATEDRA INFORMATIKY
UNIVERZITA PALACKÉHO V OLOMOUCI

Indukce a rekurze

- provázané jevy
- jsou přítomny v mnoha úvahách v matematice a informatice:
  - důkaz matematickou indukcí,
  - rekurzívní algoritmy,
  - rekurzívní definice, ...
- i jinde (umění, např. rekurzívní obrazce)

Indukce a rekurze jako provázané jevy kolem nás

- indukce a rekurze = dvě strany stejné mince
- „je to indukce nebo rekurze?“
  často těžko odpovědět, je to věc kontextu nebo pohledu
- indukce $\approx$ od menšího k většímu (složitějšímu), „bottom up“
  př.: induktivní definice, induktivní důkaz, ...
- rekurze $\approx$ definice pojmu pomocí pojmu samotného, „top down“
  př.: rekurzívní procedura, rekurzívně definovaný pojem

První příklady

faktoriál

f(n)
1 **if** $n = 1$ **then return** 1
2 **return** $n *$ f($n - 1$)

- rekurzívní funkce (rekurzívně definovaný pojem faktoriál čísla n)
- ř. 1: limitní (ukončující podmínka); jinak se procedura (definice) „zacyklí“

f(4) = 4 * f(3) = 4 * 3 * f(2) = 4 * 3 * 2 * f(1) = 4 * 3 * 2 * 1

jinak

1. pro $n = 1$ je $f(n) = 1$
2. pro $n > 1$ je $f(n) = n * f(n-1)$

nebo jinak zapsáno

$$f(n) = \begin{cases} 1, & \text{pokud } n = 1, \\ n * f(n-1), & \text{pokud } n > 1. \end{cases}$$

- induktivní definice
- definujeme nejprve pro základní prvky (pro $n = 1$)
- pro složitější prvky ($n > 1$) definujeme pomocí toho, co jsme definovali pro jednodušší prvky ($f(n-1)$).

definice mocniny čísla a^n:

power(a, n)
1 **if** $n = 0$ **then return** 1
2 **return** $a *$ power$(a, n - 1)$

1. pro $n = 0$ je $a^n = 1$
2. pro $n > 1$ je $a^n = a * a^{n-1}$

Stejné schéma má definice mocniny R^n relace R.

induktivní definice množiny L všech lichých čísel:

1. pro $1 \in L$
2. pokud $n \in L$, pak $n + 2 \in L$
   (nebo úplně: pro každé $n > 1$: pokud $n \in L$, pak $n + 2 \in L$)

Matematickou indukcí lze např. dokázat, že každé $n \in L$ je liché.

induktivní definice množiny $A \subseteq \mathbb{N}_0 \times \mathbb{N}_0$

1. pro $\langle 0, 0 \rangle \in A$
2. pokud $\langle m, n \rangle \in A$, pak $\langle m + 5, n + 1 \rangle \in A$

Je $S = \{\langle 0, 0 \rangle, \langle 5, 1 \rangle, \langle 10, 2 \rangle, \langle 15, 3 \rangle, \}$

Zobecněnou matematickou indukcí lze např. dokázat, že pro každé $\langle m, n \rangle \in A$ je $m + n$ dělitelné 3.

formule výrokové logiky na množinou $V = \{p, q, r, \dots\}$ výrokových symbolů

1. každý výrokový symbol p je formule (tzv. atomická formule);
2. jsou-li φ a ψ formule, jsou i výrazy

   $\neg\varphi$,
   $(\varphi \wedge \psi)$,
   $(\varphi \vee \psi)$,
   $(\varphi \to \psi)$,
   $(\varphi \leftrightarrow \psi)$

   formule (tzv. složené formule).

– induktivně definovaná syntaktická struktura
– v pozadí je tzv. strukturální indukce (zobecnění matematické indukce)

Sierpinského trojúhelníky $S(n)$

$S(1)$ $S(2)$ $S(3)$ $S(4)$ $S(5)$

Droste efekt (Drosteho kakao, 1904)

Matematická indukce (připomenutí ze školy)

Umožňuje dokazovat tvrzení tvaru

$$\text{pro každé přirozené číslo } n \text{ platí } V(n),$$

kde $V(n)$ je nějaké tvrzení, které závisí na n, např.

$$\text{pro každé přirozené číslo } n \text{ platí } 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Základem je:

Věta (princip indukce)
Nechť je pro každé $n \in \mathbb{N}$ dáno tvrzení $V(n)$. Předpokládejme, že platí

(a) $V(1)$ (indukční předpoklad),

(b) pro každé $n \in \mathbb{N}$: z $V(n)$ plyne $V(n+1)$ (indukční krok).

Pak $V(n)$ platí pro každé $n \in \mathbb{N}$.

Lze princip indukce dokázat?

- Jednoduchá odpověď:
  - Ano, s použitím následující vlastnosti $\mathbb{N}$:
  - Každá neprázdná podmnožina množiny $\mathbb{N}$ má nejmenší prvek.
- Ale, jak víme, že každá neprázdná podmnožina $\mathbb{N}$ má nejmenší prvek?!
  - Vede na otázku: Co jsou vlastně přirozená čísla?
  - Axiomatická výstavba $\mathbb{N}$, Peanovy axiomy, atd.
  - Tím se podrobně zabývat nebudeme (detaily [DS1]).

Důkaz principu indukce

Sporem: Předpokládejme, že princip indukce neplatí, tj. existuje tvrzení $V(\cdot)$, splňující

(a) $V(1)$,

(b) pro každé $n \in \mathbb{N}$: z $V(n)$ plyne $V(n+1)$,

ale pro nějaké $n' \in \mathbb{N}$ tvrzení $V(n')$ neplatí.

Označme

$$K = \{m \in \mathbb{N} \mid V(m) \text{ neplatí}\}$$

K je neprázdná (neboť $n' \in K$).

K má tedy nejmenší prvek ka ten je různý od 1 (protože $V(1)$ platí).

Pak tedy $k-1 \notin K$, tedy $V(k-1)$ platí.

Z indukčního kroku plyne, že platí i $V(k)$, tedy $k \notin K$, což je spor s $k \in K$. □

Příklad

Dokažme, že pro každé $n \in \mathbb{N}$ je

$$\text{pro každé } n \in \mathbb{N} \text{ je } 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Tedy $V(n)$ je tvrzení $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

(a) Indukční předpoklad: $V(1)$ je tvrzení $1 = \frac{1 \cdot (1+1)}{2}$, což platí.

(b) Indukční krok: dokázat, že z $V(n)$ plyne $V(n+1)$.

Tedy dokázat, že z $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ plyne $1 + 2 + \cdots + (n+1) = \frac{(n+1)(n+2)}{2}$

$$1 + \cdots + n + (n+1) = (1 + \cdots + n) + (n+1) = \text{(dle indukčního předpokladu } V(n)\text{)}$$
$$\frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{n^2 + 3n + 2}{2} = \frac{(n+1) \cdot (n+2)}{2}.$$

Pozor na chyby

Příklad Dokažte, že pro každou posloupnost n prvků $a_1, \ldots, a_n$ platí, že všechny prvky v ní jsou stejné.

Důkaz matematickou indukcí:

Indukční předpoklad: Pro číslo 1 je tvrzení triviálně splněno.

Indukční krok: Předpokládejme, že tvrzení platí pro k prvků. Uvažujme posloupnost libovolných $k+1$ prvků $a_1, \ldots, a_{k+1}$.

Pak $a_1, \ldots, a_k$ je posloupnost k prvků a $a_2, \ldots, a_{k+1}$ je posloupnost k prvků, a podle předpokladu tedy $a_1 = \cdots = a_k$ a $a_2 = \cdots = a_{k+1}$. Odtud plyne $a_1 = \cdots = a_{k+1}$.

Kde je chyba?

Další příklady

Příklad Dokažte indukcí, že $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

$V(n)$ je tvrzení $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

$V(1)$ platí, protože je to tvrzení $1^2 = \frac{1(1+1)(2+1)}{6}$.

Předpokládejme, že platí $V(n)$ a dokažme $V(n+1)$, tj. dokažme

$$\sum_{k=1}^{n+1} k^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6}.$$

Je

$$\begin{aligned} \sum_{k=1}^{n+1} k^2 &= \sum_{k=1}^{n} k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6} \\ &= \frac{2n^3+9n^2+13n+6}{6} = \frac{(n+1)(n+2)(2(n+1)+1)}{6}. \end{aligned}$$

1. Dokažte indukcí, že součet prvních n lichých čísel je n^2, tj.

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

2. Dokažte indukcí, že $\sum_{k=1}^{n} k^3 = [\frac{n(n+1)}{2}]^2$.
3. Dokažte indukcí, že pro $n \in \mathbb{N}$ je $2^{n+2} + 3^{2n+1}$ dělitelné 7.
4. Dokažte, že pro $n \in \mathbb{N}$ je $(1 + \frac{1}{3})^n \geq 1 + \frac{n}{3}$.

Odbočka: o přirozených číslech

– S přirozenými čísly pracujeme jako se známou strukturou, tj. $\mathbb{N}$, $+$, $\cdot$, $\leq$.
Předpokládáme vlastnosti, které známe.
– Otázky jako „proč platí princip indukce?“ nebo „proč má každá $A \subseteq \mathbb{N}$ nejmenší prvek“ vedou k otázce:

Co jsou vlastně přirozená čísla?

– Jsou budována axiomaticky, tj. je to struktura splňující jisté axiomy.
– Za základní (nedefinovatelné) jsou považovány
  –
  – Konstanta 1.
  (alternativně 0 míst 1; pak je i 0 považována za přirozené číslo; je to otázka vkusu a technické výhodnosti)
  – Unární operace S. $S(x)$ je interpretován jako následovník čísla x.
  (tedy $S(1) = 2$, $S(2) = 3$, $S(3) = 4$, $\dots$)

Co jsou vlastně přirozená čísla?

- Jsou budována axiomaticky, tj. je to struktura splňující jisté axiomy.
- Za základní (nedefinovatelné) jsou považovány:
  - Konstanta 1.
    (alternativně 0 míst 1; pak je i 0 považována za přirozené číslo; je to otázka vkusu a technické výhodnosti)
  - Unární operace S. $S(x)$ je interpretován jako následovník čísla x.
    (tedy $S(1) = 2$, $S(2) = 3$, $S(3) = 4$, ...)
- Přirozená čísla jsou pak definována jako struktura $\langle \mathbb{N}, 1, S \rangle$, kde $1 \in \mathbb{N}$ a $S : \mathbb{N} \to \mathbb{N}$, splňující tzv. Peanovy axiomy.

Peanovy axiomy (výběr):

- ...
- pokud $m \neq n$, pak $S(m) \neq S(n)$
- neexistuje $n \in N$ tak, že $S(n) = 1$

  (1 není následovníkem žádného přirozeného čísla)
- Pokud $K \subseteq \mathbb{N}$ je množina splňující
  - $1 \in K$
  - pro každé $n \in \mathbb{N}$: pokud $n \in K$, pak $n + 1 \in K$,

  pak $K = \mathbb{N}$.

Další operace a relace ($+$, $\cdot$, $\leq$) jsou definované jako odvozené; např.

- $n + 1 := S(n)$
- $n + S(m) = S(n + m)$

Poslední axiom:

- Pokud $K \subseteq \mathbb{N}$ je množina splňující
  - $1 \in K$
  - pro každé $n \in \mathbb{N}$: pokud $n \in K$, pak $n + 1 \in K$,

  pak $K = \mathbb{N}$.

říká právě to, co princip důkazu matematickou indukcí!

Skutečně: Položíme-li v tom principu $K = \{n \mid V(n) \text{ platí}\}$, pak tvrzení principu je shodné s tvrzením axiomu.

Tedy

- Při tomto pohledu (axiomatickém) na přirozená čísla tedy není třeba princip důkazu indukcí dokazovat (je to axiom).
- Proč jsme ho tedy dokazovali?
  - Protože s přirozenými čísly pracujeme intuitivně, jako se strukturou splňující známé vlastnosti.
  - Jednou z nich je: Každá $A \subseteq \mathbb{N}$ má nejmenší prvek (vzhledem k $\leq$).
    Jinými slovy: $\langle \mathbb{N}, \leq \rangle$ je dobře uspořádaná.
  - Tu jsme použili v důkazu principu.

Důležité:

- Víme: Každá $A \subseteq \mathbb{N}$ má nejmenší prvek $\Rightarrow$ princip důkazu matematickou indukcí
- Platí ale také:
  Princip důkazu matematickou indukcí $\Rightarrow$ každá $A \subseteq \mathbb{N}$ má nejmenší prvek.

Varianty důkazu matematickou indukcí

Věta (začátek v k)
Nechť $k \in \mathbb{Z}$, $K = \{k, k+1, k+2, \dots\}$ a pro každé $n \in K$ je dáno tvrzení $V(n)$.
Předpokládejme, že platí

(a) $V(k)$ (indukční předpoklad),

(b) pro každé $n \in K$: z $V(n)$ plyne $V(n+1)$ (indukční krok).

Pak $V(n)$ platí pro každé $n \in K$.

Indukce nemusí začínat 1. Např. $K = \{4, 5, 6, \dots\}$, $K = \{-3, -2, -1, 0, 1, \dots\}$.

Důkaz Plyne ze základního principu indukce:

Uvažujme tvrzení $W(n)$ pro $n = 1, 2, 3, \ldots$ definované:

$$W(n) = V(n + (k - 1)).$$

Pak $W(1)$ je $V(k)$, $W(2)$ je $V(k + 1)$, atd.

Podmínky (a) a (b) výše jsou pak podmínky $W(1)$ a $W(n) \Rightarrow W(n + 1)$ ze základního principu.

Dle základního principu tedy platí $W(1)$, $W(2)$, $\ldots$

Tedy platí $V(1)$, $V(2)$, z...

Příklad Zobecněte vzorec

$$1 + 2 + \cdots + n = \frac{n \cdot (n+1)}{2}$$

pro

$$k + (k+1) + \cdots + n$$

Dokažte uvedeným zobecněním principu indukce. Viz [DS1].

Věta (více předpokladů, tzv. silný princip indukce)
Nechť je pro každé $n \in \mathbb{N}$ dáno tvrzení $V(n)$. Předpokládejme, že platí

(a) $V(1)$ (indukční předpoklad),

(b) pro každé $n \in K$: z $V(1), \ldots, V(n)$ plyne $V(n+1)$ (indukční krok).

Pak $V(n)$ platí pro každé $n \in \mathbb{N}$.

Důkaz Snadné ze základního principu indukce. Viz [DS1].

Platí i pokud začneme libovolným $k \in \mathbb{N}$ (ne nutně $k = 1$).

Platí i naopak: základní princip indukce plyne ze silného principu.

Příklad Dokažte, že každé $n \in \mathbb{N}$ má prvočíselný rozklad.

Silným principem indukce se začátkem v $k = 2$.

indukční předpoklad: $V(2)$

Platí, protože 2 je prvočíslo, tedy $2 = 2^1$ je požadovaný rozklad.

indukční krok: z $V(2), \ldots, V(n)$ plyne $V(n+1)$

Buď je $n+1$ prvočíslo, pak rozklad je $n+1 = (n+1)^1$,

nebo n je složené, tedy $n = r \cdot s$, kde $2 \leq r, s < n$.
Pak dle $V(r)$ a $V(s)$ existují rozklady $r = p_1^{n_1} \cdots p_k^{n_k}$ a $s = q_1^{m_1} \cdots q_l^{m_l}$, a tedy požadovaný rozklad je

$$n+1 = p_1^{n_1} \cdots p_k^{n_k} \cdot q_1^{m_1} \cdots q_l^{m_l}.$$

Definice matematickou indukcí

Např. faktoriál:

1. pro $n = 1$ je $f(n) = 1$
2. pro $n > 1$ je $f(n) = n * f(n-1)$

Intuitivně jasné. Jaké je pozadí (zdůvodnění)?

Věta Nechť je dána množina V, prvek $a \in V$ a funkce $G : \mathbb{N} \times V \to V$. Pak existuje právě jedna funkce

$$F : \mathbb{N} \to V,$$

pro kterou platí

- $F(1) = a$,
- pro každé $n \in N$: $F(n+1) = G(n, F(n))$.

Důkaz Viz [DS1].

Příklad Pro definici faktoriálu $f(n)$ výše je:

$$F = f, \quad V = \mathbb{N}, \quad a = 1, \quad G(m, n) = (m+1) \cdot n.$$

Příklad Uvažujme předpis:

1. pro $n = 0$ je $f(n) = 1$
2. pro $n > 0$ je $f(n+1) = -f(n)$

Dle věty (resp. její modifikace pro $\mathbb{N}_0$) je jím jednoznačně určena funkce $f : \mathbb{N}_0 \to \mathbb{Z}$. ($V = \mathbb{Z}$, $a = 1$, $G(m, n) = -F(n)$)

Snadno se vidí, že $f(n) = (-1)^n$.

Příklad (zobecněná definice indukcí, dle modifikace uvedené věty) Uvažujme předpis:

1. $f(1) = 3$, $f(2) = 5$,
2. $f(n+1) = 2f(n) - f(n-1)$.

Dle věty (resp. její modifikace pro více předpokladů) je jím jednoznačně určena funkce $f : \mathbb{N} \to \mathbb{Z}$. Detaily viz [DS1].

Snadno se dokáže, že $f(n) = 2n + 1$.

Strukturální indukce

- Je zobecněním matematické indukce.
- Místo $\mathbb{N}$ pracuje s množinou T.
- T je často množina řetězců utvořených podle induktivních pravidel. Př. Definice formule:
  - (bazické/atmoické) $p \in T$ pro každý výrokový symbol p;
  - (složené) pokud $\varphi, \psi \in T$, pak $\neg\varphi \in T$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $(\varphi \leftrightarrow \psi)$
- Důkaz strukturální indukcí: Že tvrzení V platí pro všechny prvky $t \in T$ se dokáže takto (př. formule):
  - indukční předpoklad: V platí pro všechny atomické (bázické) $t \in T$
  - indukční krok: pokud V platí pro φ a ψ, pak $\varphi, \psi \in T$, pak $\neg\varphi \in T$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $(\varphi \leftrightarrow \psi)$

Příklad Dokažte, že v každé formuli výrokové logiky je počet levých i pravých závorek stejný.

Označme $l(\varphi)$ a $r(\varphi)$ počty levých a pravých závorek ve φ.

indukční předpoklad: $l(p) = 0 = r(p)$

indukční krok: např. pro $\wedge$:

předpokládáme $l(\varphi) = r(\varphi)$ a $l(\psi) = r(\psi)$

pak

$$l((\varphi \wedge \psi)) = 1 + l(\varphi) + l(\psi) = 1 + r(\varphi) + r(\psi) = r((\varphi \wedge \psi)).$$

Definice strukturální indukcí

- definujeme pro bazické prvky T
- definujeme pro složené prvky T

Příklad počet $\#\varphi$ výskytů výrokových proměnných ve formuli φ, tedy např. $\#(p \wedge (\neg p \vee q)) = 3$

- $\#p = 1$,
- $\#(\neg\varphi) = \#\varphi$,
  $\#(\varphi \wedge \psi) = \#\varphi + \#\psi$,
  $\ldots$

Další množiny T struktur, pro které lze použít strukturální indukci:

- aritmetické výrazy nad $X = \{x, y, \dots\}$ a funkčními symboly $+$ a $\cdot$
  - pokud $t \in X$, pak $t \in T$ (atomický),
  - pokud $t_1, t_2 \in T$, pak $(t_1 + t_2) \in T$ a $(t_1 \cdot t_2) \in T$ (složený)
- rekurzívně definované seznamy,
- rekurzívně definované stromy,
- ...
- přirozená čísla jsou speciálním případem:
  - $1 \in T$ (první číslo),
  - pokud $t \in T$, pak $S(t) \in T$ (následovník)