ČO JE MATEMATICKÁ INDUKCIA?

BOHUSLAV SIVÁK, Zvolen

Prakticky každá učebnica alebo prehľad stredoškolskej matematiky sa zmieňuje o metóde dôkazu matematickou indukciou a uvádza k nej niekoľko jednoduchých príkladov. Obvykle uvádzaná schéma je však vo svojej pôvodnej forme neraz ťažko použiteľná. Preto si všimneme niektoré jej obmeny, ako aj ďalšie otázky súvisiace s touto problematikou.

1. Schémy dôkazu matematickou indukciou

Majme daný určitý predpis T, ktorý ľubovoľnému prirodzenému číslu n priradí výrok $T(n)$. Ak chceme dokázať, že $T(n)$ je pravdivý pre všetky prirodzené čísla n, môžeme postupovať takto:

(i) dokážeme, že výrok $T(1)$ je pravdivý,

(ii) pre ľubovoľné prirodzené číslo n dokážeme, že ak je pravdivý výrok $T(n)$, tak je pravdivý aj výrok $T(n + 1)$.

Presvedčenie o korektnosti tohoto dôkazu sa opiera o takúto úvahu: Podľa (i) je výrok $T(1)$ pravdivý, použitím (ii) pre $n = 1$ zistíme, že aj výrok $T(2)$ je pravdivý, použitím (ii) pre $n = 2$ zistíme, že aj výrok $T(3)$ je pravdivý atď. Tu je dôležitá predstava, že každé prirodzené číslo možno získať z čísla 1 postupným pridávaním jednotky. To však nie je také samozrejmé, ako sa na prvý pohľad zdá.

Schéma dôkazu uvedenou metódou vyzerá v obvyklom zápise logiky takto (symbol $\forall$ čítame „pre všetky", symbol $\Rightarrow$ „implikuje" alebo „má za následok pravdivosť výroku"):

$$\frac{\begin{array}{c} T(1) \\ (\forall n)\,[T(n) \Rightarrow T(n+1)] \end{array}}{(\forall n)\,T(n)}\,. \tag{1}$$

Príklad 1. Pomocou schémy (1) dokážeme, že $n + 1 \leqq 2^n$ pre všetky prirodzené čísla n. Nech $T(n)$ znamená „$n + 1 \leqq 2^n$". Pretože $T(1)$ je $2 \leqq 2$, vidíme, že výrok $T(1)$ je pravdivý. Predpokladajme teda, že n je prirodzené číslo a že výrok $T(n)$ je pravdivý, t. j. že platí $n + 1 \leqq 2^n$. Potom aj $2n + 2 \leqq 2^{n+1}$, a tým skôr $n + 2 \leqq 2^{n+1}$, čo je $T(n + 1)$.
Pre ľubovoľné prirodzené číslo k možno použiť schému

$$\frac{\begin{array}{c} T(k) \\ (\forall n)\{(n \geqq k) \Rightarrow [T(n) \Rightarrow T(n+1)]\} \end{array}}{(\forall n)[(n \geqq k) \Rightarrow T(n)]}\,, \tag{2}$$

z ktorej pre $k = 1$ dostávame schému (1). Táto schéma je rovnocenná so schémou (1), v ktorej miesto $T(n)$ píšeme $T(n + k - 1)$.

Príklad 2. Pomocou schémy (2) dokážeme, že ľubovoľné prirodzené číslo $n > 7$ sa dá písať v tvare $n = 3x + 5y$, kde x, y sú celé nezáporné čísla. Nech $k = 8$ a nech $T(n)$ znamená „existujú celé nezáporné čísla x, y tak, že $n = 3x + 5y$". Výrok $T(8)$ je pravdivý, lebo $8 = 3 . 1 + 5 . 1$. Nech teda $n \geqq 8$ a nech výrok $T(n)$ je pravdivý. Potom existujú celé nezáporné čísla x, y tak, že $n = 3x + 5y$. Sú dve možnosti:

a) $y = 0$, potom $3x = n \geqq 8$, z čoho $x \geqq 3$. V tomto prípade však z rovnosti $n + 1 = 3(x - 3) + 5.2$ vyplýva, že výrok $T(n + 1)$ je pravdivý.

b) $y \geqq 1$, potom zas $n + 1 = 3(x + 2) + 5\,(y - 1)$, teda výrok $T(n + 1)$ je pravdivý.

Poznamenajme, že v schéme (2) sa nevyskytujú výroky $T(n)$ pre $n < k$. Preto pri jej použití nezáleží na tom, či tieto výroky sú pravdivé, nepravdivé alebo dokonca nedefinované. V prípade, že všetky výroky $T(n)$ pre $n < k$ sú pravdivé, môžeme miesto (2) použiť schému

$$\frac{\begin{array}{c} T(1), \ldots, T(k) \\ (\forall n)\{(n \geqq k) \Rightarrow [T(n) \Rightarrow T(n + 1)]\} \end{array}}{(\forall n)\, T(n)} \tag{3}$$

z ktorej pre $k = 1$ opäť dostaneme schému (1).

Príklad 3. Dokážeme, že $n^2 - 1 \leqq 2^n$ pre všetky prirodzené čísla n. Nech $k = 3$ a nech $T(n)$ znamená „$n^2 - 1 \leqq 2^n$". Pravdivosť výrokov $T(1)$, $T(2)$, $T(3)$ overíme priamym dosadením — dostaneme výroky $0 \leqq 2$, $3 \leqq 4$, $8 \leqq 8$. Zvoľme teda prirodzené číslo $n \geqq 3$ tak, že výrok $T(n)$ je pravdivý. Potom $n^2 - 1 \leqq 2^n$, teda aj $2n^2 - 2 \leqq 2^{n+1}$, čo možno písať v tvare

$$[(n + 1)^2 - 1] + (n^2 - 2n - 2) \leqq 2^{n+1}.$$

Pretože $n \geqq 3$, platí $n^2 - 2n - 2 \geqq 3n - 2n - 2 = n - 2 > 0$, teda aj

$$(n + 1)^2 - 1 \leqq 2^{n+1},$$

čo je $T(n + 1)$. (Voľba $k = 3$ je odôvodnená tým, že pre $n < 3$ je $n^2 - 2n - 2 < 0$.)

Pri použití schém (2), (3) sa základná myšlienka indukcie (krok od $T(n)$ k $T(n + 1)$) uplatní až od čísla k. K tomu treba poznamenať, že indukcia môže začínať od ľubovoľného celého (aj záporného) čísla. V matematickej praxi sa dosť často vyskytuje indukcia začínajúca od 0.

Ďalšou obmenou schémy (1) je schéma

$$\frac{(\forall n)\{(\forall k)[(k < n) \Rightarrow T(k)] \Rightarrow T(n)\}}{(\forall n)\, T(n)}. \tag{4}$$

Príklad 4. Dokážeme, že každé prirodzené číslo n sa dá písať v tvare $n = 2^{s-1}(2t - 1)$, kde s, t sú prirodzené čísla. Použijeme schému (4), pričom $T(n)$ bude znamenať „existujú prirodzené čísla s, t tak, že

$$n = 2^{s-1}(2t - 1)".$$

Nech n je prirodzené číslo a nech výrok $T(k)$ je pravdivý pre všetky prirodzené čísla $k < n$. Podľa (4) stačí dokázať, že výrok $T(n)$ je pravdivý. Sú dve možnosti:

a) Číslo n je nepárne. Potom stačí vziať $s = 1$, $t = \frac{n+1}{2}$.

b) Číslo n je párne. Potom existuje prirodzené číslo k tak, že $n = 2k$. Pretože však $k < n$, výrok $T(k)$ je pravdivý, t. j. existujú prirodzené čísla s_1, t_1 tak, že $k = 2^{s_1-1}(2t_1 - 1)$. Stačí vziať $s = s_1 + 1$, $t = t_1$.

Pri používaní schémy (4) si treba niekedy uvedomiť, že výrok

$$(\forall k)[(k < 1) \Rightarrow T(k)] \Rightarrow T(1)$$

nie je nič iného ako $T(1)$.

Ukážeme si ešte dva odstrašujúce príklady „dôkazu" indukciou.

Príklad 5. Starí Gréci poznali tzv. Soritov paradox (pozri [1]), podľa ktorého mužovi s hustými vlasmi možno vytrhnúť ľubovoľný počet vlasov. Toto tvrdenie „dokážeme" indukciou.

Nech $T(n)$ znamená „ak mužovi s hustými vlasmi vytrhneme n vlasov, stále ešte bude mať husté vlasy." Výrok $T(1)$ je pravdivý. Zvoľme teda prirodzené číslo n tak, že výrok $T(n)$ je pravdivý. Čo sa stane, ak uvažovanému mužovi vytrhneme $n + 1$ vlasov? Ak mu vytrhneme n vlasov, podľa $T(n)$ bude mať husté vlasy, a ak mu vytrhneme ešte jeden vlas, podľa $T(1)$ bude mať ešte stále husté vlasy. To ale znamená, že výrok $T(n + 1)$ je pravdivý, a na základe schémy (1) usudzujeme, že výrok $T(n)$ je pravdivý pre všetky prirodzené čísla n.

Príklad 6. Myšlienka Soritovho paradoxu sa dá použiť aj v iných prípadoch. Nech napríklad $T(n)$ znamená „ak do poloprázdnej električky nastúpi n ľudí, električka bude ďalej poloprázdna." Výrok $T(1)$ je pravdivý. Zvoľme teda prirodzené číslo n tak, že výrok $T(n)$ je pravdivý. Čo sa stane, ak do našej električky nastúpi $n + 1$ ľudí? Ak nastúpi n ľudí, podľa $T(n)$ električka zostane poloprázdna, a po nastúpení $(n + 1)$-ého človeka bude poloprázdna podľa $T(1)$. To znamená, že výrok $T(n + 1)$ je pravdivý, a na základe schémy (1) usudzujeme, že výrok $T(n)$ je pravdivý pre všetky prirodzené čísla n, t. j. do našej električky sa zmestí ľubovoľne veľa ľudí!

2. Nedokázateľnosť schémy indukcie

Ako sme už spomenuli, obvyklé odôvodnenie schémy (1) sa opiera o predstavu, že každé prirodzené číslo možno skonštruovať z čísla 1 postupným pridávaním jednotky. V niektorých modeloch aritmetiky prirodzených čísel to však neplatí, a táto skutočnosť súvisí s nedokázateľnosťou schémy (1).

Teraz skonštruujeme jedno z tzv. elementárnych rozšírení štruktúry $(N, =, 1, \leqq)$, kde N je množina všetkých prirodzených čísel a symboly $=$, 1, $\leqq$ majú obvyklý aritmetický význam.

Príklad 7. Nech P je množina všetkých polynómov tvaru $a + bx$, kde a, b sú celé čísla, pričom $a > 0$ alebo $b = 1$. To znamená, že

$$P = \{1, 2, \ldots, \ldots, -2 + x, -1 + x, x, 1 + x, 2 + x, \ldots\}.$$

V súhlase s týmto zápisom môžeme na množine P zaviesť usporiadanie $=$ takto:

$a + bx \leqq c + dx$ práve vtedy, ak $b < d$ alebo $a \leqq c$, $b = d$. Štruktúra $(P, =, 1, \leqq)$ má potom tieto vlastnosti:

N je podmnožinou množiny P,

usporiadanie $\leqq$ množiny P splýva na N s obvyklým usporiadaním prirodzených čísel.

Ľahko sa presvedčíme, že štruktúry $(N, =, 1, \leqq)$ a $(P, =, 1, \leqq)$ sú modelmi teórie s axiomatikou D tvorenou týmito axiómami (symbol $\exists$ čítame „existuje", symbol $\wedge$ „a", symbol $\vee$ „alebo"):

$$(\forall x)\,(x \leqq x)$$
$$(\forall x)\,(1 \leqq x)$$
$$(\forall x)\,(\forall y)\,[(x \leqq y \wedge y \leqq x) \Rightarrow x = y]$$
$$(\forall x)\,(\forall y)\,(\forall z)\,[(x \leqq y \wedge y \leqq z) \Rightarrow x \leqq z]$$
$$(\forall x)\,(\forall y)\,(x \leqq y \vee y \leqq x)$$
$$(\forall x)\,(\exists y)\,S(x, y)$$
$$(\forall x)](x \neq 1) \Rightarrow (\exists y)\,S(y, x)],$$

kde $S(u, v)$ znamená

$$(u \leqq v) \wedge (u \neq v) \wedge (\forall w)[(u \leqq w \wedge w \leqq v) \Rightarrow (u = w \vee w = v)],$$

inými slovami, výrok $S(u, v)$ je splnený práve vtedy, ak v nasleduje bezprostredne za u.

A. Robinson dokázal, že táto teória je úplná, a teda v jej modeloch $(N, =, 1, \leqq)$ a $(P, =, 1, \leqq)$ sú splnené presne tie isté výroky sformulované pomocou relácií $=$, $\leqq$ a konštanty 1 (pozri [2]).

Vráťme sa k problému odvoditeľnosti schémy (1). Matematická logika sa zaoberá skúmaním formalizovaných teórií, ktorých tvrdenia sa zapisujú

pomocou tzv. formúl v nejakom formálnom jazyku. Do takého formálneho jazyka patria:

(I) logické symboly — premenné (napr. x, y, z, u, v, w, ...), logické spojky (napr. $\vee$, $\wedge$), kvantifikátory ($\forall$, $\exists$), zátvorky (napr. (,), [,], {, });

(II) mimologické symboly — konštanty, relácie, prípadne aj operácie.

V prípade aritmetiky prirodzených čísel môžu byť mimologickými symbolmi napríklad:

konštanty 1, 2, ...

relácie $=$, $\leqq$, S, ...

operácie $+$, $.$, ...

Označme symbolom A množinu všetkých pravdivých výrokov o prirodzených číslach v nejakom formálnom jazyku J. Zvoľme symbol T nepatriaci do jazyka J, ktorý budeme používať ako symbol unárnej (jednočlennej) relácie. Rozšírme jazyk J na jazyk J' pridaním symbolu T a uvažujme nasledujúci výrok v tomto jazyku:

$$\{T(1) \wedge (\forall n)(\forall m)[T(n) \wedge S(n, m) \Rightarrow T(m)]\} \Rightarrow (\forall n)\, T(n), \qquad (*)$$

kde S má ten istý význam ako v *príklade 7*. Výrok (*) je vlastne formálnym vyjadrením schémy (1).

Ukážeme, že výrok (*) nie je možné dokázať pomocou výrokov patriacich do A. Budeme postupovať nepriamo.

Predpokladajme, že výrok (*) možno dokázať pomocou výrokov patriacich do A. Takýto dôkaz je konečný, preto v ňom použijeme len konečný počet výrokov patriacich do A. Nech sú to výroky $X_1, \ldots, X_n$. Utvorme ich konjunkciu $X = X_1 \wedge \ldots \wedge X_n$. Potom $X \in A$ a výrok (*) možno dokázať pomocou výroku X.

Všimnime si, že výroky X, (*) sú zapísané v rôznych jazykoch. V takomto prípade možno použiť isté užitočné tvrdenie známe v logike ako Craigova lema (pozri napr. [2]), podľa ktorého existuje taký výrok C, že:

(i) C neobsahuje žiadne mimologické symboly okrem rovnosti a tých symbolov, ktoré vystupujú v X aj v (*),

(ii) C sa dá dokázať pomocou X,

(iii) (*) sa dá dokázať pomocou C.

Z (i), (ii) vidíme, že C je pravdivý výrok o prirodzených číslach, v ktorom nevystupujú žiadne mimologické symboly okrem $=$, 1, $\leqq$. Z *príkladu 7* vieme, že výrok C musí byť splnený v modeli (P, $=$, 1, $\leqq$), a podľa (iii) musí byť výrok (*) splnený v modeli P pri ľubovoľnom výbere relácie T. Tým však dostávame spor — definujme reláciu T takto:

$$T(a + bx) \text{ platí práve vtedy, ak } b = 0.$$

Potom výroky $T(1)$, $(\forall n)(\forall m)[T(n) \wedge S(n, m) \Rightarrow T(m)]$ sú splnené v modeli P, ale výrok $(\forall n)\, T(n)$ nie. To znamená, že ani výrok (*) nie je splnený.

Poznamenajme, že schéma (1) sa môže stať dokázateľnou, ak zmeníme axiomatiku D — napr. ak piatu axiómu nahradíme princípom dobrého usporiadania. Už z toho, čo sme si na posledných stranách povedali, však vyplýva, že pojem dobre usporiadanej množiny sa nedá definovať v rámci logiky s rovnosťou. Preto sa princíp indukcie obvykle uvádza medzi axiómami aritmetiky. Zistilo sa, že ho nemožno nahradiť žiadnym konečným počtom axióm v príslušnom jazyku. Aj tak však má obvyklý model N význačné postavenie — je to jediný prostý model aritmetiky, t. j. taký model, že každý iný model obsahuje podmodel s ním izomorfný.

Skutočnosť, že v aritmetike prirodzených čísel existujú výroky, ktoré sú pravdivé, ale nedokázateľné, má za následok existenciu tzv. neštandardných modelov aritmetiky, v ktorých existujú „nekonečné" prirodzené čísla (pozri [2]). K najjednoduchším z nich patrí model P z *príkladu 7*. Existencia neštandardných modelov aritmetiky má zas za následok existenciu neštandardných modelov teórie množín, v ktorých nachádzame konečné množiny s nekonečne veľa prvkami. O existencii takýchto modelov sa môžeme presvedčiť aj inak.

Vráťme sa k spomínanému Soritovmu paradoxu. Ak symbolom X označíme množinu všetkých mužových vlasov a symbolom Y množinu tých jeho vlasov, ktoré mu postupne povytrhávame, vidíme, že podľa úvahy z *príkladu 5* sú splnené tieto tvrdenia:

($N0$) X je konečná množina
($N1$) Y je podmnožina množiny X
($N2$) Y má aspoň dva rôzne prvky
($N3$) Y má aspoň tri rôzne prvky
. . . . . .
(Nk) Y má aspoň k rôznych prvkov

Utvorme z výrokov ($N0$), ($N1$), ..., (Nk), ... axiomatický systém $\mathcal{N}$. Tento systém je formálne bezosporný, lebo každý jeho konečný podsystém má model. Pritom je jasné, že $\mathcal{M}$ nemá model!

Základným tvrdením teórie modelov je Gödelova veta o úplnosti, podľa ktorej každý bezosporný axiomatický systém má model. Ako si teda vysvetliť situáciu so systémom $\mathcal{N}$? Odpoveď je jednoduchá: Gödelova veta platí len pre formalizované teórie. Skúsme teda formalizovať systém $\mathcal{N}$. Miesto $a \in X$, $b \in \subset$ píšme $X(a)$, $Y(b)$. Potom miesto ($N1$) môžeme formálne písať

$$(N1^*)\ (\forall a)[Y(a) \Rightarrow X(a)],$$

miesto ($N2$) podobne

$$(N2^*)(\exists a)(\exists b)[Y(a) \wedge Y(b) \wedge (a \neq b)],$$

miesto ($N3$) podobne

$$(N3^*)\ (\exists a)\ (\exists b)\ (\exists c)\ [Y(a) \wedge Y(b) \wedge Y(c) \wedge (a \neq b) \wedge (a \neq c) \wedge (b \neq c)]$$

a tak ďalej. Všetky axiómy systému $\mathscr{M}$ okrem ($N0$) teda vieme formalizovať. To znamená, že pojem konečnej množiny nie je možné formalizovať v rámci logiky s rovnosťou.

Pretože pojem konečnej množiny možno formalizovať v rámci teórie množín (napr. pomocou Tarského definície), bezospornosť systému zaručuje existenciu takého modelu teórie množín, v ktorom sú splnené všetky axiómy systému $\mathscr{M}$. Tento model je nutne neštandardný.

Teraz už dokážeme vysvetliť *príklady 5, 6*. V prípade formalizovaných teórií môžeme indukciou dokazovať len tie výroky, ktoré sú zapísané v jazyku tejto teórie. Pri obvyklých neformálnych úvahách môžeme indukciou dokazovať len tie výroky, ktorých význam je presne určený. Ak dokazujeme výrok sformulovaný pomocou nie celkom jasne definovaných termínov, ako napr. „husté vlasy" v *príklade 5* alebo „poloprázdna električka" *v príklade 6*, môže sa stať, že dôjdeme k sporným výsledkom.

Literatúra

[1] Beth, E. W.: The Foundations of Mathematics. North-Holland Publ. Comp., Amsterdam 1959

[2] Robinson, A.: Vvedenie v teoriju modelej i metamatematiku algebry. Izd. Nauka, Moskva 1967