

Úvod do matematickej logiky (Cvičenie #3)

Kubo Kováč

12. októbra 2012

1 Teória následníka a rôzne interpretácie

- na predchádzajúcom cvičení sme sa hrali s P -systémom a ukázali sme si, ako sa dá formuliam (hŕbe písmeniek) priradiť význam; to nám umožní hovoriť o *pravdivosti* pri danej interpretácii a ihneď sa objavuje zaujímavá otázka: dá sa dokázať všetko to, čo je pravdivé pri danej/pri každej interpretácii?
- na tomto cvičení sa na vec pozrieme s úplne opačného pohľadu: začneme s nejakým matematickým objektom, konkrétne prirodzenými číslami a pokúsime sa ich definovať – nájsť formálny systém, v ktorom budú platiť práve tie tvrdenia, ktoré sú pravdivé v prirodzených číslach; navyše sa budeme snažiť nájsť také axiómy, ktorým nebude vyhovovať iná interpretácia ako prirodzené čísla
- začnime tým, že si pripomenieme, čo je to *jazyk prvorádovej logiky*; skladá sa z:
 - logických spojok ($\neg, \rightarrow, \wedge, \vee, \dots$)
 - kvantifikátorov ($\forall, \exists$)
 - premenných ($x, y, z, \dots$)
 - konštánt ($c_1, c_2, c_3, \dots$)
 - funkčných symbolov ($f, g, h, \dots$)
 - predikátových symbolov ($p, q, r, \dots$)
 - prípadne zátvoriek
 - každý funkčný a predikátový symbol má priradenú *aritu* (počet argumentov)
 - termy a formule sa potom definujú indukciou
- na minulom cvičení sme si hovorili, že pod *interpretáciou* máme na mysli nejaké zobrazenie, ktoré symbolom (termom, formuliam) z jazyka priradí matematické objekty

- pri *interpretácii* jazyka prvorádovej logiky si vždy vezmeme nejaké „univerzum“
– neprázdnu množinu $\mathcal{U} \neq \emptyset$; interpretácia bude zobrazenie $\mathcal{I}$, ktoré
 - konštantám priradí prvky z $\mathcal{U}$
 - každému k -árnemu funkčnému symbolu priradí nejakú *funkciu* z $\mathcal{U}^k$ do $\mathcal{U}$
 - každému k -árnemu predikátovému symbolu priradí k -árny *predikát* nad $\mathcal{U}$ (t.j. podmnožinu $\mathcal{U}^k$)
 - interpretácia termov a formúl sa definuje induktívne (o tom inokedy; ale napr. význam $(\forall x)\varphi(x)$ bude „pre každé $x \in \mathcal{U}$ je formula $\varphi(x)$ pravdivá“)
- pod jazykom *prvorádovej logiky s rovnosťou* chápeme jazyk prvorádovej logiky, ku ktorému pridáme ešte symbol $=$, pričom tento budeme vždy interpretovať ako rovnosť v $\mathcal{U}$
- vezmeme si teraz štruktúru $(\mathbb{N}, 0, S)$, t.j. množinu prirodzených čísel $\{0, 1, 2, 3, \dots\}$ s funkciou *následníka* $S : n \mapsto n + 1$, t.j. $S(0) = 1$, $S(47) = 48$, atď.
- pokúsme sa nájsť formálny systém, ktorý túto štruktúru „vystihuje“
- náš formálny systém bude mať jazyk prvorádovej logiky s rovnosťou, s jednou konštantou (0) a jedným (unárnym) funkčným symbolom (S); v tomto jazyku sa teda dajú vytvoriť formuly zo symbolov $\neg, \rightarrow, \wedge, \vee, \forall, \exists, =, (,), 0, S, x, y, z, \dots$
- príklad formule, ktorú vieme v tomto jazyku zapísať:

$$(\forall x)(\exists y)(x = SSSy \vee x = S0)$$

pri štandardnej interpretácii, že $\mathbb{N}$ je univerzum, 0 je nula a S následník, formula vraví: pre každé $x \in \mathbb{N}$ existuje $y \in \mathbb{N}$ také, že $x = y + 3$ alebo $x = S(0) = 1$ (čo nie je pravda napríklad pre $x = 2$)

- existuje však veľa ďalších iných interpretácií tohto jazyka, napr.:
 1. $(\mathbb{N}, 10, n \mapsto n + 47)$, t.j. pri tejto interpretácii máme univerzum $\mathcal{U} = \mathbb{N}$, symbol 0 interpretujeme ako prirodzené číslo 10 a symbol S ako funkciu $n \mapsto n + 47$ (rozmyslite si, že ani pri tejto interpretácii formula nebude pravdivá)
 2. $(\mathbb{Z}, 0, n \mapsto n - 1)$
 3. $(\mathbb{Z}, 1, n \mapsto 2 \cdot n)$
 4. $(\mathbb{R}, 0, x \mapsto x^2)$
 5. $(\mathbb{Q}, 2, x \mapsto x^2)$
 6. $(\mathbb{Z}_7, 0, n \mapsto n + 5 \bmod 7)$
 7. $(\mathbb{N} \times \mathbb{N}, (0, 0), (x, y) \mapsto (x, y + 1))$

8. $(\mathbb{N}, 0, n \mapsto \lfloor n/2 \rfloor + 1)$

- skúsme teraz pridať nejaké formuly pravdivé v štandardnej interpretácii a pozrieť sa, ktoré štruktúry ich budú spĺňať
- množinu formúl budeme volať *teória* a štruktúry, v ktorých sú všetky tieto formuly pravdivé budeme volať *modely* našej teórie; budeme sa teda snažiť nájsť teóriu, ktorej jediný model je $(\mathbb{N}, 0, n \mapsto n + 1)$
- zopár axióm prirodzených čísel, s ktorými sme prišli na cvičení:

– „nula nemá predchodcu“:

$$\neg(\exists x)(Sx = 0)$$

(rozmyslite si, že táto formula je pravdivá aj pri interpretáciach č. 1., 3., 5., 7. a 8., ale nie pri tých druhých)

– naopak, „všetky nenulové prvky majú predchodcu“:

$$(\forall x)(\neg(x = 0) \rightarrow (\exists y)(Sy = x))$$

(rozmyslite si, že táto formula je pravdivá aj pri interpretáciach č. 2., 6. a 8., ale nie pri tých druhých; napríklad v 3. všetky nepárne čísla nemajú „predchodcu“; v 4. záporné čísla, v 5. napríklad prvočísla a v 7. všetky dvojice tvaru $(n, 0)$ nemajú „predchodcu“ – také y , že $Sy = x$)

– stále sme nepridali dosť axióm – ostáva nám model č. 8.; na rozdiel od prirodzených čísel, kde S je prostá funkcia, v 8. sa napríklad 4 aj 5 zobrazí na to isté; pridajme preto axiómu: „funkcia následníka je prostá“:

$$(\forall x)(\forall y)(Sx = Sy \rightarrow x = y)$$

- rozmyslite si, že takáto teória *nemá konečný model*
- je už teraz $(\mathbb{N}, 0, S)$ jediný model našej teórie? nie! vezmime si napríklad $\mathbb{N} \cup \{\infty\}$, kde 0 interpretujeme ako 0 a S ako funkciu $n \mapsto n + 1$, pričom $\infty \mapsto \infty$; v tejto štruktúre sú všetky tri tvrdenia pravdivé
- v $(\mathbb{N}, 0, S)$ sa však žiadny prvok nezobrazí sám na seba:

$$(\forall x)(\neg(Sx = x))$$

- čo ak by sme však zobrali štruktúru $\mathbb{N} \cup \{\omega_1, \omega_2\}$, kde S je $n \mapsto n + 1$, pričom $\omega_1 \mapsto \omega_2$ a $\omega_2 \mapsto \omega_1$ – toto je model všetkých štyroch axióm
- v $(\mathbb{N}, 0, S)$ však S nemá cykly dĺžky 2 ($S(S(x)) \neq x$):

$$(\forall x)(\neg(SSx = x))$$

- zrejme je jasné, že nám ostanú modely typu $\mathbb{N} \cup \mathbb{Z}'_k$, t.j. prirodzené čísla, na ktorých S je $n \mapsto n + 1$ a k tomu ešte pridané prvky $0', 1', \dots, (k-1)'$, ktoré si označme čiarkovane (sú odlišné od prvkov z $\mathbb{N}$), ktoré S zobrazuje cyklicky $0' \mapsto 1' \mapsto \dots \mapsto (k-1)' \mapsto 0'$; ak chceme tieto modely vylúčiť, potrebujeme pridať nekonečne veľa axióm tvaru

$$(\forall x)(\neg(S^{(k)}x = x))$$

kde $k > 0, k \in \mathbb{N}$

- uvedomte si, že $(\forall x)(\neg(S^{(k)}x = x))$ *nie je* formula z nášho jazyka (náš jazyk neobsahuje žiadne $S^{(k)}$); chceme tak len skrátene zapísať nekonečne veľa axióm:

$$(\forall x)(\neg(Sx = x)), \quad (\forall x)(\neg(SSx = x)), \quad (\forall x)(\neg(SSSx = x)), \dots$$

$$\dots (\forall x)(\neg(\underbrace{SS \dots S}_k x = x)), \dots$$

- otázka z cvičenia: môžeme mať teóriu s nekonečným počtom axióm? áno, môžeme; mohli by sme dokonca zobrať $\text{Thm}(\mathbb{N})$ – množinu všetkých tvrdení, ktoré sú v $(\mathbb{N}, 0, S)$ pravdivé a vyhlásiť ich za axiómy našej teórie; často však chceme, aby bola teória konečná, alebo aspoň, aby sa dalo mechanicky (algoritmicky) rozhodnúť, či daná formula φ je, alebo nie je axióm; ak za axiómy vezmeme všetky pravdivé formuly, nie je úplne jasné, či vieme o každej formule rozhodnúť, či je, alebo nie je axióm
- otázka zníe: máme už teraz jediný model?
- ak by sme zobrali napríklad $(\mathbb{N} - \{0\}, 1, n \mapsto n + 1)$ alebo $(\mathbb{N} - \{0, 1, 2\}, 3, n \mapsto n + 1)$, dostali by sme opäť model našej teórie; podobne, ak by sme zobrali iba párne prirodzené čísla s nulou a $n \mapsto n + 2$, opäť dostaneme model teórie
- intuitívne však asi cítime, že tieto modely nie sú veľmi odlišné; v skutočnosti sú izomorfné (myslíme tým toto: dva modely $(\mathcal{U}_1, 0_1, S_1)$ a $(\mathcal{U}_2, 0_2, S_2)$ sú izomorfné, ak existuje zobrazenie $f : \mathcal{U}_1 \rightarrow \mathcal{U}_2$ také, že $f(0_1) = 0_2$ a $f(S_1(x)) = S_2(f(x))$ pre každé $x \in \mathcal{U}_1$)
- existuje aj iný model neizomorfný s $(\mathbb{N}, 0, S)$? áno! vezmeme si $\mathbb{N} \cup \mathbb{Z}'$ – vezmeme si jednu kópiu prirodzených čísiel a pridajme k tomu jednu (odlišnú) kópiu celých čísiel (tieto označme čiarkovane)
- formálne, keby sme chceli byť poriadni, písali by sme $\mathbb{N} \cup \{0\} \times \mathbb{Z}$, teda kópiu celých čísiel by sme „označili“ nulou, boli by to dvojice $(0, n)$, kde $n \in \mathbb{Z}$; ostane však jednoducho pri prirodzených číslach $0, 1, 2, \dots$, ku ktorým pridáme „čiarkované“ celé čísla $\dots, -2', -1', 0', 1', 2', \dots$)
- nula bude 0, $S(n) = n + 1$ a $S(n') = n' + 1$;
- presvedčte sa, že tento model spĺňa všetky axiómy našej teórie

- navyše, tento model *nie je* izomorfný s $(\mathbb{N}, 0, S)$ – v $\mathbb{N}$ vieme totiž každé prirodzené číslo „dosiahnuť“ z nuly konečným počtom následníkov
- mohli by sme toto pridať ako ďalšiu axiómu? niečo ako

$$(\forall x)(\exists k \in \mathbb{N})(x = \underbrace{S \cdots S}_k 0)$$

- jediný problém je časť „ $(\exists k \in \mathbb{N})$ “, ktorá nepatrí do nášho jazyka; možno by sme toto tvrdenie vedeli nejak preformulovať a nahradiť nekonečným počtom axiém
- po troche skúšania však začneme mať pocit, že sa to nedá... najlepšie, s čím sme prišli bolo nekonečné tvrdenie tvaru

$$(\forall x)(x = 0 \vee x = S0 \vee x = SS0 \vee x = SSS0 \vee \cdots)$$

formuly však nemôžu byť nekonečné

- pár poznámok (pikošiek) na koniec:
 - v skutočnosti každá štruktúra tvaru $\mathbb{N}$ plus niekoľko rôznych kópií $\mathbb{Z}$ je model našej teórie (môžeme pridať aj nekonečne veľa kópií $\mathbb{Z}$; aj nespočítateľne veľa, napr. $\mathbb{N} \cup (\mathbb{R} \times \mathbb{Z})$; 0 je stále $0 \in \mathbb{N}$ a S je $n \mapsto n + 1$ pre $n \in \mathbb{N}$, resp. $(x, n) \mapsto (x, n + 1)$ pre $x \in \mathbb{R}, n \in \mathbb{Z}$)
 - v skutočnosti je naša teória úplná a teda aj keby sme pridali všetky pravdivé tvrdenia o $\mathbb{N}$, nevedeli by sme ostatné modely vylúčiť; v týchto modeloch platia úplne rovnaké formuly ako v $\mathbb{N}$ (teda tie formuly, ktoré sa dajú zapísať v našom jazyku s 0 a S)
 - z toho vyplýva, že tvrdenie „každý prvok vieme dosiahnuť z nuly konečným počtom následníkov“ vieme síce vyjadriť v prirodzenom jazyku, ale nevieme ho sformulovať v prvorádovom jazyku našej teórie (iba s 0 a S); toto tvrdenie sa dá vyjadriť v druhorádovom jazyku, kde môžeme kvantifikovať cez množiny prvkov, resp. cez postupnosti prvkov...
 - jednotlivé modely vieme odlíšiť „zvonku“, ale nie „vnútri“ formálneho systému

2 Čo si odniesť z tohto cvičenia

- množinu (uzavretých) formúl voláme *teória*
- štruktúry, v ktorých sú všetky tieto formuly pravdivé voláme *modely* teórie
- symboly formálneho systému môžu mať viacero rôznych interpretácií a teórie môžu mať viacero rôznych modelov