Tento text napsal Jan Pelc s použitím materiálů prof. Štěpánka. Tato verze byla vygenerována programem LaTeX dne 17.09.2008 v 16:24:18 hodin.

Použití pouze na vlastní nebezpečí!

1 Peanova aritmetika prvního řádu

1.1 Definice. *Peanova aritmetika prvního řádu* je teorie $\mathbb{P}$ prvního řádu s jazykem $L = \{0, S, +, *, \leq\}$, s rovností a s těmito speciálními axiomy:

$$
\begin{array}{ll}
\text{(Q1)} & S(x) \neq 0 \\
\text{(Q2)} & S(x) = S(y) \rightarrow x = y \\
[\text{(Q3)} & x \neq 0 \rightarrow (\exists y)(x = S(y))] \\
\text{(Q4)} & x + 0 = x \\
\text{(Q5)} & x + S(y) = S(x + y) \\
\text{(Q6)} & x * 0 = 0 \\
\text{(Q7)} & x * S(y) = (x * y) + x \\
\text{(Q8)} & x \leq y \leftrightarrow (\exists z)(z + x = y)
\end{array}
$$

Navíc je-li A libovolná formule a x proměnná, je axiomem i formule:

$$A_x[0] \rightarrow (\forall x)(A \rightarrow A_x[S(x)]) \rightarrow (\forall x)A$$

Tomuto schématu se říká *schéma indukce.*

1.2 Poznámka. Technicky vzato není nutné, aby (Q3) bylo axiomem $\mathbb{P}$, protože se dá (jak uvidíme) dokázat z ostatních axiomů. Samotné axiomy (Q1) až (Q8) bez schématu indukce však tvoří slabší *Robinsonovu aritmetiku* a takto jasně vidíme, že $\mathbb{P}$ je jejím rozšířením.

1.3 Použití rovnosti. Uvědomme si, že díky symetrii rovnosti je možné všechny axiomy, jejichž základ tvoří predikát rovnosti (čili Q4 až Q7), používat i „naopak“. Dále díky větě o rovnosti se nám dva termy rovnají, pokud druhý vznikl z prvního záměnou některých podtermů jím rovnými termy. Oba fakty budeme nadále využívat mlčky, a proto je dobré vědět, proč to z formálního hlediska smíme udělat.

1.4 Použití indukce. Většina důkazů v Peanově aritmetice se opírá o schéma indukce, a proto je důležité vědět, jak jej použít. Chceme-li dokázat, že platí formule A s volnou proměnnou x, napřed dokážeme, že A platí pro $x = 0$, neboli že platí:

$$\mathbb{P} \vdash A_x[0]$$

Potom dokážeme indukční krok, a sice implikaci, že za předpokladu A pro $x = y$ platí A pro $x = S(y)$, neboli že platí implikace:

$$\mathbb{P} \vdash A \rightarrow A_x[S(x)]$$

Pozor, z formálního hlediska nestačí pouze vyjít z předpokladu $\mathbb{P} \vdash A$ a nějak se probojovat k $\mathbb{P} \vdash A_x[S(x)]$, opravdu je nutné dokázat uvedenou implikaci[1]. Na ni pak aplikujeme pravidlo generalizace a dvěma pravidly *modus ponens* získáme z příslušné instance axiomu indukce konečně:

$$\mathbb{P} \vdash (\forall x)A$$

Pokud nyní vytvoříme uzávěr A' formule $(\forall x)A$, bude zřejmě i uzávěrem samotné formule A a z věty o uzávěru dostaneme konečně:

$$\mathbb{P} \vdash A$$

1.5 Tvrzení. V Peanově aritmetice vyplývá axiom (Q3) z ostatních axiomů, neboli:

$$\mathbb{P}' = \mathbb{P} \setminus (\mathrm{Q3}) \vdash x \neq 0 \rightarrow (\exists y)(x = S(y)) \tag{Q3}$$

Důkaz. Dokážeme indukcí podle x:

- Napřed dokazujeme:

  $$\mathbb{P}' \vdash 0 \neq 0 \rightarrow (\exists y)(0 = S(y)) \tag{1}$$

  Předpoklad zřejmě nikdy neplatí, proto použijeme větu (V2') výrokové logiky

  $$\vdash A \rightarrow \neg A \rightarrow B$$

  do které dosadíme:

  $$\vdash 0 = 0 \rightarrow 0 \neq 0 \rightarrow (\exists y)(0 = S(y))$$

  První předpoklad je instance axiomu identity pro rovnost (R1), proto odtud (1) získáme pravidlem (MP).

- Nyní musíme dokázat

  $$\mathbb{P}' \vdash [x \neq 0 \rightarrow (\exists y)(x = S(y))] \rightarrow [S(x) \neq 0 \rightarrow (\exists y)(S(x) = S(y))] \tag{2}$$

  což není vůbec těžké, protože tvrzení úplně napravo platí samo o sobě i mimo Peanovu aritmetiku:

  $$\vdash (\exists y)(S(x) = S(y)) \tag{3}$$

  Pokud dokážeme (3), máme z výrokové logiky

  $$\begin{aligned} A, B, C &\vdash C && \text{(DP)} \\ &\vdash C \rightarrow ([A] \rightarrow [B \rightarrow C]) && (3\times\ \text{VD}) \end{aligned}$$

[1] Obecně není pravda, že když za předpokladu $T \vdash A$ dokážeme $T \vdash B$, platí $T \vdash A \rightarrow B$. Jako příklad uveďme, že ačkoliv se z $\vdash A$ dá odvodit $\vdash (\forall x)A$, implikace $\vdash A \rightarrow (\forall x)A$ obecně neplatí, pokud A obsahuje x volně – není těžké najít interpretaci a ohodnocení, při kterém není splněna.

a příslušným dosazením za A, B, C a pravidlem (MP) získáme snadno (2).

Takže dokažme (3). Vyjdeme z pravidla substituce

$$\vdash A_y[t] \rightarrow (\exists y)A$$

do kterého dosadíme za A formuli $S(x) = S(y)$ a za t proměnnou x:

$$\vdash [S(x) = S(x)] \rightarrow [(\exists y)(S(x) = S(y))]$$

Předpoklad je však instancí axiomu identity, formuli (3) tedy získáme pravidlem (MP).

Dokazovaný axiom (Q3) tedy dostaneme použitím axiomu indukce popsaným v poznámce 1.4. ✩

1.6 Tvrzení.

$$\mathbb{P} \vdash S(x) \neq x$$

Důkaz. Indukcí podle x:

- Počátek indukce. Tvrzení $\mathbb{P} \vdash S(0) \neq 0$ je instance axiomu (Q1).
- Indukční krok. Vyjdeme z instance axiomu (Q2) a použijeme větu (V5):

$$\mathbb{P} \vdash [S(S(x)) = S(x)] \rightarrow [S(x) = x] \qquad \text{(Q2)}$$
$$\mathbb{P} \vdash [S(x) \neq x] \rightarrow [S(S(x)) \neq S(x)] \qquad \text{(V5, MP)}$$

✩

1.7 Pozorování (skládání rovností, zobecněná tranzitivita rovnosti). Pro proměnné (a díky větě o instancích i pro termy) $x_1, \ldots, x_n$ platí:

$$\vdash x_1 = x_2 \rightarrow x_2 = x_3 \rightarrow \ldots \rightarrow x_{n-1} = x_n \rightarrow x_1 = x_n \qquad \text{(SR)}$$

Důkaz. Zřejmě platí:

$$\vdash x_1 = x_2 \rightarrow x_2 = x_3 \rightarrow x_1 = x_3 \qquad \text{(TR)}$$
$$\vdash x_1 = x_3 \rightarrow x_3 = x_4 \rightarrow x_1 = x_4 \qquad \text{(TR)}$$
$$\vdots$$
$$\vdash x_1 = x_{n-1} \rightarrow x_{n-1} = x_n \rightarrow x_1 = x_n \qquad \text{(TR)}$$

Nyní označíme jednotlivé rovnosti tak, abychom dostali:

$$\vdash R_1 \rightarrow R_2 \rightarrow Q_1$$
$$\vdash Q_1 \rightarrow R_3 \rightarrow Q_2$$
$$\vdots$$
$$\vdash Q_{n-3} \rightarrow R_{n-1} \rightarrow R$$

Ve výrokové logice se dá dokázat věta

$$\vdash (R_1 \to R_2 \to Q_1) \to (Q_1 \to R_3 \to Q_2) \to \ldots \to (Q_{n-3} \to R_{n-1} \to R) \to \tag{1}$$
$$\to (R_1 \to R_2 \to \ldots \to R_{n-1} \to R) \tag{2}$$

a to tak, že vyjdeme z množiny předpokladů T, která obsahuje všechny závorky v (1) a všechny výrokové proměnné $R_1, \ldots, R_{n-1}$. Potom zřejmě platí:

$$\begin{array}{ll}
T \vdash R_1 & \text{(DP)} \\
T \vdash R_2 & \text{(DP)} \\
T \vdash R_1 \to R_2 \to Q_1 & \text{(DP)} \\
T \vdash Q_1 & (2\times \text{ MP}) \\
 & \\
T \vdash R_3 & \text{(DP)} \\
T \vdash Q_1 \to R_3 \to Q_2 & \text{(DP)} \\
T \vdash Q_2 & (2\times \text{ MP}) \\
\quad\vdots & \\
T \vdash R &
\end{array}$$

Z posledního řádku dostaneme násobnou aplikací věty o dedukci konečně větu $\vdash$ (1) $\to$ (2), ze které se dá pravidly (MP) dokázat z jednotlivých dílčích tranzitivit dokazovaná věta. ☆

1.8 Indukční krok s rovnostmi. V mnoha důkazech budeme v indukčním kroku skládat rovnosti $R_1, \ldots, R_n$ do výsledné rovnosti R, ale některá z dílčích rovností R_i bude vycházet z indukčního předpokladu P:

$$\vdash R_1 \to \ldots \to R_{i-1} \to R_i \to R_{i+1} \to \ldots \to R_n \to R \tag{1}$$
$$\mathbb{P} \vdash R_j \text{ pro všechna } j \neq i \tag{2}$$
$$\mathbb{P} \vdash P \to R_i \tag{3}$$

V takovém případě můžeme z (1) záměnou předpokladů dojít k

$$\vdash R_1 \to \ldots \to R_{i-1} \to R_{i+1} \to \ldots \to R_n \to R_i \to R$$

a pravidly (MP) se všemi formulemi (2) dostat:

$$\mathbb{P} \vdash R_i \to R$$

Nyní složením s implikací (3) získáme konečně

$$\mathbb{P} \vdash P \to R$$

což je obvykle to, co chceme.

Následující lemma je variantou axiomu (Q5) a bude potřeba například v důkazu komutativity sčítání.

1.9 Lemma.

$$\mathbb{P} \vdash S(x) + y = S(x + y) \tag{Q5'}$$

Důkaz. Indukcí podle y:

- Počátek indukce. Složíme dvě rovnosti:

$$\begin{aligned} \mathbb{P} &\vdash S(x) + 0 = S(x) && \text{(Q4)} \\ \mathbb{P} &\vdash S(x) = S(x + 0) && \text{(Q4, VR)} \\ \mathbb{P} &\vdash S(x) + 0 = S(x + 0) && \text{(SR)} \end{aligned}$$

- Indukční krok. Máme:

$$\begin{aligned} \mathbb{P} &\vdash S(x) + S(y) = S(S(x) + y) && \text{(Q5)} \\ \mathbb{P} &\vdash S(S(x + y)) = S(x + S(y)) && \text{(Q5, VR)} \end{aligned}$$

  A navíc z (R2) platí:

$$\vdash [S(x) + y = S(x + y)] \rightarrow [S(S(x) + y) = S(S(x + y))] \tag{1}$$

  Nyní složíme výše uvedené dvě rovnosti a rovnost v tvrzení implikace (1) a postupem popsaným v poznámce 1.8 dostaneme

$$\mathbb{P} \vdash [S(x) + y = S(x + y)] \rightarrow [S(x) + S(y) = S(x + S(y))]$$

  což je přesně to, co potřebujeme pro indukční krok.

☆

1.10 Tvrzení.

$$\mathbb{P} \vdash x + 0 = 0 + x$$

Důkaz. Indukcí podle x:

- Počátek indukce. Tvrzení $\vdash 0 + 0 = 0 + 0$ plyne ihned z axiomu identity.

- Indukční krok. Složíme rovnosti:

$$\begin{aligned} \mathbb{P} \vdash S(x) + 0 &= S(x) && \text{(Q4)} \\ &= S(x + 0) && \text{(Q4, VR)} \\ &= S(0 + x) && \text{(IP)} \\ &= 0 + S(x) && \text{(Q5)} \end{aligned}$$

  Rovnost označená jako (IP) plyne z (R2):

$$\vdash [x + 0 = 0 + x] \rightarrow [S(x + 0) = S(0 + x)]$$

  Odtud opět postupem popsaným v poznámce 1.8 dostaneme:

$$\mathbb{P} \vdash [x + 0 = 0 + x] \rightarrow [S(x) + 0 = 0 + S(x)]$$

  což potřebujeme.

☆

1.11 Tvrzení (komutativita sčítání).

$$\mathbb{P} \vdash x + y = y + x$$

Důkaz. Indukcí podle y:

- Počátek indukce. Tvrzení $\mathbb{P} \vdash x + 0 = 0 + x$ máme již dokázané (tvrzení 1.10).
- Indukční krok. Složíme rovnosti:

$$\begin{aligned} \mathbb{P} \vdash x + S(y) &= S(x + y) && \text{(Q5)} \\ &= S(y + x) && \text{(IP)} \\ &= S(y) + x && \text{(Q5')} \end{aligned}$$

  Dále (IP) plyne z axiomu (R2)

$$\vdash [x + y = y + x] \to [S(x + y) = S(y + x)]$$

  a odtud opět známým způsobem konečně:

$$\mathbb{P} \vdash [x + y = y + x] \to [x + S(y) = S(y) + x]$$

☆

1.12 Tvrzení (asociativita sčítání).

$$\mathbb{P} \vdash (x + y) + z = x + (y + z)$$

Důkaz. Indukcí podle z:

- Počátek indukce. Složíme dvě rovnosti:

$$\begin{aligned} \mathbb{P} \vdash (x + y) + 0 &= x + y && \text{(Q4)} \\ &= x + (y + 0) && \text{(Q4, VR)} \end{aligned}$$

- Indukční krok. Opět skládání rovností:

$$\begin{aligned} \mathbb{P} \vdash (x + y) + S(z) &= S((x + y) + z) && \text{(Q5)} \\ &= S(x + (y + z)) && \text{(IP)} \\ &= x + S(y + z) && \text{(Q5)} \\ &= x + (y + S(z)) && \text{(Q5, VR)} \end{aligned}$$

  Rovnost (IP) plyne z axiomu (R2)

$$\vdash [(x + y) + z = x + (y + z)] \to [S((x + y) + z) = S(x + (y + z))]$$

  a odtud známým způsobem:

$$\mathbb{P} \vdash [(x + y) + z = x + (y + z)] \to [(x + y) + S(z) = x + (y + S(z))]$$

$\star$

1.13 Tvrzení (1 + 2 = 3).

$$\mathbb{P} \vdash S(0) + S(S(0)) = S(S(S(0)))$$

Důkaz. Indukci potřebovat nebudeme (Robinson!), pouze (opět) složíme několik rovností:

$$\begin{aligned} \mathbb{P} \vdash S(0) + S(S(0)) &= S(S(0) + S(0)) && \text{(Q5)} \\ &= S(S(S(0) + 0)) && \text{(Q5, VR)} \\ &= S(S(S(0))) && \text{(Q4, VR)} \end{aligned}$$

$\star$

1.14 Tvrzení (1 ∗ 2 = 2).

$$\mathbb{P} \vdash S(0) * S(S(0)) = S(S(0))$$

Důkaz. Indukci opět potřebovat nebudeme.

$$\begin{aligned} \mathbb{P} \vdash S(0) * S(S(0)) &= (S(0) * S(0)) + S(0) && \text{(Q7)} \\ &= ((S(0) * 0) + S(0)) + S(0) && \text{(Q7, VR)} \\ &= (0 + S(0)) + S(0) && \text{(Q6, VR)} \\ &= S(0 + 0) + S(0) && \text{(Q5, VR)} \\ &= S(0) + S(0) && \text{(Q4, VR)} \\ &= S(S(0) + 0) && \text{(Q5)} \\ &= S(S(0)) && \text{(Q4, VR)} \end{aligned}$$

$\star$

1.15 Tvrzení.

$$\mathbb{P} \vdash 0 \leq x$$

Důkaz. Podle axiomu (Q8) stačí dokázat:

$$\mathbb{P} \vdash (\exists z)(z + 0 = x) \tag{1}$$

Vyjdeme z pravidla substituce

$$\vdash A_z[t] \to (\exists z)A$$

do kterého dosadíme za A formuli $z + 0 = x$ a za t term x:

$$\vdash x + 0 = x \to (\exists z)(z + 0 = x)$$

Protože předpoklad je axiom (Q4), získáme (1) snadno jediným (MP). $\star$

1.16 Tvrzení.

$$\mathbb{P} \vdash S(x) = x + S(0)$$

Důkaz. Indukci potřebovat nebudeme.

$$\begin{aligned} \mathbb{P} \vdash S(x) &= S(x+0) && \text{(Q4, VR)} \\ &= x + S(0) && \text{(Q5)} \end{aligned}$$

☆

Nyní bude následovat důkaz komutativity násobení. Ten bude potřebovat několik pomocných tvrzení, mezi nimi i obdobu axiomu (Q5) označenou jako (Q5') a dokázanou jako lemma 1.9. Všechny následující důkazy jsou již zapsány velmi zkráceně, podrobnější vysvětlení a formální zdůvodnění nalezne čtenář v předchozím textu.

1.17 Tvrzení.

$$\mathbb{P} \vdash 0 * y = y * 0$$

Důkaz. Indukcí podle y:

- Počátek indukce. Formule $0 * 0 = 0 * 0$ je instancí axiomu identity.
- Indukční krok.

$$\begin{aligned} \mathbb{P} \vdash 0 * S(y) &= (0 * y) + 0 && \text{(Q7)} \\ &= (y * 0) + 0 && \text{(IP)} \\ &= 0 + 0 && \text{(Q6)} \\ &= 0 && \text{(Q4)} \\ &= S(y) * 0 && \text{(Q6)} \end{aligned}$$

☆

1.18 Lemma.

$$\mathbb{P} \vdash (a + b) + c = (a + c) + b$$

Důkaz. Indukcí podle b:

- Počátek indukce.

$$\begin{aligned} \mathbb{P} \vdash (a+0) + c &= a + c && \text{(Q4)} \\ &= (a + c) + 0 && \text{(Q4)} \end{aligned}$$

- Indukční krok.

$$\begin{aligned} \mathbb{P} \vdash (a + S(b)) + c &= S(a+b) + c && \text{(Q5)} \\ &= S((a+b)+c) && \text{(Q5')} \\ &= S((a+c)+b) && \text{(IP)} \\ &= (a+c) + S(b) && \text{(Q5)} \end{aligned}$$

$\star$

1.19 Lemma.

$$\mathbb{P} \vdash S(y) * x = (y * x) + x$$

Důkaz. Indukcí podle x:

- Počátek indukce.

$$\begin{aligned} \mathbb{P} \vdash S(y) * 0 &= 0 && \text{(Q6)} \\ &= 0 * 0 && \text{(Q6)} \\ &= (y * 0) * 0 && \text{(Q6)} \end{aligned}$$

- Indukční krok.

$$\begin{aligned} \mathbb{P} \vdash S(y) * S(x) &= (S(y) * x) + S(y) && \text{(Q7)} \\ &= S((S(y) * x) + y) && \text{(Q5)} \\ &= S(((y * x) + x) + y) && \text{(IP)} \\ &= S(((y * x) + y) + x) && \text{(lemma 1.18)} \\ &= ((y * x) + y) + S(x) && \text{(Q5)} \\ &= (y * S(x)) + S(x) && \text{(Q7)} \end{aligned}$$

$\star$

1.20 Tvrzení (komutativita násobení).

$$\mathbb{P} \vdash x * y = y * x$$

Důkaz. Indukcí podle x:

- Počátek indukce. Tvrzení $\mathbb{P} \vdash 0 * y = y * 0$ máme již dokázané (tvrzení 1.17).
- Indukční krok.

$$\begin{aligned} \mathbb{P} \vdash S(x) * y &= (x * y) + y && \text{(lemma 1.19)} \\ &= (y * x) + y && \text{(IP)} \\ &= y * S(x) && \text{(Q7)} \end{aligned}$$

$\star$

1.21 Tvrzení (distributivita násobení).

$$\mathbb{P} \vdash (a * b) + (a * c) = a * (b + c)$$

Důkaz. Indukcí podle c:

- Počátek indukce:

$$(a * b) + (a * 0) = (a * b) + 0 = a * b = a * (b + 0)$$

- Indukční krok. Využijeme již dokázanou asociativitu sčítání:

$$\begin{aligned}(a * b) + (a * S(c)) = (a * b) + ((a * c) + a) = ((a * b) + (a * c)) + a) = \\ = (a * (b + c)) + a = a * S(b + c) = a * (b + S(c))\end{aligned}$$

☆

1.22 Tvrzení (asociativita násobení).

$$\mathbb{P} \vdash (a * b) * c = a * (b * c)$$

Důkaz. Indukcí podle c:

- Počátek indukce:

$$(a * b) * 0 = 0 = a * 0 = a * (b * 0)$$

- Indukční krok. Využijeme již dokázanou distributivitu násobení:

$$\begin{aligned}(a * b) * S(c) = ((a * b) * c) + (a * b) = (a * (b * c)) + (a * b) = \\ = a * ((b * c) + b) = a * (b * S(c))\end{aligned}$$

☆