

Asociatívnosť sčítovania

1 Jazyk

funkčné symboly: $0, S(\cdot), P(\cdot, \cdot)$

relačné symboly: $=, \neq$

2 Axiómy

$R1: x = x$

$R2: x_1 = y_1 \rightarrow (x_2 = y_2 \rightarrow (\dots (x_k = y_k \rightarrow (f(x_1, x_2, \dots, x_k) = f(y_1, y_2, \dots, y_k))) \dots))$

$R3: x_1 = y_1 \rightarrow (x_2 = y_2 \rightarrow (\dots (x_k = y_k \rightarrow (P(x_1, x_2, \dots, x_k) \leftrightarrow P(y_1, y_2, \dots, y_k))) \dots))$

$R4: x = y \wedge y = z \rightarrow x = z$

$R5: x = y \leftrightarrow y = x$

$N1: S(x) \neq 0$

$N2: S(m) = S(n) \rightarrow m = n$

$P1: P(0, b) = b$

$P2: P(S(a), b) = S(P(a, b))$

Nech φ je ľubovoľný unárny predikát (s jednou voľnou premennou), potom

$$(\varphi(0) \wedge ((\forall n)(\varphi(n) \rightarrow \varphi(S(n)))))) \rightarrow (\forall n)(\varphi(n))$$

3 Úloha a riešenie

Dokážte, že $P(a, P(b, c)) = P(P(a, b), c)$.

Ukážeme si teraz niekoľko riešení. Čím ďalej tým viac formálnejšie (a za viac bodov)

Riešenie 1:

Pôjdeme na to indukciou cez a .

1°

Chceme dokázať $P(0, P(b, c)) = P(P(0, b), c)$

Dosadíme do axiómy $P1$ za a nulu a za b výraz $P(b, c)$ a dostaneme

$$P(0, P(b, c)) = P(b, c).$$

Teraz opäť napíšeme axiómu $P1$, ale v základnom tvare:

$$P(0, b) = b.$$

Zo symetrickosti rvonosti ($R5$) platí zjavne aj naopak ($b = P(0, b)$). Keď teraz postupne vhodne zameníme výrazy, o ktorých sme práve zistili že sa rovnajú, dostaneme

$$P(0, P(b, c)) = P(b, c) = P(P(0, b), c).$$

Čím je dôkaz bázy indukcie hotový. 2°

Chceme dokázať $P(n, P(b, c)) = P(P(n, b), c) \rightarrow P(S(n), P(b, c)) = P(P(S(n), b), c)$

Chceme teda dokázať, že

$$P(S(n), P(b, c)) = P(P(S(n), b), c).$$

Viacnásobným použitím (a vhodným dosadením do) axiómy $P2$ dostaneme

$$\begin{aligned} P(S(n), P(b, c)) &= S(P(n, P(b, c))) \\ P(S(n), b) &= S(P(n, b)) \\ P(S(P(n, b)), c) &= S(P(P(n, b), c)) \end{aligned}$$

Po opätovnom *vhodnom* dosadení výrazov ktoré sa navzájom rovnajú dostaneme

$$\begin{aligned} P(S(n), P(b, c)) &= S(P(n, P(b, c))) \\ P(P(S(n), b), c) &= P(S(P(n, b)), c) = S(P(P(n, b), c)) \end{aligned}$$

Indukčný predpoklad nám vraví $P(n, P(b, c)) = P(P(n, b), c)$. Axióma $R2$ vraví

$$P(n, P(b, c)) = P(P(n, b), c) \rightarrow S(P(n, P(b, c))) = S(P(P(n, b), c)).$$

Ich zkombinovaním (použitím Modus Ponens) dostávame

$$P(S(n), P(b, c)) = S(P(n, P(b, c))) = S(P(P(n, b), c)) = P(S(P(n, b)), c) = P(P(S(n), b), c).$$

Z čoho jasne vyzíza požadovaná rovnosť $P(S(n), P(b, c)) = P(P(S(n), b), c)$. QED.

Čo je na dôkaze nepostačujúce? Pracovanie s rovnosťou a trošku indukcia. Totiž každá zámena rovnakých vecí by sa mala robiť pekne korektne s využitím axiómy $R2$ alebo $R3$. Pre dokázanie druhého kroku indukcie by sme nemali

použiť predpoklad, ale jednoducho dokázať platnosť implikácie. V ďalšom texte je ukážka, ako by tak asi mohol vyzerat úplne tuti-fruti dôkaz. Červenou farbou sú vyznačené zmeny oproti prvému

Riešenie 2:

Pre dôkaz použijeme schému indukcie. Najprv si teda potrebujeme určiť, čo aký tvar bude mať formula $\varphi(n)$:

$$\varphi(n) \Leftrightarrow P(n, P(b, c)) = P(P(n, b), c).$$

Dôkaz $\varphi(0)$

Chceme dokázať $P(0, P(b, c)) = P(P(0, b), c)$

Dosadíme do axiomy $P1$ za a nulu a za b výraz $P(b, c)$ a dostaneme

$$P(0, P(b, c)) = P(b, c).$$

Teraz opäť napíšeme axiómu $P1$, ale v základnom tvare:

$$P(0, b) = b.$$

Zo symetrickosti rvonosti ($R5$) platí zjavne aj naopak ($b = P(0, b)$). Axióma $R2$ nám vraví (pri vhodnom dosadení za premenné)

$$b = P(0, b) \rightarrow P(b, c) = P(P(0, b), c).$$

Použitím Modus Ponens¹ na dva predchádzajúce riadky dostávame

$$P(b, c) = P(P(0, b), c).$$

Použitím tranzitívnosti rovnosti ($R4$) dostávame požadované tvrdenie

$$P(0, P(b, c)) = P(P(0, b), c).$$

Čím je dôkaz bázy indukcie hotový.

Dôkaz $\varphi(n) \rightarrow \varphi(S(n))$

Chceme dokázať $P(n, P(b, c)) = P(P(n, b), c) \rightarrow P(S(n), P(b, c)) = P(P(S(n), b), c)$

Viacnásobným použitím (a vhodným dosadením do) axiomy $P2$ dostaneme

$$P(S(n), P(b, c)) = S(P(n, P(b, c)))$$

$$P(S(n), b) = S(P(n, b))$$

$$P(S(P(n, b)), c) = S(P(P(n, b), c))$$

¹Modus ponens je pravidlo ktoré nám vraví, že ak vieme, že platí nejaký výrok A a zároveň aj výrok v tvare $A \rightarrow B$, tak potom musí nutne platiť aj samotný výrok B .

Opäť si napíšeme axiómu $R2$ s vhodným dosadeniami za premenné

$$P(S(n), b) = S(P(n, b)) \rightarrow P(P(S(n), b), c) = P(S(P(n, b)), c)$$

Použitím MP^2 dostaneme

$$P(P(S(n), b), c) = P(S(P(n, b)), c)$$

Použitím MP na axiómu tranzitívnosti rovnosti $R4$ a doteraz dokázané tvrdenia dostaneme

$$P(P(S(n), b), c) = S(P(P(n, b), c)).$$

Vidíme teda, že platia nasledujúce formulky

$$\begin{aligned} P(S(n), P(b, c)) &= S(P(n, P(b, c))) \\ P(P(S(n), b), c) &= S(P(P(n, b), c)) \end{aligned}$$

Poznámka: Ak ste vydržali doteraz, tak sa nezdávajte! Blížime sa do cieľovej rovinky!

Teraz vhodným³ použitím $R2$ dostávame

$$P(n, P(b, c)) = P(P(n, b), c) \rightarrow S(P(n, P(b, c))) = S(P(P(n, b), c))$$

Použitím axiómy $R5$ a MP na predchádzajúce riadky a nasledovným vhodným dosadením do axiómy pre rovnosť $R3$ dostaneme dlhú formulu

$$\begin{aligned} S(P(n, P(b, c))) &= P(S(n), P(b, c)) \rightarrow \\ (S(P(P(n, b), c)) &= P(P(S(n), b), c) \rightarrow \\ (S(P(n, P(b, c))) &= S(P(P(n, b), c)) \rightarrow (P(S(n), P(b, c)) \rightarrow P(P(S(n), b), c))) \end{aligned}$$

Dvojnásobným použitím MP dostaneme

$$(S(P(n, P(b, c))) = S(P(P(n, b), c)) \rightarrow (P(S(n), P(b, c)) \rightarrow P(P(S(n), b), c))).$$

No a teraz použitím pravidla jednoduchého sylogizmu⁴ dostaneme

$$P(n, P(b, c)) = P(P(n, b), c) \rightarrow P(S(n), P(b, c)) = P(P(S(n), b), c).$$

²Modus Ponens

³za x dosadíme $P(n, P(b, c))$, za y zasa $P(P(n, b), c)$ a ako f použijeme S .

⁴Ktoré hovorí ak platí $A \rightarrow B$ a zároveň $B \rightarrow C$ tak potom platí aj $A \rightarrow C$.

Hurá. Hurá. Hurá.

Takže teraz nám nezostáva už nič iné ako oba prípady našrôbovať do schémy pre indukciu a použiť modus ponens a máme výsledok. Našrôbovanie vyzerá takto:

$$(P(0, P(b, c)) = P(P(0, b), c))$$

$$\wedge (P(n, P(b, c)) = P(P(n, b), c) \rightarrow P(S(n), P(b, c)) = P(P(S(n), b), c))$$

$$\rightarrow (\forall n)(P(n, P(b, c)) = P(P(n, b), c)).$$

Po MP dostávame

$$(\forall n)(P(n, P(b, c)) = P(P(n, b), c)).$$

QED.