Logika dla informatyków

wykład 2

9 października 1998

1 Rachunek kwantyfikatorów (język I rzędu)

1.1 Składnia

W *rachunku kwantyfikatorów* używamy tzw. *zmiennych indywiduowych* pochodzących z nieskończonego zbioru $X = \{x, y, z, x_1, x_2, \dots\}$ i n-argumentowych ($n \geq 0$) *symboli relacji* $p, q, p_1, p_2, \dots$ Symbole relacji można uważać za uogólnienie zmiennych zdaniowych z rachunku zdań. *Formuły atomowe* są napisami postaci $p(x)$, $q(x,y)$ itp. *Formuły rachunku kwantyfikatorów* (ktore będziemy oznaczać ϕ, ψ,...) budujemy z *formuł atomowych* za pomocą *spójników logicznych* w sposób podobny jak w rachunku zdań. Ponadto możemy używać kwantyfikatorów $\forall$ i $\exists$. Formalna składnia rachunku kwantyfikatorów jest następująca:

$$
\begin{array}{rcl}
\phi & ::= & p(x_1, \dots, x_n) \\
 & & \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1 \Rightarrow \phi_2 \mid \phi_1 \Leftrightarrow \phi_2 \\
 & & \mid \forall x.\phi \mid \exists x.\phi
\end{array}
$$

Mówimy że w formule $\forall x.\phi$ kwantyfikator $\forall$ *wiąże* zmienną x. Wszystkie wystąpienia zmiennej x w formule ϕ są *związane* przez ten kwantyfikator. Zmienne, które nie są związane w danej formule, są *wolne*.

Formalnie zbiór $\mathrm{FV}(\phi)$ zmiennych wolnych formuły ϕ definiujemy następująco

$$
\begin{array}{rcll}
\mathrm{FV}(p(x_1, \dots, x_n)) & = & \{x_1, \dots, x_n\} & \\
\mathrm{FV}(\neg\phi) & = & \mathrm{FV}(\phi) & \\
\mathrm{FV}(\phi \circ \psi) & = & \mathrm{FV}(\phi) \cup \mathrm{FV}(\psi) & \quad \text{gdzie } \circ = \vee, \wedge, \Rightarrow, \Leftrightarrow \\
\mathrm{FV}(\forall x.\phi) & = & \mathrm{FV}(\phi) \backslash \{x\} & \\
\mathrm{FV}(\exists x.\phi) & = & \mathrm{FV}(\phi) \backslash \{x\} &
\end{array}
$$

Podobnie definiujemy zbiór zmiennych związanych.

Prawami rachunku kwantyfikatorów są np. *prawa negowania kwantyfikatorów* stwierdzające, że kwantyfikatory $\forall$ i $\exists$ są *dualne*:

$$\begin{aligned} \neg(\forall x.\phi) &\iff \exists x.\neg\phi \\ \neg(\exists x.\phi) &\iff \forall x.\neg\phi \end{aligned}$$

Ich intuicyjny sens jest jasny: „nieprawda że *dla każdego* x formuła ϕ jest prawdziwa" oznacza, że „*istnieje* x, dla którego formuła ϕ nie jest prawdziwa." Podobnie „nieprawda że *istnieje* x, dla którego formuła ϕ jest prawdziwa" oznacza, że „*dla każdego* x formuła ϕ nie jest prawdziwa."

2 Zbiory

W teorii mnogości *zbiór* i relację $\in$ należenia do zbioru przyjmujemy za pojęcia pierwotne. Własności relacji $\in$ są zadane przez *aksjomaty* (tj. formuły rachunku kwantyfikatorów, które przyjmujemy za prawdziwe).
Zasada ekstensjonalności stwierdza, że dwa zbiory są *równe*, co zapisujemy $A = B$, jeżeli zawierają dokładnie te same elementy, tj.

$$A = B \iff \forall x.(x \in A \Leftrightarrow x \in B)$$

Zbiór A jest *podzbiorem* zbioru B, jeżeli B zawiera wszystkie elementy zbioru A, tj.

$$A \subseteq B \iff \forall x.(x \in A \Rightarrow x \in B)$$

Zauważmy że dwa zbiory są równe, jeśli są nawzajem swoimi podzbiorami, tj.

$$A = B \iff A \subseteq B \wedge B \subseteq A$$

Zbiór pusty $\emptyset$ jest zbiorem nie zawierającym żadnego elementu:

$$\forall x.(x \notin \emptyset)$$

Mówimy że zbiór A *ma* n *elementów* ($n \geq 0$), co zapisujemy $|A| = n$, jeżeli istnieje wzajemnie jednoznaczne przyporządkowanie elementom tego zbioru liczb $1, 2, \ldots, n$, tj. jeśli elementy tego zbioru można ponumerować liczbami $1, 2, \ldots, n$. Zbiór pusty ma zatem 0 elementów.

Na zbiorach wprowadzamy operacje *sumy* $\cup$, *przekroju* $\cap$ i *różnicy* $\setminus$:

$$\begin{aligned} x \in A \cup B &\iff x \in A \vee x \in B \\ x \in A \cap B &\iff x \in A \wedge x \in B \\ x \in A \setminus B &\iff x \in A \wedge x \notin B \end{aligned}$$

Powyższe operacje mają wiele ciekawych własności. Dla przykładu prawdziwe są tzw. *prawa rozdzielności*:

$$\begin{aligned} A\setminus(B\cup C) &= (A\setminus B)\cap(A\setminus C) \\ A\cap(B\cup C) &= (A\cap B)\cup(A\cap C) \end{aligned}$$

Udowodnimy pierwsze z nich. Na mocy prawa ekstensjonalności wystarczy pokazać, że dla każdego x zachodzi

$$x\in A\setminus(B\cup C) \iff x\in(A\setminus B)\cap(A\setminus C)$$

Istotnie, z definicji różnicy zbiorów

$$x\in A\setminus(B\cup C) \iff x\in A\wedge\neg(x\in B\cup C)$$

Następnie z definicji sumy zbiorów mamy

$$x\in A\wedge\neg(x\in B\cup C) \iff x\in A\wedge\neg(x\in B\vee x\in C)$$

Korzystając z prawa de Morgana $\neg(p\vee q)\Leftrightarrow\neg p\wedge\neg q$ otrzymujemy

$$x\in A\wedge\neg(x\in B\vee x\in C) \iff x\in A\wedge(x\notin B\wedge x\notin C)$$

Na mocy tautologii $p\Leftrightarrow(p\wedge p)$ możemy do formuły dopisać jeszcze jedno wystąpienie $x\in A$. Ponadto koniunkcja jest łączna i przemienna, możemy zatem dowolnie pogrupować jej czynniki:

$$\begin{aligned} x\in A\wedge(x\notin B\wedge x\notin C) &\iff x\in A\wedge x\in A\wedge(x\notin B\wedge x\notin C) \\ &\iff (x\in A\wedge x\notin B)\wedge(x\in A\wedge x\notin C) \end{aligned}$$

Korzystając dwukrotnie z definicji różnicy zbiorów mamy

$$(x\in A\wedge x\notin B)\wedge(x\in A\wedge x\notin C) \iff (x\in A\setminus B)\wedge(x\in A\setminus C)$$

Na mocy definicji przekroju zbiorów mamy ostatecznie

$$(x\in A\setminus B)\wedge(x\in A\setminus C) \iff x\in(A\setminus B)\cap(A\setminus C)$$

Rozpoczęliśmy od formuły $x\in A\setminus(B\cup C)$. Przechodząc przez szereg formuł równoważnych otrzymaliśmy ostatecznie $x\in(A\setminus B)\cap(A\setminus C)$. Twierdzenie jest zatem udowodnione.

2.1 Operacje nieskończone na zbiorach

Dwuargumentowe operacje sumy i przekroju zbiorów można rozszerzyć na dowolne rodziny[1] zbiorów. Suma wszystkich zbiorów z rodziny $\{A_s\}_{s\in S}$, gdzie S jest pewnym

[1]Z powodów językowych zbiory zbiorów nazywa się *rodzinami*. Z matematycznego punktu widzenia są to zwykłe zbiory.

zbiorem *indeksów*, jest zbiorem zawierającym elementy występujące w którymkolwiek ze zbiorów A_s. Podobnie przekrój tej rodziny jest zbiorem zawierającym elementy występujące w każdym ze zbiorów A_s. Formalnie:

$$x \in \bigcup_{s \in S} A_s \iff \exists s \in S . x \in A_s$$
$$x \in \bigcap_{s \in S} A_s \iff \forall s \in S . x \in A_s$$

2.2 Zbiór potęgowy

Rodzinę wszystkich podziorów zbioru A nazywamy *zbiorem potęgowym* zbioru A i oznaczamy $\mathcal{P}(A)$. Formalnie:

$$\mathcal{P}(A) = \{B | B \subseteq A\}$$