Logika dla informatyków

Notatki do wykładów

21 kwietnia 2002

Niniejszy dokument zawiera listę najważniejszych definicji i twierdzeń omawianych na wykładzie z *Logiki dla Informatyków* i określa zakres materiału, który jest wymagany na egzaminie z tego przedmiotu. Podstawowym podręcznikiem do wykładu jest skrypt Jerzego Tiuryna pt. *Wstęp do teorii mnogości i logiki*. Skrypt ten można zakupić w pokoju 24. Jego elektroniczna wersja jest dostępna pod adresem `http://zls.mimuw.edu.pl/~tiuryn/skrypt-98.ps.gz`.

Spis treści

1. Rachunek zdań

1.1. Składnia

Definicja 1. *Formuły rachunku zdań* (ktore będziemy oznaczać ϕ, ψ,...) budujemy ze *zmiennych zdaniowych*, pochodzących z nieskończonego zbioru $V = \{p, q, p_1, p_2, \ldots\}$ i *spójników logicznych* fałszu $\bot$, negacji $\neg$, koniunkcji $\wedge$, alternatywy $\vee$, implikacji $\Rightarrow$ i równoważności $\Leftrightarrow$ w następujący sposób:

$$\phi \quad ::= \quad p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1 \Rightarrow \phi_2 \mid \phi_1 \Leftrightarrow \phi_2$$

W razie wątpliwości używamy nawiasów do wskazania sposobu rozbioru formuły. Niekiedy nawiasy opuszczamy zakładając następującą kolejność wiązania (od najsilniejszego do najsłabszego): $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ i przyjmując, że $\wedge$ i $\vee$ łaczą w lewo (tj. $p \vee r \vee s$ znaczy $(p \vee r) \vee s$), zaś $\Rightarrow$ i $\Leftrightarrow$ — w prawo (tj. $p \Rightarrow r \Rightarrow s$ znaczy $(p \Rightarrow r) \Rightarrow s$). Zatem np. $p \vee q \vee r \wedge s$ oznacza $(p \vee q) \vee (r \wedge s)$.

$\bot$
F

ϕ	$\neg\phi$
F	T
T	F

ϕ	ψ	$\phi \wedge \psi$
F	F	F
F	T	F
T	F	F
T	T	T

ϕ	ψ	$\phi \wedge \psi$
F	F	F
F	T	F
T	F	F
T	T	T

ϕ	ψ	$\phi \vee \psi$
F	F	F
F	T	T
T	F	T
T	T	T

ϕ	ψ	$\phi \Rightarrow \psi$
F	F	T
F	T	T
T	F	F
T	T	T

ϕ	ψ	$\phi \Leftrightarrow \psi$
F	F	T
F	T	F
T	F	F
T	T	T

Rysunek 1: Znaczenie spójników logicznych

1.2. Wartości logiczne i znaczenie formuł zdaniowych

Definicja 2. Zbiór *wartości logicznych* $\mathcal{B} = \{\mathsf{T}, \mathsf{F}\}$ zawiera dwa elementy: T (prawdziwe, *true*) i F (fałszywe, *false*). *Wartościowanie zmiennych* to odwzorowanie $\sigma : V \to \mathcal{B}$. Nadaje ono wartości logiczne zmiennym zdaniowym.

Wartość logiczna dowolnej formuły zdaniowej zależy jedynie od wartościowania występujących w niej zmiennych i można ją wyznaczyć korzystając z tabelek z rysunku 1.

Definicja 3. Formuła jest:

spełniona przy danym wartościowaniu zmiennych, jeżeli przy tym wartościowaniu ma wartość T;

spełnialna, jeżeli istnieje wartościowanie zmiennych, przy którym ta formuła ma wartość T;

prawdziwa (jest tautologią), jeśli ma wartość T dla każdego wartościowania zmiennych;

sprzeczna, jeśli ma wartość F dla każdego wartościowania zmiennych.

O formule spełnionej przez dane wartościowanie zmiennych będziemy niekiedy mówić, że jest *prawdziwa* przy tym wartościowaniu. Podobnie formuła nie spełniona będzie *fałszywa*.

1.3. Metoda zero-jedynkowa sprawdzania tautologii

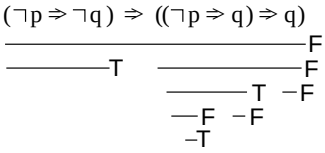
Przykładami tautologii są formuły $\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$ oraz $\neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$ zwane *prawami de Morgana*. Istotnie, rysujemy tabelkę (rysunek 2) umieszczając w kolumnach 1 i 2 wartości zmiennych zdaniowych p i q. W kolumnie 3 umieszczamy wartości formuły $p \vee q$ wyliczone z użyciem tabelki dla alternatywy. W kolumnie 4 obliczamy, w oparciu o tabelkę negacji, wartości formuły $\neg(p \vee q)$. Kolumy 5 i 6 wyznaczamy również w oparciu o tabelkę negacji. Aby wyznaczyć wartości formuły $(\neg p) \wedge (\neg q)$ korzystamy z wartości zapisanych w kolumnach 5 i 6 i z tabelki koniunkcji. Ostatnią, ósmą kolumnę wyznaczamy przy użyciu tabelki dla równoważności z wartości logicznych zapisanych w kolumnach 6 i 7. Po skonstruowaniu tabelki zauważamy, że dla każdego z czterech możliwych wartościowań zmiennych p i q formuła $\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$ ma wartość logiczną T, jest więc tautologią.

1.4. Metoda zero-jedynkowa skrócona

Sprawdzenie czy formuła jest tautologią można znacznie przyspieszyć, jeśli zamiast bezmyślnie sprawdzać wartość formuły dla wszystkich możliwych wartościowań zmiennych, będziemy świadomie poszukiwać wartościowania, dla którego formuła nie jest spełniona. Ustalenie takiego wartościowania przekona nas, że formuła nie jest tautologią, dojście do sprzeczności zaś — że nią jest. Rozważmy dla ustalenia uwagi formułę $(\neg p \Rightarrow \neg q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow q)$. Formuła ta nie jest spełniona, jeśli poprzednik implikacji $\neg p \Rightarrow \neg q$

1	2	3	4	5	6	7	8
p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$(\neg p) \wedge (\neg q)$	$\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$
F	F	F	T	T	T	T	T
F	T	T	F	T	F	F	T
T	F	T	F	F	T	F	T
T	T	T	F	F	F	F	T

Rysunek 2: Tabelkowa metoda sprawdzenia, że prawo de Morgana jest tautologią



Rysunek 3: Wartościowanie, dla którego formuła $(\neg p \Rightarrow \neg q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow q)$ nie jest spełniona

jest prawdziwy, jej następnik $(\neg p \Rightarrow q) \Rightarrow q$ zaś — fałszywy. Formuła $(\neg p \Rightarrow q) \Rightarrow q$ jest fałszywa tylko wówczas, gdy $\neg p \Rightarrow q$ jest spełniona oraz $\sigma(q) = \mathsf{F}$. Ale $\neg p \Rightarrow q$ jest spełniona dla $\sigma(q) = \mathsf{F}$ tylko wówczas, gdy $\neg p$ nie jest spełniona, tj. gdy $\sigma(p) = \mathsf{T}$. Zauważamy na koniec, że przy wartościowaniu $\sigma(p) = \mathsf{T}$ i $\sigma(q) = \mathsf{F}$ nasza wyjściowa formuła istotnie nie jest spełniona, nie jest więc tautologią (rysunek 3).

Rozważmy teraz formułę $\phi = p \Rightarrow (q \Rightarrow p)$. Aby ϕ nie była spełniona, musi być $\sigma(p) = \mathsf{T}$ oraz powinna nie być spełniona formuła $q \Rightarrow p$. Formuła ostatnia nie jest spełniona tylko wówczas, gdy $\sigma(q) = \mathsf{T}$ oraz $\sigma(p) = \mathsf{F}$. Zatem aby ϕ nie była spełniona, musiałoby być jednocześnie $\phi(p) = \mathsf{T}$ i $\phi(p) = \mathsf{F}$, co jest niemożliwe. Formuła ϕ jest zatem tautologią.

Przykład 4. Przykładami tautologii są także

$$(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$$

$$(\neg p \Rightarrow \neg q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow q)$$

1.5. Funkcje boolowskie i systemy spójników

Definicja 5. Funkcje $f : \mathcal{B}^n \to \mathcal{B}$ nazywamy n-argumentowymi funkcjami boolowskimi, $n \geq 0$. Funkcje boolowskie możemy opisywać za pomocą formuł zdaniowych, np.

$$f(p, q, r) \quad \equiv \quad (p \wedge q) \Rightarrow (p \vee r)$$

Definicja 6. Zbiór spójników logicznych jest *zupełny*, jeżeli dowolną funkcję boolowską można opisać za pomocą formuły zdaniowej zawierającej jedynie spójniki z tego zbioru i zmienne. Zbiór spójników jest *2-zupełny*, jeżeli każdą *co najwyżej dwuargumentową* funkcję boolowską można opisać za pomocą formuły zdaniowej zawierającej jedynie spójniki z tego zbioru i zmienne.

Na ćwiczeniach pokażemy, że

- każdy zbiór 2-zupełny jest zupełny;
- $\{\vee, \wedge, \Leftrightarrow\}$ nie jest zupełny;
- $\{\vee, \wedge\}$ nie jest zupełny;
- $\{\Rightarrow, \bot\}$ jest zupełny;
- $\{\wedge, \neg\}$ jest zupełny;
- istnieje binarny spójnik $\uparrow$, taki, że $\{\uparrow\}$ jest zupełny.

i wskażemy inne przykłady systemów zupełnych.

2. Rachunek kwantyfikatorów (język I rzędu)

2.1. Składnia

Definicja 7. W *rachunku kwantyfikatorów* używamy tzw. *zmiennych indywiduowych* pochodzących z nieskończonego zbioru $X = \{x, y, z, x_1, x_2, \ldots\}$ i n-argumentowych ($n \geq 0$) *symboli relacji* $p, q, p_1, p_2, \ldots$ 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:

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

Definicja 8. 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

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

Podobnie definiujemy zbiór zmiennych związanych.

Przykład 9. Prawami rachunku kwantyfikatorów są np. *prawa negowania kwantyfikatorów* stwierdzające, że kwantyfikatory $\forall$ i $\exists$ są *dualne*:

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

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."

3. 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).

Definicja 10. *Zasada ekstensjonalności* stwierdza, że dwa zbiory są *równe*, co zapisujemy $A = B$, jeżeli zawierają dokładnie te same elementy, tj.

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

Definicja 11. Zbiór A jest *podzbiorem* zbioru B, jeżeli B zawiera wszystkie elementy zbioru A, tj.

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

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

$$A = B \quad \Leftrightarrow \quad A \subseteq B \wedge B \subseteq A$$

Definicja 12. *Zbiór pusty* $\emptyset$ jest zbiorem nie zawierającym żadnego elementu:

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

Definicja 13. 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.

Definicja 14. Na zbiorach wprowadzamy operacje *sumy* $\cup$, *przekroju* $\cap$ i *różnicy* $\setminus$:

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

Fakt 15. Powyższe operacje mają wiele ciekawych własności. Dla przykładu prawdziwe są tzw. *prawa rozdzielności*:

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

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

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

Istotnie, z definicji różnicy zbiorów

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

Następnie z definicji sumy zbiorów mamy

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

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

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

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:

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

Korzystając dwukrotnie z definicji różnicy zbiorów mamy

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

Na mocy definicji przekroju zbiorów mamy ostatecznie

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

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.

3.1. Operacje nieskończone na zbiorach

Definicja 16. 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 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:

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

3.2. Zbiór potęgowy

Definicja 17. Rodzinę wszystkich podziorów zbioru A nazywamy *zbiorem potęgowym* zbioru A i oznaczamy $\mathcal{P}(A)$. Formalnie:

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

4. Relacje

4.1. Para uporządkowana

Definicja 18. Parę elementów a i b będziemy zapisywać w postaci $\langle a, b\rangle$. Para będzie dla nas pojęciem pierwotnym. Przyjmujemy następujący aksjomat:

$$\langle a, b\rangle = \langle c, d\rangle \quad \Leftrightarrow \quad a = c \wedge b = d$$

Specjaliści od podstaw matematyki pragną za pojęcia pierwotne uważać jedynie zbiór i relację należenia do zbioru i wolą *zdefiniować* parę następująco:

$$\langle a, b\rangle \quad = \quad \{\{a\}, \{a, b\}\}$$

Para w takim ujęciu składa się ze zbioru dwuelementowego, w którym wyróżniliśmy, który element jest pierwszy. Zauważmy, że ostatnia definicja spełnia aksjomat „naszej" pary.

4.2. Iloczyn (produkt) kartezjański

Definicja 19. *Iloczynem kartezjańskim* dwóch zbiorów nazywamy zbiór wszystkich par złożonych z elementów tych zbiorów:

$$A \times B \quad = \quad \{\langle a, b\rangle \mid a \in A, b \in B\}$$

4.3. Relacje

Definicja 20. Dowolny podzbiór $R \subseteq A \times B$ produktu kartezjańskiego zbiorów A i B nazywamy *relacją dwuargumentową* (*binarną*). Jeśli $\langle a, b\rangle \in R$, to mówimy, że elementy $a \in A$ i $b \in B$ *są ze sobą w relacji*. Zamist pisać $\langle a, b\rangle \in R$, piszemy też niekiedy aRb. Podzbiory A^2 są *binarnymi relacjami na zbiorze* A.

Przykład 21. Relacjami binarnymi są:

- identyczność (równość, przekątna) na zbiorze A: $\{\langle x, x\rangle \mid x \in A\}$
- relacja mniejszości $\leq$ na zbiorze A: $\{\langle x, y\rangle \mid x \leq y\}$
- $R \subseteq \mathbb{Z} \times \mathbb{N}$, taka, że xRy gdy $y = x^2$.

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

4.4. Krotki (n-tki) uporządkowane

Definicja 22. Pojęcie pary łatwo uogólnić na ciągi uporządkowane dowolnej, skończonej długości. Zakładamy, że $\langle a_1, \ldots, a_n\rangle$ jest pojęciem pierwotnym i przyjmujemy aksjomat

$$\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle \quad \Leftrightarrow \quad a_1 = b_1 \wedge \ldots \wedge a_n = b_n$$

Krotki można również *zdefiniować* za pomocą pojęcia pary: krotka dwuelementowa jest parą, krotka $n+1$-elementowa jest parą złożoną z pierwszego elementu i krotki n-elementowej:

$$\begin{cases} \langle a_1, a_2\rangle = \langle a_1, a_2\rangle & \text{(krotka dwuelementowa jest parą)} \\ \langle a_0, a_1, \ldots, a_n\rangle = \langle a_0, \langle a_1, \ldots, a_n\rangle\rangle \end{cases}$$

Krotka stuelementowa jest nazywana stokrotką.

Definicja 23. W oczywisty sposób uogólniamy pojęcie *produktu* na n zbiorów:

$$A_1 \times \ldots \times A_n \quad = \quad \{\langle a_1, \ldots, a_n\rangle \mid a_1 \in A_1, \ldots, a_n \in A_n\}$$

Relacją n-argumentową nazywamy dowolny podzbiór produktu n zbiorów. Dla przykładu

$$\{a, b, c \in \mathbb{N} \mid a \cdot b = c\} \qquad \{a, b, c \in \mathbb{N} \mid a \cdot b < c\}$$

są relacjami trójargumentowymi na zbiorze $\mathbb{N}$.

4.5. Złożenie relacji. Relacja odwrotna

Definicja 24. Dane są relacje $P \subseteq A \times B$ i $Q \subseteq B \times C$. Relacja

$$PQ = \{\langle a, c\rangle \mid \exists b.(aPb \wedge bQr)\} \subseteq A \times C$$

nazywa się *złożeniem* relacji P i Q. Relacja

$$P^{-1} = \{\langle b, a\rangle \mid \langle a, b\rangle \in P\} \subseteq B \times A$$

nazywa się *relacją odwrotną* do P.

Twierdzenie 25. Dla dowolnych relacji $T \subseteq A \times B$, $S \subseteq B \times C$ i $R \subseteq C \times D$:

$$\begin{aligned} T(SR) &= (TS)R \\ (SR)^{-1} &= R^{-1}S^{-1} \end{aligned}$$

5. Funkcje

Definicja 26. Relację $f \subseteq A \times B$ nazywamy *funkcją o dziedzinie A i zbiorze wartości (przeciwdziedzinie) B*, jeżeli

1. $\forall a \in A.\exists b \in B.\langle a, b\rangle \in f$
2. $\forall a \in A.\forall b_1 \in B.\forall b_2 \in B.(\langle a, b_1\rangle \in f \wedge \langle a, b_2\rangle \in f \Rightarrow b_1 = b_2)$

Zbiór wszystkich funkcji o dziedzinie A i przeciwdziedzinie B oznaczamy B^A.

Relację spełniającą jedynie warunek 2 nazywamy *funkcją częściową*. *Dziedziną* funkcji częściowej f nazywamy zbiór

$$\mathrm{Dom}(f) = \{a \in A \mid \exists b \in B.\, f(a) = b\}$$

Zamist $f \subseteq A \times B$ piszemy zwykle $f : A \to B$, zaś zamiast afb albo $\langle a, b\rangle \in f$ piszemy $b = f(a)$.

Pytanie 27. Ile jest funkcji $f : A \to B$? Ile jest funkcji $f : \emptyset \to B$, a ile $f : A \to \emptyset$?

Z pomocą pojęcia funkcji możemy jeszcze inaczej zdefiniować n-tki uporządkowane: $\langle a_1, \ldots, a_n \rangle$ jest funkcją $f : \{1, \ldots, n\} \to A$. Wówczas $f(i)$ jest i-tym elementem krotki.

Definicja 28. Funkcja $f : A \to B$ jest *różnowartościowa* (jest *injekcją*), jeżeli

$$\forall a_1, a_2 \in A.(f(a_1) = f(a_2) \Rightarrow a_1 = a_2)$$

Funkcja $f : A \to B$ jest *„na”* (jest *surjekcją*), jeżeli

$$\forall b \in B.\exists a \in A.\, f(a) = b$$

Funkcja f jest *odwzorowaniem wzajemnie jednoznacznym* (*bijekcją*), jeśli jest różnowartościowa i „na”.

6. Funkcje odwrotne, złożenie funkcji

Twierdzenie 29. Jeśli $f : A \to B$ oraz $g : B \to C$ są funkcjami, to relacja $gf \subseteq A \times C$ jest funkcją z A w C. Dla $a \in A$, $(gf)(a) = g(f(a))$. Funkcja fg jest różnowartościowa, gdy f i g obie są różnowartościowe. Funkcja fg jest „na”, jeśli f i g sa „na”.

Definicja 30. Niech $f : A \to B$ będzie funkcją. Wtedy funkcja $f : B \to A$ jest *funkcją odwrotną* do f, jeśli $gf = I_A$ oraz $fg = I_B$ (gdzie I_A, I_B oznaczają funkcje identycznościowe odpowiednio na zbiorach A i B).

Twierdzenie 31. Niech $f : A \to B$ będzie funkcją. Wtedy następujące warunki są równoważne:

1. f ma funkcję odwrotną,
2. f jest bijekcją,
3. relacja odwrotna f^{-1} jest funkcją.

Funkcję odwrotną do f oznaczamy f^{-1}.

7. Obraz i przeciwobraz zbioru

Definicja 32. Niech $f : A \to B$ będzie funkcją i niech $X \subseteq A$. *Obrazem zbioru X w odwzorowaniu f* nazywamy zbiór

$$\vec{f}(X) \;=\; \{b \in B \mid (\exists a)(f(a) = b)\}$$

Przeciwobrazem zbioru $Y \subseteq B$ nazywamy zbiór

$$\vec{f}^{-1}(X) \;=\; \{a \in A \mid f(a) \in Y\}$$

Definicja 33. Niech $\mathcal{X}$ bedzie rodziną podzbiorów zbioru A. Wtedy

$$\bigcup \mathcal{X} \;=\; \bigcup_{X \in \mathcal{X}} X$$
$$\bigcap \mathcal{X} \;=\; \bigcap_{X \in \mathcal{X}} X$$

Twierdzenie 34. Niech $f : A \to B$ będzie funkcją i niech $\mathcal{X}$ bedzie rodziną podzbiorów zbioru A. Wtedy

$$\vec{f}(\bigcup \mathcal{X}) \;=\; \bigcup\{\vec{f}(X) \mid X \in \mathcal{X}\} \tag{1}$$

Jeśli $\mathcal{X} \neq \emptyset$, to
$$\vec{f}(\bigcap \mathcal{X}) \;\subseteq\; \bigcap\{\vec{f}(X) \mid X \in \mathcal{X}\} \tag{2}$$

$$\vec{f}^{-1}(\bigcup \mathcal{Y}) \;=\; \bigcup\{\vec{f}^{-1}(Y) \mid Y \in \mathcal{Y}\} \tag{3}$$

Jeśli $\mathcal{Y} \neq \emptyset$, to
$$\vec{f}^{-1}(\bigcap \mathcal{Y}) \;=\; \bigcap\{\vec{f}^{-1}(Y) \mid Y \in \mathcal{Y}\} \tag{4}$$

Pytanie 35. Czy symbol „$\subseteq$” we wzorze (2) można zastąpić symbolem „$=$”?

8. Relacje równoważności

Definicja 36. Relacja $R \subseteq A \times A$ jest

- *zwrotna*, jeśli $a\,R\,a$ dla każdego $a \in A$,
- *symetryczna*, jeśli $a\,R\,b \Rightarrow b\,R\,a$ dla każdych $a, b \in A$,
- *przechodnia*, jeśli $a\,R\,b \wedge b\,R\,c \Rightarrow a\,R\,c$ dla wszelkich $a, b, c \in A$.

Relację zwrotną, symetryczną i przechodnią nazywamy *relacją równoważności*.

Definicja 37. *Klasą abstrakcji* elementu $a \in A$ względem relacji równoważności $\sim \subseteq A \times A$ nazywamy zbiór

$$[a]_\sim \quad = \quad \{b \in A \mid a \sim b\}$$

Definicja 38. *Podziałem zbioru* A nazywamy dowolną rodzinę niepustych zbiorów parami rozłącznych pokrywającą A.

Lemat 39. Dla dowolnej relacji równoważności $\sim \subseteq A \times A$ i elementów $a, b \in A$

$$a \sim b \quad \Leftrightarrow \quad [a]_\sim = [b]_\sim$$

Twierdzenie 40 (Zasada Abstrakcji).

1. Klasy abstrakcji dowolnej relacji równoważności tworzą podział zbioru A.
2. Dla każdego podziału zbioru A istnieje dokładnie jedna relacja równoważności której klasy abstrakcji wyznaczają ten podział.

Przykład 41. Niech $a, b, c, d \in \mathbb{Z}$, $c, d \neq 0$. Definiujemy relację $\sim \subseteq (\mathbb{Z} \times (\mathbb{Z}\backslash\{0\}) \times (\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ wzorem

$$\langle a, b\rangle \sim \langle c, d\rangle \quad \Leftrightarrow \quad a \cdot d = b \cdot c$$

Relacja $\sim$ jest relacją równoważności na $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$. Dowód polega na sprawdzeniu wprost z definicji, czy $\sim$ jest zwrotna, symetryczna i przechodnia.

9. Równoliczność zbiorów

Definicja 42. Zbiory A i B *są równoliczne*, jeżeli istnieje bijekcja $f : A \to B$. Piszemy wówczas $A \sim B$.

Przykład 43. Następujące zbiory są równoliczne:

- zbiór par liczb naturalnych i zbiór liczb naturalnych: $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$;
- zbiór liczb naturalnych i zbiór liczb naturalnych parzystych: $\mathbb{N} \sim \mathbb{P}$;
- dowolny niepusty przedział $(a, b) \subseteq \mathbb{R}$, $a < b$, i odcinek $(0, 1)$: $(a, b) \sim (0, 1)$.

Twierdzenie 44. Dla dowolnych zbiorów A, B, C

1. $A \sim A$
2. $A \sim B \Leftrightarrow B \sim A$
3. $(A \sim B \wedge B \sim C) \Leftrightarrow A \sim C$

Definicja 45. *Mocą zbioru* (którą oznaczamy $|A|$) nazywamy obiekt spełniający następującą własność: $A \sim B \Leftrightarrow |A| = |B|$.

Definicja 46. $\underline{n} = \{0, 1, \ldots, n-1\}$ oznacza zbiór liczb naturalnych mniejszych od n.

Definicja 47. Zbiór A jest *zbiorem skończonym*, jeśli istnieje liczba naturalna $n \in \mathbb{N}$, taka, że $A \sim \underline{n}$. Mówimy wówczas, że zbiór A ma n elementów.

10. Teoria mocy

Definicja 48 (Wzorce mocy (liczb kardynalnych)). Mówiąc o liczbach kardynalnych posługujemy się następującymi reprezentantami zbiorów danej mocy:

- zbiory skończone: $\underline{n} = \{0, 1, \ldots, n-1\}$;
- liczby naturalne: $\mathbb{N} = \{0, 1, \ldots\}$;
- liczby rzeczywiste: $\mathbb{R}$.

Definicja 49. Wprowadzamy następujące oznaczenia mocy zbiorów:

- zbiory skończone: $|\underline{n}| = n$;
- liczby naturalne: $|\mathbb{N}| = \aleph_0$ (*alef zero*);
- liczby rzeczywiste: $|\mathbb{R}| = \mathfrak{c}$ (*continuum*).

Twierdzenie 50.

1. Dla każdego $n \in \mathbb{N}$ nie istnieje funkcja różnowartościowa z $\underline{n+1}$ w $\underline{n}$.
2. Jeżeli istnieje funkcja różnowartościowa z $\underline{m}$ w $\underline{n}$, to $m \leq n$ (czyli $\underline{m} \subseteq \underline{n}$).
3. Jeżeli $\underline{m} \sim \underline{n}$, to $m = n$.
4. Dla każdego $m \in \mathbb{N}$, $\underline{m} \not\sim \mathbb{N}$.

Definicja 51. Mówimy, że moc zbioru A jest nie większa niż moc zbioru B i piszemy $|A| \leq |B|$, jeśli istnieje funkcja różnowartościowa $f : A \to B$.

Twierdzenie 52 (Cantor-Bernstein). Jeśli $|A| \leq |B|$ oraz $|B| \leq |A|$, to $|A| = |B|$.

Definicja 53. Mówimy, że moc zbioru A jest mniejsza niż moc zbioru B i piszemy $|A| < |B|$, jeśli $|A| \leq |B|$ oraz $A \not\sim B$.

Twierdzenie 54.

1. $|A| \leq |A|$
2. jeśli $|A| \leq |B|$ i $|B| \leq |C|$, to $|A| \leq |C|$
3. jeśli $n < m$, to $|\underline{n}| < |\underline{m}|$
4. $|\underline{n}| < \aleph_0$

Definicja 55. Jeśli $X \subseteq A$, to $f : A \to \{0, 1\}$ jest *funkcją charakterystyczną* zbioru A, jeśli dla dowolnego $a \in A$

$$f(a) \quad = \quad \begin{cases} 0, & \text{gdy } a \notin X; \\ 1, & \text{gdy } a \in X. \end{cases}$$

Fakt 56. $\underline{2}^A \sim \mathcal{P}(A)$.

Twierdzenie 57. Niech A i B będą zbiorami, przy czym $|B| \geq 2$. Wtedy

$$|\mathcal{P}(A)| \quad \leq \quad |B^A|$$

gdzie $B^A = \{f : A \to B\}$ a $\mathcal{P}(A)$ oznacza zbiór potęgowy zbioru A.

Twierdzenie 58 (Cantor). Dla żadnego A nie istnieje funkcja z A *na* zbiór potęgowy $\mathcal{P}(A)$.

Dowód. Przypuśćmy przeciwnie, że pewna funkcja $f : A \to \mathcal{P}(A)$ przekształca A *na* $\mathcal{P}(A)$. Niech

$$A_0 \quad = \quad \{a \in A \mid a \notin f(a)\}$$

Ponieważ $A_0 \subseteq A$ i f odwzorowuje A *na* $\mathcal{P}(A)$, więc istnieje $a_0 \in A$, takie, że $f(a_0) = A$. Mamy wtedy

$$a_0 \in A_0 \quad \Leftrightarrow \quad a_0 \in f(a_0) \quad \Leftrightarrow \quad a_0 \notin A_0$$

Założenie istnienia funkcji f doprowadziło do sprzeczności.

Dowód (twierdzenia Cantora dla przypadku $A = \mathbb{N}$). Przypuśćmy przeciwnie, że pewna funkcja $f : \mathbb{N} \to \underline{2}^{\mathbb{N}}$ przekształca $\mathbb{N}$ *na* $\underline{2}^{\mathbb{N}}$. Tworzymy nieskończoną tablicę

$$\begin{array}{cccccc}
\boxed{(\mathrm{f}(0))(0)} & (f(0))(1) & (f(0))(2) & (f(0))(3) & (f(0))(4) & \cdots \\
(f(1))(0) & \boxed{(\mathrm{f}(1))(1)} & (f(1))(2) & (f(1))(3) & (f(1))(4) & \cdots \\
(f(2))(0) & (f(2))(1) & \boxed{(\mathrm{f}(2))(2)} & (f(2))(3) & (f(2))(4) & \cdots \\
(f(3))(0) & (f(3))(1) & (f(3))(2) & \boxed{(\mathrm{f}(3))(3)} & (f(3))(4) & \cdots \\
(f(4))(0) & (f(4))(1) & (f(4))(2) & (f(4))(3) & \boxed{(\mathrm{f}(4))(4)} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Tworzymy nową funkcję charakterystyczną

$$g(i) \quad = \quad 1 - (f(i))(i)$$

dla każdego $i \in \mathbb{N}$. Wtedy $g \neq f(i)$ dla dowolnego $i \in \mathbb{N}$, gdyż $g(i) = 1 - (f(i))(i) \neq f(i)$. Otrzymaliśmy sprzeczność z założeniem, że f jest *na*.

Twierdzenie 59. Dla każdego zbioru A, $|\mathcal{P}(A)| > |A|$. Jeśli $|B| > 2$, to $|B^A| > |A|$.

11. Zbiory przeliczalne

Definicja 60. Zbiór A jest *przeliczalny*, gdy A jest skończony lub jest równoliczny ze zbiorem liczb naturalnych.

Twierdzenie 61. Zbiór A jest przeliczalny wtedy i tylko wtedy, gdy $A = \emptyset$ lub istnieje funkcja z $\mathbb{N}$ *na* A.

Definicja 62. *Ciągiem elementów zbioru A* nazywamy funkcję $f : \mathbb{N} \to A$.

Definicja 63. Zbiór niepusty jest przeliczalny, gdy jego elementy można ustawić w ciąg.

Twierdzenie 64.

1. Podzbiór zbioru przeliczalnego jest przeliczalny.
2. Jeśli $f : A \to B$ oraz $X \subseteq A$ jest zbiorem przeliczalnym, to $f(X)$ też jest zbiorem przeliczalnym.
3. Jeśli A i B są przeliczalne, to $A \times B$ jest przeliczalny.
4. Jeśli $\{A_i \mid i \in I\}$ jest przeliczalną rodziną zbiorów przeliczalnych (tzn. I jest przeliczalny i każdy ze zbiorów A_i jest przeliczalny), to $\bigcup_{i \in I} A_i$ jest zbiorem przeliczalnym.

Twierdzenie 65. Zbiór liczb rzeczywistych jest równoliczny ze zbiorem $\{0, 1\}^{\mathbb{N}}$. Zatem zbiór $\{0, 1\}^{\mathbb{N}}$ ma moc continuum.

12. Porządki częściowe

Definicja 66. Relacja R jest *słabo antysymetryczna*, jeśli dla dowolnych a, b

$$\text{jeśli } aRb \text{ oraz } bRa \text{ to } a = b$$

Definicja 67. *Częściowym porządkiem* w zbiorze A nazywamy relację „$\leq$" (będącą podzbiorem A^2), która jest *zwrotna, przechodnia* i *słabo antysymetryczna*, tzn.

$$\forall a.a \leq a$$
$$\forall a, b.(a \leq b \wedge b \leq a \Rightarrow a = b)$$
$$\forall a, b, c.(a \leq b \wedge b \leq c \Rightarrow a \leq c)$$

Definicja 68. Jeśli $\leq$ jest częściowym porządkiem na A, to $a < b$ oznacza $a \leq b \wedge a \neq b$.

Definicja 69. *Zbiór częściowo uporządkowany*, to zbiór A z relacją częściowego porządku $\leq$. Zbiór częściowo uporządkowany oznaczamy czasem $\langle A, \leq \rangle$.

Przykład 70. Oto przykłady zbiorów uporządkowanych:

1. $\langle \mathcal{P}(A), \subseteq \rangle$ (rodzina podzbiorów zbioru A z relacją inkluzji);
2. $\langle \mathbb{N}, \leq \rangle$ (zbiór liczb naturalnych ze zwykłym porządkiem);
3. $\langle \mathcal{B}, \subseteq \rangle$, gdzie $\mathcal{B} \subseteq \mathcal{P}(A)$;
4. $\langle \mathbb{N}, | \rangle$, gdzie $a|b \Leftrightarrow \exists x.(ax = b)$.

Definicja 71. Porządek częściowy $\leq$ w zbiorze A jest *liniowy*, jeśli $(\forall a, b \in A)((a \leq b) \vee (b \leq a))$.

Przykład 72. Porządkiem liniowym jest relacja $\leq$ na zbiorze liczb rzeczywistych. Porządkiem liniowym nie jest relacja inkluzji $\subseteq$ na zbiorze $\mathcal{P}(\mathbb{N})$.

13. Słowa

Definicja 73. Niech A będzie dowolnym zbiorem. Będziemy nazywać go *alfabetem*. *Słowem* nad alfabetem A nazywamy dowolny skończony ciąg elementów zbioru A. Słowo puste (ciąg długości zero) oznaczamy ϵ. Przez A^* oznaczamy zbiór wszystkich słów nad alfabetem A. Jeżeli $u = u_1u_2 \ldots u_n$ i $w = w_1w_2 \ldots w_m$, to uw oznacza *złożenie* (*konkatenację*) słów u i w, tj. słowo $u_1u_2 \ldots u_nw_1w_2 \ldots w_m$. Słowo U jest *przedrostkiem* (*prefiksem*) słowa w, jeśli istnieje słowo v, takie, że $uv = w$.

Fakt 74. Niech A będzie dowolnym zbiorem i niech $u \leq w$ oznacza, że u jest przedrostkiem w. Wtedy $\langle A, \leq \rangle$ jest zbiorem częściowo uporządkowanym.

14. Kresy zbiorów

Definicja 75. Niech $\langle P, \leq \rangle$ będzię porządkiem częściowym i niech $X \subseteq P$. Element $x \in X$ jest *elementem największym* (odpowiednio *najmniejszym*) w X, jeśli dla każdego $y \in X$ zachodzi $y \leq x$ (odpowiednio $x \leq y$). Element najmniejszy oznacza się $\bot$, zaś największy $\top$.

Definicja 76. Element $x \in X$ jest elementem *maksymalnym* (odpowiednio *minimalnym*) w X, jeśli dla każdego $y \in X$, jeśli $x \leq y$ (odpowiednio $y \leq x$), to $x = y$.

Definicja 77. Niech $\langle P, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Porządek $\langle P, \leq^{-1} \rangle$ nazywamy porządkiem *dualnym* do $\langle P, \leq \rangle$. Jeśli dane jest pojęcie $\mathcal{Q}$ dotyczące porządków, to pojęcie $\mathcal{Q}^{-1}$ dualne do niego otrzymujemy przez zastąpienie w definicji $\mathcal{Q}$ symbolu $\leq$ przez symbol $\leq^{-1}$. Zauważmy, że pojęcia minimalny i maksymalny oraz najmniejszy i największy są dualne.

Twierdzenie 78. Niech $\langle P, \leq \rangle$ będzie częściowym porządkiem i niech $X \subseteq P$. Wtedy element największy w X jest elementem maksymalnym w X.

Twierdzenie 79. Istnieje co najwyżej jeden element największy.

Przykład 80. Niech X będzie zbiorem niepustym i niech $P = \mathcal{P}(X) \setminus \emptyset$. Wtedy w zbiorze uporządkowanym $\langle P, \subseteq \rangle$ jest $|X|$ elementów minimalnych.

Definicja 81. Niech $\langle P, \leq \rangle$ będzie częściowym porządkiem i niech $X \subseteq P$. Element $a \in P$ jest *ograniczeniem górnym* zbioru X, jeśli dla każdego $x \in X$ zachodzi $x \leq a$. *Kresem górnym* zbioru X nazywamy najmniejszy element zbioru $\{a : a \text{ jest ograniczeniem górnym } X\}$. Kres górny zbioru X oznaczamy $\bigvee X$. Dualnie można zdefiniować pojęcia *ograniczenia dolnego* i *kresu dolnego* (kres dolny zbioru X oznaczamy $\bigwedge X$).

Definicja 82. Porządek $\langle P, \leq \rangle$ jest *kratą zupełną*, jeśli każdy podzbiór zbioru P ma kres górny i kres dolny. Porządek $\langle P, \leq \rangle$ jest *kratą*, jeśli każdy skończony podzbiór zbioru P ma kres górny i kres dolny.

Twierdzenie 83. Niech $\langle P, \leq \rangle$ będzie porządkiem. Wtedy następujące warunki są równoważne:

1. $\langle P, \leq \rangle$ jest kratą zupełną.
2. Każdy podzbiór P ma kres górny w $\langle P, \leq \rangle$
3. Każdy podzbiór P ma kres dolny w $\langle P, \leq \rangle$

Definicja 84. Niech $\langle P, \leq_P \rangle$ oraz $\langle Q, \leq_Q \rangle$ będą zbiorami częściowo uporządkowanymi. Funkja $F : P \to Q$ jest *monotoniczna*, jeśli $(\forall x, y \in P)((x \leq_P y) \Rightarrow (f(x) \leq_Q f(y)))$.

Definicja 85. Funkcja f jest *izomorfizmem porządkowym*, jeśli jest bijekcją oraz f i f^{-1} są monotoniczne.

Twierdzenie 86 (Knaster, Tarski). Niech $\langle P, \leq \rangle$ będzie kratą zupełną i niech $f : P \to P$ będzie funkcją monotoniczną. Wtedy istnieje $a \in P$ taki, że

1. $f(a) = a$
2. dla każdego $b \in P$, jeśli $f(b) = b$, to $a \leq b$.

Element a nazywamy *najmniejszym punktem stałym* funkcji f. Element spełniający tylko warunek 1 nazywamy *punktem stałym*.

Definicja 87. Niech $\langle P, \leq_P \rangle$ będzie zbiorem częściowo uporządkowanym. Wtedy zbiór $X \neq \emptyset$ jest zbiorem *skierowanym*, jeśli $(\forall x, y \in X)(\exists z \in X)(x \leq z \wedge y \leq z)$. Zbiór $\langle P, \leq_P \rangle$ jest *porządkiem zupełnym*, jeśli P ma element najmniejszy oraz każdy skierowany podzbiór X zbioru P ma kres górny.

Definicja 88. Niech $\langle P, \leq_P \rangle$ oraz $\langle Q, \leq_Q \rangle$ będą porządkami zupełnymi. Funkcja $f : P \to Q$ jest *ciągła*, jeśli zachowuje kresy górne, to znaczy, gdy dla dowolnego zbioru skierowanego $X \subseteq P$, $\vec{f}(X)$ ma kres górny oraz $f(\bigvee X) = \bigvee \vec{f}(X)$.

Twierdzenie 89.

1. Każda funkcja ciągła jest monotoniczna.
2. Złożenie funkcji ciągłych jest funkcją ciągłą.

Twierdzenie 90. Niech $\langle P, \leq_P \rangle$ będzie porządkiem zupełnym oraz niech $f : P \to P$ będzie funkcją ciągłą. Wtedy element $a = \bigvee \{ f^n(\bot) : n \in N \}$ jest najmniejszym punktem stałym funkcji f.

15. Dobry porządek

Definicja 91. Porządek częściowy $\langle P, \leq \rangle$ jest regularny (dobrze ufundowany), jeśli nie istnieje nieskończony ciąg $a_0, a_1, a_2, \ldots$ taki, że $(\forall i \in \mathbb{N})(a_{i+1} < a_i)$. Mówimy, że porządek jest *dobry*, jeśli jest liniowy i regularny.

Twierdzenie 92. Porządek częściowy $\langle P, \leq \rangle$ jest *regularny*, jeśli w każdym niepustym zbiorze $X \subseteq P$ istnieje element minimalny.

16. Indukcja

Twierdzenie 93. Niech $\langle P, \leq \rangle$ będzie regularnym porządkiem częściowym. Jesli $X \subseteq P$ spełnia warunek:

$$(\forall x)((\forall y \leq x)(y \in X) \Rightarrow x \in X)$$

to $X = P$.

Twierdzenie 94 (O definiowaniu przez indukcję). Niech A, B będą dowolnymi zbiorami. Niech $g : A \to B$ oraz $h : B \times A \times \mathbb{N} \to B$ będą dowolnymi funkcjami. Wtedy istnieje dokładnie jedna funkcja $f : A \times \mathbb{N} \to B$ spełniająca warunki:

1. $(\forall a \in A)\Big(f(a, 0) = g(a)\Big)$
2. $(\forall a \in A)(\forall n \in \mathbb{N})\Big(f(a, n+1) = h(f(a, n), a, n)\Big)$.

Twierdzenie 95 (Drugie twierdzenie o definiowaniu przez indukcje). Niech A, B będą dowolnymi zbiorami. Niech $g : A \to B$ oraz $h : B^* \times A \times \mathbb{N} \to B$ będą dowolnymi funkcjami. Wtedy istnieje dokładnie jedna funkcja $f : A \times \mathbb{N} \to B$ spełniająca warunki:

1. $(\forall a \in A)\Big(f(a, 0) = g(a)\Big)$
2. $(\forall a \in A)(\forall n \in \mathbb{N})\Big(f(a, (n+1)) = h((f(a, 0), \ldots, f(a, n)), a, n)\Big)$.

Definicja 96. Niech A, B będą dowolnymi zbiorami. Funkcją częściową z A w B nazywamy każdą relację $f \subseteq A \times B$ spełniającą warunek:

$$(\forall a \in A)(\forall b_1, b_2 \in B)((((\langle a, b_1 \rangle \in f) \wedge (\langle a, b_2 \rangle \in f)) \Rightarrow b_1 = b_2).$$

Zbiór funkcji częściowych z A w B oznaczamy $B^{\subseteq A}$. Podobnie jak w przypadku funkcji (całkowitych) piszemy $f(a) = b$ jeśli $\langle a, b \rangle \in f$.

Twierdzenie 97 (O definiowaniu funkcji przez indukcję noetherowską). Niech $\langle A, \leq \rangle$ będzie zbiorem regularnym i niech B, C będą dowolnymi zbiorami. Dla dowolnej funkcji funkcji $h : B^{\subseteq A \times C} \times A \times C \to B$ istnieje dokładnie jedna funcja spełniająca warunek:

$$f(x, c) = h(f \cap (\{y \in A : y < x\} \times C \times B), x, c).$$

(Napis $x < y$ oznacza $x \leq y \wedge x \neq y$).

17. Elementy algebry uniwersalnej

Definicja 98. *Sygnaturą* nazywamy rodzinę $\Sigma = \{\Sigma_n : n \in N\}$ zbiorów parami rozłącznych. Elementy zbioru Σ_n nazywamy *symbolami relacji n-argumentowych*. Elementy Σ_0 nazywamy *symbolami stałych* (lub po prostu *stałymi*).

Definicja 99. *Algebrą nad* Σ (lub Σ*-algebrą*) nazywamy niepusty zbiór A wraz z interpretacją $\cdot^{\mathcal{A}}$, czyli przyporządkowaniem, które każdemu symbolowi $f \in \Sigma_n$ przyporządkowuje funkcję $f^{\mathcal{A}} : A^n \to A$. Tak opisaną algebrę oznaczamy przez $\mathcal{A}$ lub $\langle A, f^{\mathcal{A}} : f \in \Sigma \rangle$. Zbiór A nazywamy *nośnikiem* algebry $\mathcal{A}$.

17.1. Algebra termów

Definicja 100. Niech Σ będzie sygnaturą i niech $V = \{v_i : i \in N\}$ będzie zbiorem zmiennych (zakładamy, że $\Sigma \cap V = \emptyset$). Przez $T(\Sigma, V)$ będziemy oznaczać zbiór termów nad Σ, czyli najmniejszy zbiór zawierający zmienne, symbole stałych (to znaczy $V \subseteq T(\Sigma, V)$, $\Sigma_0 \subseteq T(\Sigma, V)$), i zamknięty względem Σ (to znaczy jeśli $f \in \Sigma_n$, $t_1, \ldots, t_n \in T(\Sigma, V)$, to $f(t_1, \ldots, t_n) \in T(\Sigma, V)$).

Przez $T(\Sigma)$ będziemy oznaczać zbiór *termów stałych* nad Σ, czyli najmniejszy zbiór zawierający symbole stałych (to znaczy $\Sigma_0 \subseteq T(\Sigma)$) i zamknięty względem Σ (to znaczy jeśli $f \in \Sigma_n$, $t_1, \ldots, t_n \in T(\Sigma)$, to $f(t_1, \ldots, t_n) \in T(\Sigma)$.

Zbiór termów stałych można też zdefiniować jako zbiór tych termów, w których nie występują zmienne.

W zbiorze termów $T(\Sigma, V)$ łatwo określić interpretację $\cdot^{\mathcal{F}}$ sygnatury Σ, czyli algebrę

$$\langle T(\Sigma, V),\ f^{\mathcal{F}} : f \in \Sigma \rangle$$

kładąc $f^{\mathcal{F}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$ dla $f \in \Sigma_n$, $t_1, \ldots, t_n \in T(\Sigma, V)$. Podobnie jeśli $\Sigma_0 \neq \emptyset$, można określić interpretację $\mathcal{H}$ sygnatury Σ w $T(\Sigma)$.

Algebry $\mathcal{F}$, $\mathcal{H}$ są przykładami algebr wolnych nad Σ. Algebra $\mathcal{H}$ jest nazywana *uniwersum Herbranda* nad Σ.

Definicja 101. Niech $t, t' \in T(\Sigma, V)$. Mówimy, że t' jest *podtermem* t, jeśli $t = t'$, lub $t = f(t_1, \ldots, t_n)$ i t' jest podtermem t_i dla pewnego $i \leq n$. Jeśli t' jest podtermem t to piszemy $t' \sqsubseteq t$.

17.2. Inna definicja zbioru termów. Drzewa

Definicja 102. Niech A będzie dowolnym zbiorem. Zbiór $T \subseteq A^*$ jest *drzewem* jeśli jest zaknięty na przedrostki (to znaczy, jeśli $u \prec w$ (u jest przedrostkiem w) oraz $w \in T$, to $u \in T$.

Elementy drzewa nazywamy *wierzchołkami*. Każde drzewo zawiera słowo puste ϵ. Słowo puste nazywamy *korzeniem drzewa*. Jeśli $w \in T$ oraz $wa \in T$ dla $w \in A^*$, $a \in A$, to mówimy, że wa jest *następnikiem* (*synem*) w w T, w nazywamy *poprzednikiem* (*ojcem*) wa. Wierzchołek T, który nie ma następników nazywamy *liściem*. *Ścieżką* w drzewie T nazywamy dowolny podzbiór T liniowo uporządkowany relacją $\prec$. Ścieżka w drzewie T jest *gałęzią*, jeśli jest maksymalnym podzbiorem T liniowo uporządkowanym relacją $\prec$. Każda gałąź zawiera korzeń drzewa. Jeśli ścieżka jest skończona, to zawiera dokładnie jeden liść. *Stopniem* wierzchołka w w drzewie T nazywamy ilość następników w. *Długością ścieżki* π nazywamy moc zbioru π. *Wysokością drzewa* T nazywamy kres górny długości ścieżek w T. Jeśli drzewo T jest skończone, to jego wysokość jest równa długości najdłuższej gałęzi w T.

Definicja 103. Niech T będzie drzewem i niech $w \in T$. Kładziemy

$$T_w = \{u \in A^* \mid wu \in T\}$$

Łatwo sprawdzić, że T_w jest drzewem. T_w nazywamy *podrzewem drzewa T ukorzenionym w w*. U jest podrzewem T, jeśli $U = T_w$ dla pewnego $w \in T$.

Definicja 104. *Drzewem adresów* nazywamy drzewo T nad $\mathbb{N}$ o tej własności, że dla każdego $w \in T$ zbiór następników w jest odcinkiem początkowym $\mathbb{N}$, to znaczy jeśli $wn \in T$ dla pewnego $n \in N$, oraz $m < n$, to $wm \in T$.

Definicja 105. Niech Σ będzie sygnaturą. *Termem* nad Σ nazywamy dowolną parę $t = \langle T, e \rangle$, gdzie T jest drzewem adresów, $e : T \to \Sigma$ zaś funkcją, taką, że jeśli $w \in T$, $e(w) \in \Sigma_n$, to w ma stopień n.

Definicja 106. Niech $t = \langle T, e \rangle$ będzie termem i niech $w \in T$. *Podtermem* t w w nazywamy term $t_w = \langle T_w, e_w \rangle$, gdzie $e_w(u) = e(wu)$. t' jest podtermem t, jeśli $t' = t_w$ dla pewnego $w \in T$.

Definicja 107. Niech $\mathcal{A} = \langle A, f^{\mathcal{A}} : f \in \Sigma \rangle$ będzie algebrą nad sygnaturą Σ. Niech $T(\Sigma, X)$ będzie zbiorem termów sygnatury Σ ze zmiennymi ze zbioru X. *Wartościowaniem* X w algebrze $\mathcal{A}$ nazywamy funkcję $\sigma : X \to A$. *Wartością termu* $t \in T(\Sigma, X)$ przy wartościowaniu σ nazywamy element $\mathcal{A}$ otrzymany z termu t po zastąpieniu każdej zmiennej x przez $\sigma(x)$, zastąpieniu symboli funkcji z Σ przez ich interpretacje w $\mathcal{A}$ oraz obliczenie tak otrzymanego wyrażenia w $\mathcal{A}$.

Bardziej formalnie, wartościowanie σ rozszerza się do funkcji $\sigma^* : T(\Sigma, X) \to A$ zdefiniowanej w następujący sposób:

$$\begin{aligned} \sigma^*(x) &= \sigma(x), \text{ dla } x \in X \text{ oraz} \\ \sigma^*(f(t_1, ..., t_n)) &= f^{\mathcal{A}}(\sigma(f_1), ..., \sigma(f_n)), \text{ dla } f \in \Sigma_n, t_1, ..., t_n \in T(\Sigma, X) \end{aligned}$$

Jeśli nie będzie prowadzić to do nieporozumień, będziemy pisali σ zamiast σ^*. Funkcję σ nazywamy *wartościowaniem zmiennych*, a funkcję σ^* *wartościowaniem termów*. Element $\sigma^*(t)$ algebry $\mathcal{A}$ nazywamy wartością termu t w algebrze $\mathcal{A}$. Zauważmy, że jeśli term t nie zawiera zmiennych, to $\sigma^*(t)$ nie zależy od σ. Ogólniej, jeśli zmienna x nie występuje w t to $\sigma^*(t)$ nie zależy od $\sigma(x)$.

Przykład 108. Zdefiniowane powyżej wartościowanie termów jest przykładem *homomorfizmu* algebr, jest to przykład homomorfizmu z algebry termów $\mathcal{F}$ w algebrę $\mathcal{A}$.

Definicja 109. Niech $\mathcal{A}$ i $\mathcal{B}$ będą algebrami nad sygnaturą Σ. Funkcja $h : A \to B$ jest homomorfizmem algebry $\mathcal{A}$ w algebrę $\mathcal{B}$, jeśli dla każdego $f \in \Sigma_n$ i dowolnych $a_1, ..., a_n \in A$ zachodzi równość

$$h(f^{\mathcal{A}}(a_1, ..., a_n)) = f^{\mathcal{B}}(h(a_1), ..., h(a_n))$$

Przykład 110. Innym przykładem homomorfizmu jest *podstawienie*.

Definicja 111. Niech Σ będzie sygnaturą. Podstawienie σ w algebrze termów $\mathcal{F} = \langle T(\Sigma, X), f : f \in \Sigma \rangle$ jest funkcją przyporządkowująca zmiennym ze zbioru $X \subseteq V$ elementy $T(\Sigma, V)$. Jest to więc wartościowanie w algebrze termów. Jak poprzednio wartościowanie σ rozszerzamy do $\sigma^* : T(\Sigma, V) \to T(\Sigma, V)$ kładąc $\sigma(y) = y$ dla $y \in V \setminus X$. Oczywiście, tak jak poprzednio $\sigma^*(x) = \sigma(x)$ dla $x \in X$ oraz $\sigma^*(f(t_1, ..., t_n) = f(\sigma(t_1), ..., \sigma(t_n))$. Term $\sigma^*(t)$ nazywamy wartością termu t przy podstawieniu σ. Podobnie jak poprzednio, jeśli nie prowadzi to do nieporozumień, piszemy σ zamiast σ^*. Wartość termu t przy podstawieniu σ jest termem uzyskanym z termu t przez zastąpienie każdego wystąpienia zmiennej x w termie t przez term $\sigma(x)$.

18. Problem unifikacji

Definicja 112. Niech Σ będzie sygnaturą. *Problemem unifikacji* nazywamy następujące zadanie: „mając dany zbiór $\{(t_1, u_1), ..., (t_n, u_n)\}$, znaleźć takie podstawienie σ, żeby dla każdego $i \leq n$ zachodziło $\sigma(t_i) = \sigma(u_i)$." To znaczy, należy znaleźć takie przyporządkowanie termów zmiennym występującym w termach $t_1, u_1, ..., t_n, u_n$, żeby po podstawieniu tych termów za odpowiednie zmienne uzyskać termy równe. Podstawienie σ nazywamy *unifikatorem* zbioru $\{(t_1, u_1), ..., (t_n, u_n)\}$. Często ten zbiór (nazywany czasem *instancją problemu unifikacji*) zapisujemy jako $\{t_1 = u_1, ..., t_n = u_n\}$.

Definicja 113. Jeśli σ i τ są unifikatorami zbioru $\{(t_1, u_1), ..., (t_n, u_n)\}$, to mówimy, że σ jest *ogólniejsze* od τ, (co oznaczamy $\tau \leq \sigma$) jeśli istnieje podstawienie ϱ, takie, że $\tau = \varrho(\sigma)$, gdzie $(\varrho(\sigma))(x) = \varrho(\sigma(x))$. Podstawienie σ nazywamy *najogólniejszym unifikatorem* zbioru

$$PU = \{(t_1, u_1), ..., (t_n, u_n)\}$$

jeśli σ jest unifikatorem PU oraz σ jest ogólniejsze od każdego innego unifikatora PU.

Twierdzenie 114. Istnieje algorytm, który dla zadanej instancji

$$\{(t_1, u_1), ..., (t_n, u_n)\}$$

problemu unifikacji znajduje jego najogóniejszy unifikator lub odpowiada „nie ma unifikatora".

19. Systemy dowodzenia

19.1. System Hilberta dla rachunku zdań ze spójnikami $\to$ i $\bot$

Definicja 115. Litera Δ oznacza dowolny zbiór formuł zdaniowych, zaś litery α, β, γ oznaczają dowolne formuły. Dla dowolnej formuły α zapis $\neg\alpha$ jest skrótem zapisu $\alpha \to \bot$.

Wyrażenie postaci $\Delta \vdash \alpha$ nazywamy *sekwentem*. Wyrażenie $\vdash \alpha$ oznacza $\emptyset \vdash \alpha$. Wyrażenie Δ, α oznacza $\Delta \cup \{\alpha\}$.

Aksjomaty systemu Hilberta

$$\begin{aligned}
\Delta, \alpha &\vdash \alpha \\
\Delta &\vdash \alpha \to (\beta \to \alpha) \\
\Delta &\vdash (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to \alpha \to \gamma)) \\
\Delta &\vdash \neg\neg\alpha \to \alpha
\end{aligned}$$

Reguła dowodzenia (reguła odrywania)

$$\frac{\Delta \vdash \alpha \quad \Delta \vdash \alpha \to \beta}{\Delta \vdash \beta}$$

Sekwenty nad poziomą kreską nazywamy *przesłankami*, a sekwent pod kreską nazywamy *konkluzją*. Dowodem (sekwentu $\Delta \vdash \alpha$) nazywamy skończone drzewo etykietowane sekwentami, którego korzeń ma etykietę $\Delta \vdash \alpha$, liście są etykietowane aksjomatami oraz dla każdego wierzchołka jego etykieta jest konkluzją reguły wnioskowania, której przesłankami są etykiety następników tego wierzchołka. Jeśli istnieje dowód, którego korzeń jest etykietowany sekwentem $\Delta \vdash \alpha$, to mówimy, że sekwent $\Delta \vdash \alpha$ jest *wyprowadzalny* w systemie Hilbertowskim. Mówimy, że $\Delta \vdash \alpha$, jeśli sekwent $\Delta \vdash \alpha$ jest wyprowadzalny w systemie Hilbertowskim.

Twierdzenie 116 (O dedukcji). Dla dowolnego zbioru formuł Δ oraz dowolnych formuł α i β, jeśli $\Delta, \alpha \vdash \beta$, to $\Delta \vdash \alpha \to \beta$.

Twierdzenie 117 (O adekwatności). Jeśli $\Delta \vdash \alpha$, to dla każdego wartościowania zmiennych zdaniowych, jeśli spełnia ono wszystkie formuły z Δ, to spełnia także formułę α. W szczególności, jeśli $\vdash \alpha$, to α jest tautologią.

Twierdzenie 118. Dla dowolnych formuł α i β zbudowanych ze zmiennych zdaniowych przy użyciu spójników $\bot$ i $\to$, następujące sekwenty są wyprowadzalne w systemie Hilbertowskim:

$$\vdash \alpha \to (\neg\beta \to \neg(\alpha \to \beta))$$
$$\vdash \bot \to \alpha$$
$$\vdash (\alpha \to \beta) \to ((\neg\alpha \to \beta) \to \beta)$$

Twierdzenie 119 (Kalmar). Niech α będzie formułą zbudowaną przy ze zmiennych $q_1, q_2, \ldots, q_n$ przy użyciu spójników $\bot$ i $\to$ i niech $\upsilon : P \to \{0, 1\}$ będzie dowolnym wartościowaniem. Dla $i = 1, \ldots, n$ definiujemy formuły:

$$q_i' = \begin{cases} q_i & \text{jeśli } \upsilon(q_i) = 1, \\ \neg q_i & \text{jeśli } \upsilon(q_i) = 0. \end{cases}$$

Niech α' będzie formuła identyczną z α, jeśli wartościowanie υ spełnia formułę α. Jeśli natomiast wartościowanie υ nie spełnia formuły α, to jako α' bierzemy $\neg\alpha$. Wówczas $\{q_1, \ldots, q_n\} \vdash \alpha$.

Twierdzenie 120. Dla dowolnego zbioru formuł Δ i dowolnych formuł α i β, jeśli $\Delta, \alpha \vdash \beta$ i $\Delta, \neg\alpha \vdash \beta$, to $\Delta \vdash \beta$.

Twierdzenie 121 (O pełności). Jeśli α jest tautologią zbudowaną ze zmiennych zdaniowych przy użyciu spójników $\to$ i $\bot$, to $\vdash \alpha$.

19.2. System Hilberta dla rachunku zdań ze spójnikami $\vee$ i $\wedge$

System Hilberta rozszerzamy o następujące aksjomaty:

$$\begin{aligned}
\Delta &\vdash (\alpha \wedge \beta) \to \neg(\alpha \to \neg\beta) \\
\Delta &\vdash \neg(\alpha \to \neg\beta) \to (\alpha \wedge \beta) \\
\Delta &\vdash (\alpha \vee \beta) \to (\neg\alpha \to \beta) \\
\Delta &\vdash (\neg\alpha \to \beta) \to (\alpha \vee \beta)
\end{aligned}$$

i pozwalamy, by formuły z Δ oraz α i β zawierały spójniki $\vee$ i $\wedge$. Aby odróżnić ten system od poprzedniego, jego sekwenty będziemy oznaczać $\Delta \vdash_{H^+} \alpha$.

Twierdzenie 122. Dla dowolnej formuły zdaniowej α istnieje formuła $\tilde{\alpha}$ zbudowana ze zmiennych zdaniowych jedynie przy użyciu spójnkiów $\bot$ i $\to$, taka, że $\vdash_{H^+} \alpha \to \tilde{\alpha}$ oraz $\vdash_{H^+} \tilde{\alpha} \to \alpha$.

Dla rozszerzonego systemu również są prawdziwe twierdzenia o adekwatności i pełności.

20. Język pierwszego rzędu

20.1. Składnia

Definicja 123. *Sygnaturą* języka pierwszego rzędu nazywamy zbiór $\Sigma = \Sigma^F \cup \Sigma^R$, gdzie Σ^F jest zbiorem *symboli funkcyjnych* a Σ^R zbiorem *symboli relacyjnych*, przy czym $\Sigma^F = \bigcup_{i\in\mathbb{N}} \Sigma^F_i$ i $\Sigma^R = \bigcup_{i\in\mathbb{N}} \Sigma^R_i$, gdzie Σ^F_i i Σ^R_i są odpowiednio zbiorami symboli funkcyjnych i relacji i-argumentowych ($i \geq 0$).

Definicja 124. Zbiór termów $\mathcal{T}(\Sigma, V) = \mathcal{T}(\Sigma^F, V)$ definiujemy jako najmniejszy zbiór zawierający zmienne ze zbioru V i zamknięty ze względu na tworzenie termów złożonych zawierających symbole funkcji z Σ^F, tj. jeśli $t_1, \ldots, t_n$ są termami, zaś $f \in \Sigma^F_n$, to $f(t_1, \ldots, t_n)$ też jest termem.

Definicja 125. Zbiór formuł atomowych jest zbiorem napisów postaci $R(t_1, \ldots, t_n)$, gdzie $R \in \Sigma^R_n$, zaś $t_1, \ldots, t_n$ są termami.

Definicja 126. Zbiór *formuł rachunku predykatów pierwszego rzędu* jest najmniejszym zbiorem napisów zawierającym formuły atomowe, zamkniętym ze względu na spójniki zdaniowe $\vee$, $\wedge$, $\neg$, $\bot$, $\Rightarrow$, $\Leftrightarrow$, oraz kwantyfikatory $\forall$ i $\exists$, tzn. jeśli α i β są formułami zaś x jest zmienną (z V), to formułami są także $\bot$, $\neg\alpha$, $\alpha \vee \beta$, $\alpha \wedge \beta$, $\alpha \Rightarrow \beta$, $\alpha \Leftrightarrow \beta$, $\forall x.\alpha$, $\exists x.\alpha$.

Definicja 127. Zbiór zmiennych *wolnych* $\mathrm{FV}(\alpha)$ formuły α definiujemy indukcyjnie:

$$\mathrm{FV}(\bot) = \emptyset$$

$$\mathrm{FV}(R(t_1, \ldots, t_n)) = \mathrm{FV}(t_1) \cup \ldots \cup \mathrm{FV}(t_n)$$

$$\mathrm{FV}(\alpha \vee \beta) = \mathrm{FV}(\alpha \wedge \beta) = \mathrm{FV}(\alpha \Rightarrow \beta) = \mathrm{FV}(\alpha \Leftrightarrow \beta) = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta)$$

$$\mathrm{FV}(\forall x.\alpha) = \mathrm{FV}(\exists x.\alpha) = \mathrm{FV}(\alpha) \setminus \{x\}$$

gdzie dla termów $\mathrm{FV}(t_i)$ oznacza zbiór wszystkich zmiennych występujących w t_i.

Definicja 128. Wszystkie wolne wystąpienia zmiennej x w formule α stają się *związanie* w formule $\forall x.\alpha$ i $\exists x.\alpha$. Mówimy że kwantyfikator *wiąże* te wystąpienia.

Definicja 129. Formuła bez zmiennych wolnych nazywa się *zdaniem*.

20.2. Semantyka

Definicja 130. *Struktura* $\mathfrak{A}$ *sygnatury* Σ to niepusty zbiór A zwany jej *uniwersum* i *interpretacja*, czyli funkcja $\cdot^{\mathfrak{A}}$, która każdemu symbolowi funkcji $f \in \Sigma_n^F$ przyporządkowuje funkcję $f^{\mathfrak{A}} : A^n \to A$ i każdemu symbolowi relacji $R \in \Sigma_n^R$ przyporządkowuje relację $R^{\mathfrak{A}} \subseteq A^n$.

Definicja 131. *Wartościowaniem* w strukturze $\mathfrak{A}$ nazywamy dowolną funkcję $\upsilon : V \to A$. Ponadto niech

$$(\upsilon_x^a)(y) \quad = \quad \begin{cases} \upsilon(y), & \text{gdy } x \neq y, \\ a, & \text{gdy } x = y, \end{cases}$$

dla dowolnego wartościowania $\upsilon : V \to A$, zmiennej $x \in V$ i elementu $a \in A$.

Definicja 132. Dla dowolnego termu z $\mathcal{T}(\Sigma^F, V)$ definiujemy jego *interpretację* $t^{\mathfrak{A}}[\upsilon]$ przy zadanym wartościowaniu zmiennych $\upsilon : V \to A$ indukcyjnie:

$$\begin{aligned} x^{\mathfrak{A}}[\upsilon] &= \upsilon(x) \\ (f(t_1, \ldots, t_n))^{\mathfrak{A}}[\upsilon] &= f^{\mathfrak{A}}(t_1^{\mathfrak{A}}[\upsilon], \ldots, t_n^{\mathfrak{A}}[\upsilon]) \end{aligned}$$

Definicja 133. Poniżej definujemy indukcyjnie relację $\models$. Gdy ona zachodzi, co oznaczamy $\mathfrak{A} \models \alpha[\upsilon]$, to mówimy że *struktura* $\mathfrak{A}$ *spełnia formułę* α *przy wartościowaniu* $\upsilon : V \to A$.

1. Nigdy nie zachodzi $\mathfrak{A} \models \bot[\upsilon]$.
2. $\mathfrak{A} \models R(t_1, \ldots, t_n)[\upsilon]$ wtw $(t_1^{\mathfrak{A}}[\upsilon], \ldots, t_n^{\mathfrak{A}}[\upsilon]) \in R^{\mathfrak{A}}$.
3. $\mathfrak{A} \models (t_1 = t_2)[\upsilon]$ wtw $t_1^{\mathfrak{A}}[\upsilon] = t_2^{\mathfrak{A}}[\upsilon]$.
4. $\mathfrak{A} \models (\alpha \wedge \beta)[\upsilon]$ wtw gdy zachodzą jednocześnie $\mathfrak{A} \models \alpha[\upsilon]$ i $\mathfrak{A} \models \beta[\upsilon]$.
5. $\mathfrak{A} \models (\alpha \vee \beta)[\upsilon]$ wtw gdy $\mathfrak{A} \models \alpha[\upsilon]$ lub $\mathfrak{A} \models \beta[\upsilon]$.
6. $\mathfrak{A} \models (\alpha \Rightarrow \beta)[\upsilon]$ wtw gdy nie zachodzi $\mathfrak{A} \models \alpha[\upsilon]$ lub zachodzi $\mathfrak{A} \models \beta[\upsilon]$.
7. $\mathfrak{A} \models (\alpha \Leftrightarrow \beta)[\upsilon]$ wtw jednocześnie nie zachodzą $\mathfrak{A} \models \alpha[\upsilon]$ i $\mathfrak{A} \models \beta[\upsilon]$, lub jednocześnie zachodzą $\mathfrak{A} \models \alpha[\upsilon]$ i $\mathfrak{A} \models \beta[\upsilon]$.
8. $\mathfrak{A} \models (\forall x.\alpha)[\upsilon]$ wtw dla każdego elementu $a \in A$ zachodzi $\mathfrak{A} \models \alpha[\upsilon_x^a]$.
9. $\mathfrak{A} \models (\exists x.\alpha)[\upsilon]$ wtw istnieje element $a \in A$ dla którego zachodzi $\mathfrak{A} \models \alpha[\upsilon_x^a]$.

Definicja 134. Formuła α jest *spełnialna w* $\mathfrak{A}$, jeśli istnieje wartościowanie $\upsilon : V \to A$ dla którego zachodzi $\mathfrak{A} \models \alpha[\upsilon]$. Formuła α jest *spełnialna*, jeśli istnieje struktura $\mathfrak{A}$, w której α jest spełnialna. Formuła α jest *prawdziwa w* $\mathfrak{A}$ (struktura $\mathfrak{A}$ jest *modelem dla* α), jeśli dla każdego wartościowania $\upsilon : V \to A$ zachodzi $\mathfrak{A} \models \alpha[\upsilon]$. Formuła α jest *prawdziwa* (jest *tautologią*), jeśli dla każdej struktury $\mathfrak{A}$, formuła α jest prawdziwa w $\mathfrak{A}$.

20.3. Podstawienia

Definicja 135. Dla dowolnej formuły α napis $\alpha[x/t]$ oznacza wynik podstawienia termu t w każde wolne wystąpienie x w α. Podstawienie to jest *dopuszczalne*, jeśli w wyniku tego podstawienia żadna zmienna z t nie staje się związana, tj. każde wystąpienie x w α nie znajduje się w zasięgu żadnego kwantyfikatora wiążącego zmienną występującą w t.

Twierdzenie 136 (O podstawianiu.). Dla dowolnech termów s i t i zmiennej x zachodzi

$$(t[x/s])^{\mathfrak{A}}[\upsilon] \quad = \quad t^{\mathfrak{A}}[\upsilon_x^{s^{\mathfrak{A}}[\upsilon]}]$$

Dla dowolnej formuły α, jeśli podstawienie $[x/s]$ jest dopuszczalne w α, to $\mathfrak{A} \models (\alpha[x/s])[\upsilon]$ wtw $\mathfrak{A} \models \alpha[\upsilon_x^{s^{\mathfrak{A}}[\upsilon]}]$.

Fakt 137. Dla dowolnej formuły α, zmiennej x i termu s, jeśli podstawienie $[x/s]$ jest dopuszczalne w α, to formuła $(\forall x.\alpha) \Rightarrow (\alpha[x/s])$ jest tautologią.

20.4. Hilbertowski system dowodzenia

20.4.1. Aksjomaty

$$
\begin{aligned}
\Delta, \alpha &\vdash \alpha \\
\Delta &\vdash \alpha \Rightarrow (\beta \Rightarrow \alpha) \\
\Delta &\vdash (\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)) \\
\Delta &\vdash \neg\neg\alpha \Rightarrow \alpha \\
\Delta &\vdash (\alpha \wedge \beta) \Rightarrow \neg(\alpha \Rightarrow \neg\beta) \\
\Delta &\vdash \neg(\alpha \Rightarrow \neg\beta) \Rightarrow (\alpha \wedge \beta) \\
\Delta &\vdash (\alpha \vee \beta) \Rightarrow (\neg\alpha \Rightarrow \beta) \\
\Delta &\vdash (\neg\alpha \Rightarrow \beta) \Rightarrow (\alpha \vee \beta) \\
\Delta &\vdash (\alpha \Leftrightarrow \beta) \Rightarrow ((\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)) \\
\Delta &\vdash ((\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)) \Rightarrow (\alpha \Leftrightarrow \beta) \\
\Delta &\vdash (\forall x.(\alpha \Rightarrow \beta)) \Rightarrow ((\forall x.\alpha) \Rightarrow (\forall x.\beta)) \\
\Delta &\vdash \alpha \Rightarrow (\forall x.\alpha), \qquad \text{jeśli } x \notin \mathrm{FV}(\alpha) \\
\Delta &\vdash (\forall x.\alpha) \Rightarrow \alpha[x/t], \qquad \text{jeśli } [x/t] \text{ jest dopuszczalne w } \alpha \\
\Delta &\vdash x = x \\
\Delta &\vdash x_1 = y_1 \Rightarrow (\ldots \Rightarrow (x_n = y_n \Rightarrow (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)))), \\
&\qquad \text{gdzie } f \in \Sigma_n^F \\
\Delta &\vdash x_1 = y_1 \Rightarrow (\ldots \Rightarrow (x_n = y_n \Rightarrow (R(x_1, \ldots, x_n) \Rightarrow R(y_1, \ldots, y_n)))), \\
&\qquad \text{gdzie } R \in \Sigma_n^R
\end{aligned}
$$

Reguła dowodzenia

$$\frac{\Delta \vdash \alpha \Rightarrow \beta \quad \Delta \vdash \alpha}{\Delta \vdash \beta}$$

Zbiór formuł Δ jest *sprzeczny*, jeśli $\Delta \vdash \bot$. Zbiór który nie jest sprzeczny, jest *niesprzeczny*.

Twierdzenie 138 (O dedukcji). Dla dowolnego zbioru formuł Δ oraz dowolnych formuł α i β, jeśli $\Delta, \alpha \vdash \beta$, to $\Delta \vdash \alpha \to \beta$.

Definicja 139. Napis $\Delta \models \alpha$ oznacza, że dla każdej struktury $\mathfrak{A}$ i każdego wartościowania v, jeśli dla każdej formuły $\beta \in \Delta$ zachodzi $\mathfrak{A} \models \beta[v]$, to również $\mathfrak{A} \models \alpha$.

Twierdzenie 140 (O adekwatności). Jeśli $\Delta \vdash \alpha$, to $\Delta \models \alpha$. W szczególności, jeśli $\vdash \alpha$, to α jest tautologią.

Twierdzenie 141 (O istnieniu modelu). Dla dowolnej sygnatury Σ, każdy niesprzeczny zbiór zdań nad Σ ma model.

Twierdzenie 142 (Silne twierdzenie o pełności). Dla dowolnego zbioru formuł Δ oraz dowolnej formuły α, jeśli $\Delta \models \alpha$, to $\Delta \vdash \alpha$. W szczególności, jeśli α jest tautologią, to $\vdash \alpha$.

Twierdzenie 143 (O α-konwersji). Jeśli $\Delta \vdash \forall x.\beta$ oraz podstawienie $[x/y]$ jest dopuszczalne w β, oraz $y \notin \mathrm{FV}(\forall x.\beta)$, to $\Delta \vdash \forall y.(\beta[x/y])$.

Twierdzenie 144 (O generalizacji). Jeśli $\Delta \vdash \alpha$, to dla dowolnej zmiennej x, jeśli $x \notin \mathrm{FV}(\Delta)$, to $\Delta \vdash \forall x.\alpha$.