Podstawy matematyki

Wykład 1 - Spójniki zdaniowe, rachunek zdań, kwantyfikatory

Oskar Kędzierski

1 marca 2020

Literatura

i) W. Guzicki, P. Zakrzewski *Wykłady ze wstępu do matematyki*, PWN, 2012.

ii) W. Marek, J. Onyszkiewicz, *Elementy logiki i teorii mnogości w zadaniach*, PWN, 1996.

iii) H. Rasiowa, *Wstęp do matematyki współczesnej*, PWN, 1975.

iv) K. A. Ross, C. R. B. Wright *Matematyka dyskretna*, PWN, 1996.

v) *Logika i teoria mnogości*, Ważniak, `http://goo.gl/AUECP9`.

vi) *Logika dla informatyków*, Ważniak, `https://goo.gl/SrLvcz`.

vii) *Teoria kategorii dla informatyków*, Ważniak, `https://bit.ly/329gETs`.

viii) C. C. Pinter, *A Book of Abstract Algebra*, Dover, 2010.

Oznaczenia

i) $\emptyset$ =zbiór pusty,

ii) $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ zbiór liczb naturalnych,

iii) $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ zbiór liczb całkowitych,

iv) $\mathbb{Q} = \{\frac{m}{n} \colon m, n \in \mathbb{Z},\ n \neq 0\}$ zbiór liczb wymiernych,

v) $\mathbb{R}$ =zbiór liczb rzeczywistych,

vi) $\mathbb{C}$ =zbiór liczb zespolonych.

Klasyczny rachunek zdań

Definicja

Zdaniem nazywamy poprawnie zbudowane wyrażenie, któremu możemy przypisać jednoznacznie wartość logiczną prawda lub fałsz.

Zdania będziemy oznaczać małymi literami (zmiennymi zdaniowymi) p, q, r. Zbiór zmiennych zdaniowych będziemy oznaczać przez ZZ.
Wartości logiczne prawdę i fałsz będziemy oznaczali odpowiednio symbolami 1 i 0. Formułą zdaniową φ nazywamy formułę zbudowaną ze zmiennych zdaniowych połączonych spójnikami logicznymi.

Funkcję $\rho\colon ZZ \to \{0, 1\}$ przypisującą zmiennym zdaniowym dowolne wartości logiczne nazywamy **wartościowaniem.** Każde wartościowanie ρ przypisuje jednoznacznie wartość logiczną, oznaczaną $[\![\varphi]\!]_\rho$, dowolnej formule zdaniowej φ.

Zdania cd.

Przykłady

Zdaniami są:

i) Bolesław Chrobry był królem Polski.

ii) Każda liczba naturalna dodana do siebie jest podzielna przez dwa.

iii) Każda osoba w tej sali ma co najmniej 10 lat.

Zdaniami **nie** są:

i) Chodź tutaj.

ii) Dobrze jest długo spać.

iii) Za dwa lata wyjadę na wakacje.

Funkcje zdaniowe

Definicja

Funkcją zdaniową (lub **predykatem** lub **relacją** n-**argumentową**) nazywamy wyrażenie zawierające zmienne, które staje się zdaniem, gdy za zmienne podstawimy przedmioty z pewnych zbiorów, zwanych **zakresami zmiennych**.

Funkcje zdaniowe o zmiennych $x_1, \ldots, x_n$ i zakresach $X_1, \ldots, X_n$ będziemy oznaczać $P(x_1, \ldots, x_n), Q(x_1, \ldots, x_n)$, gdzie $x_1 \in X_1, \ldots, x_n \in X_n$.

Funkcje zdaniowe cd.

Przykłady

Funkcjami zdaniowymi są

i) $P(x) =$ „x był królem Polski”, gdzie zakresem zmiennej x jest zbiór wszystkich ludzi żyjących na Ziemi,

ii) $P(n) =$ „n jest podzielna przez 2”, gdzie $n \in \mathbb{Z}$,

iii) $P(x, y) =$ „x ma więcej lat niż y”, gdzie zakresem zmiennych x, y są osoby na tej sali.

Funkcje zdaniowe cd.

Definicja

Mówimy, że układ $(a_1, \ldots, a_n)$, gdzie $a_1 \in X_1, \ldots, a_n \in X_n$ **spełnia** funkcję zdaniową $P(x_1, \ldots, x_n)$ jeśli $[\![P(a_1, \ldots, a_n)]\!] = 1$ (tzn. po podstawieniu $a_1, \ldots, a_n$ staje się zdaniem prawdziwym).
Funkcję zdaniową $P(x_1, \ldots, x_n)$ nazywamy **spełnialną**, jeśli istnieje spełniający ją układ $(a_1, \ldots, a_n)$.
Funkcję zdaniową $P(x_1, \ldots, x_n)$ nazywamy **prawdziwą**, jeśli jest spełniana przez każdy układ $(a_1, \ldots, a_n)$, gdzie a_i należą do odpowiednich zakresów.

Uwaga

Prawdziwość funkcji zdaniowej na ogół zależy do jej zakresu. Na przykład, funkcja zdaniowa

$$P(x) = \text{„jeśli } x^2 \geq 4, \text{ to } x \geq 2\text{”}$$

jest prawdziwa dla $x \in \mathbb{N}$ i nie jest prawdziwa dla $x \in \mathbb{Z}$.

Spójniki zdaniowe

Definicja

Spójnikiem zdaniotwórczym $n-$argumentowym nazywamy przypisanie każdemu układowi $(x_1, \dots, x_n)$, gdzie x_i jest wartością logiczną prawda lub fałsz, wartości logicznej prawda lub fałsz.

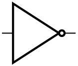
Dzięki spójnikom zdaniowym, ze zdań (lub zmiennych zdaniowych) możemy budować inne zdania. Spójników zdaniowych $n-$argumentowych jest 2^{2^n}. Za spójniki $0-$argumentowe możemy uznać zdanie prawdziwe (ozn. $\top$) oraz zdanie fałszywe (ozn. $\bot$). Wśród spójników zdaniotwórczych $1-$argumentowych wyróżniamy **negację** oznaczaną symbolem $\neg$. Wśród spójników zdaniotwórczych $2-$argumentowych wyróżniamy **koniunkcję** (ozn. $\wedge$), **alternatywę** (ozn. $\vee$), **implikację** (ozn. $\rightarrow$) oraz **równoważność** (ozn. $\leftrightarrow$). Spójniki zdaniotwórcze możemy przedstawiać przy pomocy tabeli.

Negacja

Negacja odpowiada wyrażeniu „nieprawda, że”.

p	$\neg p$
0	1
1	0

Negacja zdania prawdziwego jest fałszywa, i negacja zdania fałszywego jest prawdziwa.
W elektronice negacja odpowiada bramce NOT.

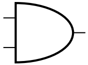


Koniunkcja

Koniunkcja odpowiada spójnikowi „i”.

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Koniunkcja dwóch zdań jest prawdziwa wyłącznie, gdy oba zdania są prawdziwe.
W elektronice koniunkcja odpowiada bramce AND.

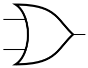


Alternatywa

Alternatywa odpowiada spójnikowi „lub”.

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Alternatywa dwóch zdań jest prawdziwa wyłącznie, gdy co najmniej jedno ze zdań jest prawdziwe.
W elektronice alternatywa odpowiada bramce OR.



Implikacja

Implikacja odpowiada wyrażeniu „jeśli, to".

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Zdanie p nazywamy **poprzednikiem** implikacji a zdanie q **następnikiem** implikacji. Implikacja dwóch zdań jest fałszywa wyłącznie, gdy poprzednik jest prawdziwy a następnik fałszywy (potocznie „z prawdy wynika fałsz").

Uwaga

W logice wartość logiczna implikacji (i innych spójników logicznych) zależy jedynie od wartości logicznej zdań, a nie od faktycznego wynikania. Zatem zdanie „jeśli dziś jest słoneczny dzień, to $2 + 2 = 4$" jest prawdziwe.

Równoważność

Równoważność odpowiada wyrażeniu „wtedy i tylko wtedy, gdy”.

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Równoważność dwóch zdań jest prawdziwa wyłącznie, gdy oba zdania są prawdziwe lub gdy oba zdania są fałszywe.

Siła wiązania spójników logicznych

Największy priorytet mają

i) negacja $\neg$,
ii) koniunkcja $\wedge$ i alternatywa $\vee$,
iii) implikacja $\rightarrow$ i równoważność $\leftrightarrow$.

Przykład

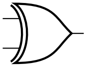
Formułę logiczną $p \wedge \neg q \rightarrow r$ należy interpretować jako $[p \wedge (\neg q)] \rightarrow r$.

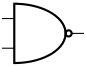
Alternatywa rozłączna i dysjunkcja

Alternatywa rozłączna (oznaczana $\veebar$) odpowiada wyrażeniu „albo, albo”. **Dysjunkcja** (oznaczana $\uparrow$) odpowiada wyrażeniu „nieprawda, że zarazem” (lub „ani, ani”).

p	q	$p \veebar q$	$p \uparrow q$
0	0	0	1
0	1	1	1
1	0	1	1
1	1	0	0

W elektronice alternatywa rozłączna odpowiada bramce XOR, a dysjunkcja bramce NAND.





Tautologie

Definicja

Tautologią nazywamy formułę zdaniową, która jest prawdziwa dla dowolnego wartościowania.

Przykład

Wyrażenie $p \to p$ jest tautologią.

Wyrażenie $[(p \to q) \wedge q] \to p$ nie jest tautologią, ponieważ $[\![[(p \to q) \wedge q] \to p]\!]_\rho = 0$ dla $\rho(p) = 0$ oraz $\rho(q) = 1$.

Prawa identyczności

i) $p \wedge \bot \leftrightarrow \bot$,

ii) $p \wedge \top \leftrightarrow p$,

iii) $p \vee \bot \leftrightarrow p$,

iv) $p \vee \top \leftrightarrow \top$.

Klasyczne tautologie

i) $(p \wedge p) \leftrightarrow p$ (idempotentność koniunkcji),
ii) $(p \vee p) \leftrightarrow p$ (idempotentność alternatywy),
iii) $p \leftrightarrow \neg\neg p$ (prawo podwójnego przeczenia),
iv) $p \vee \neg p$ (prawo wyłączonego środka),
v) $\neg(p \wedge \neg p)$ (prawo sprzeczności),
vi) $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ (prawo transpozycji)
vii) $[\neg(p \rightarrow q)] \leftrightarrow (p \wedge \neg q)$ (zaprzeczenie implikacji),
viii) $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$,
ix) $[(p \rightarrow q) \wedge (q \rightarrow p)] \leftrightarrow (p \leftrightarrow q)$,
x) $[p \wedge (q \wedge r)] \leftrightarrow [(p \wedge q) \wedge r)]$ (łączność koniunkcji),
xi) $[p \vee (q \vee r)] \leftrightarrow [(p \vee q) \vee r)]$ (łączność alternatywy),

Klasyczne tautologie cd.

xii) $[p \wedge (q \vee r)] \leftrightarrow [(p \wedge q) \vee (p \wedge r)]$ (rozdzielność koniunkcji względem alternatywy),

xiii) $[p \vee (q \wedge r)] \leftrightarrow [(p \vee q) \wedge (p \vee r)]$ (rozdzielność alternatywy względem koniunkcji),

xiv) $[(\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q)] \rightarrow p$ (reductio ad absurdum, sprowadzenie do sprzeczności),

xv) $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$ (prawo sylogizmu),

xvi) $[(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r)] \rightarrow r$ (dowód „przez przypadki”).

Metoda zero–jedynkowa

Aby sprawdzić, czy formuła jest tautologią należy podstawić do niej wszystkie możliwe wartościowania zdań. Ten sposób postępowania nazywamy **metodą zero–jedynkową**.

Przykład

p	q	$p \to q$	$(p \to q) \wedge p$	$[(p \to q) \wedge p] \to q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

Formula $[(p \to q) \wedge p] \to q$ jest tautologią, bo w ostatniej kolumnie stoją wyłącznie jedynki.

Metoda zero–jedynkowa cd.

Przykład

p	q	$p \to q$	$(p \to q) \wedge q$	$[(p \to q) \wedge q] \to p$
0	0	1	0	1
0	1	1	1	0
1	0	0	0	1
1	1	1	1	1

Formula $[(p \to q) \wedge q] \to p$ nie jest tautologią, bo w ostatniej kolumnie stoi co najmniej jedno zero.

Zaprzeczenie implikacji – dowód

p	q	$p \rightarrow q$	$\neg(p \rightarrow q)$	$\neg q$	$p \wedge \neg q$	$\neg(p \rightarrow q) \leftrightarrow (p \wedge \neg q)$
0	0	1	0	1	0	1
0	1	1	0	0	0	1
1	0	0	1	1	1	1
1	1	1	0	0	0	1

Rozdzielność koniunkcji względem alternatywy – dowód

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$	$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$
0	0	0	0	0	0	0	0	1
0	0	1	1	0	0	0	0	1
0	1	0	1	0	0	0	0	1
0	1	1	1	0	0	0	0	1
1	0	0	0	0	0	0	0	1
1	0	1	1	1	0	1	1	1
1	1	0	1	1	1	0	1	1
1	1	1	1	1	1	1	1	1

Dowodzenie tautologii

Aby dowieść, ze dana formuła jest (lub nie jest) tautologią można szukać przypadku, w którym jest fałszywa.
Na przykład, jeśli formuła $[(p \to q) \land q] \to p$ jest fałszywa dla wartościowania ρ, to wyłącznie w przypadku, gdy

$$[\![(p \to q) \land q]\!]_\rho = 1, \quad \rho(p) = 0.$$

Koniunkcja prawdziwa jest wyłącznie, gdy prawdziwy jest każdy z jej składników.

$$[\![p \to q]\!]_\rho = 1, \quad \rho(p) = 0, \quad \rho(q) = 1.$$

Zatem dla $\rho(p) = 0$, $\rho(q) = 1$ formuła zdaniowa $[(p \to q) \land q] \to p$ jest fałszywa, tzn.

$$[\![[(p \to q) \land q] \to p]\!]_\rho = 0.$$

Prawa de Morgana

Prawa de Morgana, to tautologie dotyczące zaprzeczenia koniunkcji i zaprzeczenia alternatywy.

$$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$$

$$\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$$

Prawa de Morgana – dowód

p	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
0	0	1	1	0	1	1	1
0	1	1	0	0	1	1	1
1	0	0	1	0	1	1	1
1	1	0	0	1	0	0	1

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$	$\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
0	0	1	1	0	1	1	1
0	1	1	0	1	0	0	1
1	0	0	1	1	0	0	1
1	1	0	0	1	0	0	1

Dowodzenie tautologii – cd.

Tautologie można dowodzić wykorzystując dane wcześniej tautologie. Na przykład

$$(p \rightarrow q) \overset{\substack{\text{prawo podwójnego} \\ \text{przeczenia}}}{\leftrightarrow} [\neg\neg(p \rightarrow q)] \overset{\substack{\text{zaprzeczenie} \\ \text{implikacji}}}{\leftrightarrow} [\neg(p \wedge \neg q)] \overset{\substack{\text{prawo} \\ \text{de Morgana}}}{\leftrightarrow}$$

$$\leftrightarrow (\neg p \vee q)$$

Dowód prawa transpozycji

$$(p \rightarrow q) \leftrightarrow (\neg p \vee q) \overset{\substack{\text{prawo podwójnego} \\ \text{przeczenia}}}{\leftrightarrow} [\neg(\neg q) \vee \neg p] \leftrightarrow (\neg q \rightarrow \neg p)$$

Dysjunkcja a inne spójniki

Każdy inny spójnik da się wyrazić przez dysjunkcję $\uparrow$. Zachodzą następujące tautologie

i) $(p \uparrow q) \leftrightarrow \neg(p \wedge q)$,

ii) $\neg p \leftrightarrow (p \uparrow p)$,

iii) $p \vee q \leftrightarrow [(p \uparrow p) \uparrow (q \uparrow q)]$,

iv) $p \wedge q \leftrightarrow [(p \uparrow q) \uparrow (p \uparrow q)]$,

v) $(p \rightarrow q) \leftrightarrow [p \uparrow (q \uparrow q)]$.

Wniosek

W elektronice można używać wyłącznie bramek NAND.

Rachunek zdań – podejście formalne

Rachunek zdań (inaczej logika zdaniowa lub język logiki zerowego rzędu) jest jednym z najprostszych systemów formalnych i zajmuje się zależnościami pomiędzy zdaniami oraz prawdziwością zdań złożonych, w zależności od prawdziwości zdań składowych (z pominięciem ich znaczenia). Zdaniom składowym będą odpowiadać zmienne zdaniowe, zdania złożone buduje sie przy pomocy spójników logicznych $\wedge, \vee, \neg, \rightarrow$ oraz stałych logicznych $\perp$ (fałsz) oraz $\top$ (prawda).

Definicja

Przez zbiór ZZ będziemy oznaczać nieskończony, przeliczalny (tj. posiadający tyle samo elementów co liczby naturalne) zbiór zmiennych zdaniowych, zwykle oznaczanych literami p, q, r itp.

Rachunek zdań – formuły zdaniowe

Pojęcie formuły zdaniowej definiuje się przez rekurencje.

Definicja

Formułą zdaniową nazywamy każdy napis powstały w następujący sposób

i) stałe $\bot, \top$ oraz zmienne zdaniowe ze zbioru ZZ to formuły zdaniowe,

ii) jeśli napis φ jest formułą zdaniową, to napis $\neg\varphi$ też jest formułą zdaniową,

iii) jeśli napisy φ, ϕ są formułami zdaniowymi, to napisy $(\varphi \to \phi), (\varphi \wedge \phi), (\varphi \vee \phi)$ też są formułami zdaniowymi.

Równoważnie, zbiór formuł zdaniowych $\mathcal{F}_Z$ to najmniejszy zbiór zawierający $ZZ \cup \{\top, \bot\}$ spełniający warunek

$$\text{jeśli } \varphi, \phi \in \mathcal{F}_Z, \text{ to } \neg\varphi, (\varphi \to \phi), (\varphi \wedge \phi), (\varphi \vee \phi) \in \mathcal{F}_Z.$$

Rachunek zdań – wartościowanie

W logice klasycznej, po ustaleniu wartości zmiennych zdaniowych zdaniu złożonemu możemy przypisać jednoznacznie jedną z wartości logicznych: prawdę (tj. 1) lub fałsz (tj. 0). W rachunku zdań proces ten nazywamy wartościowaniem i definiujemy rekurencyjnie

Definicja

Wartościowaniem nazywamy dowolną funkcję

$$\rho\colon ZZ \longrightarrow \{0,1\},$$

przypisującą każdej zmiennej zdaniowej wartość logiczną 0 lub 1.

Wartość formuły zdaniowej $\varphi \in \mathcal{F}_Z$ przy wartościowaniu ρ oznaczamy przez $[\![\varphi]\!]_\rho$ i określamy w następujący sposób

Rachunek zdań – wartościowanie

i) $[\![\bot]\!]_\rho = 0, \ [\![\top]\!]_\rho = 1,$

ii) $[\![p]\!]_\rho = \rho(p)$, gdy $p \in ZZ$ jest zmienną zdaniową,

iii) $[\![\neg\varphi]\!]_\rho = 1 - [\![\varphi]\!]_\rho,$

iv) $[\![\varphi \wedge \psi]\!]_\rho = \min\{[\![\varphi]\!]_\rho, [\![\psi]\!]_\rho\},$

v) $[\![\varphi \vee \psi]\!]_\rho = \max\{[\![\varphi]\!]_\rho, [\![\psi]\!]_\rho\},$

vi) $[\![\varphi \to \psi]\!]_\rho = \begin{cases} 0 & [\![\varphi]\!]_\rho = 1 \text{ i } [\![\psi]\!]_\rho = 0, \\ 1 & \text{w przeciwnym przypadku.} \end{cases}$

Rachunek zdań – spójniki

Uwaga

Uwaga, spójniki $\neg, \vee, \wedge$ oraz stałą $\top$ można zdefiniować wyłącznie przy pomocy spójnika $\rightarrow$ i stałej $\bot$ w następujący sposób

i) $\neg\varphi$ jest równoważne $\varphi\rightarrow\bot$,

ii) $\top$ jest równoważne $\neg\bot$,

iii) $\varphi \vee \psi$ jest równoważne $\neg\varphi\rightarrow\psi$,

iv) $\varphi \wedge \psi$ jest równoważne $\neg(\varphi\rightarrow\neg\psi)$.

Spełnialność, konsekwencja

Definicja

Niech φ będzie formułą zdaniową a ρ wartościowaniem. Jeśli zachodzi $[\![\varphi]\!]_\rho = 1$, to piszemy

$$\rho \models \varphi \quad \text{lub} \quad \models \varphi[\rho],$$

i mówimy, że formuła φ jest **spełniona** przez wartościowanie ρ. Jeśli $\Gamma \subset \mathcal{F}_Z$ jest zbiorem formuł zdaniowych oraz zachodzi $\rho \models \varphi$ dla każdej formuły $\varphi \in \Gamma$, to piszemy

$$\rho \models \Gamma.$$

Zapis

$$\Gamma \models \varphi$$

oznacza, że każde wartościowanie spełniające wszystkie formuły z Γ spełnia także formułę φ. W takim przypadku φ nazywamy **(semantyczną) konsekwencją** zbioru Γ.

Tautologia, równoważność

Definicja

Jeśli formuła φ jest konsekwencją zbioru pustego, tj.

$$\emptyset \models \varphi,$$

to φ nazywamy **tautologią** i piszemy

$$\models \varphi.$$

Oznacza to, że φ jest spełniona przez dowolne wartościowanie.
Formuły φ, ψ nazywamy **równoważnymi** jeśli

$$\models (\varphi \leftrightarrow \psi),$$

tzn. równoważność $\varphi \leftrightarrow \psi$, jest tautologią. Zachodzi to wtedy, gdy φ i ψ przyjmują te same wartości przy dowolnym wartościowaniu.
Piszemy wtedy

$$\varphi \equiv \psi.$$

Formuła spełnialna, zbiór spełnialny

Definicja

Formułę φ nazywamy **spełnialną**, jeśli istnieje wartościowanie ρ takie, że

$$\rho \models \varphi,$$

tzn. jeśli φ jest spełniona przez ρ.

Zbiór formuł $\Gamma \subset \mathcal{F}_Z$ nazywamy **spełnialnym**, jeśli istnieje wartościowanie ρ takie, że

$$\rho \models \Gamma,$$

każda formuła w Γ jest spełniona przez ρ.

Instancje

Definicja

Niech S będzie funkcją przypisującą zmiennym zdaniowym pewne formuły zdaniowe. Jeśli φ jest formułą, to przez $S(\varphi)$ oznaczamy formułę φ, w której każdą zmienną zdaniową p zastąpiono formułą $S(p)$. Jeśli $\Gamma \subset \mathcal{F}_Z$ jest zbiorem formuł to definiujemy

$$S(\Gamma) = \{S(\varphi) \mid \varphi \in \Gamma\}.$$

Definicja

Mówimy, że formuła zdaniowa $S(\varphi)$ jest **instancją** formuły zdaniowej φ.

Stwierdzenie

Jeśli $\Gamma \subset \mathcal{F}_Z$ jest zbiorem formuł oraz $\Gamma \models \varphi$, to $S(\Gamma) \models S(\varphi)$. W szczególności, jeśli φ jest tautologią, to $S(\varphi)$ też jest tautologią.

Koniunkcyjna postać normalna formuły

Definicja

Literałem nazywamy każde wyrażenie postaci

$$p \quad \text{lub} \quad \neg p,$$

dla dowolnej zmiennej zdaniowej $p \in ZZ$.

Definicja

Formuła φ jest w **koniunkcyjnej postaci normalnej**, jeśli jest koniunkcją alternatyw literałów, tj.

$$\varphi = (q_1^1 \vee \ldots \vee q_1^{k_1}) \wedge \ldots \wedge (q_r^1 \vee \ldots \vee q_r^{k_r}),$$

gdzie q_i^j są literałami oraz $r \geq 0, k_i \geq 0$ dla $i = 1, \ldots, r$ (przy czym, gdy $r = 0$, to za pustą koniunkcję uważamy symbol $\top$, co odpowiada tzw. pustej spełnialności, a symbol $\bot$, za pustą alternatywę, tj. gdy pewne $k_i = 0$).

Koniunkcyjna postać normalna formuły cd.

Stwierdzenie

Każda formuła zdaniowa φ posiada równoważną formułę w koniunkcyjnej postaci normalnej.

Dowód.

Dowód przez indukcję na długość formuły (liczbę spójników). Literały i symbole $\perp, \top$ są w koniunkcyjnej postaci formalnej. Jeśli formuła φ jest w koniunkcyjnej postaci normalnej, to formułę $\neg\varphi$ można przekształcić do koniunkcyjnej postaci normalnej stosując prawa de Morgana i prawo rozdzielności

$$\psi \vee (\vartheta \wedge \zeta) \leftrightarrow (\psi \vee \vartheta) \wedge (\psi \vee \zeta).$$

Koniunkcyjna postać normalna formuły cd.

Dowód.

Gdy formuła φ jest koniunkcją formuł w postaci normalnej, to φ jest w postaci normalnej. Gdy formuła φ jest alternatywą formuł w postaci normalnej, to korzystamy z prawa rozdzielności. Gdy formuła φ jest implikacją formuł w postaci normalnej, to korzystamy z prawa

$$(\psi \rightarrow \vartheta) \leftrightarrow (\neg\psi \vee \vartheta)$$

oraz poprzednich przypadków.

Koniunkcyjna postać normalna tautologii

Stwierdzenie

Niech formuła φ będzie równoważna formule

$$(q_1^1 \vee \ldots \vee q_1^{k_1}) \wedge \ldots \wedge (q_r^1 \vee \ldots \vee q_r^{k_r})$$

w koniunkcyjnej postaci normalnej. Wtedy φ jest tautologią wtedy i tylko wtedy, gdy dla każdego $i = 1, \ldots, r$ dla pewnych $1 \leq m, n \leq k_i$ jeden z literałów q_i^m oraz q_i^n jest zmienną a drugi negacją tej zmiennej.

Dowód.

Ćwiczenie.

Systemy dowodzenia

Definicja

Systemem dowodzenia nazywamy metodę dowodzenia prawdziwości formuł rachunku zdań (i szerzej, formuł języka logiki pierwszego rzędu) na podstawie przyjętych **metod dowodzenia** w oparciu o pewien początkowym zbiór formuł, zwanych **aksjomatami**.

Metody dowodzenia przekształcają pewne formuły w inne formuły.

System Hilberta

Definicja

Systemem Hilberta nazywamy system dowodzenia formuł, w którym występuje jedynie spójniki $\neg, \to$, stała $\bot$ oraz zmienne zdaniowe (przy czym $\neg\varphi$ jest skrótem na $\varphi\to\bot$), z aksjomatami

A1) $\varphi\to(\psi\to\varphi)$,

A2) $(\varphi\to(\psi\to\vartheta))\to((\varphi\to\psi)\to(\varphi\to\vartheta))$,

A3) $\neg\neg\varphi\to\varphi$,

gdzie φ, ψ, ϑ są dowolnym formułami. Jedyną regułą dowodzenia jest **reguła odrywania**, zwana też regułą **modus ponens**

$$\frac{\varphi,\ \varphi\to\psi}{\psi}.$$

System Hilberta cd.

Definicja

Dowodem w systemie Hilberta nazywamy taki ciąg formuł, w którym każda formuła albo jest aksjomatem albo została otrzymana przez zastosowanie reguły odrywania do poprzedzających ją formuł. Formuła φ **ma dowód** (lub jest **twierdzeniem systemu Hilberta**), jeśli istnieje dowód zawierający φ. Piszemy wtedy

$$\vdash_H \varphi.$$

Mówimy, że formuła φ ma dowód ze zbioru hipotez (przesłanek) Δ, gdy posiada dowód w systemie Hilberta z aksjomatami rozszerzonymi o Δ. Piszemy wtedy

$$\Delta \vdash_H \varphi.$$

System Hilberta – przykład

Stwierdzenie

$$\vdash_H (p \to p)$$

Dowód.

i) $(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$ (instancja A2)),
ii) $p \to ((p \to p) \to p)$ (instancja A1)),
iii) $(p \to (p \to p)) \to (p \to p)$ (reguła odrywania zast. do i),ii)),
iv) $p \to (p \to p)$ (instancja A1)),
v) $p \to p$ (reguła odrywania zast. do iii) oraz iv).

Powyższy dowód działa także dla dowolnej instancji formuły $p \to p$, tj. formuły $\varphi \to \varphi$.

Twierdzenie o dedukcji

Twierdzenie

Jeśli formuła ψ ma dowód w systemie Hilberta ze zbioru hipotez $\Delta \cup \{\varphi\}$, to formuła $\varphi \to \psi$ ma dowód w systemie Hilberta ze zbioru hipotez Δ. Tzn.,

$$\textit{jeśli } \Delta \cup \{\varphi\} \vdash_H \psi, \;\; \textit{to } \Delta \vdash_H (\varphi \to \psi).$$

Dowód.

Dowód przez indukcję na liczbę formuł w dowodzie ψ. Jeśli jest to jedna formuła, to zachodzą trzy przypadki: $\varphi = \psi$ lub $\psi \in \Delta$ lub ψ jest aksjomatem. W pierwszym przypadku stosujemy dowód jak dla $p \to p$ (poprzedni slajd). W dwóch pozostałych stosujemy instancję aksjomatu $A1$), tj. $\psi \to (\varphi \to \psi)$ i regułę odrywania.

Twierdzenie o dedukcji – dowód

Dowód.

Niech dowód ψ zawiera co najmniej dwie formuły. Załóżmy, że ostatnim krokiem w dowodzie ψ było zastosowanie reguły odrywania do $(\vartheta \rightarrow \psi)$, gdzie ϑ jest pewną formułą. Zatem $\Delta \cup \{\varphi\} \vdash_H (\vartheta \rightarrow \psi)$, skąd założenia indukcyjnego

$$\Delta \vdash_H \varphi \rightarrow (\vartheta \rightarrow \psi),$$

$$\Delta \vdash_H \varphi \rightarrow \vartheta$$

(zarówno formuła ϑ jak i $\vartheta \rightarrow \psi$ mają dowód z hipotez $\Delta \cup \{\varphi\}$). Z aksjomatu $A2$) mamy

$$(\varphi \rightarrow (\vartheta \rightarrow \psi)) \rightarrow ((\varphi \rightarrow \vartheta) \rightarrow (\varphi \rightarrow \psi)),$$

i po podwójnym zastosowaniu reguły odrywania dostajemy

$$\varphi \rightarrow \psi.$$

Twierdzenie o poprawności

Twierdzenie

Każda formuła φ posiadająca dowód w systemie Hilberta z hipotez Δ jest konsekwencją semantyczną zbioru formuł Δ, tzn.

$$\textit{jeśli } \Delta \vdash_H \varphi, \ \textit{ to } \Delta \models \varphi.$$

W szczególności, każde twierdzenie w systemie Hilberta jest tautologią.

Twierdzenie o poprawności – dowód

Dowód.

Dowód przez indukcję na liczbę formuł w dowodzie φ. Jeśli jest to jedna formuła, to zachodzą dwa przypadki: $\varphi \in \Delta$ lub φ jest aksjomatem. W obu przypadkach $\Delta \models \varphi$.

Niech dowód φ zawiera co najmniej dwie formuły. Załóżmy, że ostatnim krokiem w dowodzie φ było zastosowanie reguły odrywania do $(\psi \to \varphi)$, gdzie ψ jest pewną formułą. Zatem ψ oraz $\psi \to \varphi$ mają dowód ze zbioru hipotez Δ, skąd z założenia indukcyjnego

$$\Delta \models \psi \text{ oraz } \Delta \models (\psi \to \varphi).$$

Twierdzenie o poprawności – dowód cd.

Dowód.

Zatem każde wartościowanie ρ, które spełnia Δ, spełnia także ψ oraz $\psi \to \varphi$. Zatem przy każdym wartościowaniu ρ spełniającym Δ formuła φ jest także spełniona. Stąd

$$\Delta \models \varphi.$$

Twierdzenie o pełności

Twierdzenie

Jeśli formuła zbudowana jedynie ze zmiennych zdaniowych, spójnika $\to$ oraz symbolu $\perp$ jest tautologią, to jest twierdzeniem systemu Hilberta (tzn. każda formuła prawdziwa ma dowód). Równoważnie, zachodzi

$$\textit{jeśli } \models \varphi, \textit{ to } \vdash_H \varphi.$$

Dowód.

Pomijamy.

Poprawność i pełność oznaczają, ze twierdzenia systemu Hilberta to dokładnie tautologie.

Twierdzenie o zwartości

Twierdzenie

Zbiór $\Gamma \subset \mathcal{F}_Z$ jest spełnialny wtedy i tylko wtedy, gdy każdy jego skończony podzbiór jest spełnialny.

Dowód.

Pomijamy, wykorzystuje lemat Kuratowskiego–Zorna.

Wniosek (silne twierdzenie o pełności)

Dla dowolnego zbioru formuł $\Delta \subset \mathcal{F}_Z$ oraz formuły $\varphi \in \mathcal{F}_Z$,

$$\text{jeśli } \Delta \models \varphi, \text{ to } \Delta \vdash_H \varphi,$$

tzn. jeśli φ jest konsekwencją Δ, to istnieje dowód φ w systemie Hilberta z hipotez Δ.

Twierdzenie o zwartości cd.

Dowód.

Jeśli $\Delta \models \varphi$, to zbiór $\Delta \cup \{\neg\varphi\}$ nie jest spełnialny. Na mocy twierdzenia o zwartości istnieje zatem skończony podzbiór

$$\{\psi_1, \ldots, \psi_n\} \subset \Delta \cup \{\neg\varphi\},$$

który nie jest spełnialny. Tym bardziej zbiór $\{\psi_1, \ldots, \psi_n, \neg\varphi\}$ nie jest spełnialny. Stąd $\{\psi_1, \ldots, \psi_n\} \models \varphi$, zatem formuła

$$\psi_1 \to (\psi_2 \to \ldots \to (\psi_n \to \varphi) \ldots),$$

jest tautologią oraz posiada dowód w systemie Hilberta, tj.

$$\vdash_H \psi_1 \to (\psi_2 \to \ldots \to (\psi_n \to \varphi) \ldots).$$

Po n-krotnym zastosowaniu formuły odrywania dostajemy dowód φ na podstawie hipotez Δ, tj. $\Delta \vdash_H \varphi$.

Kwantyfikatory

Definicja

Kwantyfikatorem ogólnym (ew. **dużym**,**uniwersalnym**) nazywamy symbol $\forall$ (ew. $\bigwedge$) odpowiadający wyrażeniu „dla każdego”. Formułę $\forall_x P(x)$ czytamy „dla każdego x zachodzi $P(x)$”. Jeśli forma zdaniowa $P(x)$ jest prawdziwa w zakresie X piszemy $\forall_{x \in X} P(x)$, co jest równoważne $\forall_x x \in X \rightarrow P(x)$

Kwantyfikatorem szczegółowym (ew. **małym**) nazywamy symbol $\exists$ (ew. $\bigvee$) odpowiadający wyrażeniu „istnieje”. Formułę $\exists_x P(x)$ czytamy „istnieje takie x, że $P(x)$”. Jeśli forma zdaniowa $P(x)$ jest spełniona w zakresie X piszemy $\exists_{x \in X} P(x)$, co jest równoważne wyrażeniu $\exists_x x \in X \wedge P(x)$.

Kwantyfikatory – cd.

Uwaga

Z definicji wynika, że zdanie $\forall_{x \in \emptyset} P(x)$ jest prawdziwe dla każdej formuły zdaniowej $P(x)$ (z fałszu wynika prawda i fałsz).

Analogicznie, zdanie $\exists_{x \in \emptyset} P(x)$ jest fałszywe dla każdej formuły zdaniowej $P(x)$ (koniunkcja zdania fałszywego z jakimkolwiek innym zdaniem jest fałszywa).

Prawa de Morgana rachunku kwantyfikatorów – cd.

Wniosek

Dla dowolnej formuły zdaniowej $P(x)$ poniższe formuły są tautologiami

$$\neg\forall_{x\in X} P(x) \leftrightarrow \exists_{x\in X} \neg P(x),$$

$$\neg\exists_{x\in X} P(x) \leftrightarrow \forall_{x\in X} \neg P(x).$$