Zdania

Definicja (Zdanie logiczne)

Zdaniem logicznym nazywamy dowolne stwierdzenie, któremu można przyporządkować wartość logiczną **prawda** lub **fałsz**.

Zdania

Definicja (Zdanie logiczne)

Zdaniem logicznym nazywamy dowolne stwierdzenie, któremu można przyporządkować wartość logiczną **prawda** lub **fałsz**.

Czy to są zdania?

- $\rightsquigarrow$ Wisła jest rzeką.
- $\rightsquigarrow$ Kraków jest rzeką.
- $\rightsquigarrow$ Czy Odra jest rzeką?

Zdania

Definicja (Zdanie logiczne)

Zdaniem logicznym nazywamy dowolne stwierdzenie, któremu można przyporządkować wartość logiczną **prawda** lub **fałsz**.

Czy to są zdania?

- $\rightsquigarrow$ Wisła jest rzeką. TAK
- $\rightsquigarrow$ Kraków jest rzeką.
- $\rightsquigarrow$ Czy Odra jest rzeką?

Zdania

Definicja (Zdanie logiczne)

Zdaniem logicznym nazywamy dowolne stwierdzenie, któremu można przyporządkować wartość logiczną **prawda** lub **fałsz**.

Czy to są zdania?

- $\rightsquigarrow$ Wisła jest rzeką. TAK
- $\rightsquigarrow$ Kraków jest rzeką. TAK
- $\rightsquigarrow$ Czy Odra jest rzeką?

Zdania

Definicja (Zdanie logiczne)

Zdaniem logicznym nazywamy dowolne stwierdzenie, któremu można przyporządkować wartość logiczną **prawda** lub **fałsz**.

Czy to są zdania?

- $\rightsquigarrow$ Wisła jest rzeką. TAK
- $\rightsquigarrow$ Kraków jest rzeką. TAK
- $\rightsquigarrow$ Czy Odra jest rzeką? NIE

Wartości logiczne

prawda $\equiv 1 \equiv$ **T** **fałsz** $\equiv 0 \equiv$ **F**

Funktory zdaniotwórcze

$\rightsquigarrow$ **koniunkcja**: $\wedge$

$p \wedge q$ czytamy: p i q

Funktory zdaniotwórcze

- **koniunkcja**: $\wedge$

  $p \wedge q$ czytamy: p i q

- **alternatywa**: $\vee$

  $p \vee q$ czytamy: p lub q

Funktory zdaniotwórcze

- **koniunkcja**: $\wedge$
  $p \wedge q$ czytamy: p i q

- **alternatywa**: $\vee$
  $p \vee q$ czytamy: p lub q

- **implikacja**: $\Rightarrow$
  $p \Rightarrow q$ czytamy: jeżeli p, to q (lub: z p wynika q)

Funktory zdaniotwórcze

- **koniunkcja**: $\wedge$
  $p \wedge q$ czytamy: p i q
- **alternatywa**: $\vee$
  $p \vee q$ czytamy: p lub q
- **implikacja**: $\Rightarrow$
  $p \Rightarrow q$ czytamy: jeżeli p, to q (lub: z p wynika q)
- **równoważność**: $\Leftrightarrow$
  $p \Leftrightarrow q$ czytamy: p jest równoważne q

Funktory zdaniotwórcze

- **koniunkcja**: $\wedge$

  $p \wedge q$ czytamy: p i q

- **alternatywa**: $\vee$

  $p \vee q$ czytamy: p lub q

- **implikacja**: $\Rightarrow$

  $p \Rightarrow q$ czytamy: jeżeli p, to q (lub: z p wynika q)

- **równoważność**: $\Leftrightarrow$

  $p \Leftrightarrow q$ czytamy: p jest równoważne q

- **zaprzeczenie**: $\neg$ $\sim$

  $\neg p$ czytamy: nie p

Funktory zdaniotwórcze

- **koniunkcja**: $\wedge$
  $p \wedge q$ czytamy: p i q
- **alternatywa**: $\vee$
  $p \vee q$ czytamy: p lub q
- **implikacja**: $\Rightarrow$
  $p \Rightarrow q$ czytamy: jeżeli p, to q (lub: z p wynika q)
- **równoważność**: $\Leftrightarrow$
  $p \Leftrightarrow q$ czytamy: p jest równoważne q
- **zaprzeczenie**: $\neg$
  $\neg p$ czytamy: nie p
- ...

Funktory zdaniotwórcze

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$	$p * q$
T	T	T	T	T	T	T/F
T	F	F	T	F	F	T/F
F	T	F	T	T	F	T/F
F	F	F	F	T	T	T/F

16

p	$\neg p$	$\# p$			
T	F	T/F	T	T	F
F	T	T/F	F	T	F

4

Funktory zdaniotwórcze

- **alternatywa wykluczająca** lub **XOR**: $\oplus$

  $p \oplus q \quad \equiv \quad \neg(p \Leftrightarrow q)$

Funktory zdaniotwórcze

- **alternatywa wykluczająca** lub **XOR**: $\oplus$
  $p \oplus q \quad \equiv \quad \neg(p \Leftrightarrow q)$
- **kreska Sheffera** lub **NAND**: $|$
  $p \mid q \quad \equiv \quad \neg(p \wedge q)$

Funktory zdaniotwórcze

- $\rightsquigarrow$ **alternatywa wykluczająca** lub **XOR**: $\oplus$

  $p \oplus q \quad \equiv \quad \neg(p \Leftrightarrow q)$

- $\rightsquigarrow$ **kreska Sheffera** lub **NAND**: $|$

  $p \mid q \quad \equiv \quad \neg(p \wedge q)$

- $\rightsquigarrow$ **strzałka Peirce'a** lub **NOR**: $\downarrow$

  $p \downarrow q \quad \equiv \quad \neg(p \vee q)$

Funktory zdaniotwórcze

- **alternatywa wykluczająca** lub **XOR**: $\oplus$
  $p \oplus q \quad \equiv \quad \neg(p \Leftrightarrow q)$
- **kreska Sheffera** lub **NAND**: $|$
  $p \mid q \quad \equiv \quad \neg(p \wedge q)$
- **strzałka Peirce'a** lub **NOR**: $\downarrow$
  $p \downarrow q \quad \equiv \quad \neg(p \vee q)$

p	q	$p \oplus q$	$p \mid q$	$p \downarrow q$
T	T	F	F	F
T	F	T	T	F
F	T	T	T	F
F	F	F	T	T

Warunek konieczny i dostateczny

$$p \Rightarrow q$$

Warunek konieczny i dostateczny

$$p \Rightarrow q$$

- p jest warunkiem **dostatecznym** (wystarczającym) dla q.
- q jest warunkiem **koniecznym** dla p.

Warunek konieczny i dostateczny

$$p \Rightarrow q$$

- $\rightsquigarrow$ p jest warunkiem **dostatecznym** (wystarczającym) dla q.
- $\rightsquigarrow$ q jest warunkiem **koniecznym** dla p.

Przykład

Niech

$$p = \text{„liczba } n \text{ jest podzielna przez 3''}$$

$$q = \text{„liczba } n \text{ jest podzielna przez 6''}$$

$q \Rightarrow p$

Warunek konieczny i dostateczny

$$p \Rightarrow q$$

$\rightsquigarrow$ p jest warunkiem **dostatecznym** (wystarczającym) dla q.

$\rightsquigarrow$ q jest warunkiem **koniecznym** dla p.

Przykład

Niech

$$p = \text{„liczba } n \text{ jest podzielna przez 3''}$$

$$q = \text{„liczba } n \text{ jest podzielna przez 6''}$$

$\rightsquigarrow$ p jest warunkiem koniecznym dla q.

$\rightsquigarrow$ q jest warunkiem wystarczającym dla p.

Funkcje zdaniowe i tautologie

Definicja (Zmienna logiczna)

Zmienną logiczną nazywamy zmienną, zwykle oznaczaną p, q, r, $\ldots$, która może przyjąć tylko dwie wartości: prawda lub fałsz.

Funkcje zdaniowe i tautologie

Definicja (Zmienna logiczna)

Zmienną logiczną nazywamy zmienną, zwykle oznaczaną p, q, r, ..., która może przyjąć tylko dwie wartości: prawda lub fałsz.

Definicja (Funkcja zdaniowa)

Funkcją zdaniową nazywamy wyrażenie złożone ze zmiennych logicznych połączonych w poprawny sposób funktorami i nawiasami.

Funkcje zdaniowe i tautologie

Definicja (Zmienna logiczna)

Zmienną logiczną nazywamy zmienną, zwykle oznaczaną p, q, r, $\ldots$, która może przyjąć tylko dwie wartości: prawda lub fałsz.

Definicja (Funkcja zdaniowa)

Funkcją zdaniową nazywamy wyrażenie złożone ze zmiennych logicznych połączonych w poprawny sposób funktorami i nawiasami.

$$\big\{[(p \Rightarrow s) \Rightarrow (q \wedge s)] \wedge \neg(q \wedge s)\big\} \Rightarrow \neg(p \Rightarrow s)$$

Funkcje zdaniowe i tautologie

Definicja (Zmienna logiczna)

Zmienną logiczną nazywamy zmienną, zwykle oznaczaną p, q, r, $\ldots$, która może przyjąć tylko dwie wartości: prawda lub fałsz.

Definicja (Funkcja zdaniowa)

Funkcją zdaniową nazywamy wyrażenie złożone ze zmiennych logicznych połączonych w poprawny sposób funktorami i nawiasami.

$$\Big\{\big[(p \Rightarrow s) \Rightarrow (q \wedge s)\big] \wedge \neg(q \wedge s)\Big\} \Rightarrow \neg(p \Rightarrow s)$$

Definicja (Tautologia, prawo rachunku zdań)

Tautologią nazywamy funkcję zdaniową, która dla dowolnego wartościowania zmiennych w niej występujących przyjmuje wartość **prawda**.

Zupełność

Definicja (Zupełny zbiór funktorów)

Powiemy, że zbiór funktorów A jest **zupełny**, jeżeli każda funkcja zdaniowa może być w sposób równoważny zapisana przy wykorzystaniu wyłącznie funktorów ze zbioru A.

Zupełność

Definicja (Zupełny zbiór funktorów)

Powiemy, że zbiór funktorów A jest **zupełny**, jeżeli każda funkcja zdaniowa może być w sposób równoważny zapisana przy wykorzystaniu wyłącznie funktorów ze zbioru A.

Twierdzenie

Zbiory

$$\{\wedge, \neg\}, \quad \{\vee, \neg\}, \quad \boxed{\{|\}, \quad \{\downarrow\}}$$

są zupełne.

NAND NOR

Prawa rachunku zdań

- **Prawo podwójnego przeczenia**
  $\neg(\neg p) \equiv p$

Prawa rachunku zdań

- **Prawo podwójnego przeczenia**
  $\neg(\neg p) \equiv p$
- **Prawa przemienności**
  $(p \vee q) \equiv (q \vee p)$
  $(p \wedge q) \equiv (q \wedge p)$

Prawa rachunku zdań

- **Prawo podwójnego przeczenia**
  $\neg(\neg p) \equiv p$
- **Prawa przemienności**
  $(p \vee q) \equiv (q \vee p)$
  $(p \wedge q) \equiv (q \wedge p)$
- **Prawa łączności**
  $[(p \vee q) \vee r] \equiv [p \vee (q \vee r)]$
  $[(p \wedge q) \wedge r] \equiv [p \wedge (q \wedge r)]$

$(a+b)+c = a+(b+c)$

Prawa rachunku zdań

- **Prawo podwójnego przeczenia**

  $\neg(\neg p) \equiv p$

- **Prawa przemienności**

  $(p \vee q) \equiv (q \vee p)$

  $(p \wedge q) \equiv (q \wedge p)$

- **Prawa łączności**

  $[(p \vee q) \vee r] \equiv [p \vee (q \vee r)]$

  $[(p \wedge q) \wedge r] \equiv [p \wedge (q \wedge r)]$

- **Prawa rozdzielności**

  $[p \vee (q \wedge r)] \equiv [(p \vee q) \wedge (p \vee r)]$

  $[p \wedge (q \vee r)] \equiv [(p \wedge q) \vee (p \wedge r)]$.

$a \overset{\wedge}{\cdot} (b \overset{\vee}{+} c) = a \overset{\wedge}{\cdot} b \overset{\vee}{+} a \overset{\wedge}{\cdot} c$

Prawa rachunku zdań

- **Prawo podwójnego przeczenia**
  $\neg(\neg p) \equiv p$
- **Prawa przemienności**
  $(p \vee q) \equiv (q \vee p)$
  $(p \wedge q) \equiv (q \wedge p)$
- **Prawa łączności**
  $[(p \vee q) \vee r] \equiv [p \vee (q \vee r)]$
  $[(p \wedge q) \wedge r] \equiv [p \wedge (q \wedge r)]$
- **Prawa rozdzielności**
  $[p \vee (q \wedge r)] \equiv [(p \vee q) \wedge (p \vee r)]$
  $[p \wedge (q \vee r)] \equiv [(p \wedge q) \vee (p \wedge r)]$.
- **Prawa de Morgana**
  $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$
  $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$

Prawa rachunku zdań

- **Prawo podwójnego przeczenia**
  $\neg(\neg p) \equiv p$
- **Prawa przemienności**
  $(p \vee q) \equiv (q \vee p)$
  $(p \wedge q) \equiv (q \wedge p)$
- **Prawa łączności**
  $[(p \vee q) \vee r] \equiv [p \vee (q \vee r)]$
  $[(p \wedge q) \wedge r] \equiv [p \wedge (q \wedge r)]$
- **Prawa rozdzielności**
  $[p \vee (q \wedge r)] \equiv [(p \vee q) \wedge (p \vee r)]$
  $[p \wedge (q \vee r)] \equiv [(p \wedge q) \vee (p \wedge r)]$.
- **Prawa de Morgana**
  $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$
  $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$
- **Prawo kontrapozycji**
  $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$

Prawa rachunku zdań

- $\rightsquigarrow$ $(p \Rightarrow q) \equiv (\neg p \vee q)$
- $\rightsquigarrow$ $(p \Rightarrow q) \equiv \neg(p \wedge \neg q)$
- $\rightsquigarrow$ $(p \vee p) \equiv p$
- $\rightsquigarrow$ $(p \wedge p) \equiv p$
- $\rightsquigarrow$ $\boxed{(p \Rightarrow p) \equiv \mathsf{T}}$
- $\rightsquigarrow$ $(p \overset{\Leftrightarrow}{\cancel{\equiv}} p) \equiv \mathsf{T}$
- $\rightsquigarrow$ $(p \vee \neg p) \equiv \mathsf{T}$
- $\rightsquigarrow$ $(p \wedge \neg p) \equiv \mathsf{F}$
- $\rightsquigarrow$ $(p \wedge \mathsf{F}) \equiv \mathsf{F}$
- $\rightsquigarrow$ $(p \wedge \mathsf{T}) \equiv p$
- $\rightsquigarrow$ $(p \vee \mathsf{F}) \equiv p$
- $\rightsquigarrow$ $(p \vee \mathsf{T}) \equiv \mathsf{T}$
- $\rightsquigarrow$ $\boxed{(p \Rightarrow \mathsf{F}) \equiv \neg p}$
- $\rightsquigarrow$ $(p \Rightarrow \mathsf{T}) \equiv \mathsf{T}$
- $\rightsquigarrow$ $(\mathsf{F} \Rightarrow p) \equiv \mathsf{T}$
- $\rightsquigarrow$ $(\mathsf{T} \Rightarrow p) \equiv p.$

Przykłady

Wykazać, że poniższe funkcje zdaniowe są tautologiami:

- $(\neg p \Rightarrow q) \Rightarrow [(\neg p \Rightarrow \neg q) \Rightarrow p]$,
- $[(p \wedge q) \Rightarrow r] \Leftrightarrow [(p \wedge \neg r) \Rightarrow \neg q]$,
- $\{[(p \Rightarrow s) \Rightarrow (q \wedge s)] \wedge \neg(q \wedge s)\} \Rightarrow \neg(p \Rightarrow s)$.

Przykłady

Wykazać, że poniższe funkcje zdaniowe są tautologiami:

- $(\neg p \Rightarrow q) \Rightarrow [(\neg p \Rightarrow \neg q) \Rightarrow p]$,
- $[(p \wedge q) \Rightarrow r] \Leftrightarrow [(p \wedge \neg r) \Rightarrow \neg q]$,
- $\{[(p \Rightarrow s) \Rightarrow (q \wedge s)] \wedge \neg(q \wedge s)\} \Rightarrow \neg(p \Rightarrow s)$.

Metody

- Tabela prawdy (próby zero-jedynkowe, „brute-force”).
- Prawa rachunku zdań.
- „Drzewko”.

Przykłady

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

p	q	$\neg p$	$\overbrace{\neg p \Rightarrow q}^{A}$	$\neg q$	$\neg p \Rightarrow \neg q$	$\overbrace{(\neg p \Rightarrow \neg q) \Rightarrow p}^{B}$	$A \Rightarrow B$
T	T	F	T	F	T	T	T
T	F	F	T	T	T	T	T
F	T	T	T	F	F	T	T
F	F	T	F	T	T	F	T

Przykłady

$$[(p \wedge q) \Rightarrow r] \Leftrightarrow [(p \wedge \neg r) \Rightarrow \neg q]$$

$(p \Rightarrow q) \equiv (\sim p \vee q)$ p. de Morgana

$$\underbrace{(p \wedge q)}_{p} \Rightarrow \underbrace{r}_{q} \equiv \underbrace{\neg(p \wedge q) \vee r}_{} \equiv (\neg p \vee \neg q) \vee r$$

$$(p \wedge \neg r) \Rightarrow \neg q \equiv \neg(p \wedge \neg r) \vee \neg q \equiv$$

$$\equiv (\neg p \vee r) \vee \neg q \equiv$$

$$\equiv \neg p \vee \neg q \vee r$$

Przykłady

$$\{[(p \Rightarrow s) \Rightarrow (q \wedge s)] \wedge \neg(q \wedge s)\} \Rightarrow \boxed{\neg(p \Rightarrow s)}$$

$\neg p$ F F F F F $\neg p$ F

$s = T$

$\equiv$

$$[\underbrace{(T \Rightarrow q)}_{q} \wedge \neg q] \Rightarrow F$$

$\equiv$

$$(q \wedge \neg q) \Rightarrow F$$

$\equiv$

$$F \Rightarrow F$$

$\equiv$

$$T$$

$s = F$

$$((\neg p \Rightarrow F) \wedge T) \Rightarrow p$$

$\equiv$

$$(p \wedge T) \Rightarrow p$$

$\equiv$

$$p \Rightarrow p$$

$\equiv$

$$T$$

Uwagi

- $\rightsquigarrow$ Im więcej zmiennych, tym (dużo) większa tabela prawdy.

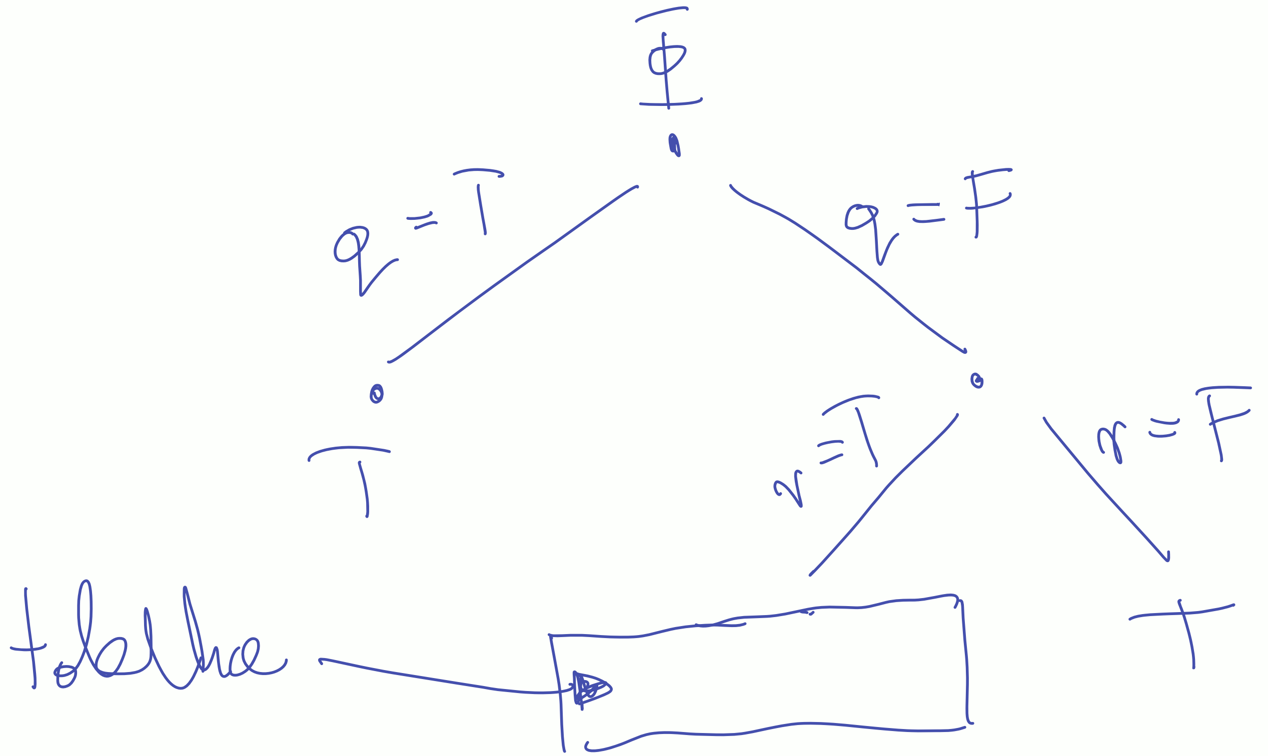
Uwagi

- Im więcej zmiennych, tym (dużo) większa tabela prawdy. Dla n zmiennych tabela ma 2^n wierszy!

Uwagi

⇝ Im więcej zmiennych, tym (dużo) większa tabela prawdy. Dla n zmiennych tabela ma 2^n wierszy!

⇝ Podane metody można łączyć.



Uwagi

- Im więcej zmiennych, tym (dużo) większa tabela prawdy. Dla n zmiennych tabela ma 2^n wierszy!
- Podane metody można łączyć.
- Aby sprawdzić, że funkcja zdaniowa nie jest tautologią, wystarczy podać **jedno** wartościowanie zmiennych, przy którym funkcja ta przyjmuje wartość F.

p	q	r	$\ldots$	$\ldots$	$\boxed{\Phi}$
$\vdots$	$\vdots$	$\vdots$			
T	F	T	$\ldots$	$\ldots$	F
$\vdots$	$\vdots$	$\vdots$			

Postacie normalne

Koniunkcja alternatyw

Definicja (Koniunkcyjna postać normalna, CNF)

Powiemy, że funkcja zdaniowa jest zapisana w **koniunkcyjnej postaci normalnej**, jeżeli jest postaci

$$(p_1 \vee \ldots \vee p_{n_p}) \wedge (q_1 \vee \ldots \vee q_{n_q}) \wedge \ldots \wedge (r_1 \vee \ldots \vee r_{n_r}),$$

przy czym wszystkie wyrażenia występujące w nawiasach są **literałami** (zmienną logiczną bądź negacją zmiennej logicznej — p lub $\neg p$).

$\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg, \oplus, \boxed{|, \downarrow}$

$\{\wedge, \neg\}, \quad \{\vee, \neg\}$

Postacie normalne

Definicja (Koniunkcyjna postać normalna, CNF)

Powiemy, że funkcja zdaniowa jest zapisana w **koniunkcyjnej postaci normalnej**, jeżeli jest postaci

r / $\neg r$

$$(p_1 \vee \ldots \vee p_{n_p}) \wedge (q_1 \vee \ldots \vee q_{n_q}) \wedge \ldots \wedge (r_1 \vee \ldots \vee r_{n_r}),$$

przy czym wszystkie wyrażenia występujące w nawiasach są **literałami** (zmienną logiczną bądź negacją zmiennej logicznej — p lub $\neg p$).

Definicja (Dysjunkcyjna postać normalna, DNF)

$\neg p$

$$\underbrace{(p_1 \wedge \ldots \wedge p_{n_p})}_{\text{klauzula koniunkcji}} \vee (q_1 \wedge \ldots \wedge q_{n_q}) \vee \ldots \vee (r_1 \wedge \ldots \wedge r_{n_r}).$$

p

Postacie normalne

Definicja (Koniunkcyjna postać normalna, CNF)

Powiemy, że funkcja zdaniowa jest zapisana w **koniunkcyjnej postaci normalnej**, jeżeli jest postaci

$$(p_1 \vee \ldots \vee p_{n_p}) \wedge (q_1 \vee \ldots \vee q_{n_q}) \wedge \ldots \wedge (r_1 \vee \ldots \vee r_{n_r}),$$

przy czym wszystkie wyrażenia występujące w nawiasach są **literałami** (zmienną logiczną bądź negacją zmiennej logicznej — p lub $\neg p$).

Definicja (Dysjunkcyjna postać normalna, DNF)

$$(p_1 \wedge \ldots \wedge p_{n_p}) \vee (q_1 \wedge \ldots \wedge q_{n_q}) \vee \ldots \vee (r_1 \wedge \ldots \wedge r_{n_r}).$$

Twierdzenie

Każdą funkcję zdaniową można zapisać w równoważnej jej postaci normalnej (CNF i DNF).

$$\Phi \qquad \{\{p \Rightarrow [(q \vee r) \oplus q]\} \Rightarrow \underline{(s \mid u)}\}$$

5 zmiennych

$$\Phi(p,q,r,s,u) \in \{T, F\}$$

DNF

ψ

$s = u = F \qquad s \mid u = T$

x_i – pełne wartościowanie $\{p,q,r,s,u\}$

dla którego $\boxed{\Phi(x_i)} = \Phi(p_i, q_i, r_i, s_i, u_i) = T$

n

$$\text{np. } x_1 = \begin{pmatrix} p & q & r & s & u \\ T, & T, & F, & F, & F \end{pmatrix}$$

$$x_1 \rightsquigarrow \Phi_1 \rightsquigarrow p \wedge q \wedge \neg r \wedge \neg s \wedge \neg u$$

$$\Phi_1(p,q,r,s,u) = T \equiv (p,q,r,s,u) = x_1$$

$$\Phi \equiv \Phi_1 \vee \Phi_2 \vee \ldots \vee \Phi_n$$

$$\Phi(x) = T \Leftrightarrow x = x_i \Leftrightarrow \Phi_i(x_i) = T$$

$\Longrightarrow$ Istnieje DNF równoważna Φ.

$$\neg(\text{DNF}) \qquad \neg(p \vee q) \equiv \neg p \wedge \neg q$$

$\parallel$ prawo de Morgana

CNF

Spełnialność funkcji zdaniowych

Definicja (Funkcja spełnialna)

Powiemy, że funkcja zdaniowa jest **spełnialna**, jeżeli **istnieje** takie wartościowanie zmiennych w niej występujących, przy którym funkcja przyjmie wartość T.

Spełnialność funkcji zdaniowych

Definicja (Funkcja spełnialna)

Powiemy, że funkcja zdaniowa jest **spełnialna**, jeżeli **istnieje** takie wartościowanie zmiennych w niej występujących, przy którym funkcja przyjmie wartość T.

$$\{[(p \Rightarrow r) \Rightarrow (q \wedge s)] \wedge \neg(q \wedge s)\} \wedge (\neg p \Rightarrow s)$$

Spełnialność funkcji zdaniowych

Definicja (Funkcja spełnialna)

Powiemy, że funkcja zdaniowa jest **spełnialna**, jeżeli **istnieje** takie wartościowanie zmiennych w niej występujących, przy którym funkcja przyjmie wartość T.

$$\{[(p \Rightarrow r) \Rightarrow (q \wedge s)] \wedge \neg(q \wedge s)\} \wedge (\neg p \Rightarrow s)$$

$$p = \mathrm{T}, \qquad q = \mathrm{F}, \qquad r = \mathrm{F}, \qquad s = \mathrm{F}$$

Spełnialność funkcji zdaniowych

Definicja (Funkcja spełnialna)

Powiemy, że funkcja zdaniowa jest **spełnialna**, jeżeli **istnieje** takie wartościowanie zmiennych w niej występujących, przy którym funkcja przyjmie wartość T.

$$\{[(p \Rightarrow r) \Rightarrow (q \wedge s)] \wedge \neg(q \wedge s)\} \wedge (\neg p \Rightarrow s)$$

$$p = \mathrm{T}, \qquad q = \mathrm{F}, \qquad r = \mathrm{F}, \qquad s = \mathrm{F}$$

Twierdzenie

Jeżeli Φ jest funkcją zdaniową, to

Φ jest spełnialna wtedy i tylko wtedy, gdy $\neg\Phi$ nie jest tautologią.

Problem SAT i P = NP

Pytanie

Jak sprawdzić, czy funkcja zdaniowa jest spełnialna?

$$\Phi(p_1, p_2, \ldots, p_n) \xrightarrow{?} \text{TAK}/\text{NIE}$$

$$T/F \quad T/F \quad \ldots \quad T/F$$

$$2^n$$

Problem SAT i P = NP

$p \wedge \ldots \wedge \neg p$

DNF $\quad (\ldots \wedge \ldots \wedge \ldots) \vee \underbrace{(\ldots \wedge \ldots \wedge \ldots)} \vee \ldots$

Pytanie

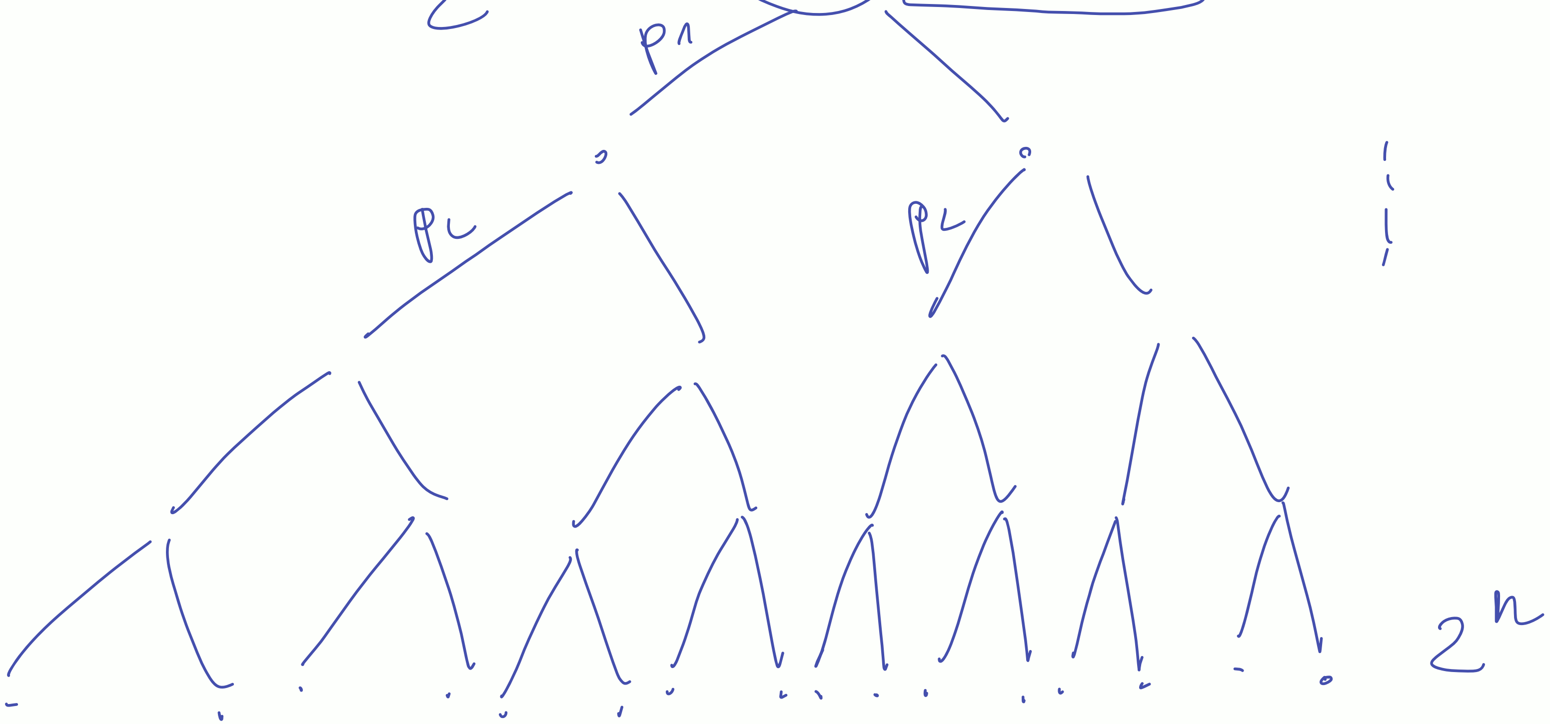
Jak sprawdzić, czy funkcja zdaniowa jest spełnialna?

Czy istnieje coś lepszego niż brute-force (czyli tabela prawdy)?

$10 \longrightarrow \text{DNF}$

2^{10}

$\overset{n}{\Phi} \;\boxed{\longrightarrow}\; \text{DNF}(\Phi)^{2^n}$



Problem SAT i $\boxed{P = NP}$

Pytanie

Jak sprawdzić, czy funkcja zdaniowa jest spełnialna?

Czy istnieje coś lepszego niż brute-force (czyli tabela prawdy)?

Nie wiadomo!

Problem SAT i P = NP

Pytanie

Jak sprawdzić, czy funkcja zdaniowa jest spełnialna?

Czy istnieje coś lepszego niż brute-force (czyli tabela prawdy)?

Nie wiadomo!

Nagroda za rozwiązanie: \$1,000,000.

$P \overset{?}{=} NP$ / $P \neq NP$?

$$\underbrace{[1, 5, 2, 1, -10, 100, \ldots, 103]}_{n}$$

$S = 15$ n 2^n

2^n podzbiorów

$([\ \ ], S) \longrightarrow$ TAK/NIE

istnieje podzbiór tej tablicy o sumie S.

$[\ , \ldots, \ ]^{n}$

$([\ \ ], M) \to$ TAK/NIE

istnieje liczba $> M$

Problem typu P

n ← rozmiar danych

n^k ← rozwiązanie w czasie wielomianowym

$$2^n \gg n^k$$

NP

Problem SAT i P = NP

Pytanie

Jak sprawdzić, czy funkcja zdaniowa jest spełnialna?

Czy istnieje coś lepszego niż brute-force (czyli tabela prawdy)?

Nie wiadomo!

Nagroda za rozwiązanie: $1,000,000.

Jeżeli da się to zrobić szybko, to da się również (szybko) złamać RSA.

Dowody nie wprost

Jak można dowieść twierdzenia postaci

$$p \Rightarrow q?$$

Dowody nie wprost

Jak można dowieść twierdzenia postaci

$$p \Rightarrow q?$$

Prawo kontrapozycji:

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

Dowody nie wprost

Jak można dowieść twierdzenia postaci

$$p \Rightarrow q?$$

Prawo kontrapozycji:

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

Twierdzenie

Jeżeli dla liczb naturalnych m i n zachodzi $m + n \geqslant 33$, to $m \geqslant 17$ lub $n \geqslant 17$.

Dowody nie wprost

Jak można dowieść twierdzenia postaci

$$p \Rightarrow q?$$

Prawo kontrapozycji:

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

Twierdzenie

Jeżeli dla liczb naturalnych m i n zachodzi $m + n \geqslant 33$, to $m \geqslant 17$ lub $n \geqslant 17$.

Dowód

$\rightsquigarrow$ Załóżmy, że $m \leqslant 16$ **i** $n \leqslant 16$.

Dowody nie wprost

Jak można dowieść twierdzenia postaci

$$p \Rightarrow q?$$

Prawo kontrapozycji:

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

Twierdzenie

Jeżeli dla liczb naturalnych m i n zachodzi $m + n \geqslant 33$, to $m \geqslant 17$ lub $n \geqslant 17$.

Dowód

- $\rightsquigarrow$ Załóżmy, że $m \leqslant 16$ **i** $n \leqslant 16$.
- $\rightsquigarrow$ Wtedy $m + n \leqslant 16 + 16 \leqslant 32 < 33$.

Dowody nie wprost

$$\boxed{(p \Rightarrow q) \iff (\neg q \Rightarrow \neg p)}$$

$$(p \Rightarrow q) \equiv [(p \wedge \neg q) \Rightarrow \mathsf{F}]$$

Dowody nie wprost

$$(p \Rightarrow q) \equiv [(p \wedge \neg q) \Rightarrow \mathsf{F}]$$

p q

Twierdzenie

Jeżeli liczba naturalna n jest złożona, to ma dzielnik większy od 1, który jest mniejszy lub równy $\sqrt{n}$.

$p \iff n = ab, \quad a, b \geq 2$

$\neg q \iff$ Jeżeli $c \geq 2$, jest dzielnikiem n, to $c > \sqrt{n}$,

$\Rightarrow a, b > \sqrt{n} \Rightarrow a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$

$n \Rightarrow \mathsf{F}$

Dowody nie wprost

$$(p \Rightarrow q) \equiv [(p \wedge \neg q) \Rightarrow \mathsf{F}]$$

Twierdzenie

Jeżeli liczba naturalna n jest złożona, to ma dzielnik większy od 1, który jest mniejszy lub równy $\sqrt{n}$.

Dowód

Istnieją takie liczby naturalne $a, b \geqslant 2$, że $n = ab$.

Dowody nie wprost

$$(p \Rightarrow q) \equiv [(p \wedge \neg q) \Rightarrow \mathsf{F}]$$

Twierdzenie

Jeżeli liczba naturalna n jest złożona, to ma dzielnik większy od 1, który jest mniejszy lub równy $\sqrt{n}$.

Dowód

Istnieją takie liczby naturalne $a, b \geqslant 2$, że $n = ab$.

$\leadsto$ Załóżmy, że liczba n nie ma dzielnika, który jest mniejszy lub równy $\sqrt{n}$.

Dowody nie wprost

$$(p \Rightarrow q) \equiv [(p \wedge \neg q) \Rightarrow \mathsf{F}]$$

Twierdzenie

Jeżeli liczba naturalna n jest złożona, to ma dzielnik większy od 1, który jest mniejszy lub równy $\sqrt{n}$.

Dowód

Istnieją takie liczby naturalne $a, b \geqslant 2$, że $n = ab$.

- ⇝ Załóżmy, że liczba n nie ma dzielnika, który jest mniejszy lub równy $\sqrt{n}$.
- ⇝ Oznacza to, że $a > \sqrt{n}$ i $b > \sqrt{n}$.

Dowody nie wprost

$$(p \Rightarrow q) \equiv [(p \wedge \neg q) \Rightarrow \mathrm{F}]$$

Twierdzenie

Jeżeli liczba naturalna n jest złożona, to ma dzielnik większy od 1, który jest mniejszy lub równy $\sqrt{n}$.

Dowód

Istnieją takie liczby naturalne $a, b \geqslant 2$, że $n = ab$.

- $\leadsto$ Załóżmy, że liczba n nie ma dzielnika, który jest mniejszy lub równy $\sqrt{n}$.
- $\leadsto$ Oznacza to, że $a > \sqrt{n}$ i $b > \sqrt{n}$.
- $\leadsto$ Stąd $n = ab > \sqrt{n}\sqrt{n} = n$.

Dowody nie wprost

$$(p \Rightarrow q) \equiv [(p \wedge \neg q) \Rightarrow \mathrm{F}]$$

Twierdzenie

Jeżeli liczba naturalna n jest złożona, to ma dzielnik większy od 1, który jest mniejszy lub równy $\sqrt{n}$.

Dowód

Istnieją takie liczby naturalne $a, b \geqslant 2$, że $n = ab$.

- $\rightsquigarrow$ Załóżmy, że liczba n nie ma dzielnika, który jest mniejszy lub równy $\sqrt{n}$.
- $\rightsquigarrow$ Oznacza to, że $a > \sqrt{n}$ i $b > \sqrt{n}$.
- $\rightsquigarrow$ Stąd $n = ab > \sqrt{n}\sqrt{n} = n$.
- $\rightsquigarrow$ Otrzymana sprzeczność kończy dowód.

Dowody nie wprost

p

$$(\neg p \Rightarrow \mathsf{F}) \Rightarrow p$$

Dowody nie wprost

$$(\neg p \Rightarrow \mathsf{F}) \Rightarrow p$$

p

Ćwiczenie

⇝ Dowieść, że liczba $\sqrt{2}$ jest niewymierna.

$\neg p \iff \sqrt{2}$ jest liczbą wymierną

Funkcje zdaniowe

Definicja (Funkcja zdaniowa jednej zmiennej)

Funkcją zdaniową jednej zmiennej nazywamy wyrażenie postaci $\Phi(x)$, zależne od zmiennej $x \in X$, które dla dowolnej wartości x staje się zdaniem logicznym.

Zbiór X nazywamy **zakresem zmienności** lub **dziedziną** funkcji zdaniowej Φ.

Funkcje zdaniowe

Definicja (Funkcja zdaniowa jednej zmiennej)

Funkcją zdaniową jednej zmiennej nazywamy wyrażenie postaci $\Phi(x)$, zależne od zmiennej $x \in X$, które dla dowolnej wartości x staje się zdaniem logicznym.

Zbiór X nazywamy **zakresem zmienności** lub **dziedziną** funkcji zdaniowej Φ.

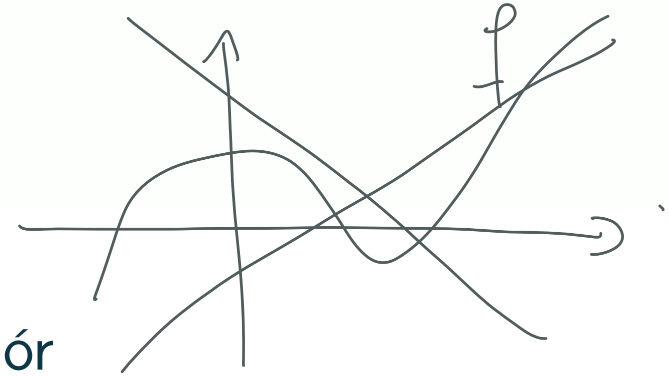
Przykłady

- $\Phi(x) \equiv (x = x)$, $X = \mathbb{R}$
- $\Phi(x) \equiv (x \neq x)$, $X = \mathbb{R}$
- $\Phi(x) \equiv (x^2 \geqslant 2x)$, $X = (0, +\infty)$
- $\Phi(x) \equiv (x^2 < 2)$, $X = \mathbb{N}$

$x \in \mathbb{R}$

$f(x) = x + 1$

Funkcje zdaniowe



Definicja (Wykres funkcji zdaniowej)

Wykresem funkcji zdaniowej Φ nazywamy zbiór

$$\boxed{S(\Phi) := \{x \in X \colon \Phi(x)\},}$$

to znaczy zbiór wszystkich elementów $x \in X$, dla których zdanie $\Phi(x)$ ma wartość logiczną T.

Funkcje zdaniowe

Definicja (Wykres funkcji zdaniowej)

Wykresem funkcji zdaniowej Φ nazywamy zbiór

$$S(\Phi) := \{x \in X : \Phi(x)\},$$

to znaczy zbiór wszystkich elementów $x \in X$, dla których zdanie $\Phi(x)$ ma wartość logiczną T.

Przykłady

- $X = \mathbb{R}$, $\Phi(x) \equiv (x = x)$, $S(\Phi) = \mathbb{R}$
- $X = \mathbb{R}$, $\Phi(x) \equiv (x \neq x)$, $S(\Phi) = \emptyset$
- $X = (0, +\infty)$, $\Phi(x) \equiv \boxed{(x^2 \geqslant 2x)}$, $S(\Phi) = \langle 2, +\infty)$ $\quad x(x-2) \geq 0$
- $X = \mathbb{N}$, $\Phi(x) \equiv (x^2 < 2)$, $S(\Phi) = \{1\}$

$\mathbb{N} = \{1, 2, \ldots\}$

Funkcje zdaniowe

Definicja (Funkcja zdaniowa wielu zmiennych)

Funkcją zdaniową n zmiennych nazywamy wyrażenie postaci $\Phi(x_1, \ldots, x_n)$, które dla dowolnych wartości $\underbrace{x_1 \in X_1}, \ldots, x_n \in X_n$ staje się zdaniem logicznym.

Funkcje zdaniowe

Definicja (Funkcja zdaniowa wielu zmiennych)

Funkcją zdaniową n zmiennych nazywamy wyrażenie postaci $\Phi(x_1, \ldots, x_n)$, które dla dowolnych wartości $x_1 \in X_1, \ldots, x_n \in X_n$ staje się zdaniem logicznym.

Definicja (Wykres funkcji zdaniowej wielu zmiennych)

Wykresem funkcji zdaniowej $\Phi(x_1, \ldots, x_n)$ nazywamy zbiór

$$S(\Phi) := \{x_1 \in X_1, \ldots, x_n \in X_n \colon \Phi(x_1, \ldots, x_n)\}.$$

Kwantyfikatory

Definicja (Kwantyfikator ogólny)

Zdanie

$$\text{dla każdego } x \text{ zachodzi } \Phi(x)$$

zapisujemy w postaci

$$\boxed{\bigwedge_x \Phi(x),}$$

$$\bigwedge_x \overbrace{(x = x)}^{\Phi(x)}$$

zdanie

a symbol $\bigwedge$ nazywamy **kwantyfikatorem ogólnym**.

Kwantyfikatory

Definicja (Kwantyfikator ogólny)

Zdanie

$$\text{dla każdego } x \text{ zachodzi } \Phi(x)$$

zapisujemy w postaci

$$\bigwedge_x \Phi(x),$$

a symbol $\bigwedge$ nazywamy **kwantyfikatorem ogólnym**.

Jeżeli X jest zakresem zmienności funkcji Φ, to możemy również pisać

$$\bigwedge_{x \in X} \Phi(x). \qquad \bigwedge_{x \in \mathbb{R}} (x = x)$$

Kwantyfikatory

Definicja (Kwantyfikator ogólny)

Zdanie

$$\text{dla każdego } x \text{ zachodzi } \Phi(x)$$

zapisujemy w postaci

$$\bigwedge_{x} \Phi(x),$$

a symbol $\bigwedge$ nazywamy **kwantyfikatorem ogólnym**.

Jeżeli X jest zakresem zmienności funkcji Φ, to możemy również pisać

$$\bigwedge_{x \in X} \Phi(x).$$

Czasami zamiast $\bigwedge$ piszemy również $\forall$. for all

Kwantyfikatory

Definicja (Kwantyfikator szczegółowy)

Zdanie

$$\text{istnieje taki } x \text{, że zachodzi } \Phi(x)$$

zapisujemy w postaci

$$\bigvee_{x} \Phi(x),$$

a symbol $\bigvee$ nazywamy **kwantyfikatorem szczegółowym**.

Kwantyfikatory

Definicja (Kwantyfikator szczegółowy)

Zdanie

$$\text{istnieje taki } x, \text{ że zachodzi } \Phi(x)$$

zapisujemy w postaci

$$\bigvee_{x} \Phi(x),$$

a symbol $\bigvee$ nazywamy **kwantyfikatorem szczegółowym**.

Jeżeli X jest zakresem zmienności funkcji Φ, to możemy również pisać

$$\bigvee_{x \in X} \Phi(x).$$

Kwantyfikatory

Definicja (Kwantyfikator szczegółowy)

Zdanie

$$\text{istnieje taki } x\text{, że zachodzi } \Phi(x)$$

zapisujemy w postaci

$$\bigvee_{x} \Phi(x),$$

a symbol $\bigvee$ nazywamy **kwantyfikatorem szczegółowym**.

Jeżeli X jest zakresem zmienności funkcji Φ, to możemy również pisać

$$\bigvee_{x \in X} \Phi(x).$$

Czasami zamiast $\bigvee$ piszemy $\exists$. exists

Kwantyfikatory ograniczone

Jeżeli A jest podzbiorem zakresu zmienności funkcji zdaniowej $\Phi(x)$, to

$$\bigwedge_{x}[x \in A \Rightarrow \Phi(x)] \qquad \text{zapisujemy w postaci} \qquad \boxed{\bigwedge_{x \in A} \Phi(x),}$$

a

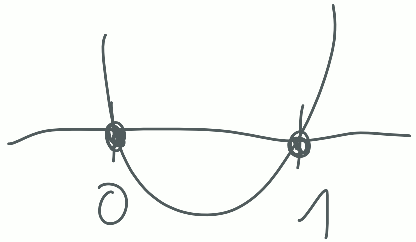
$$\bigvee_{x}[x \in A \Rightarrow \Phi(x)] \qquad \text{zapisujemy w postaci} \qquad \bigvee_{x \in A} \Phi(x).$$

Przykłady

$\phi(x)$

- $\rightsquigarrow$ $\displaystyle \boxed{\bigvee_{x\in\mathbb{R}} x^3 = 1}$ T
- $\rightsquigarrow$ $\displaystyle \bigvee_{x\in\mathbb{R}} x^2 = -1$ F
- $\rightsquigarrow$ $\displaystyle \bigvee_{x\in\mathbb{N}} x^2 = 2$ F
- $\rightsquigarrow$ $\displaystyle \boxed{\bigwedge_{x\in\mathbb{R}} x + 1 > \sqrt[3]{x}}$ F $x = -8$ -7 $\cancel{x}$ -2
- $\rightsquigarrow$ $\displaystyle \bigwedge_{x\in\mathbb{Z}} x^2 - x \geqslant 0$ T

$x(x-1) \geq 0$



Zmienne wolne i związane

$$\bigvee_y \bigwedge_x \phi(x,y), \quad \bigwedge_x \bigwedge_y \phi(x,y), \quad \bigwedge_x \bigvee_y \phi(x,y)$$

Niech $\Phi(x, y)$ będzie funkcją zdaniową dwóch zmiennych x i y.

Zmienne wolne i związane

Niech $\Phi(x, y)$ będzie funkcją zdaniową dwóch zmiennych x i y.

Wyrażenie

$$\overset{\Psi(y)}{\boxed{\bigwedge_x \Phi(x, y)}} \quad \text{lub} \quad \overset{\Psi(y)}{\boxed{\bigvee_x \Phi(x, y)}}$$

jest funkcją zdaniową jednej zmiennej y.

Zmienne wolne i związane

Niech $\Phi(x, y)$ będzie funkcją zdaniową dwóch zmiennych x i y.

Wyrażenie

$$\bigwedge_x \Phi(x, y) \qquad \text{lub} \qquad \bigvee_x \Phi(x, y)$$

jest funkcją zdaniową jednej zmiennej y.

Zmienną x nazywamy zmienną **związaną**, a y zmienną **wolną**.

Przykłady

- $\Phi(y) \equiv \left(\bigvee_{x \in \mathbb{R}} xy = 1 \right),\ y \in \mathbb{R}$

- $\Psi(x) \equiv \left(\bigwedge_{y \in \mathbb{R}} y^2 > x \right),\ x \in \mathbb{R}$

Przykłady

$$x = \frac{1}{y}$$

$\rightsquigarrow$ $\Phi(y) \equiv \left(\bigvee_{x\in\mathbb{R}} xy = 1 \right)$, $y \in \mathbb{R}$

$\rightsquigarrow$ $\Psi(x) \equiv \left(\bigwedge_{y\in\mathbb{R}} y^2 > x \right)$, $x \in \mathbb{R}$

$$S(\Phi) = \mathbb{R} \setminus \{0\}$$

$$\Phi(0) = \bigvee_{x\in\mathbb{R}} x \cdot 0 \overset{0}{=} 1$$

$$\Downarrow$$

$$0 \notin S(\Phi)$$

Jakie są wykresy funkcji Φ i Ψ?

$$S(\Psi) = (-\infty, 0)$$

$$x \geqslant 0 \quad , \quad \bigwedge_{y\in\mathbb{R}} y^2 > x \quad F$$

$$y = 0 \Rightarrow y^2 = 0 \cancel{>} x$$

Przykłady

- $\rightsquigarrow$ $\Phi(y) \equiv \left(\bigvee_{x \in \mathbb{R}} xy = 1 \right),\ y \in \mathbb{R}$
- $\rightsquigarrow$ $\Psi(x) \equiv \left(\bigwedge_{y \in \mathbb{R}} y^2 > x \right),\ x \in \mathbb{R}$

Jakie są wykresy funkcji Φ i Ψ?

- $\rightsquigarrow$ $S(\Phi) = \mathbb{R} \setminus \{0\}$

Przykłady

- $\rightsquigarrow$ $\Phi(y) \equiv \left(\bigvee_{x \in \mathbb{R}} xy = 1 \right),\ y \in \mathbb{R}$
- $\rightsquigarrow$ $\Psi(x) \equiv \left(\bigwedge_{y \in \mathbb{R}} y^2 > x \right),\ x \in \mathbb{R}$

Jakie są wykresy funkcji Φ i Ψ?

- $\rightsquigarrow$ $S(\Phi) = \mathbb{R} \setminus \{0\}$
- $\rightsquigarrow$ $S(\Psi) = (-\infty, 0)$

Prawa rachunku kwantyfikatorów

$\rightsquigarrow$ **Prawa de Morgana**

$$\neg\left(\phi(x_1)\wedge\phi(x_2)\wedge\phi(x_3)\wedge\ldots\right)\equiv\left(\neg\phi(x_1)\vee\neg\phi(x_2)\ldots\right)$$

$$\neg\left[\bigwedge_x \Phi(x)\right] \equiv \bigvee_x \neg\Phi(x), \qquad \neg(p\wedge q)\equiv\neg p\vee\neg q$$

$$\neg\left[\bigvee_x \Phi(x)\right] \equiv \bigwedge_x \neg\Phi(x).$$

$x\in\mathbb{R}$

$$\phi(x)\equiv x\in\langle 0,1\rangle$$

$$\neg\bigwedge_{x\in\mathbb{R}} x\in\langle 0,1\rangle \equiv \bigvee_{x\in\mathbb{R}} x\notin\langle 0,1\rangle$$

Prawa rachunku kwantyfikatorów

⇝ Prawa de Morgana

$$\neg\Big[\bigwedge_x \Phi(x)\Big] \equiv \bigvee_x \neg\Phi(x),$$

$$\neg\Big[\bigvee_x \Phi(x)\Big] \equiv \bigwedge_x \neg\Phi(x).$$

⇝ Prawa przemienności

$$\bigwedge_x \bigwedge_y \Phi(x,y) \equiv \bigwedge_y \bigwedge_x \Phi(x,y) \equiv \bigwedge_{x,y} \Phi(x,y),$$

$$\bigvee_x \bigvee_y \Phi(x,y) \equiv \bigvee_y \bigvee_x \Phi(x,y) \equiv \bigvee_{x,y} \Phi(x,y).$$

Prawa rachunku kwantyfikatorów

⇝ Prawa de Morgana

$$\neg\left[\bigwedge_x \Phi(x)\right] \equiv \bigvee_x \neg\Phi(x),$$

$$\neg\left[\bigvee_x \Phi(x)\right] \equiv \bigwedge_x \neg\Phi(x).$$

$$\bigwedge_y \bigvee_x \ldots \not\equiv \bigvee_x \bigwedge_y \ldots$$

⇝ Prawa przemienności

$$\bigwedge_x \bigwedge_y \Phi(x,y) \equiv \bigwedge_y \bigwedge_x \Phi(x,y) \equiv \bigwedge_{x,y} \Phi(x,y),$$

$$\bigvee_x \bigvee_y \Phi(x,y) \equiv \bigvee_y \bigvee_x \Phi(x,y) \equiv \bigvee_{x,y} \Phi(x,y).$$

⇝

$$\bigvee_x \bigwedge_y \Phi(x,y) \Rightarrow \bigwedge_y \bigvee_x \Phi(x,y).$$

$\cancel{\Leftarrow}$

x jest niezależne od y

x może zależeć od y