Rachunek zdań

Materiały pomocnicze do wykładu

wykładowca: **dr Magdalena Kacprzak**

RACHUNEK ZDAŃ

Zdania

Definicja

Zdanie

jest to stwierdzenie w języku naturalnym, któremu można przypisać wartość **prawdy** lub **fałszu** (ale nie obie wartości jednocześnie).

Zgodnie z notacją stosowaną w większości języków programowania będziemy używać liczby 1 dla oznaczenia prawdy i liczby 0 dla oznaczenia fałszu.

Czy podane wyrażenie jest zdaniem?

Czy program P „zapętla się” dla danej wejściowej x=1? NIE

Czy zdam egzamin z matematyki? NIE

Napisz ten algorytm! NIE

x+y=2 NIE

Czy podane wyrażenie jest zdaniem?

2+2=5 TAK

W dowolnym zbiorze uporządkowanym, element najmniejszy jest też elementem minimalnym. TAK

Jeżeli zbiór jest uporządkowany liniowo, to posiada element największy i najmniejszy. TAK

Które zdanie jest prawdziwe, a które fałszywe?

2+2=5 0

W dowolnym zbiorze uporządkowanym, element najmniejszy jest też elementem minimalnym. 1

Jeżeli zbiór jest uporządkowany liniowo, to posiada element największy i najmniejszy. 0

Które zdanie jest prawdziwe, a które fałszywe?

$(n+1)! = O(3^{n+1})$ 0

Każda funkcja różnowartościowa jest funkcją „na”. 0

Operacja składania relacji nie jest przemienna. 1

Spójniki logiczne

$\neg$ - negacja (czyt. „nieprawda, że”)

$\wedge$ - koniunkcja (czyt. „i”)

$\vee$ - alternatywa (czyt. „lub”)

$\rightarrow$ - implikacja (czyt. „jeśli ..., to...”)

$\leftrightarrow$ - równoważność (czyt. „wtedy i tylko wtedy, gdy”, w skrócie „wttw”)

Przykłady

$2 \cdot 3 > 5$ i 1 jest liczbą pierwszą.

p - $2 \cdot 3 > 5$
q - 1 jest liczbą pierwszą

$$p \wedge q$$

Przykłady

Jeśli r jest relacją przeciwsymetryczną,
to r jest relacją przeciwzwrotną.

p - jest relacją przeciwsymetryczną,
q - jest relacją przeciwzwrotną.

$$p \to q$$

Przykłady

Zostanę w domu lub pójdę na wykład.

p - zostanę w domu
q - pójdę na wykład

$$p \vee q$$

Składnia

Definicja

Niech V będzie zbiorem

zdań elementarnych

(nazywać je będziemy zmiennymi zdaniowymi).

Zbiór wyrażeń poprawnych, tzw.

formuł rachunku zdań,

jest to najmniejszy (w sensie inkluzji) zbiór wyrażeń zawierający V i taki, że jeśli p i q są zdaniami, to wyrażenia:

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

są zdaniami.

Które wyrażenie jest formułą rachunku zdań?

$\neg (p \wedge q) \leftrightarrow s \vee t$ TAK

$p \neg p \wedge q$ NIE

$(s \wedge t) \vee (q \rightarrow (s \leftrightarrow t))$ TAK

Priorytet operacji

$$\neg\ ,\ \wedge\ ,\ \vee\ ,\ \rightarrow\ ,\ \leftrightarrow$$

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

$$s \wedge t \rightarrow s \equiv ((s \wedge t) \rightarrow s)$$

Semantyka

Wartościowanie

Wartościowaniem nazywamy funkcję, która każdej zmiennej zdaniowej przyporządkowuje wartość logiczną 0 lub 1.

Funkcję taką, w naturalny sposób można rozszerzyć na zbiór wszystkich formuł rachunku zdań.

Przykład

Dane są zdania p, q, r, s.

Przykładowe wartościowanie w:

$w(p)=1$, $w(q)=0$, $w(r)=0$, $w(s)=1$,

Wartościowanie c.d

Mając dane wartościowanie zmiennych (wartości zdań prostych) można określić wartość logiczną zdań złożonych. Podaną na kolejnym slajdzie tablicę nazywamy

matrycą logiczną

Definiuje ona sens operacji zdaniotwórczych i pozwala obliczyć wartość dowolnych zdań złożonych (formuł rachunku zdań).

Wartościowanie c.d

Wartość logiczną zdania złożonego możemy obliczyć wyznaczając po kolei wartości logiczne zdań prostszych, z których jest ono zbudowane.

Matryca logiczna

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Wyznacz wartość logiczną zdania

Jeśli $(2 \cdot 3 > 5)$ i 1 jest liczbą pierwszą, to $(2+2=5)$.

p - $2 \cdot 3 > 5$
q - 1 jest liczbą pierwszą
r – $2+2=5$

$$(p \wedge q) \to r$$

$$w(p)=1,\ w(q)=0,\ w(r)=0$$

$$w(p \wedge q) = 0$$

$$w((p \wedge q) \to r)=1$$

TAUTOLOGIE

Tautologia

Zdanie złożone, którego wartością jest prawda, niezależnie od wartości zmiennych zdaniowych w nim występujących, nazywamy

tautologią

lub

prawem rachunku zdań.

Następujące formuły są tautologiami rachunku zdań

- $(a \to a)$ - prawo tożsamości dla implikacji
- $(a \vee \neg a)$ - prawo wyłączonego środka
- $\neg(\neg a) \leftrightarrow a$ - prawo podwójnego przeczenia
- $\neg a \to (a \to b)$ - prawo Dunsa Scotusa
- $(\neg a \to a) \to a$ - prawo Claviusa

Następujące formuły są tautologiami rachunku zdań

- $\neg(\neg a) \leftrightarrow a$ - prawo podwójnego przeczenia

- $(a \wedge b) \leftrightarrow (b \wedge a)$ - prawo przemienności
- $(a \vee b) \leftrightarrow (b \vee a)$ - prawo przemienności

- $((a \wedge b) \wedge c) \leftrightarrow (a \wedge (b \wedge c))$ - prawo łączności
- $(a \wedge (b \vee c)) \leftrightarrow ((a \wedge b) \vee (a \wedge c))$ - prawo rozdzielności

Następujące formuły są tautologiami rachunku zdań

- $(a \lor a) \leftrightarrow a$ - prawo idempotentności
- $(a \land a) \leftrightarrow a$ - prawo idempotentności

- $\neg(a \lor b) \leftrightarrow (\neg a \land \neg b)$ – prawo de Morgana
- $\neg(a \land b) \leftrightarrow (\neg a \lor \neg b)$ – prawo de Morgana

Następujące formuły są tautologiami rachunku zdań

- $(a \rightarrow b) \leftrightarrow (\neg b \rightarrow \neg a)$ - prawo kontrapozycji
- $(a \rightarrow b) \leftrightarrow (\neg a \vee b)$ - określenie implikacji za pomocą alternatywy
- $a \rightarrow (a \vee b)$ - wprowadzenie alternatywy
- $(a \wedge b) \rightarrow a$ - opuszczenie koniunkcji

Sprawdź, czy formuła jest tautologią

$(a \rightarrow b) \rightarrow (\neg a \vee b)$

a	b	$\neg a$	$\neg a \vee b$	$a \rightarrow b$	$(a \rightarrow b) \rightarrow (\neg a \vee b)$
0	0				
0	1				
1	0				
1	1				

Sprawdź, czy formuła jest tautologią

$(a \to b) \to (\neg a \lor b)$

a	b	$\neg a$	$\neg a \lor b$	$a \to b$	$(a \to b) \to (\neg a \lor b)$
0	0	1			
0	1	1			
1	0	0			
1	1	0			

Sprawdź, czy formuła jest tautologią

$(a \to b) \to (\neg a \vee b)$

a	b	$\neg a$	$\neg a \vee b$	$a \to b$	$(a \to b) \to (\neg a \vee b)$
0	0	1	1		
0	1	1	1		
1	0	0	0		
1	1	0	1		

Sprawdź, czy formuła jest tautologią

$(a \rightarrow b) \rightarrow (\neg a \vee b)$

a	b	$\neg a$	$\neg a \vee b$	$a \rightarrow b$	$(a \rightarrow b) \rightarrow (\neg a \vee b)$
0	0	1	1	1	
0	1	1	1	1	
1	0	0	0	0	
1	1	0	1	1	

Sprawdź, czy formuła jest tautologią

$(a \to b) \to (\neg a \vee b)$

a	b	$\neg a$	$\neg a \vee b$	$a \to b$	$(a \to b) \to (\neg a \vee b)$
0	0	1	1	1	1
0	1	1	1	1	1
1	0	0	0	0	1
1	1	0	1	1	1

Zdanie sprzeczne

Zdanie złożone, którego wartością jest fałsz, niezależnie od wartości zmiennych zdaniowych w nim występujących, nazywamy

zdaniem sprzecznym.

Przykład

$(\neg a \vee b) \wedge \neg(a \to b)$

a	b	$\neg a$	$\neg a \vee b$	$a \to b$	$\neg(a \to b)$	$(\neg a \vee b) \wedge \neg(a \to b)$
0	0	1	1	1	0	0
0	1	1	1	1	0	0
1	0	0	0	0	1	0
1	1	0	1	1	0	0

Zdania logicznie równoważne

Dwa zdania złożone p i q są zdaniami

logicznie równoważnymi,

jeśli mają takie same wartości logiczne dla wszystkich kombinacji wartości logicznych ich zmiennych zdaniowych p i q.

Przykład

Formuły $\neg(a \vee b)$ i $(\neg a \wedge \neg b)$ są logicznie równoważne.

a	b	$\neg a$	$\neg b$	$\neg a \wedge \neg b$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	0	0	0

a	b	$a \vee b$	$\neg(a \vee b)$
0	0	0	1
0	1	1	0
1	0	1	0
1	1	1	0

Twierdzenie

Jeżeli formuła zależna od zmiennych zdaniowych $p_1, \ldots, p_n$ jest tautologią, to wstawiając na miejsce zmiennych zdaniowych dowolne zdania otrzymamy zawsze zdanie prawdziwe. Co więcej, jeśli na miejsce zmiennych wstawimy dowolne schematy zdań (dowolne formuły), to otrzymany schemat będzie również tautologią.

Przykład

Formuła $\neg(a \vee b) \leftrightarrow (\neg a \wedge \neg b)$ jest tautologią.

Wstawmy teraz w miejsce a zdanie

„x jest elementem A",

a w miejsce b zdanie

„x jest elementem B".

Otrzymamy zdanie prawdziwe postaci:

"nie jest prawdą, że x jest elementem A lub x jest elementem B wtedy i tylko wtedy, gdy x nie jest elementem A i x nie jest elementem B".

Po uproszczeniu otrzymamy prawo algebry zbiorów:

jeśli x nie należy do sumy zbiorów A i B, to x nie należy ani do A ani do B.

Przykład

Formuła $\neg(a \vee b) \leftrightarrow (\neg a \wedge \neg b)$ jest tautologią.

Wstawmy teraz w miejsce a zdanie

$$p \rightarrow q$$

a w miejsce b zdanie

$$\neg t$$

Otrzymamy zdanie prawdziwe postaci:

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

Twierdzenie

Jeśli zdanie złożone P zawiera zdanie Q i jeśli zdanie Q zastąpimy zdaniem logicznym z nim równoważnym, to otrzymane zdanie złożone jest logicznie równoważne ze zdaniem P.

Przykład

Rozważmy zdanie

$$(\neg(a \vee b)) \leftrightarrow r.$$

Wiemy, że formuły $\neg(a \vee b)$ i $(\neg a \wedge \neg b)$ są logicznie równoważne.

Zastąpmy więc zdanie $\neg(a \vee b)$ zdaniem $(\neg a \wedge \neg b)$. Wówczas otrzymamy zdanie logicznie równoważne:

$$(\neg a \wedge \neg b) \leftrightarrow r.$$

Sprzeczność i niesprzeczność

Zbiór niesprzeczny

Zbiór zdań (formuł) X jest

niesprzeczny

wtedy i tylko wtedy, gdy istnieje taka interpretacja zdań ze zbioru X, tzn. taki układ *w* wartości zmiennych zdaniowych występujących w tych formułach, że $w(\alpha) = 1$ dla wszystkich formuł $\alpha \in X$.

Przykład

Załóżmy, że dana wejściowa x programu P musi spełniać podane warunki:

- x nie jest liczbą parzystą i x nie jest liczbą pierwszą,
- x nie jest liczbą parzystą,
- jeśli x jest liczbą parzystą, to x jest liczbą pierwszą.

Czy zbiór danych wejściowych jest niepusty?

Przykład

Wprowadźmy oznaczenia:

a – x jest liczbą parzystą

b – x jest liczbą pierwszą.

Rozważmy teraz zbiór formuł

$\{\neg a \wedge \neg b,\ \neg a,\ a \rightarrow b\}.$

Czy istnieje wartościowanie spełniające jednocześnie wszystkie powyższe formuły?

Przykład

Jeśli przyjmiemy, że

$$w(a)=0,\ w(b)=0,$$

to

$$w(\neg a \wedge \neg b)=1,\ w(\neg a)=1,\ w(a \rightarrow b)=1,$$

czyli zbiór $\{\neg a \wedge \neg b,\ \neg a,\ a \rightarrow b\}$ jest niesprzeczny.

Zatem zbiór danych wejściowych programu P jest niepusty.

Przykład

Załóżmy, że dana wejściowa x programu P musi spełniać podane warunki:

- jeśli x jest liczbą naturalną, to x jest liczbą większą od 10 i x jest liczbą parzystą,
- x jest liczbą naturalną i x nie jest liczbą parzystą.

Czy zbiór danych wejściowych jest niepusty?

Przykład

Wprowadzamy oznaczenia:

a - x jest liczbą naturalną,

b - x jest liczbą większą od 10,

c - x jest liczbą parzystą

i sprawdzamy, czy zbiór formuł

$$\{a \rightarrow (b \wedge c),\ \ a \wedge \neg c\}$$

jest niesprzeczny.

Przykład

Zbiór NIE jest niesprzeczny,
bo nie istnieje wartościowanie
spełniające jednocześnie formuły

$a \rightarrow (b \wedge c)$, $a \wedge \neg c$.

Reguły wnioskowania

Definicja

Regułą dowodzenia
(inaczej zwaną **regułą wnioskowania**)
nazywamy przekształcenie postaci

$$\frac{\alpha_1, \ldots, \alpha_n}{\beta}$$

które skończonemu zbiorowi formuł $\alpha_1, \ldots, \alpha_n$, zwanych **przesłankami**, przyporządkowuje formułę β zwaną **wnioskiem**, w taki sposób, że przy dowolnie wybranych wartościach zmiennych występujących w formułach $\alpha_1, \ldots, \alpha_n$, β, jeśli przesłanki są zdaniami prawdziwymi, to wniosek też jest zdaniem prawdziwym. Będziemy wtedy mówili, że β jest logiczną konsekwencją formuł $\alpha_1, \ldots, \alpha_n$.

Reguła MODUS PONENS

$$\frac{\alpha,\ \alpha \to \beta}{\beta}$$

Przykład

Przesłanki:

- Jeśli otrzymam 45 punktów ze sprawdzianów, to zaliczę ćwiczenia.
- Otrzymałem 45 punktów ze sprawdzianów.

Wniosek: Zaliczę ćwiczenia.

Poprawność reguły **MODUS PONENS**

Załóżmy, że $w(\alpha)=1$ i $w(\alpha \to \beta)=1$. Wówczas zachodzi jeden z przypadków:

(1) $w(\alpha)=1$ i $w(\alpha)=w(\beta)=1$, czyli $w(\beta)=1$,

(2) $w(\alpha)=1$ i $w(\alpha)=w(\beta)=0$ – sprzeczność,

(3) $w(\alpha)=1$ i $w(\alpha)=0$, $w(\beta)=1$– sprzeczność.

Ostatecznie jeśli $w(\alpha)=1$ i $w(\alpha \to \beta)=1$, to $w(\beta)=1$.

Reguły wnioskowania

reguła sylogizmu warunkowego (hipotecznego)

$$\frac{\alpha \to \beta,\ \beta \to \gamma}{\alpha \to \gamma}$$

Przykład

Przesłanki:

- Jeśli otrzymam 90 punktów ze sprawdzianów, to zaliczę ćwiczenia na ocenę bdb.
- Jeśli zaliczę ćwiczenia na ocenę bdb, to będę zwolniony z egzaminu.

Wniosek: Jeśli otrzymam 90 punktów ze sprawdzianów, to będę zwolniony z egzaminu.

Reguły wnioskowania

reguła modus tollens

$$\frac{\alpha \to \beta,\ \neg \beta}{\neg \alpha}$$

Przykład

Przesłanki:

- Jeśli otrzymam 90 punktów ze sprawdzianów, to będę zwolniony z egzaminu.
- Nie jestem zwolniony z egzaminu.

Wniosek: Nie otrzymałem 90 punktów ze sprawdzianów.

Reguły wnioskowania

reguła wprowadzania alternatywy

$$\frac{\alpha}{\alpha \vee \beta}$$

reguła opuszczenia koniunkcji

$$\frac{\alpha \wedge \beta}{\alpha}$$

Reguły wnioskowania

reguła wprowadzania koniunkcji

$$\frac{\alpha,\ \beta}{\alpha \wedge \beta}$$

reguła modus ponendo tollens (sylogizm alternatywny)

$$\frac{\alpha \vee \beta,\ \neg\alpha}{\beta}$$

Reguły wnioskowania

dylemat konstrukcyjny

$$\frac{\alpha \to \beta,\ \neg\alpha \to \beta}{\beta}$$

dylemat destrukcyjny

$$\frac{\alpha \to \beta,\ \alpha \to \neg\beta}{\neg\alpha}$$

Reguły wnioskowania

prawo kompozycji dla koniunkcji

$$\frac{\alpha \to \beta,\ \gamma \to \delta}{\alpha \wedge \gamma \to \beta \wedge \delta}$$

prawo kompozycji dla alternatywy

$$\frac{\alpha \to \beta,\ \gamma \to \delta}{\alpha \vee \gamma \to \beta \vee \delta}$$

Reguły wnioskowania

dowód niewprost (sprowadzenie do sprzeczności)

$$\frac{(\alpha \land \neg\beta) \rightarrow (\delta \land \neg\delta)}{\alpha \rightarrow \beta}$$

dowód niewprost (kontrapozycja)

$$\frac{(\alpha \land \neg\beta) \rightarrow \neg\alpha}{\alpha \rightarrow \beta}$$

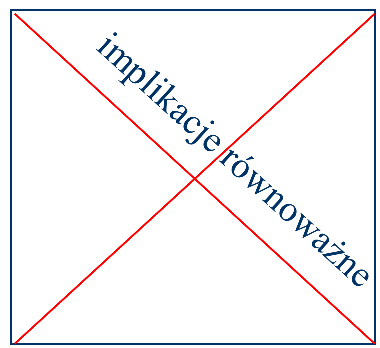
Kwadrat logiczny

implikacja prosta

$\alpha \to \beta$

implikacja odwrotna

$\beta \to \alpha$



$\neg\alpha \to \neg\beta$

implikacja przeciwna

$\neg\beta \to \neg\alpha$

implikacja przeciwstawna

Jeżeli implikacja $\alpha \to \beta$ jest twierdzeniem,
to α jest warunkiem wystarczającym na to, aby β,
a β warunkiem koniecznym na to, aby α.

Kwadrat logiczny

implikacja prosta

$\alpha \to \beta$

implikacja odwrotna

$\beta \to \alpha$

$\neg\alpha \to \neg\beta$

implikacja przeciwna

$\neg\beta \to \neg\alpha$

implikacja przeciwstawna

Dla dowodu twierdzenia $\alpha \leftrightarrow \beta$ wystarczy udowodnić jedną z par implikacji położonych przy sąsiadujących ze sobą wierzchołkach kwadratu logicznego.

Kwadrat logiczny

implikacja prosta

$\alpha \to \beta$

implikacja odwrotna

$\beta \to \alpha$

$\neg\alpha \to \neg\beta$

implikacja przeciwna

$\neg\beta \to \neg\alpha$

implikacja przeciwstawna

Na przykład:

$$\frac{\alpha \to \beta,\ \neg\alpha \to \neg\beta}{\alpha \leftrightarrow \beta}$$

Twierdzenie

Jeśli wszystkie przesłanki pewnej reguły wnioskowania są tautologiami, to wniosek w tej regule też jest tautologią.

Twierdzenie

Niech $\alpha_1, \ldots, \alpha_n, \beta$ będą formułami rachunku zdań.

Formuła $(\alpha_1 \wedge \ldots \wedge \alpha_n) \to \beta$ jest tautologią, wtedy i tylko wtedy, gdy

$$\frac{\alpha_1, \ldots, \alpha_n}{\beta}$$

jest regułą dowodzenia.

Przykład

Sprawdź, czy poprawne jest rozumowanie:

Jeśli daną wejściową programu P jest liczba 2, to program P ma obliczenie skończone i dana wyjściowa spełnia warunek W. Zatem jeśli dana wyjściowa nie spełnia warunku W, to daną wejściową programu P nie jest liczba 2.

Przykład

Sprawdź, czy poprawne jest rozumowanie:

Jeśli daną wejściową programu P jest liczba 2, to program P ma obliczenie skończone i dana wyjściowa spełnia warunek W. Zatem jeśli daną wejściową nie jest liczba 2, to program P nie ma obliczenia skończonego lub dana wyjściowa nie spełnia warunku W.

Przykład

Sprawdź, czy poprawne jest rozumowanie:

Jeśli daną wejściową programu P jest liczba 2, to program P ma obliczenie skończone i dana wyjściowa spełnia warunek W. Zatem jeśli program P ma obliczenie skończone i dana wyjściowa spełnia warunek W, to daną wejściową jest liczba 2.

Przykład

Sprawdź, czy poprawne jest rozumowanie:

Z faktu, że program P ma obliczenie skończone wynika, że dana wyjściowa programu P spełnia warunek W oraz z faktu, że program P ma obliczenie skończone wynika, że dana wyjściowa programu P nie spełnia warunku W. Zatem program P nie ma obliczenia skończonego.

Przykład

Sprawdź, czy poprawne jest rozumowanie:

Z faktu, że program P ma obliczenie skończone i dana wyjściowa programu P spełnia warunek W wynika, że program P nie ma obliczenia skończonego. Zatem jeśli program P ma obliczenie skończone, to dana wyjściowa nie spełnia warunku W.

Przykład

Sprawdź, czy poprawne jest rozumowanie:

Z faktu, że program P ma obliczenie skończone i dana wyjściowa programu P spełnia warunek W wynika, że program P nie ma obliczenia skończonego. Zatem jeśli program P nie ma obliczenia skończonego, to dana wyjściowa nie spełnia warunku W.

Przykład

Sprawdź, czy poprawne jest rozumowanie:

Z faktu, że daną wejściową programu P jest liczba 2 i dana wyjściowa programu P spełnia warunek W wynika, że program P ma obliczenie skończone i program P nie ma obliczenia skończonego. Zatem jeśli daną wejściową jest liczba 2, to dana wyjściowa nie spełnia warunku W.

Dowód

Definicja

Skończony ciąg formuł $\alpha_1, \ldots, \alpha_n$ nazywamy

dowodem

formuły α wtedy i tylko wtedy, gdy każda z formuł α_i (i=1,2...n) jest albo aksjomatem albo jest wnioskiem w regule modus ponens, w której przesłankami są formuły α_k i $(\alpha_k \rightarrow \alpha_i)$ występujące wcześniej w tym ciągu.

Metody dowodzenia

Metody dowodzenia

Przypuśćmy, że mamy zbiór założeń $Z_1, \ldots, Z_n$, z których chcemy wyprowadzić wniosek W. Wówczas możemy zastosować jedną z metod

- dowód wprost,
- dowód niewprost – kontrapozycja,
- dowód niewprost – sprowadzenie do sprzeczności.

Dowód wprost

$$Z_1 \wedge \ldots \wedge Z_n \Rightarrow W$$

Przykład

Pokażemy dowód zdania α ze zbioru założeń $\{\beta \wedge \gamma, \beta \vee \gamma \to \alpha\}$

(1) $\beta \wedge \gamma$ - założenie

(2) β - z (1) i prawa opuszczania koniunkcji

(3) $\beta \vee \gamma$ - z (2) i prawa wprowadzania alternatywy

(4) $\beta \vee \gamma \to \alpha$ - założenie

(5) α - z (3), (4) i reguły Modus Ponens

Dowód niewprost - kontrapozycja

$$\neg W \Rightarrow (\neg Z_1 \vee \ldots \vee \neg Z_n)$$

Dowód niewprost - kontrapozycja

Niech m,n $\in$N. Udowodnimy, że

jeśli $m+n \geq 11$, to $m \geq 6$ lub $n \geq 6$.

W tym celu dowodzimy kontrapozycji

jeśli $\neg(m \geq 6$ lub $n \geq 6)$, to $\neg(m+n \geq 11)$.

Dowód: Jeśli $\neg(m \geq 6$ lub $n \geq 6)$, to $m<6$ i $n<6$.

Wówczas, $m+n<11$,

czyli nie prawda, że $m+n \geq 11$.

Dowód niewprost – sprowadzenie do sprzeczności

$$(Z_1 \wedge \ldots \wedge Z_n) \wedge \neg W \Rightarrow (Q \wedge \neg Q)$$

Dowód niewprost – sprowadzenie do sprzeczności

Pokażemy, że formuła $((\alpha \wedge \beta) \to \gamma) \to (\alpha \to (\beta \to \gamma))$ jest tautologią.

Załóżmy, że istnieje wartościowanie w takie, że

$$w((\alpha \wedge \beta) \to \gamma) \to (\alpha \to (\beta \to \gamma))=0$$

Wówczas

(1) $w((\alpha \wedge \beta) \to \gamma))=1$

(2) $w(\alpha \to (\beta \to \gamma))=0$

Dowód niewprost – sprowadzenie do sprzeczności

(1) $w((\alpha \wedge \beta) \to \gamma))=1$
(2) $w(\alpha \to (\beta \to \gamma))=0$

(3) $w(\alpha)=1$– z (2)

(4) $w(\beta \to \gamma)=0$ – z (2)

(5) $w(\beta)=1$ – z (4)

(6) $w(\gamma)=0$ – z (4)

(7) $w(\alpha \wedge \beta)=1$ – z (3) i (5)

(8) $w((\alpha \wedge \beta) \to \gamma)=0$ – z (6) i (7)
– sprzeczność z (1)

Przykład dowodu nie wprost

Twierdzenie: pierwiastek trzeciego stopnia z 5 jest liczbą niewymierną.

Dowód.

Załóżmy, że $\sqrt[3]{5} = \frac{p}{q}, \;\; p, q \in Z, \;\; q \neq 0$

Możemy przyjąć, że liczby całkowite p i q są względnie pierwsze.

Przykład dowodu nie wprost

Zatem

$$5=p^3/q^3,$$

czyli

$$5q^3=p^3.$$

Stąd p^3 jest podzielne przez 5 i w konsekwencji p jest podzielne przez 5, co możemy zapisać

$$p=5k,$$

gdzie k jest liczbą całkowitą.

Przykład dowodu nie wprost

Zatem $$5q^3=5^3k^3,$$
czyli
$$q^3=25k^3.$$
Stąd q^3 jest podzielne przez 5 i q jest podzielne przez 5.

Otrzymujemy sprzeczność z założeniem, że liczby p i q są względnie pierwsze.

Przykład dowodu nie wprost

Twierdzenie: Jest nieskończenie wiele liczb pierwszych.

Dowód. Załóżmy, że mamy n liczb pierwszych:

$$p_1, p_2, \ldots, p_n.$$

Rozważmy liczbę

$$a = (p_1 \cdot p_2 \cdot \ldots \cdot p_n) + 1.$$

Liczba ta nie dzieli się przez żadną z liczb pierwszych $p_1, p_2, \ldots, p_n$.

Przykład dowodu nie wprost

Z Podstawowego twierdzenia arytmetyki, istnieje liczba pierwsza (inna niż wymienione) dzieląca liczbę a. Zatem nie wymieniliśmy wszystkich liczb pierwszych. Otrzymujemy sprzeczność.

Podstawowe twierdzenie arytmetyki:
Każdą liczbę naturalną większą od 1 można jednoznacznie przedstawić w postaci iloczynu liczb pierwszych.

Zadania

Zadanie 1

Udowodnij, że jeśli relacje r i s określone w zbiorze U są zwrotne, to relacja r ° s określona w zbiorze U też jest zwrotna.

r i s są zwrotne $\Rightarrow$ r ° s jest zwrotna

Metoda wprost

Załóżmy, że relacje r i s są zwrotne. Pokażemy, że relacja $r \circ s$ też jest zwrotna.

Jeśli r jest relacją zwrotną, to dla każdego $u \in U$ zachodzi $(u,u) \in r$. Podobnie jeśli s jest relacją zwrotną, to dla każdego $u \in U$ zachodzi $(u,u) \in s$. Zatem istnieje $z=u$ takie, że $(u,z) \in r$ i $(z,u) \in s$. Stąd dla każdego $u \in U$, $(u,u) \in r \circ s$, czyli relacja $r \circ s$ jest zwrotna.

Metoda wprost

Stąd dla każdego $u \in U$,

$$(u,u) \in r \circ s,$$

czyli relacja $r \circ s$ jest relacją zwrotną w zbiorze U.

Zadanie 2

Udowodnij, że jeśli relacja r określona w zbiorze U jest przeciwsymetryczna, to jest w tym zbiorze przeciwzwrotna.

przeciwsymetryczna $\Rightarrow$ przeciwzwrotna

Metoda niewprost (kontrapozycja)

Pokażemy, że jeśli r nie jest relacją przeciwzwrotną w zbiorze U, to r nie jest relacją przeciwsymetryczną w zbiorze U.

$\neg$ **przeciwzwrotna** $\Rightarrow$ $\neg$ **przeciwsymetryczna**

Metoda niewprost (kontrapozycja)

Załóżmy, że r nie jest relacją przeciwzwrotną w zbiorze U. Zatem istnieje $a \in U$ takie, że a r a. Przyjmijmy teraz, że x=y=a. Zatem x r y i y r x. Stąd nie jest prawdą, że dla każdego $x,y \in U$ jeśli x r y, to nie prawda, że y r x.

Zatem r nie jest relacją przeciwsymetryczną w zbiorze U.

Zadanie 3

Udowodnij, że jeśli relacja r określona w zbiorze U jest jednocześnie symetryczna i antysymetryczna, to jest w zbiorze U przechodnia.

symetryczna $\wedge$ antysymetryczna $\Rightarrow$ przechodnia

Metoda niewprost (doprowadzenie do sprzeczności)

Pokażemy, że jednoczesne założenie, że relacja jest symetryczna, antysymetryczna i nie jest przechodnia, prowadzi do sprzeczności

$$\textbf{symetryczna} \wedge \textbf{antysymetryczna} \wedge \neg\textbf{przechodnia} \Rightarrow \mathbf{Q} \wedge \neg \mathbf{Q}$$

Metoda niewprost (doprowadzenie do sprzeczności)

Załóżmy, że relacja r jest symetryczna, antysymetryczna i nie jest przechodnia w zbiorze U. Jeśli relacja r nie jest przechodnia, to istnieją elementy x,y,z zbioru U takie, że

$$(x,y)\in r \ \text{ i } (y,z)\in r \text{ i nieprawda, że } (x,z)\in r.$$

Metoda niewprost (doprowadzenie do sprzeczności)

Jeśli $(y,z)\in r$, to z symetryczności relacji r wynika, że $(z,y)\in r$. Dalej z antysymetryczności relacji r wynika, że $y=z$.

Mamy zatem

$$(x,y)\in r \text{ i } y=z.$$

Stąd wynika, że $(x,z)\in r$, co jest sprzeczne z założeniem, że $(x,z)\notin r$.

Zadanie 4

Sprawdź, czy z faktu, że relacja r określona w zbiorze U jest symetryczna wynika, że r nie jest relacją antysymetryczną w zbiorze U.

symetryczna $\Rightarrow \neg$ antysymetryczna ???

Kontrprzykład

Pokażemy, że istnieje relacja, która jest symetryczna i antysymetryczna jednocześnie.

Kontrprzykład

Niech r będzie relacją określoną w zbiorze liczb naturalnych taką, że dla każdego x,y,

x r y wttw x=y.

Zauważmy, że dla każdego x,y, jeśli x r y, to y r x oraz dla każdego x,y jeśli x r y i y r x, to x=y. Zatem r jest relacją symetryczną i antysymetryczną w zbiorze U.

Zadanie 5

Sprawdź, czy z faktu, że relacja r określona w zbiorze U jest symetryczna wynika, że r nie jest relacją przeciwysymetryczną w zbiorze U.

symetryczna $\Rightarrow \neg$ przeciwsymetryczna ???

Inne metody dowodzenia twierdzeń

- Przez litość – *Nie będę Państwa zamęczał dowodem...*.
- Przez sztuciec – *A nuż wyjdzie*.
- Przez przykład – *Widzą państwo? Działa*.
- Cybernetyczny - To automatycznie wynika z…
- Ezoteryczna – *Intuicyjnie czujemy, że...*.
- Lekkoatletyczna – *Rzut oka na tablice i widać...*.
- Satanistyczna – *Diabli wiedzą jak to udowodnić*.
- Humorystyczna – *Cały dowcip polega na tym...*.
- Teologiczna – *Co tu dowodzić? Wystarczy trochę wiary.*.