

Definicja:

Niech X będzie zbiorem niepustym.

Zbiór ten będziemy nazywać **alfabetem**.

Skończony ciąg elementów alfabetu X będziemy nazywać **słowem**
a liczbę elementów tego ciągu nazywamy **długością słowa**.

Na zbiorze wszystkich słów w alfabecie X definiujemy operację mnożenia słów, która polega na dopisywaniu do pierwszego słowa drugiego słowa.

Niech $*$ będzie znakiem tej operacji binarnej.

Wtedy mamy, na przykład,

$$x * yy = xyy, xy * xxxyyxy = xyxxxxyxy.$$

Jest rzeczą oczywistą, że operacja $*$ w zbiorze słów jest łączna oraz dla każdego słowa w w alfabecie X mamy

$$1 * w = w = w * 1.$$

A więc zbiór wszystkich słów w alfabecie X z operacją $*$ jest monoidem.

Monoid ten oznaczamy symbolem X^* i nazywamy **monoidem wolnym z alfabetem X** .

Definicja:

Językiem formalnym L nad alfabetem Σ nazywamy podzbiór monoidu wolnego Σ^* , a więc pewien zbiór słów tego alfabetu. Zarówno w matematyce jak i w komputerologii słowo “formalny” bywa zwykle pomijane i mówimy zwyczajnie o językach.

Definicja:

Niech Σ będzie dowolnym alfabetem i niech L będzie ustalonym językiem nad tym alfabetem.

Regułą wnioskowania nazywamy relację $r \subset 2^L \times L$ taką, że istnieje pewna liczba naturalna $n \in \mathbb{N}$, że o ile $|\Pi| = n$, to $(\Pi, A) \in r$. Zbiór Π zwiemy zbiorem **przesłanek**, a A **wnioskiem** reguły r .

Zamiast $(\Pi, A) \in r$ piszemy na ogół $\frac{\Pi}{A}r$.

Jeśli zbiór Π jest skończony, powiedzmy $\Pi = \{\pi_1, \dots, \pi_k\}$, to zamiast $\frac{\{\pi_1, \dots, \pi_k\}}{A}r$ piszemy po prostu $\frac{\pi_1, \dots, \pi_k}{A}r$.

Regułę bez przesłanek nazywać będziemy **aksjomatem**.

Dla uproszczenia będziemy więc myśleć o aksjomatach jak o pewnym zbiorze formuł języka L .

Systemem dedukcyjnym (lub **aksjomatycznym**) nazywać będziemy dowolny zbiór reguł wnioskowania.

Dla poprawienia czytelności na ogół będziemy zapisywać system dedukcyjny S jako parę (AX, R) , gdzie AX jest pewnym zbiorem aksjomatów, a R pewnym zbiorem reguł wnioskowania, które nie są aksjomatami.

Ustalmy system dedukcyjny S .

Dowodem formuły A w systemie S na gruncie zbioru formuł Γ nazywamy skończony ciąg formuł $A_1, \dots, A_n$ taki, że

1. $A_n = A$,
2. dla dowolnego $1 \leq i \leq n$ albo

$$A_i \in AX \cup \Gamma$$

albo istnieją $i_1, \dots, i_k < i$ oraz $r \in R$ takie, że

$$\frac{A_{i_1}, \dots, A_{i_k}}{A_i} r.$$

Formułę A nazywamy **dowodliwą** w S na gruncie Γ , gdy istnieje dowód A w S na gruncie Γ .

Piszemy wtedy

$$\Gamma \vdash A.$$

Gdy $\Gamma = \emptyset$ to mówimy, że A jest **tezą** systemu S .

Piszemy wtedy

$$\vdash_S A.$$

Na ogół, o ile będzie jasne, z jakim systemem dedukcyjnym pracujemy, będziemy po prostu pisać $\vdash$ zamiast $\vdash_S$.

Mówimy, że zbiór formuł Γ jest **niesprzeczny**, gdy istnieje formuła A taka, że $\Gamma \not\vdash A$.

W przeciwnym wypadku mówimy, że Γ jest sprzeczny.

Mówimy, że system S jest **sprzeczny**, gdy $\vdash A$ dla każdej formuły A .

Definicja:

Alfabet języka logiki zdań składa się z nieskończonego (najczęściej zakładamy: przeliczalnego) zbioru P , o którym myślimy jak o zbiorze **zmiennych zdaniowych** i skończonego zbioru symboli, o których myślimy jak o **spójnikach zdaniowych**:

- ▶ $\neg$ – jednoargumentowy, negacja;
- ▶ $\wedge$ – dwuargumentowy, koniunkcja;
- ▶ $\vee$ – dwuargumentowy, alternatywa;
- ▶ $\rightarrow$ – dwuargumentowy, implikacja.

Dodatkowo “dorzucamy” też do naszego alfabetu nawiasy (i).

Język logiki zdań L definiujemy teraz jako najmniejszy podzbiór monoidu L^* spełniający warunki:

1. $P \subset L$;
2. jeśli $A, B \in L$, to do L należą również następujące formuły:

$$\neg A, \quad A \wedge B, \quad A \vee B, \quad A \rightarrow B.$$

Niech $A, B, C, \dots$ oznaczają formuły. Przyjmujemy następujące aksjomaty:

1. $A \rightarrow (B \rightarrow A)$ (prawo poprzedzania),
2. $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ (sylogizm Fregego),
3. $A \wedge B \rightarrow A$,
4. $A \wedge B \rightarrow B$,
5. $(A \rightarrow B) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow (B \wedge C)))$,
6. $A \rightarrow A \vee B$,
7. $B \rightarrow A \vee B$,
8. $(B \rightarrow A) \rightarrow ((C \rightarrow A) \rightarrow (B \vee C \rightarrow A))$,
9. $\neg A \rightarrow (A \rightarrow B)$ (prawo Dunsza Szkota),
10. $(A \rightarrow \neg A) \rightarrow \neg A$ (prawo redukcji do absurdu),
11. $\neg\neg A \rightarrow A$ (mocne prawo podwójnego przeczenia);

oraz następującą regułę, zwaną **regułą odrywania**:

$$\frac{A \rightarrow B, A}{B} r_0.$$

Lemat:

$\vdash A \rightarrow A.$

Twierdzenie o dedukcji [Herbrand, 1930]

Niech $\Gamma \subset L$, $A, B \in L$. Wówczas

$\Gamma \vdash A \rightarrow B$ wtedy i tylko wtedy, gdy $\Gamma, A \vdash B$

Regułę r nazywamy **wyprowadzalną** w S , gdy dla dowolnych Π, A

$$\text{jeżeli } \frac{\Pi}{A} \in r \text{ to } \Pi \vdash_S A.$$

Jest jasne, że stosowanie reguł wyprowadzalnych nie zmienia zbioru tez systemu.

Przykłady:

(1) Reguła **sylogizmu hipotetycznego**:

$$\frac{A \rightarrow B, B \rightarrow C}{A \rightarrow C}$$

jest wyprowadzalna w KRZ.

(2) Reguła **wewnętrznego odrywania**:

$$\frac{A \rightarrow (B \rightarrow C), B}{A \rightarrow C}$$

jest wyprowadzalna w KRZ.

Lemat:

$\Gamma \vdash A \wedge B$ wtedy i tylko wtedy, gdy $\Gamma \vdash A$ oraz $\Gamma \vdash B$.

Wniosek:

Reguła **mnożenia**:

$$\frac{A, B}{A \wedge B}$$

jest wyprowadzalna w KRZ.

Lemat:

Zbiór Γ jest sprzeczny wtedy i tylko wtedy, gdy $\Gamma \vdash A \wedge \neg A$ dla pewnej formuły A (czyli, wobec poprzedniego lematu, gdy $\Gamma \vdash A$ oraz $\Gamma \vdash \neg A$).

Lemat:

$\Gamma, A \wedge B \vdash C$ wtedy i tylko wtedy, gdy $\Gamma, A, B \vdash C$.

Wniosek:

$\Gamma \cup \{A \wedge B\}$ jest sprzeczny wtedy i tylko wtedy, gdy $\Gamma \cup \{A, B\}$ jest sprzeczny.

Lemat:

$\Gamma, A \vee B \vdash C$ wtedy i tylko wtedy, gdy $\Gamma, A \vdash C$ oraz $\Gamma, B \vdash C$.

Wniosek:

$\Gamma \cup \{A \vee B\}$ jest sprzeczny wtedy i tylko wtedy, gdy $\Gamma \cup \{A\}$ oraz $\Gamma \cup \{B\}$ są sprzeczne.

Lemat:

$\Gamma \vdash \neg A$ wtedy i tylko wtedy, gdy $\Gamma \cup \{A\}$ jest sprzeczny.

Lemat:

$\Gamma \vdash A$ wtedy i tylko wtedy, gdy $\Gamma \cup \{\neg A\}$ jest sprzeczny.

Lemat:

1. $\vdash A \leftrightarrow \neg\neg A$ (prawo podwójnego przeczenia),
2. $\vdash (A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$ (prawo kontrapozycji)

Dowód:

(1) Oczywiście $\vdash \neg\neg A \rightarrow A$.

Na mocy reguły mnożenia wystarczy pokazać, że

$$\vdash A \rightarrow \neg\neg A.$$

Zauważmy jednak, że $\{A, \neg A\}$ jest sprzeczny; zatem $A \vdash \neg\neg A$,
czyli z twierdzenia o dedukcji

$$\vdash A \rightarrow \neg\neg A.$$

(2) Zauważmy, że $\{A \rightarrow B, \neg B, A\}$ jest sprzeczny.
Czyli $A \rightarrow B, \neg B \vdash \neg A$.

Stąd stosując dwukrotnie twierdzenie o dedukcji

$$\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A).$$

Ponadto $\{\neg B \rightarrow \neg A, A, \neg B\}$ jest sprzeczny.

Zatem

$$\neg B \rightarrow \neg A, A \vdash \neg \neg B.$$

Stąd na mocy (11)

$$\neg \neg B \rightarrow B$$

oraz $\neg B \rightarrow \neg A, A \vdash B$, czyli $\vdash (\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$.

Twierdzenie o ekstensjonalności:

Niech A^* będzie formułą, która powstaje z formuły A przez zastąpienie pewnych wystąpień formuły D formułą D' . Przy tych oznaczeniach reguła **ekstensjonalności**:

$$\frac{D \leftrightarrow D'}{A \leftrightarrow A^*}$$

jest wyprowadzalna w KRZ.

Dowód:

Należy pokazać, że

$$D \leftrightarrow D' \vdash A \leftrightarrow A^*.$$

Jeżeli na A nie wykonamy żadnych zastąpień, to A^* jest identyczna z A , tym bardziej $\vdash A \leftrightarrow A^*$.

Jeżeli $A = D$, to oczywiście $A^* = D'$, czyli $D \leftrightarrow D' \vdash A \leftrightarrow A^*$.

W pozostałych przypadkach dowód prowadzimy metodą indukcji ze względu na budowę formuły.

Założmy, że A jest zmienną.

Wówczas zachodzi jeden z powyższych przypadków.

Założmy, że $A = \neg B$.

Założenie indukcyjne:

$$D \leftrightarrow D' \vdash B \leftrightarrow B^*.$$

Stąd na mocy prawa kontrapozycji

$$D \leftrightarrow D' \vdash \underbrace{\neg B}_A \leftrightarrow \underbrace{\neg B^*}_{A^*}.$$

Założmy, że $A = B \rightarrow C$.

Założenie indukcyjne:

$$D \leftrightarrow D' \vdash B \leftrightarrow B^*, \quad D \leftrightarrow D' \vdash C \leftrightarrow C^*.$$

Zauważmy, że $D \leftrightarrow D', B \rightarrow C, B^* \vdash C^*$.

Stąd $D \leftrightarrow D' \vdash (B \rightarrow C) \rightarrow (B^* \rightarrow C^*)$.

Podobnie $D \leftrightarrow D' \vdash (B^* \rightarrow C^*) \rightarrow (B \rightarrow C)$.

Zatem $D \leftrightarrow D' \vdash A \leftrightarrow A^*$.

Założmy, że $A = B \wedge C$.

Założenie indukcyjne:

$$D \leftrightarrow D' \vdash B \leftrightarrow B^*, \quad D \leftrightarrow D' \vdash C \leftrightarrow C^*.$$

Zauważmy, że:

$$D \leftrightarrow D', B \vdash B^*, \text{ zatem } D \leftrightarrow D', B, C \vdash B^*,$$

$$D \leftrightarrow D', C \vdash C^*, \text{ zatem } D \leftrightarrow D', B, C \vdash C^*.$$

Stąd

$$D \leftrightarrow D', B, C \vdash B^* \wedge C^*,$$

$$D \leftrightarrow D', B \wedge C \vdash B^* \wedge C^*,$$

czyli

$$D \leftrightarrow D' \vdash (B \wedge C) \rightarrow (B^* \wedge C^*).$$

Podobnie pokazujemy

$$D \leftrightarrow D' \vdash (B^* \wedge C^*) \rightarrow (B \wedge C),$$

a zatem

$$D \leftrightarrow D' \vdash A^* \leftrightarrow A.$$

Przypadek $A = B \vee C$ zostawiamy jako ćwiczenie.

Lemat:

Tezami KRZ są:

1. $A \vee B \leftrightarrow B \vee A,$
2. $A \wedge B \leftrightarrow B \wedge A,$
3. $(\neg A \wedge \neg B) \leftrightarrow \neg(A \vee B),$
4. $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B),$
5. $\neg(A \wedge \neg A),$
6. $A \vee \neg A,$
7. $(A \rightarrow B) \leftrightarrow (\neg A \vee B),$
8. $A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C),$
9. $A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C).$

Semantyka klasycznego rachunku zdań.

Niech L będzie językiem logiki zdań. Na zbiorze L definiujemy następujące operacje:

- ▶ $Neg(A) = \neg A$,
- ▶ $Alt(A, B) = A \vee B$,
- ▶ $Kon(A, B) = A \wedge B$,
- ▶ $Imp(A, B) = A \rightarrow B$.

Algebrę $\mathbf{L} = (L, Neg, Alt, Kon, Imp)$ nazywamy **algebrą języka logiki zdań**. Jest to algebra o typie $\tau_{\mathbf{L}} = (1, 2, 2, 2)$. Algebra $\mathbf{L}$ jest algebrą absolutnie wolną ze zbiorem zmiennych zdaniowych P jako zbiorem wolnych generatorów.

Matrycą (Łukasiewicz, Tarski, 1930) dla języka logiki zdaniowej nazywamy parę

$$\mathcal{M} = (\mathbf{M}, M^*),$$

gdzie $\mathbf{M}$ jest algebrą podobną do algebry języka logiki zdań, zaś zbiór $\emptyset \neq M^* \subset M$ nazywamy zbiorem elementów wyróżnionych matrycy (zakładamy często, że M^* jest jednoelementowy).

Piszemy też

$$\mathcal{M} = (M, M^*, F_{\neg}, F_{\wedge}, F_{\vee}, F_{\rightarrow}).$$

Niech $\mathcal{M}$ będzie pewną matrycą dla języka logiki zdań.

Wartościowaniem w $\mathcal{M}$ nazywamy dowolne odwzorowanie $\varphi : P \rightarrow M$. Każde takie odwzorowanie przedłuża się jednoznacznie do homomorfizmu algebry **L** w algebrę **M**. Homomorfizm ten będziemy również oznaczać przez φ .

Niech A będzie dowolną formułą języka zdań i niech $\mathcal{M}$ będzie matrycą. Ustalmy wartościowanie $\varphi : P \rightarrow M$. Mówimy, że φ **spełnia** A w $\mathcal{M}$, gdy $\varphi(A) \in M^*$. Formułę A nazwiemy **tautologią matrycy** $\mathcal{M}$, gdy A jest spełniona w $\mathcal{M}$ przy każdym wartościowaniu (mówimy wtedy też, że A jest **prawdziwe** w $\mathcal{M}$). Zbiór wszystkich tautologii matrycy $\mathcal{M}$ nazywamy **zawartością** tej matrycy i oznaczamy przez $E(\mathcal{M})$. Mówimy, że A **wynika logicznie** z B w matrycy $\mathcal{M}$, jeżeli dla każdego wartościowania $\varphi : P \rightarrow M$

$$\text{jeżeli } \varphi(A) \in M^*, \text{ to } \varphi(B) \in M^*.$$

Mówimy, że A i B są **logicznie równoważne** w matrycy $\mathcal{M}$, gdy dla każdego wartościowania $\varphi : P \rightarrow M$

$$\varphi(A) = \varphi(B).$$

Przykłady: (1) Niech $\mathcal{M}_2 = (\{0, 1\}, \{1\}, F_{\neg}, F_{\wedge}, F_{\vee}, F_{\rightarrow})$, gdzie

- ▶ $F_{\neg}(x) = 1 - x$ w $\mathbb{Z}$,
- ▶ $F_{\wedge}(x, y) = \min\{x, y\}$ w $\mathbb{Z}$,
- ▶ $F_{\vee}(x, y) = \max\{x, y\}$ w $\mathbb{Z}$,
- ▶ $F_{\rightarrow}(x, y) = \min\{1, 1 - x + y\}$ w $\mathbb{Z}$.

$\mathcal{M}_2$ nazywamy matrycą klasycznej (dwuwartościowej) logiki zdań.

Funkcje F spełniają funkcję przybliżenia języka naturalnego.

Algebrę matrycy $\mathcal{M}_2$ możemy utożsamić z $\mathbf{B}_2$.

(2) Niech $\mathcal{M}_3 = (\{0, \frac{1}{2}, 1\}, \{1\}, F_{\neg}, F_{\wedge}, F_{\vee}, F_{\rightarrow})$, z funkcjami $F_{\neg}, F_{\wedge}, F_{\vee}, F_{\rightarrow}$ zdefiniowanymi tak, jak przed chwilą. $\mathcal{M}_3$ nazywamy matrycą trójwartościowej logiki zdań Łukasiewicza.

(3) Niech $\mathcal{M}_T = (\tau(\mathbb{R}), \{\mathbb{R}\}, G_{\neg}, G_{\wedge}, G_{\vee}, G_{\rightarrow})$, gdzie $\tau(\mathbb{R})$ oznacza rodzinę wszystkich zbiorów otwartych oraz

- ▶ $G_{\neg}(X) = \text{Int}(\mathbb{R} \setminus X)$,
- ▶ $G_{\wedge}(X, Y) = X \cap Y$,
- ▶ $G_{\vee}(X, Y) = X \cup Y$,
- ▶ $G_{\rightarrow}(X, Y) = \text{Int}(\mathbb{R} \setminus X \cup Y)$.

$\mathcal{M}_T$ nazywamy matrycą topologicznej logiki Tarskiego.

Lemat

Zachodzą następujące tautologie:

1. $p \rightarrow (p \vee q) \in E(\mathcal{M}_2) \cap E(\mathcal{M}_3) \cap E(\mathcal{M}_T),$
2. $p \vee \neg p \in E(\mathcal{M}_2) \setminus E(\mathcal{M}_3) \setminus E(\mathcal{M}_T),$
3. $(p \vee \neg p) \rightarrow q \in E(\mathcal{M}_2) \cap E(\mathcal{M}_T) \setminus E(\mathcal{M}_3),$
4. $(\neg(p \wedge q) \rightarrow (\neg p \vee \neg q)) \in E(\mathcal{M}_2) \cap E(\mathcal{M}_3) \setminus E(\mathcal{M}_T),$
5. $(p \rightarrow q) \notin E(\mathcal{M}_2) \cup E(\mathcal{M}_3) \cup E(\mathcal{M}_T).$

Dowód: Udowodnimy, dla przykładu, część (1) lematu. Zgodnie z podanymi wcześniej definicjami, tabelki wartości funkcji

$F_{\neg}, F_{\wedge}, F_{\vee}, F_{\rightarrow}$ w macierzy $\mathcal{M}_2$ przedstawiają się następująco:

$$\begin{array}{c|c|c} F_{\neg} & 0 & 1 \\ \hline & 1 & 0 \end{array}, \quad \begin{array}{c|c|c} F_{\wedge} & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}, \quad \begin{array}{c|c|c} F_{\vee} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \text{ oraz } \begin{array}{c|c|c} F_{\rightarrow} & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 0 & 1 \end{array}.$$

Wobec tego

p	q	$p \vee q$	$p \rightarrow (p \vee q)$
1	1	1	1
1	0	1	1
0	1	1	1
0	0	0	1

i tym samym $p \rightarrow (p \vee q)$ jest tautologią matrycy $\mathcal{M}_2$.

Podobnie, tabelki wartości funkcji $F_{\neg}, F_{\wedge}, F_{\vee}, F_{\rightarrow}$ w macierzy $\mathcal{M}_3$ wyglądają tak:

$F_{\neg}$	0	$\frac{1}{2}$	1
	1	$\frac{1}{2}$	0

,

$F_{\wedge}$	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

,

$F_{\vee}$	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	1	1	1

 oraz

$F_{\rightarrow}$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	1	1
1	0	$\frac{1}{2}$	1

.

Zatem

p	q	$p \vee q$	$p \rightarrow (p \vee q)$
1	1	1	1
1	$\frac{1}{2}$	1	1
1	0	1	1
$\frac{1}{2}$	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
$\frac{1}{2}$	0	$\frac{1}{2}$	1
0	1	1	1
0	$\frac{1}{2}$	$\frac{1}{2}$	1
0	0	0	1

i $p \rightarrow (p \vee q)$ jest tautologią matrycy $\mathcal{M}_3$.

Na koniec sprawdzamy, że dla zbiorów otwartych $X, Y \subset \mathbb{R}$:

$$\text{Int}((\mathbb{R} \setminus X) \cup X \cup Y) = \text{Int}(\mathbb{R}) = \mathbb{R},$$

a więc $p \rightarrow (p \vee q)$ jest tautologią matrycy $\mathcal{M}_T$.

Lemat

Niech $A(p_1, \dots, p_n)$ będzie formułą języka logiki zdań i $\mathcal{M}$ niech będzie matrycą dla tego języka. Niech ponadto ϕ, ψ będą dowolnymi wartościowaniami takimi, że

$$\phi(p_i) = \psi(p_i) \text{ dla } 1 \leq i \leq n.$$

Wówczas $\phi(A) = \psi(A)$.

Dowód.

Dowód prowadzimy przez indukcję względem budowy A . Jeśli $A = p_i$, to $\phi(A) = \psi(A)$ z założenia.

Jeśli $A = \neg B$, to mamy

$$\phi(A) = \phi(\neg B) = F_{neg}(\phi(B)) = F_{\neg}(\psi(B)) = \psi(\neg B) = \psi(A).$$

Przypadki gdy $A = B \vee C$, $A = B \wedge C$ oraz $A = B \rightarrow C$ pozostawiamy czytelnikowi jako ćwiczenia.



Dowolną funkcję $f : \{0, 1\}^n \rightarrow \{0, 1\}$ nazywamy **funkcją booleowską**.

Każda formuła języka logiki zdań wyznacza pewną funkcję booleowską f_A taką, że dla dowolnego $\phi : P \rightarrow \{0, 1\}$:

$$\phi(A) = f_A(\phi(p_1), \dots, \phi(p_m)),$$

o ile $A = A(p_1, \dots, p_m)$.

Okazuje się, że twierdzenie odwrotne też jest prawdziwe.

Twierdzenie

Każda funkcją booleowska jest wyznaczona przez pewną formułę języka logiki zdań, przy czym w formule tej występują tylko spójniki $\neg, \vee, \wedge$.

Dowód: Niech $f(p_1, \dots, p_k)$ będzie dowolną funkcją booleowską.
Rozważmy następującą tablicę:

	p_1	p_2	$\dots$	p_n	
ϕ_0	0	0	$\dots$	0	$f(0, \dots, 0)$
ϕ_1	0	0	$\dots$	1	$f(0, \dots, 1)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
ϕ_k	e_1	e_2	$\dots$	e_n	$f(e_1, \dots, e_n)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
ϕ_{2^n-1}	1	1	$\dots$	1	$f(1, \dots, 1)$

W powyższej tabelce mamy $\phi_0(p_i) = 0$. Zdefiniujemy 2^n formuł $C_0, \dots, C_{2^n-1}$ w następujący sposób:

$$C_k = {}^*p_1^k \wedge \dots \wedge {}^*p_k^k,$$

gdzie

$${}^*p_i^k = \begin{cases} p_i, & \text{jeśli } \phi_k(p_i) = 1, \\ \neg p_i, & \text{jeśli } \phi_k(p_i) = 0. \end{cases}$$

Zauważmy, że

$$\phi_k(C_k) = 1$$

oraz

$$\phi_i(C_j) = 0, \text{ jeśli } i \neq j.$$

Definiujemy

$$A(p_1, \dots, p_n) = \bigvee \{C_k : f(\phi_k(p_1), \dots, \phi_k(p_n)) = 1\}.$$

Pokażemy, że $A(p_1, \dots, p_n)$ generuje f . Jeśli $f(\phi_k(p_1), \dots, \phi_k(p_n)) = 1$, to C_k występuje w A i mamy wtedy

$$\phi_k(C_k) = 1.$$

Zatem $\phi_k(A) = 1$. Jeśli $f(\phi_k(p_1), \dots, \phi_k(p_n)) = 0$, to C_k nie występuje w A i mamy wtedy

$$\phi_k(A) = 0.$$

Formuła A jest w **alternatywnej postaci normalnej**, gdy A jest postaci

$$B_1 \vee \dots \vee B_n,$$

gdzie każda z formuł B_j jest koniunkcją zmiennych zdaniowych lub negacji zmiennych zdaniowych.

Wniosek

Dowolna formuła jest logicznie równoważna pewnej formule A^ w alternatywnej postaci normalnej.*

Wniosek

Dowolną funkcję booleowską można wygenerować za pomocą formuł zawierających tylko spójniki

1. $\vee, \neg$,
2. $\wedge, \neg$,
3. $\rightarrow, \neg$.

Dowód.

Wystarczy zauważyć, że:

1. $p \wedge q \equiv \neg(\neg p \vee \neg q),$
2. $p \vee q \equiv \neg(\neg p \wedge \neg q),$
3. $p \vee q \equiv \neg p \rightarrow q.$



Zbiór formuł Σ jest **spełnialny**, gdy istnieje wartościowanie ϕ takie, że dla każdego $A \in \Sigma$ mamy $\phi(A) = 1$. Mówimy, że Σ jest **skończenie spełnialny**, gdy każdy skończony podzbiór zbioru Σ jest spełnialny.

Twierdzenie (o zwartości)

Zbiór formuł Σ jest spełnialny wtedy i tylko wtedy, gdy Σ jest skończenie spełnialny.

Dowód: Oczywiście wystarczy pokazać, że jeśli zbiór jest skończenie spełnialny, to jest też spełnialny. Załóżmy więc, że Σ jest skończenie spełnialny. Niech V będzie zbiorem wszystkich zmiennych występujących w formułach zbioru Σ . Rozważmy $\{0, 1\}^V$ jako produkt przestrzeni dyskretnych $\{0, 1\}$. Wobec twierdzenia Tichonowa $\{0, 1\}^V$ jest przestrzenią zwartą. Zbiory

$$B_{p,i} = \{\phi \in \{0, 1\}^V : \phi(p) = i\}$$

stanowią podbazę przestrzeni $\{0, 1\}^V$. Ponadto $B_{p,i}$ są domknięto-otwarte, bo $\{0, 1\}^V \setminus B_{p,0} = B_{p,1}$.

Dla dowolnej formuły $A \in \Sigma$ niech

$$D(A) = \{\phi \in \{0, 1\}^V : \phi(A) = 1\}.$$

Z założenia wiemy, że każdy skończony podzbiór Σ_0 zbioru Σ jest spełnialny. Zatem

$$\bigcap \{D(A) : A \in \Sigma_0\} \neq \emptyset \text{ dla skończonego podzbioru } \Sigma_0 \subset \Sigma.$$

Zbiory $D(A)$ są zbiorami domknięto-otwartymi (jako skończone sumy skończonych przekrojów zbiorów podbazowych). Zatem

$$\bigcap \{D(A) : A \in \Sigma\} \neq \emptyset,$$

a zatem Σ jest spełnialny.

Stwierdzenie

Wszystkie aksjomaty KRZ są tautologiami w matrycy $\mathcal{M}_2$. Reguła odrywania jest regułą niezawodną w $\mathcal{M}_2$, czyli każda teza systemu klasycznego rachunku zdań jest tautologią matrycy $\mathcal{M}_2$.

Dowód.

Sprawdzimy, dla przykładu, aksjomat (1):

A	B	$B \rightarrow A$	$A \rightarrow (B \rightarrow A)$
1	1	1	1
1	0	1	1
0	1	0	1
0	0	1	1



Niech L będzie językiem KRZ. rozważmy relację $\sim \subset L^2$:

$A \sim B$ wtedy i tylko wtedy gdy $\vdash A \leftrightarrow B$.

Stwierdzenie

Relacja $\sim$ jest równoważnością

Dowód.

Wobec rezultatów udowodnionych na ostatnim wykładzie:

- ▶ zwrotność zachodzi, ponieważ mamy $\vdash A \leftrightarrow A$ wobec Lematu 1,
- ▶ symetria zachodzi, ponieważ mamy $\vdash A \leftrightarrow B$ wtedy i tylko wtedy, gdy $\vdash B \leftrightarrow A$ wobec definicji,
- ▶ przechodniość zachodzi, ponieważ mamy, że jeśli $\vdash A \leftrightarrow B$ oraz $\vdash B \leftrightarrow C$, to $\vdash A \leftrightarrow C$ wobec twierdzenia o ekstensjonalności.



Oznaczmy przez $L^\sim$ zbiór klas abstrakcji relacji $\sim$. Klasy abstrakcji oznaczać będziemy po prostu przez $[A]$. W zbiorze $L^\sim$ definiujemy relację

$$[A] \leq [B] \text{ wtedy i tylko wtedy gdy } \vdash A \rightarrow B.$$

Wobec twierdzenia o ekstensjonalności, relacja powyższa jest dobrze określona. Pokażemy jednak coś znacznie silniejszego.

Twierdzenie

$(L^\sim, \leq)$ jest dystrybutywną kratą komplementarną.

Dowód: Sprawdzenie, że $\leq$ jest relacją porządku, pozostawiamy czytelnikowi jako proste ćwiczenie.

Pokażemy, że $[A] \cap [B] = [A \wedge B]$. Istotnie, mamy:

$$\vdash A \wedge B \rightarrow A,$$

$$\vdash A \wedge B \rightarrow B.$$

Zatem $[A \wedge B] \leq [A]$ oraz $[A \wedge B] \leq [B]$. Niech $[C] \leq [A]$ oraz $[C] \leq [B]$. Wtedy $\vdash C \rightarrow A$ oraz $\vdash C \rightarrow B$. Ponadto

$$\vdash (C \rightarrow A) \rightarrow ((C \rightarrow B) \rightarrow (C \rightarrow A \wedge B)).$$

Stąd $\vdash C \rightarrow A \wedge B$, co oznacza $[C] \leq [A \wedge B]$.

Pokażemy, że $[A] \cup [B] = [A \vee B]$. Istotnie, mamy:

$$\vdash A \rightarrow A \vee B,$$

$$\vdash B \rightarrow A \vee B.$$

Zatem $[A] \leq [A \vee B]$ oraz $[B] \leq [A \vee B]$. Niech teraz $[A] \leq [C]$ oraz $[B] \leq [C]$. Wtedy $\vdash A \rightarrow C$ oraz $\vdash B \rightarrow C$. Ponadto:

$$\vdash (A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C)).$$

Stąd $\vdash A \vee B \rightarrow C$, co oznacza $[A \vee B] \leq [C]$.

Dystrybutywność wynika wprost z udowodnionych ostatnio tez:

$$A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C),$$

oraz

$$A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C).$$

Pokażemy, że $1 = [A]$ wtedy i tylko wtedy, gdy $\vdash A$. Istotnie, założymy, że $1 = [A]$. Wtedy dla dowolnej formuły B mamy $\vdash B \rightarrow A$, w szczególności dla dowolnej tezy. Stosując regułę odrywania otrzymujemy, że $\vdash A$. Na odwrót, założymy, że $\vdash A$. Niech B będzie dowolną formułą. Mamy wówczas

$$\vdash A \rightarrow (B \rightarrow A).$$

Stąd $\vdash B \rightarrow A$, czyli $[B] \leq [A]$, a zatem $[A] = 1$.

Pokażemy, że $0 = [A]$ wtedy i tylko wtedy, gdy $\vdash \neg A$. Istotnie, założymy, że $0 = [A]$. Wtedy dla dowolnej formuły B mamy $\vdash A \rightarrow B$, w szczególności dla $B = \neg A$ mamy $\vdash A \rightarrow \neg A$. Ponadto:

$$\vdash (A \rightarrow \neg A) \rightarrow \neg A.$$

Stosując regułę odrywania otrzymujemy, że $\vdash \neg A$. Na odwrót, założymy, że $\vdash \neg A$. Niech B będzie dowolną formułą. Mamy wówczas

$$\vdash \neg A \rightarrow (A \rightarrow B).$$

Stąd $\vdash A \rightarrow B$, czyli $[A] \leq [B]$, a zatem $[A] = 0$.

Na koniec pokażemy, że $\neg[A] = [\neg A]$. Istotnie, mamy

$$[A] \cup [\neg A] = [A \vee \neg A] = 1,$$

$$[A] \cap [\neg A] = [A \wedge \neg A] = 0.$$

Algebrę $(L^\sim, \leq)$ nazywamy **algebrą Lindenbauma** KRZ. Działania w $(L^\sim, \leq)$ określone są następująco:

- ▶ $[A] \cap [B] = [A \wedge B]$,
- ▶ $[A] \cup [B] = [A \vee B]$,
- ▶ $-[A] = [\neg A]$,
- ▶ $1 = [p \vee \neg p]$,
- ▶ $0 = [p \wedge \neg p]$.

W dalszym ciągu rozważać będziemy algebrę Boole'a jako podobną do algebry języka KRZ, czyli algebrę postaci

$$(B, -, \cup, \cap, \Rightarrow),$$

gdzie

$$x \Rightarrow y = -x \cup y.$$

W szczególności zauważmy, iż w algebrze Lindenbauma:

$$[A] \Rightarrow [B] = -[A] \cup [B] = [\neg A \vee B] = [A \rightarrow B].$$

Twierdzenie (o zgodności)

Każda teza KRZ jest tautologią matrycy $\mathcal{M}_2$.

Dowód.

Zauważyliśmy już, że każdy aksjomat jest tautologią i że zbiór tautologii jest domknięty na regułę odrywania. Dowód przeprowadzimy przez indukcję ze względu na długość tezy. Niech $\vdash A$ i niech $A_1, \dots, A_l = A$ będzie dowodem A . Jeśli $l = 1$, to $A_1 = A$ jest aksjomatem, a więc tautologią. Załóżmy, że $i > 1$ i że dla $j < i$ A_j są tautologiami. A zatem A_j jest aksjomatem, a więc tautologią, albo dla pewnych $j, k < i$ mamy

$$A_k = A_j \rightarrow A_i, \dots, A_j, \dots, A_j \rightarrow A_i, \dots, A_i.$$

Z założenia indukcyjnego A_j oraz $A_j \rightarrow A_i$ są tautologiami, a zatem A_i jest tautologią. □

Twierdzenie (o pełności)

Każda tautologia $\mathcal{M}_2$ jest tezą KRZ.

Dowód twierdzenia poprzedzimy lematem. Oznaczmy przez AL algebrę Lindenbauma KRZ.

Lemat

Niech ϕ będzie homomorfizmem AL w $\mathbf{B}_2$. Niech $\psi : P \rightarrow \{0, 1\}$ będzie wartościowaniem takim, że

$$\psi(p) = \phi([p]) \text{ dla } p \in P.$$

Wówczas

$$\psi(A) = \phi([A]) \text{ dla dowolnej formuły } A.$$

Wartościowanie takie jak w lemacie nazywać będziemy **indukowanym** przez ϕ .

Dowód.

Dowód prowadzimy przez indukcję względem budowy formuły A .
Zauważmy na wstępie, że ψ przedłuża się jednoznacznie do homomorfizmu algebry języka KRZ w $\mathbf{B}_2$.

Założmy, że A jest zmienną, $A = p$ – wówczas twierdzenie jest prawdziwe w myśl założenia.

Założmy, że $A = \neg B$. Wówczas:

$$\psi(A) = \psi(\neg B) = -\psi(B) = -\phi([B]) = \phi(-[B]) = \phi([\neg B]) = \phi([A]).$$

Przypadki, gdy $A = B \wedge C$, $A = B \vee C$ oraz $A = B \rightarrow C$ pozostawiamy czytelnikowi jako ćwiczenie.



Przechodzimy teraz do dowodu twierdzenia o pełności.

Dowód.

Założmy, że $\not\models A$.

Pokażemy, że $A \notin E(\mathcal{M}_2)$.

Istotnie, skoro $\not\models A$, to w AL mamy, że $[A] \neq 1$.

Zatem $\neg[A] \neq 0$, czyli $[\neg A] \neq 0$.

Wobec twierdzenia o istnieniu ultrafiltru istnieje ultrafiltr F algebry AL zawierający $[\neg A]$. W szczególności $AL/F \cong \mathbf{B}_2$.

Niech ψ będzie wartościowaniem indukowanym przez kanoniczny homomorfizm $\kappa : AL \rightarrow AL/F$.

Wówczas

$$\psi(\neg A) = \kappa([\neg A]) = 1,$$

a zatem $\psi(A) = 0$, czyli $A \notin E(\mathcal{M}_2)$.



Wniosek

KRZ jest rozstrzygalny w intuicyjnym sensie, tzn. istnieje efektywna procedura dająca odpowiedź, czy $\vdash A$ czy $\nvdash A$.

Twierdzenie (Malcev)

Niech Σ będzie dowolnym zbiorem formuł języka KRZ. Wówczas Σ jest niesprzeczny wtedy i tylko wtedy, gdy Σ jest spełnialny.

Dowód: ($\Leftarrow$) Załóżmy, że Σ jest sprzeczne. Zatem pewien jego skończony podzbiór Σ' jest sprzeczny. Mamy

$$\Sigma' \vdash A \wedge A'$$

dla pewnej formuły A . Niech $B = \bigwedge \{C : C \in \Sigma'\}$. Na mocy twierdzenia o dedukcji:

$$\vdash B \rightarrow (A \wedge \neg A).$$

Z twierdzenia o zgodności

$$B \rightarrow (A \wedge \neg A) \in E(\mathcal{M}_2),$$

czyli dla każdego wartościowania $\phi : P \rightarrow \{0, 1\}$ mamy

$$\phi(B \rightarrow (A \wedge \neg A)) = 1.$$

Ale zawsze mamy również

$$\phi(A \wedge \neg A) = 0.$$

Stąd $\phi(B) = 0$ dla każdego wartościowania ϕ , czyli Σ' jest niespełnialny, a więc i Σ jest niespełnialny.

($\Rightarrow$) Załóżmy, że Σ jest niespełnialny. Z twierdzenia o zwartości, pewien skończony podzbiór Σ' zbioru Σ jest niespełnialny. Niech

$$B = \bigwedge \{C : C \in \Sigma'\}.$$

Stąd $\phi(B) = 0$ dla każdego wartościowania ϕ , więc B jest kontrtautologią. A zatem $\neg B \in E(\mathcal{M}_2)$. Stąd, na mocy twierdzenia o pełności, $\vdash \neg B$. Ale

$$\Sigma' \vdash C \text{ dla } C \in \Sigma'$$

więc w szczególności

$$\Sigma' \vdash B.$$

Zatem $\Sigma' \vdash B \wedge \neg B$, czyli Σ' jest sprzeczny, a więc i Σ jest sprzeczny.