

Definicja:

Niepusty podzbiór F uniwersum algebry Boole'a $\mathbf{B}$ nazywamy **filtrem**, gdy

1. $\forall x, y \in F (x \cap y \in F)$,
2. $\forall x \in F \forall y \in B (x \leq y \Rightarrow y \in F)$.

Twierdzenie:

Niech F będzie filtrem maksymalnym algebry Boole'a $\mathbf{B}$. Wówczas następujące warunki są równoważne:

1. F jest maksymalny,
2. F jest pierwszy,
3. dla dowolnego $a \in B$ albo $a \in F$, albo $-a \in F$,
4. $\mathbf{B}/F \cong \mathbf{B}_2$.

Definicja:

Dowolny filtr właściwy spełniający jeden z powyższych równoważnych warunków nazywamy **ultrafiltrem**.

Interesować nas będą głównie ultrafiltry w algebrach potęgowych.
Niech $I \neq \emptyset$.

Mówimy, że F jest **filtrem nad zbiorem I** , gdy F jest filtrem w algebrze potęgowej $(2^I, \subset)$.

Wprost z definicji filtrem głównym w algebrze potęgowej będzie

$$F_A = \{X : A \subset X\}.$$

Uwaga:

Niech F będzie filtrem głównym nad I . Wówczas F jest ultrafiltrem wtedy i tylko wtedy, gdy F jest generowany przez zbiór jednoelementowy.

Dowód:

$(\Rightarrow)$:

Niech X generuje F i przypuśćmy, że $x, y \in X$ dla $x \neq y$.

Rozważmy $\{x\}$.

Ponieważ F jest ultrafiltrem, więc:

$$\{x\} \in F \text{ albo } -\{x\} \in F.$$

W pierwszym przypadku $\{x\} \cap X \in F$, czyli $\{x\} \in F$, co daje sprzeczność.

W drugim przypadku sprzeczność otrzymujemy wobec faktu, że $X \setminus \{x\} \in F$.

($\Leftarrow$:)

Założmy, że $F = \{Y \subset I : \{a\} \subset Y\} = \{Y : a \in Y\}$.

Weźmy dowolny $Z \subset I$.

Mamy:

$$a \in Z \text{ lub } a \notin Z, \text{ czyli } a \in -Z.$$

W pierwszym przypadku $Z \in F$, a w drugim $-Z \in F$.

Wobec tego F jest ultrafiltrem.

Uwaga:

Jeśli F jest ultrafiltrem niegłównym nad I , to do F nie należy żaden zbiór skończony.

Dowód:

Założmy, że F jest filtrem niegłównym w pewnej algebrze potęgowej nad I i przypuśćmy, że pewien zbiór skończony należy do F .

Niech K będzie takim zbiorem o minimalnej liczbie elementów. Przypuśćmy ponadto, że dla $x \neq y$ mamy $x, y \in K$.

Wówczas

$$\{x\} \notin F,$$

ponieważ K był minimalnym zbiorem skończonym należącym do F oraz

$$-\{x\} \notin F,$$

ponieważ w przeciwnym razie $-\{x\} \cap K \in F$, co daje sprzeczność z minimalnością K .

Oznacza to, że F nie mógłby być ultrafiltrem.

Uwaga:

W dowolnej nieskończonej algebrze potęgowej istnieją ultrafiltry niegłówne.

Dowód:

Niech I będzie zbiorem nieskończonym.

Rozważmy

$$F = \{X \subset I : X \text{ jest zbiorem skończonym}\}.$$

Z łatwością sprawdzamy, że F jest filtrem.

F jest filtrem właściwym, bo $\emptyset \notin F$.

F możemy rozszerzyć do ultrafiltru.

Z kolei łatwo sprawdzamy, że każdy ultrafiltr rozszerzający F jest niegłówny.

Monoidy wolne.

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 przykład, jeśli $x, y \in X$, to $x, yy, xy, xxxyyxy$ są słowami o długościach 1, 2, 2, 7.

Pusty ciąg jest także dopuszczalny i będziemy go oznaczać symbolem 1.

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** .

Zauważmy, że formalnie rzecz biorąc zbiór X nie jest podzbiorem X^* .

W dalszym ciągu dla każdego $x \in X$ będziemy utożsamiać słowo jednoelementowe x (czyli ciąg jednoelementowy) z elementem x , i wobec tego będziemy mogli uważać, że $X \subset X^*$.

Iniekcja $\mu : X \hookrightarrow X^*$ ma następującą własność uniwersalną.

Twierdzenie:

Niech X będzie zbiorem niepustym. Dla dowolnego monoidu M i dowolnego odwzorowania $f : X \rightarrow M$ istnieje dokładnie jeden homomorfizm monoidów $h : X^* \rightarrow M$ taki, że $h \circ \mu = f$ a więc taki, że następujący diagram jest przemienny:

$$\begin{array}{ccc} X & \xrightarrow{\mu} & X^* \\ & \searrow f & \downarrow h \\ & & M \end{array}$$

Dowód:

Definiujemy $h : X^* \rightarrow M$ kładąc $h(1) = 1_M$, gdzie 1_M jest jedyneką monoidu M , oraz $h(x_1 x_2 \dots x_n) = f(x_1) \cdot f(x_2) \cdot \dots \cdot f(x_n)$ dla dowolnego niepustego słowa $x_1 x_2 \dots x_n$ w alfabecie X .

Tutaj, po prawej stronie równości definiującej odwzorowanie h , kropki oznaczają ją działanie w monoidzie M .

Jest rzeczą oczywistą, że wtedy $h(w_1 * w_2) = h(w_1) \cdot h(w_2)$ dla dowolnych słów $w_1, w_2 \in X^*$.

A więc h jest homomorfizmem monoidów i ponadto, wobec utożsamienia $x \in X$ ze słowem jednoelementowym $x \in X^*$ mamy $\mu(x) = x$, czyli $h \circ \mu(x) = h(x) = f(x)$ dla każdego $x \in X$.

Dowiedliśmy więc istnienia homomorfizmu h .

Z drugiej strony, jeśli $h : X^* \rightarrow M$ jest jakimkolwiek homomorfizmem monoidów spełniającym warunek $h \circ \mu = f$, to dla każdego $x \in X$ mamy $h(x) = h \circ \mu(x) = f(x)$ i dla każdego słowa $x_1 x_2 \dots x_n \in X^*$ mamy

$$\begin{aligned} h(x_1 x_2 \dots x_n) &= h(x_1 * x_2 * \dots * x_n) \\ &= h(x_1) \cdot h(x_2) \dots h(x_n) \\ &= f(x_1) \cdot f(x_2) \dots f(x_n). \end{aligned}$$

A więc homomorfizm h jest jednoznacznie wyznaczony przez warunek $h \circ \mu = f$.

Własność uniwersalną można także odczytać w następujący sposób: każde odwzorowanie f zbioru X w dowolny monoid M można przedłużyć do homomorfizmu h monoidu wolnego X^* w monoid M .

Rzeczywiście, dla każdego $x \in X$ mamy $h(x) = h(\mu(x)) = f(x)$. Jeżeli niepustemu zbiorowi X przyporządkujemy monoid wolny X^* , to możemy też powiedzieć, że monoid X^* powstaje z X przez zastosowanie operacji **gwiazdki Kleene'a**.

Języki formalne.

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.

W myśl powyższej definicji formalny język jest tylko zbiorem słów i niczym więcej.

W praktyce istnieje wiele języków, które mogą być skonstruowane przez pewne zestawy zasad.

To, co intuicyjnie rozumiemy jako "język" w praktyce bliższe jest pojęciu formalnej gramatyki, którego nie będziemy tu formalnie definiować.

Naciągając nieco pojęcie języka często mówiąc o języku będziemy więc myśleli o języku wyposażonym w pewną gramatykę formalną, która go opisuje.

Przykłady:

- (1) $L = \Sigma^*$, zbiór wszystkich słów w danym alfabecie.
- (2) $L = \{a\}^*$, zbiór słów do budowy których użyto tylko jednego symbolu, a mianowicie "a".
- (3) Zbiór syntaktycznie poprawnych programów napisanych w danym języku programowania.
- (4) Zbiór programów, po których wykonaniu zatrzymuje się dana maszyna Turinga.

(5) Przykład odrobinę ambitniejszy: rozważmy alfabet $\Sigma = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, +, =\}$ i podzbiór Σ^* zdefiniowany następującymi zasadami:

- ▶ L zawiera wszystkie słowa, które nie zawierają $+$ lub $=$;
- ▶ L zawiera słowo 0 ;
- ▶ L zawiera słowo zawierające $=$ wtedy i tylko wtedy, gdy zawiera tylko jeden symbol $=$, który rozdzieli dwa słowa należące do L ;
- ▶ L zawiera słowo zawierające $+$ ale nie zawierające $=$ wtedy i tylko wtedy, gdy $+$ rozdziela dwa słowa należące do L ;
- ▶ L nie zawiera żadnych słów ponad te zdefiniowane powyżej.

Wobec powyższych zasad, słowo $12345 + 5678 = 987654321$ jest słowem języka L , ale $= 234 + +$ już nie jest.

Język ten, jak widzimy, opisuje liczby naturalne, poprawnie zbudowane wyrażenia określające dodawanie i poprawnie zbudowane wyrażenia określające równość dodawania.

Zwróćmy też uwagę, że język ten opisuje tylko to, jak dane wyrażenia wyglądają (a więc ich syntaktykę), nie odwołuje się natomiast do ich znaczenia (a więc semantyki).

W kontekście tego, co będziemy tu dalej robić, zamiast “słowo” danego języka będziemy na ogół pisać “formuła” danego języka. Jest to pierwszy z długiej listy przykładów tego, jak w zależności od kontekstu i zastosowania w logice jedno pojęcie ma 10 różnych nazw...

Systemy dedukcyjne.

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

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

Zauważmy, że alternatywnie możemy myśleć o dowodzie formuły A na gruncie formuł Γ jak o drzewie skończonym D , którego zbiór węzłów $D_0 \subset L$ i które spełnia następujące dwa warunki:

1. każdy liść jest elementem zbioru $AX \cup \Gamma$,
2. jeśli węzeł B jest wnioskiem z reguły

$$\frac{A_{i_1}, \dots, A_{i_k}}{B} r,$$

to wówczas $|B^+| = \{A_{i_1}, \dots, A_{i_k}\}$,

3. A jest korzeniem drzewa D .

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 .

Lemat:

Niech S będzie dowolnym systemem aksjomatycznym i niech $\Gamma, \Gamma', \Delta \subset L$ oraz $A \in L$. Wówczas:

1. jeżeli $\Gamma \vdash A$ oraz $\Gamma' \supset \Gamma$, to $\Gamma' \vdash A$;
2. $\Gamma \vdash A$ wtedy i tylko wtedy, gdy $\Gamma' \vdash A$ dla pewnego skończonego $\Gamma' \subset \Gamma$;
3. jeżeli $\Delta \vdash B$ dla każdego $B \in \Gamma$ oraz $\Gamma \vdash A$, to $\Delta \vdash A$.

Język logiki zdań.

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:

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

Klasyczny rachunek zdań.

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**:

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

Zauważmy, że klasyczny rachunek zdań zdefiniowaliśmy za pomocą nieskończonej liczby aksjomatów, ale skończonej liczby schematów. Dla językowych purystów powinniśmy więc mówić o metaaksjomatach.

Przyjmijmy też następujący skrót:

$$A \leftrightarrow B = (A \rightarrow B) \wedge (B \rightarrow A).$$

Zamiast pisać “klasyczny rachunek zdań” będziemy też używać skrótu KRZ.

Lemat:

$\vdash A \rightarrow A.$

Dowód:

$$(A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)) \quad (2)$$

$$A \rightarrow ((A \rightarrow) \rightarrow A) \quad (1)$$

$(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$ r_0 dla formuł z powyższych dwóch linijek

$$A \rightarrow (A \rightarrow A) \quad (1)$$

$A \rightarrow A$ r_0 dla formuł z powyższych dwóch linijek.

Twierdzenie o dedukcji [Herbrand, 1930]

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

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

Dowód:

($\Rightarrow$) Załóżmy, że $\Gamma \vdash A \rightarrow B$.

Niech $C_1, C_2, \dots, C_n = A \rightarrow B$ będzie dowodem $A \rightarrow B$ na gruncie Γ .

Wtedy, wobec reguły odrywania:

$$C_1, C_2, \dots, C_n = A \rightarrow B, A, B$$

jest dowodem B na gruncie Γ, A .

($\Leftarrow$) Załóżmy, że $\Gamma, A \vdash B$.

Niech $B_1, \dots, B_n = B$ będzie odpowiednim dowodem.

Pokażemy, że dla określonego $1 \leq i \leq n$ $\Gamma \vdash A \rightarrow B_i$.

Dowód prowadzimy przez indukcję.

Niech $i = 1$. Jeżeli $B_1 \in AX \cup \Gamma$, to:

$\vdash B_1 \rightarrow (A \rightarrow B_1)$ (1)

$\Gamma \vdash B_1$

$\Gamma \vdash A \rightarrow B_1$ r_0 .

Jeżeli $B_1 = A$, to wobec lematu $\vdash A \rightarrow A = B_1$.

Założmy, że $\Gamma \vdash A \rightarrow B_i$ dla $i < k$.

Pokażemy, że

$$\Gamma \vdash A \rightarrow B_k.$$

Jeżeli $B_k \in AX \cup \Gamma \cup \{A\}$, to:

$$\vdash B_k \rightarrow (A \rightarrow B_k) \text{ (1),}$$

$$\Gamma \vdash B_k$$

$$\Gamma \vdash A \rightarrow B_k \text{ } r_0.$$

Jeżeli istnieją takie $j, l < k$, że $B_j = B_l \rightarrow B_k$ (i B_k otrzymujemy przez zastosowanie r_0 do B_j i B_l), to wobec założenia indukcyjnego mamy:

$$\Gamma \vdash A \rightarrow B_l, \quad \Gamma \vdash A \rightarrow (B_l \rightarrow B_k).$$

Stosując (2) otrzymujemy

$$\Gamma \vdash (A \rightarrow (B_l \rightarrow B_k)) \rightarrow ((A \rightarrow B_l) \rightarrow (A \rightarrow B_k))$$

i stosując dwukrotnie r_0 dostajemy $\Gamma \vdash A \rightarrow B_k$.

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.

Dowód:

Należy pokazać, że

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

Wobec twierdzenia o dedukcji wystarczy pokazać, że

$$A \rightarrow B, B \rightarrow C, A \vdash C$$

co jest oczywiste wobec dwukrotnego zastosowania r_0 .

(2) Reguła **wewnętrznego odrywania**:

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

jest wyprowadzalna w KRZ.

Dowód:

Należy pokazać, że

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

Wobec twierdzenia o dedukcji wystarczy pokazać, że

$$A \rightarrow (B \rightarrow C), B, A \vdash C$$

co jest oczywiste wobec dwukrotnego zastosowania r_0 .

Lemat:

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

Dowód:

($\Rightarrow$) Załóżmy, że $\Gamma \vdash A \wedge B$ i zauważmy, że:

$$\vdash A \wedge B \rightarrow A \text{ (3)}$$

$$\vdash A \wedge B \rightarrow B \text{ (4)}$$

Wobec r_0 $\Gamma \vdash A$ oraz $\Gamma \vdash B$.

($\Leftarrow$) Załóżmy, że $\Gamma \vdash A$, $\Gamma \vdash B$. Wówczas:

$\vdash (A \rightarrow A) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow (A \wedge B)))$ (5),

$\vdash A \rightarrow A$,

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

$\vdash B \rightarrow (A \rightarrow B)$ (1),

$\Gamma \vdash B$ wobec założeń,

$\Gamma \vdash A \rightarrow B$ z poprzednich dwóch linijek,

$\Gamma \vdash A \rightarrow (A \wedge B)$ z linijki poprzedniej i trzeciej,

$\Gamma \vdash A$ wobec założeń,

$\Gamma \vdash A \wedge B$ z poprzednich dwóch linijek.

Wniosek:

Reguła **mnożenia**:

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

jest wyprowadzalna w KRZ.

Dowód:

$A, B \vdash A \wedge B$, co wynika z lematu dla $\Gamma = \{A, B\}$.

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 $\Gamma \vdash \neg A$).

Dowód:

$(\Rightarrow)$ oczywiste.

$(\Leftarrow)$ Załóżmy, że $\Gamma A \wedge \neg A$ dla pewnego A .

Wtedy $\Gamma \vdash A$ oraz $\Gamma \vdash \neg A$.

Ale wobec (9):

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

dla dowolnej formuły B .

Stąd, stosując dwukrotnie r_0 , $\Gamma \vdash B$ dla wszystkich B .

Czyli Γ jest sprzeczny.

Lemat:

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

Dowód:

($\Rightarrow$) Załóżmy, że $\Gamma, A \wedge B \vdash C$. Wystarczy pokazać, że $A, B \vdash A \wedge B$, co wynika z wyprowadzalności reguły mnożenia.

($\Leftarrow$) Załóżmy, że $\Gamma, A, B \vdash C$. Wystarczy pokazać, że

$$A \wedge B \vdash A \text{ oraz } A \wedge B \vdash B.$$

Wynika to z (3), (4) i twierdzenia o dedukcji.

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 $\Gamma, B \vdash C$.

Dowód:

($\Rightarrow$) Załóżmy, że $\Gamma, A \vee B \vdash C$.

Zauważmy, że $A \vdash A \vee B$, wobec (6) i twierdzenia o dedukcji.

Stąd $\Gamma, A \vdash C$.

Podobnie $B \vdash A \vee B$, wobec (7) i twierdzenia o dedukcji.

Stąd $\Gamma, B \vdash C$.

($\Leftarrow$) Załóżmy, że $\Gamma, A \vdash C$ oraz $\Gamma, B \vdash C$.

Zatem, na mocy twierdzenia o dedukcji

$$\Gamma \vdash A \rightarrow C \text{ oraz } \Gamma \vdash B \rightarrow C.$$

Ponadto, wobec (8):

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

Stąd $\Gamma \vdash A \vee B \rightarrow C$, czyli z twierdzenia o dedukcji

$$\Gamma, A \vee B \vdash C.$$

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.

Dowód:

($\Rightarrow$) Załóżmy, że $\Gamma \vdash \neg A$.

Wtedy $\Gamma, A \vdash \neg A$ i ponadto $\Gamma, A \vdash A$, co oznacza, że $\Gamma \cup \{A\}$ jest sprzeczny.

($\Leftarrow$) Załóżmy, że $\Gamma \cup \{A\}$ jest sprzeczny.

W szczególności $\Gamma, A \vdash \neg A$.

Zauważmy, że teraz $\vdash (A \rightarrow \neg A) \rightarrow \neg A$, wobec (10), oraz z założenia i z twierdzenia o dedukcji $\Gamma \vdash A \rightarrow \neg A$.

Stąd $\Gamma \vdash \neg A$.

Lemat:

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

Dowód:

$(\Rightarrow)$ Załóżmy, że $\Gamma \vdash A$.

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

Istotnie, ponieważ $\neg A \rightarrow (A \rightarrow B)$ jest aksjomatem, mamy na mocy twierdzenia o dedukcji $\neg A, A \vdash B$.

Stąd znowu na mocy twierdzenia o dedukcji

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

Zatem $\Gamma \vdash \neg A \rightarrow B$, czyli $\Gamma, \neg A \vdash B$.

Wobec dowolności B oznacza to sprzeczność zbioru $\Gamma \cup \{\neg A\}$.

($\Leftarrow$) Załóżmy, że $\Gamma \cup \{\neg A\}$ jest sprzeczny.
W szczególności mamy

$$\Gamma, \neg A \vdash \neg \neg A.$$

Ponadto wobec (10) $\vdash (\neg A \rightarrow \neg \neg A) \rightarrow \neg \neg A$.

Zatem $\Gamma \vdash \neg \neg A$, skąd wobec (11) i $\vdash \neg \neg A \rightarrow A$ otrzymujemy
 $\Gamma \vdash A$.

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