Instytut Informatyki

Teoretyczne Podstawy Języków Programowania

Wykład 1. Rachunek zdań jako system formalny

Zdzisław Spławski

- Motta
- Systemy formalne
- Podstawowe pojęcia logiczne
- Składnia rachunku zdań
- Semantyka rachunku zdań
- Konsekwencja logiczna
- Indukcja strukturalna dla formuł rachunku zdań
- Dowody konstruktywne
- Dedukcja naturalna dla rachunku zdań
- Konsekwencja syntaktyczna
- Twierdzenie o podstawianiu
- Najważniejsze rodzaje dowodów
- Przykłady wywodów w systemie dedukcji naturalnej
- Teorie aksjomatyczne
- Własności rachunku zdań
- Alfabet grecki

Motto dla informatyków

Szybkość zmian, zachodzących w informatyce, bardzo dobrze opisuje poniższy cytat.

Bo widzisz, u nas trzeba biec z całą szybkością, na jaką *ty* w ogóle możesz się zdobyć, ażeby pozostać w tym samym miejscu. A gdybyś się chciała gdzie indziej dostać, musisz biec przynajmniej dwa razy szybciej.

Lewis Carroll, *Po drugiej stronie Lustra*
(przekład Roberta Stillera)

Każdy student informatyki musi być na to przygotowany!

Motto dla matematyków (i informatyków)

Matematykiem jest, kto umie znajdować analogie między twierdzeniami; lepszym, kto widzi analogie dowodów, i jeszcze lepszym, kto dostrzega analogie teorii, a można wyobrazić sobie i takiego, co między analogiami widzi analogie.

Stefan Banach

System formalny = język formalny + aparat dedukcyjny (system wnioskowania).
Język formalny = zbiór słów (ciągów symboli) nad zadanym alfabetem (skończonym zbiorem symboli).
Metajęzyk = język, służacy do opisania języka formalnego (który bywa nazywany *językiem przedmiotowym*).
Aparat dedukcyjny (system wnioskowania) = aksjomaty + reguły transformacji (reguły wnioskowania, reguły inferencji).

W dalszym ciągu wykładu zostanie przedstawiony klasyczny rachunek zdań jako system formalny.

Aparat dedukcyjny operuje słowami jako obiektami syntaktycznymi bez zadanej interpretacji, w przeciwnym razie system nie byłby systemem formalnym.
Jeśli system formalny ma być użyteczny, to słowom języka formalnego trzeba przypisać pewne znaczenie — *semantykę* (interpretację).
Semantyka języka formalnego L składa się ze zbioru M, zwanego *modelem*, oraz z funkcji

$$S[\![\ldots]\!] : L \to M$$

nazywanej *funkcją semantyczną*. Argumenty funkcji semantycznych z powodów historycznych umieszcza się zwykle w specjalnych nawiasach $[\![\ldots]\!]$.

Przykład: Etapy generowania zbioru słów języka L

Alfabet: $\{\triangle, \square\}$.
Produkcje:

$$\textit{słowo} ::= \triangle \mid \square \mid \textit{słowo}\triangle \mid \textit{słowo}\square$$

etap		wygenerowane słowa
0		$\{\}$
1	$\cup$	$\{\triangle, \square\}$
2	$\cup$	$\{\triangle\triangle, \square\triangle, \triangle\square, \square\square\}$
3	$\cup$	$\{\triangle\triangle\triangle, \square\triangle\triangle, \triangle\square\triangle, \square\square\triangle, \triangle\triangle\square, \square\triangle\square, \triangle\square\square, \square\square\square\}$
$\vdots$	$\vdots$	$\vdots$

Przykład: Semantyka 1

Składnia			Semantyka		
słowo	::=		S_1	:	$L \to \mathbb{N}$
	$\mid$	$\triangle$	$S_1[\![\triangle]\!]$	$=$	0
	$\mid$	$\square$	$S_1[\![\square]\!]$	$=$	1
	$\mid$	$\mathit{słowo}\triangle$	$S_1[\![\mathit{słowo}\triangle]\!]$	$=$	$2 \cdot S_1[\![\mathit{słowo}]\!]$
	$\mid$	$\mathit{słowo}\square$	$S_1[\![\mathit{słowo}\square]\!]$	$=$	$2 \cdot S_1[\![\mathit{słowo}]\!] + 1$

Ta funkcja semantyczna interpretuje słowa języka jako liczebniki zapisane w systemie binarnym.
Semantyka jest *kompozycyjna* (ang. compositional), tzn. znaczenie każdego wyrażenia jest zdeterminowane semantyką jego podwyrażeń.

Przykład: Semantyka 2

$$
\begin{array}{rcl}
 & \text{Składnia} & \\
\textit{słowo} & ::= & \\
 & | & \triangle \\
 & | & \square \\
 & | & \textit{słowo}\triangle \\
 & | & \textit{słowo}\square
\end{array}
\qquad
\begin{array}{rcl}
 & \text{Semantyka} & \\
S_2 & : & L \to \mathbb{Z} \\
S_2[\![\triangle]\!] & = & 0 \\
S_2[\![\square]\!] & = & 1 \\
S_2[\![\textit{słowo}\triangle]\!] & = & -2 \cdot S_2[\![\textit{słowo}]\!] \\
S_2[\![\textit{słowo}\square]\!] & = & -2 \cdot S_2[\![\textit{słowo}]\!] + 1
\end{array}
$$

W tej semantyce każdej liczbie całkowitej odpowiada słowo w języku L.

Funktory prawdziwościowe a mowa potoczna

Logika ma swoje korzenie w starożytnej Grecji (Arystoteles, *Organon*). Jej celem było badanie języka i form poprawnego wnioskowania (gr. $\lambda o \gamma o \varsigma$ znaczy m.in. myślenie, rozumowanie, słowo, mowa). Współczesna *logika matematyczna* narodziła się w XIX wieku (Frege, Boole, Peano, Russell i inni) jako narzędzie do analizy rozumowań w matematyce oraz do badania struktury i własności teorii matematycznych.
Spójniki logiczne, wykorzystywane w rachunku zdań precyzują i formalizują spójniki zdaniowe, wykorzystywane w mowie potocznej.
Spójniki logiczne (nazywane też *funktorami prawdziwościowymi*) służą do tworzenia zdań złożonych ze zdań prostych.
Zdaniem prostym jest każde zdanie jednowyrazowe (np. „Grzmi") i każde zdanie wielowyrazowe, którego członami głównymi nie są zdania. Zdaniami prostymi są m.in. tzw. *zdania kategoryczne*, których członami głównymi, tj. argumentami funktora głównego, są tylko nazwy, np. „Ziemia jest planetą", „Ryby żyją w wodzie".

Cele rachunku zdań

- Rachunek zdań ma na celu wyjaśnienie roli spójników zdaniowych w procesie wnioskowania. W języku rachunku zdań występują tylko dwie istotne grupy symboli: zmienne zdaniowe oraz wyróżnione spójniki zdaniowe.
- Rachunek zdań nie wnika w wewnętrzną strukturę zdań atomowych, więc nie pozwala na przeprowadzanie wnioskowań, których poprawność zależy od tej struktury. Tym zajmuje się rachunek predykatów (nazywany też rachunkiem kwantyfikatorów).
- W logice klasycznej brana jest pod uwagę **wyłącznie** wartość logiczna zdania, tzn. rozważane są tylko zdania oznajmujące, które są albo prawdziwe, albo fałszywe.

Tabela najczęściej używanych spójników logicznych

Symbol	Inne oznaczenia	Schemat zdania	Sposób czytania	Nazwa zdania
$\neg$	$\sim, N$	$\neg\varphi$	nieprawda, że φ (nie φ)	negacja
$\wedge$	$\&, K$	$\varphi \wedge \psi$	φ i ψ	koniunkcja
$\vee$	A	$\varphi \vee \psi$	φ lub ψ	alternatywa
$\rightarrow$	$\Rightarrow, \supset, C$	$\varphi \rightarrow \psi$	jeżeli φ to ψ (z φ wynika ψ)	implikacja
$\leftrightarrow$	$\Leftrightarrow, \equiv, E$	$\varphi \leftrightarrow \psi$	φ wtw, gdy ψ	równoważność

„wtw” znaczy „wtedy i tylko wtedy” (ang. iff: „if and only if”). Prefiksowe symbole N, K, A, C, E zostały wprowadzone przez Jana Łukasiewicza w jego notacji beznawiasowej (notacja polska, ang. Polish notation)..

O implikacji

Zdanie $p \to q$, zbudowane za pomocą spójnika implikacji, też bywa nazywane implikacją. p nosi miano *poprzednika* implikacji, a q — *następnika* implikacji.

Należy zwrócić uwagę na to, że spójnik implikacji jest spójnikiem ekstensjonalnym (tak jak pozostałe spójniki) —- implikacja przyjmuje wartości logiczne zależące jedynie od wartości logicznych łączonych zdań.

Zauważmy też, że jeśli poprzednik implikacji p jest fałszywy, to całe zdanie jest **prawdziwe** (ex falso [sequitur] quodlibet, z fałszu [wynika] cokolwiek). Wobec tego zdanie: „Jeśli 2=3, to księżyc jest z sera" jest w logice klasycznej prawdziwe! W mowie potocznej zwykle zakładamy, że istnieje jakiś związek (np. przyczynowy) między poprzednikiem i następnikiem implikacji. W logice **klasycznej** uwzględniana jest **wyłącznie** wartość prawdziwościowa zdania.

O alternatywie

W języku polskim spójnik „lub” jest używany w trzech różnych znaczeniach, ponadto jest on często używany zamiennie ze spójnikiem „albo”. Może on znaczyć:

(a) „co najmniej jedno z dwojga”,

(b) „co najwyżej jedno z dwojga”,

(c) „dokładnie jedno z dwojga”.

Tabela wszystkich spójników dwuargumentowych

pq 00	pq 01	pq 10	pq 11		Schemat zdania	Sposób czytania	Nazwa zdania
0	0	0	0				S_0
0	0	0	1	$\wedge$	$\varphi \wedge \psi$	p i q	koniunkcja
0	0	1	0				S_2
0	0	1	1			p, choćby nawet q	S_3
0	1	0	0				S_4
0	1	0	1				S_5
0	1	1	0	$\oplus$	$p \oplus q$	p albo q	alternatywa wykluczająca
0	1	1	1	$\vee$	$p \vee q$	p lub q	alternatywa
1	0	0	0	$\downarrow$	$p \downarrow q$	ani p, ani q	binegacja (strzałka Peirce'a)
1	0	0	1	$\leftrightarrow$	$p \leftrightarrow q$	p wtw, gdy q	równoważność
1	0	1	0				S_{10}
1	0	1	1			p zawsze wtedy, gdy q	S_{11}
1	1	0	0				S_{12}
1	1	0	1	$\rightarrow$	$p \rightarrow q$	jeżeli p, to q	implikacja
1	1	1	0	$\mid$	$p \mid q$	albo nie p, albo nie q	dysjunkcja (kreska Sheffera)
1	1	1	1				S_{15}

Tabela spójników dwuargumentowych — uwagi

- Spójnik S_3 nie ma własnej nazwy; odpowiada mu zwrot „p, choćby nawet q".
- Alternatywa wykluczająca (rozłączna), zwana też *ekskluzją*, odpowiada spójnikowi „lub" w sensie (c), tj. „dokładnie jedno z dwojga".
- Alternatywa (niewykluczająca) odpowiada spójnikowi „lub" w sensie (a), tj. „co najmniej jedno z dwojga".
- Dysjunkcja (kreska Sheffera) odpowiada spójnikowi „lub" w sensie (b), tj. „co najwyżej jedno z dwojga".
- Spójnik S_{11} nie ma własnej nazwy; odpowiada mu zwrot „p zawsze wtedy, gdy q", czyli „jeżeli q, to p".

Binegacja (strzałka Peirce'a) i dysjunkcja (funktor Sheffera) to jedyne funktory, które same wystarczają do zdefiniowania wszystkich pozostałych funktorów zdaniotwórczych (jednoargumentowych i dwuargumentowych).

Spójniki logiczne a operatory w językach programowania

Niektóre z wymienionych w tabeli spójników mają szczególne znaczenie w językach programowania (operatory bitowe i operatory logiczne) i w elektronice (bramki logiczne).

	Operator bitowy	Operator logiczny	Bramka logiczna
$\neg p$	$\sim p$	$!\, p$	NOT
$p \wedge q$	$p \;\&\; q$	$p \;\&\&\; q$	AND
$p \vee q$	$p \mid q$	$p \mid\mid q$	OR
$p \oplus q$	p ˆ q		XOR = eXclusive OR
$p \downarrow q$			NOR = Not OR
$p \mid q$			NAND = Not AND

Operatory bitowe i logiczne w różnych językach programowania mogą być różnie oznaczane. W powyższej tabeli pokazano symbole, stosowane w językach, których składnia jest oparta na składni języka C (C++, Java, C#, Scala, Ruby ...).

Składnia języka rachunku zdań I

Alfabet: $\{p, ', \bot, \top, \wedge, \vee, \to, \leftrightarrow, \neg, (,)\}$

$$
\begin{array}{rcl}
\mathcal{F} & ::= & \mathcal{A} \mid (\neg\mathcal{F}) \mid (\mathcal{F} \wedge \mathcal{F}) \\
 & & \mid (\mathcal{F} \vee \mathcal{F}) \mid (\mathcal{F} \to \mathcal{F}) \\
 & & \mid (\mathcal{F} \leftrightarrow \mathcal{F}) \\
\mathcal{A} & ::= & \mathcal{V} \mid \bot \mid \top \\
\mathcal{V} & ::= & p \mid \mathcal{V}'
\end{array}
$$

$\mathcal{F}, \mathcal{A}, \mathcal{V}$ oznaczają odpowiednio kategorie syntaktyczne formuł rachunku zdań, atomów (zdań atomowych) i zmiennych zdaniowych.
Symbol $\bot$ będziemy czytać *falsum* (łac. fałsz), a symbol $\top$ będziemy czytać *verum* (łac. prawda).

Składnia języka rachunku zdań II

Konwencje notacyjne, pozwalające na czytelniejszy zapis formuł rachunku zdań.

1. Małe litery alfabetu łacińskiego $p, q, r, s \ldots$ (być może z indeksami) będą używane jako metazmienne oznaczające zmienne zdaniowe.
2. Małe litery alfabetu greckiego $\varphi, \psi, \rho, \ldots$ (być może z indeksami) będą używane jako metazmienne oznaczające dowolne formuły rachunku zdań.
3. Priorytety spójników logicznych (funktorów zdaniotwórczych) malejąco: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.
4. $\wedge, \vee$ łączą w lewo, a $\rightarrow, \leftrightarrow$ łączą w prawo.

Semantyka rachunku zdań I

Zbiór wartości logicznych $\mathbb{B} = \{\mathtt{F}, \mathtt{T}\}$ zawiera dwa elementy: $\mathtt{T}$(prawda) i $\mathtt{F}$(fałsz).
Na zbiorze $\mathbb{B}$ zdefiniujemy funkcje $f_{\neg} : \mathbb{B} \to \mathbb{B}$ oraz $f_{\wedge}, f_{\vee}, f_{\to}, f_{\leftrightarrow} : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ za pomocą poniższej tablicy:

x	y	$f_{\neg}(x)$	$f_{\wedge}(x,y)$	$f_{\vee}(x,y)$	$f_{\to}(x,y)$	$f_{\leftrightarrow}(x,y)$
F	F	T	F	F	T	T
F	T	T	F	T	T	F
T	F	F	F	T	F	F
T	T	F	T	T	T	T

Semantyka rachunku zdań II

Waluacją (ang. valuation) formuły φ nazywamy odwzorowanie $\sigma : \mathcal{V} \to \mathbb{B}$, nadające wartości logiczne zmiennym zdaniowym danej formuły.

Funkcja semantyczna (*interpretacja*) $\mathcal{E} : \mathcal{F} \to (\mathcal{V} \to \mathbb{B}) \to \mathbb{B}$ oblicza wartości logiczne formuł rachunku zdań (dla zadanej waluacji σ).

Semantyka jest *kompozycyjna* (ang. compositional), tzn. znaczenie każdego wyrażenia jest zdeterminowane semantyką jego podwyrażeń.

$$
\begin{array}{lcl@{\qquad}rcl}
 & \text{Składnia} & & & \text{Semantyka} & \\
\mathcal{F} & ::= & & \mathcal{E} & : & \mathcal{F} \to (\mathcal{V} \to \mathbb{B}) \to \mathbb{B} \\
 & | & p & \mathcal{E}[\![p]\!]\sigma & = & \sigma(p) \\
 & | & \bot & \mathcal{E}[\![\bot]\!]\sigma & = & \mathtt{F} \\
 & | & \top & \mathcal{E}[\![\top]\!]\sigma & = & \mathtt{T} \\
 & | & (\neg\varphi) & \mathcal{E}[\![(\neg\varphi)]\!]\sigma & = & f_{\neg}(\mathcal{E}[\![\varphi]\!]\sigma) \\
 & | & (\varphi \land \psi) & \mathcal{E}[\![(\varphi \land \psi)]\!]\sigma & = & f_{\land}(\mathcal{E}[\![\varphi]\!]\sigma, \mathcal{E}[\![\psi]\!]\sigma) \\
 & | & (\varphi \lor \psi) & \mathcal{E}[\![(\varphi \lor \psi)]\!]\sigma & = & f_{\lor}(\mathcal{E}[\![\varphi]\!]\sigma, \mathcal{E}[\![\psi]\!]\sigma) \\
 & | & (\varphi \to \psi) & \mathcal{E}[\![(\varphi \to \psi)]\!]\sigma & = & f_{\to}(\mathcal{E}[\![\varphi]\!]\sigma, \mathcal{E}[\![\psi]\!]\sigma) \\
 & | & (\varphi \leftrightarrow \psi) & \mathcal{E}[\![(\varphi \leftrightarrow \psi)]\!]\sigma & = & f_{\leftrightarrow}(\mathcal{E}[\![\varphi]\!]\sigma, \mathcal{E}[\![\psi]\!]\sigma)
\end{array}
$$

Semantyka rachunku zdań III

W logice (i nie tylko) terminy „syntaktyczny” i „semantyczny” mają poniższe znaczenia:

- *syntaktyczny*: dotyczący języków formalnych lub — szerzej — systemów formalnych, bez istotnego związku z ich interpretacją;
- *semantyczny*: dotyczący interpretacji języków formalnych.

Klasyfikacja formuł

Formuła φ jest:

- *spełniona* (ang. satisfied) przy danej waluacji zmiennych σ, czyli σ *spełnia* (ang. satisfies) formułę φ, jeżeli $\mathcal{E}[\![\varphi]\!]\sigma = \mathtt{T}$;
- *spełnialna* (ang. satisfiable) jeżeli istnieje waluacja zmiennych σ takie, że $\mathcal{E}[\![\varphi]\!]\sigma = \mathtt{T}$, np. p;
- *prawdziwa* (ang. valid) lub jest *tautologią* (ang. tautology) jeżeli dla każdej waluacji σ zachodzi $\mathcal{E}[\![\varphi]\!]\sigma = \mathtt{T}$, np. $p \vee \neg p$;
- *niespełnialna* (ang. unsatisfiable) jeżeli dla każdej waluacji σ zachodzi $\mathcal{E}[\![\varphi]\!]\sigma = \mathtt{F}$, np. $p \wedge \neg p$;

Zbiór formuł Γ *jest spełnialny*, jeżeli istnieje waluacja σ, spełniające wszystkie formuły $\varphi \in \Gamma$. Jeżeli taka waluacja nie istnieje, to *zbiór formuł* Γ *jest niespełnialny*.

Wybrane tautologie rachunku zdań I

$p \to p$	prawo tożsamości
$p \vee \neg p$	prawo wyłączonego środka, *tertium non datur*
$p \vee \neg p \leftrightarrow \top$	prawo wyłączonego środka
$\neg(p \wedge \neg p)$	prawo sprzeczności
$p \wedge \neg p \leftrightarrow \bot$	prawo sprzeczności
$\neg\neg p \leftrightarrow p$	prawo podwójnej negacji
$p \to q \leftrightarrow \neg p \vee q$	prawo definiowania implikacji
$p \to q \leftrightarrow \neg q \to \neg p$	prawo kontrapozycji (zwane też prawem transpozycji)
$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$	pierwsze prawo de Morgana
$\neg(p \vee q) \leftrightarrow \neg p \wedge \neg q$	drugie prawo de Morgana
$\neg(p \to q) \leftrightarrow p \wedge \neg q$	prawo negowania implikacji
$\neg(p \leftrightarrow q) \leftrightarrow \neg(p \to q) \vee \neg(q \to p)$	prawo negowania równoważności
$p \wedge p \leftrightarrow p$	prawo idempotentności koniunkcji
$p \vee p \leftrightarrow p$	prawo idempotentności alternatywy
$p \wedge q \leftrightarrow q \wedge p$	prawo przemienności koniunkcji
$p \vee q \leftrightarrow q \vee p$	prawo przemienności alternatywy
$p \wedge (q \wedge r) \leftrightarrow (p \wedge q) \wedge r$	prawo łączności koniunkcji
$p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$	prawo łączności alternatywy

Wybrane tautologie rachunku zdań II

$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$	prawo rozdzielności koniunkcji względem alternatywy
$p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$	prawo rozdzielności alternatywy względem koniunkcji
$(p \to q \wedge \neg q) \to \neg p$	prawo redukcji do absurdu
$((p \to q) \to p) \to p$	prawo Peirce'a
$(p \to \neg p) \to \neg p$	prawo Claviusa
$p \wedge \top \leftrightarrow p \qquad p \wedge \bot \leftrightarrow \bot$	prawa upraszczania
$p \vee \top \leftrightarrow \top \qquad p \vee \bot \leftrightarrow p$	prawa upraszczania

Metoda zero-jedynkowa I

Każda zmienna zdaniowa, występująca w formule zdaniowej może przyjmować albo wartość oznaczającą fałsz, albo wartość oznaczającą prawdę, a wartość całej formuły jest jednoznacznie wyznaczona przez wartości przypisane zmiennym. Ten fakt stanowi podstawę dla tak zwanej metody zero-jedynkowej rozstrzygania, czy dana formuła jest tautologią. W tabelach metody zero-jedynkowej zawsze fałsz jest zapisywany jako 0, a prawda jako 1 (stąd nazwa tej metody).

Metoda zero-jedynkowa jest metodą semantyczną.

Metoda zero-jedynkowa II

Poniższa tablica pokazuje, że prawo kontrapozycji jest tautologią rachunku zdań.

$$p \to q \leftrightarrow \neg q \to \neg p$$

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$	$p \to q \leftrightarrow \neg q \to \neg p$
0	0	1	1	1	1	1
0	1	1	0	1	1	1
1	0	0	1	0	0	1
1	1	0	0	1	1	1

Konsekwencja logiczna (semantyczna)

Niech Γ będzie zbiorem formuł, zaś φ formułą. Mówimy, że φ jest *konsekwencją logiczną* (lub *semantyczną*) zbioru Γ, co zapisujemy symbolicznie $\Gamma \models \varphi$, jeśli każda waluacja σ, spełniające wszystkie formuły ze zbioru Γ, spełnia również formułę φ.
Zwykle skracamy $\{\psi_1, \ldots, \psi_n\} \models \varphi$ do $\psi_1, \ldots, \psi_n \models \varphi$, oraz $\Gamma \cup \{\psi\} \models \varphi$ do $\Gamma, \psi \models \varphi$, a także $\emptyset \models \varphi$ do $\models \varphi$. Zauważ, że $\models \varphi$ wtw, gdy φ jest tautologią.

Twierdzenie. $\psi_1, \ldots, \psi_n \models \varphi$ wtw, gdy $\models \psi_1 \wedge \ldots \wedge \psi_n \to \varphi$.
Twierdzenie.
Jeśli $\Gamma \models \varphi$, to dla dowolnej formuły ρ zachodzi $\Gamma, \rho \models \varphi$.
Twierdzenie. Jeśli $\Gamma \models \varphi$, a ρ jest tautologią, to $\Gamma \setminus \{\rho\} \models \varphi$.

Systemy funkcjonalnie pełne

Każda formuła φ odpowiada pewnej funkcji $f_\varphi \stackrel{\text{def}}{=} \mathcal{E}[\![\varphi]\!] : (\mathcal{V} \to \mathbb{B}) \to \mathbb{B}$, przekształcającej waluację zmiennych w niej występujących w element zbioru $\mathbb{B}$. Mówimy wtedy, że formuła φ definiuje funkcję f_φ.

Definicja. Skończony zbiór funkcji boolowskich nazywamy funkcjonalnie pełnym, jeśli każdą funkcję boolowską da się zdefiniować za pomocą formuły zbudowanej wyłącznie ze spójników odpowiadających funkcjom z tego zbioru.

Oto kilka funkcjonalnie pełnych zbiorów:
$\{\to, \perp\}, \{\wedge, \neg\}, \{\vee, \neg\}, \{\to, \neg\}, \{\downarrow\}, \{|\}$.
Jako przykład pokazano poniżej, jak można zdefiniować wszystkie spójniki logiczne za pomocą $\to, \perp$.

$\neg\varphi \stackrel{\text{def}}{=} \varphi \to \perp, \quad \top \stackrel{\text{def}}{=} \neg\perp, \quad \varphi \vee \psi \stackrel{\text{def}}{=} \neg\varphi \to \psi,$

$\varphi \wedge \psi \stackrel{\text{def}}{=} \neg(\neg\varphi \vee \neg\psi), \quad \varphi \leftrightarrow \psi \stackrel{\text{def}}{=} (\varphi \to \psi) \wedge (\psi \to \varphi).$

Indukcja strukturalna dla formuł rachunku zdań

Niech P będzie własnością formuł. $P(\varphi)$ zachodzi dla wszystkich formuł $\varphi \in \mathit{form}$ jeśli spełnione są natępujące przesłanki:

1. $P(p)$ dla każdej zmiennej zdaniowej p,
2. $P(\bot), P(\top)$,
3. jeśli $P(\varphi)$ to $P((\neg\varphi))$,
4. jeśli $P(\varphi)$ oraz $P(\psi)$ to $P((\varphi \land \psi))$,
5. jeśli $P(\varphi)$ oraz $P(\psi)$ to $P((\varphi \lor \psi))$,
6. jeśli $P(\varphi)$ oraz $P(\psi)$ to $P((\varphi \to \psi))$,
7. jeśli $P(\varphi)$ oraz $P(\psi)$ to $P((\varphi \leftrightarrow \psi))$.

Przesłanki 1–2 stanowią podstawę indukcji, a przesłanki 3–7 stanowią krok indukcji.

Twierdzenie. Istnieją dwie niewymierne liczby a i b takie, że a^b jest wymierne.

Dowód. Albo $(\sqrt{2})^{\sqrt{2}}$ jest wymierne i wtedy $a = b = \sqrt{2}$ albo $(\sqrt{2})^{\sqrt{2}}$ jest niewymierne i wtedy $a = (\sqrt{2})^{\sqrt{2}}, b = \sqrt{2}$. ■

Dowód tego twierdzenie jest oczywiście poprawny w logice klasycznej. Jest to przykład dowodu niekonstruktywnego, ze względu na wykorzystanie reguły wyłączonego środka.

Pomimo, że twierdzenie jest dowiedzione i wiadomo, że liczby a i b istnieją, to nie można (na podstawie tego dowodu) znaleźć pary liczb spełniających warunek określony w twierdzeniu. Konstruktywny dowód tego twierdzenia jest oparty na twierdzeniu Gelfonda–Schneidera. Wynika z niego, że liczby $a = (\sqrt{2})^{\sqrt{2}}, b = \sqrt{2}$ spełniają powyższe twierdzenie.

Najbardziej znaną *logiką konstruktywną* jest *logika intuicjonistyczna*, wprowadzona przez Brouwera i rozwijana przez Heytinga i wielu następców. Znajduje ona wiele zastosowań w informatyce (*izomorfizm Curry'ego–Howarda*).

Systemy wnioskowania dla rachunku zdań

Zdefiniowaliśmy już formalnie język rachunku zdań i jego semantykę. Trzeba jeszcze zdefiniować aparat dedukcyjny (system wnioskowania, system dowodzenia). Istnieją różne formalizacje aparatu dedukcyjnego rachunku zdań.

- systemy hilbertowskie (David Hilbert)
- systemy gentzenowskie (Gerhard Gentzen)
  - dedukcja naturalna (ang. natural deduction): notacja założeniowa, notacja sekwentowa, wywody w stylu Fitcha ...
  - rachunek sekwentów (ang. sequent calculus)
- i inne.

Dalej zostanie przedstawiona dedukcja naturalna w notacji sekwentowej. Taka notacja jest zwykle używana w literaturze, poświęconej typom w językach programowania.
"Kanoniczna" pozycja na temat typów w językach programowania: B.C.Pierce, *Types and Programming Languages*, MIT Press, 2002

Dedukcja naturalna

Jednym z zadań logiki jest formalizacja i badanie rozumowań matematycznych (dowodów). Najbardziej zbliżone do rozumowań potocznych są systemy *dedukcji naturalnej* (*założeniowe*). Twórcami pierwszych takich systemów byli Stanisław Jaśkowski i Gerhard Gentzen w latach trzydziestych ubiegłego wieku. Intensywnie badał te systemy Dag Prawitz w latach sześćdziesiątych i siedemdziesiątych, a po nim inni.

Wywody (derywacje, ang. derivations), będące formalną reprezentacją dowodów (ang. proofs) matematycznych, są przedstawiane w postaci drzew.

Reguły wnioskowania (r. wyprowadzania, r. inferencji, ang. inference rules, derivation rules) mają następująca postać:

$$\frac{\text{przesłanka}_1 \qquad \ldots \qquad \text{przesłanka}_n}{\text{wniosek}}\ (\textit{nazwa r. wnioskowania})$$

Reguły pierwotne i wtórne (wyprowadzone)

- *Pierwotne reguły wnioskowania* systemu przyjmujemy bez dowodu, starając się dobierać je w ten sposób, by były jak najbardziej intuicyjne.
- *Reguły wtórne* (ang. derived rules) są wyprowadzane przy użyciu reguł pierwotnych i twierdzeń, które zostały udowodnione.
- Celem reguł wtórnych jest skracanie dowodów. Teoretycznie jednak te reguły są zbyteczne, ponieważ każdą tezę udowodnioną z użyciem reguł wtórnych można udowodnić używając wyłącznie reguł pierwotnych.

Niżej przedstawione są reguły pierwotne systemu dedukcji naturalnej w tradycyjnym podziale na *reguły wprowadzania* (dołączania) i *eliminacji* (opuszczania) dla wszystkich zdefiniowanych wcześniej spójników logicznych.
Są one poprawne zarówno dla klasycznej (prawdziwościowej) logiki zdań, jak i dla logiki intuicjonistycznej.
Na końcu umieszczono reguły wnioskowania właściwe tylko dla logiki klasycznej. Wystarczy dołączyć jedną z nich. Pozostałe można otrzymać jako reguły wtórne.

Reguły wnioskowania w notacji sekwentowej I

$$\frac{}{\varphi \vdash \varphi}\,(Ass)$$

$$\frac{\Gamma \vdash \varphi}{\Gamma, \psi \vdash \varphi}\,(W)$$

reguły wprowadzania	reguły eliminacji
$\dfrac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\,(\to I)$	$\dfrac{\Gamma_1 \vdash \varphi \to \psi \qquad \Gamma_2 \vdash \varphi}{\Gamma_1, \Gamma_2 \vdash \psi}\,(\to E)$
$\dfrac{\Gamma, \varphi \vdash \bot}{\Gamma \vdash \neg\varphi}\,(\neg I)$	$\dfrac{\Gamma_1 \vdash \neg\varphi \qquad \Gamma_2 \vdash \varphi}{\Gamma_1, \Gamma_2 \vdash \bot}\,(\neg E)$

Reguły wnioskowania w notacji sekwentowej II

reguły wprowadzania	reguły eliminacji
$\dfrac{\Gamma_1 \vdash \varphi \qquad \Gamma_2 \vdash \psi}{\Gamma_1, \Gamma_2 \vdash \varphi \wedge \psi}\,(\wedge I)$	$\dfrac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\,(\wedge E_1)$ $\dfrac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\,(\wedge E_2)$
$\dfrac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\,(\vee I_1)$ $\dfrac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\,(\vee I_2)$	$\dfrac{\Gamma_1 \vdash \varphi \vee \psi \qquad \Gamma_2, \varphi \vdash \rho \qquad \Gamma_3, \psi \vdash \rho}{\Gamma_1, \Gamma_2, \Gamma_3 \vdash \rho}\,(\vee E)$
$\dfrac{}{\vdash \top}\,(\top I)$	brak
brak	$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\,(\bot E)$

Reguły wnioskowania w notacji sekwentowej III

reguły wprowadzania	reguły eliminacji
$\dfrac{\Gamma_1, \varphi \vdash \psi \qquad \Gamma_2, \psi \vdash \varphi}{\Gamma_1, \Gamma_2 \vdash \varphi \leftrightarrow \psi}\ (\leftrightarrow I)$	$\dfrac{\Gamma_1 \vdash \varphi \leftrightarrow \psi \qquad \Gamma_2 \vdash \varphi}{\Gamma_1, \Gamma_2 \vdash \psi}\ (\leftrightarrow E_1)$ $\dfrac{\Gamma_1 \vdash \varphi \leftrightarrow \psi \qquad \Gamma_2 \vdash \psi}{\Gamma_1, \Gamma_2 \vdash \varphi}\ (\leftrightarrow E_2)$

dla logiki klasycznej
$\dfrac{\Gamma, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi}\ (RAA)$ lub $\dfrac{\Gamma \vdash \neg\neg\varphi}{\Gamma \vdash \varphi}\ (\neg\neg)$ lub $\dfrac{}{\vdash \varphi \vee \neg\varphi}\ (TND)$

(RAA) — reductio ad absurdum (reguła sprowadzenia do sprzeczności)

(TND) — tertium non datur (reguła wykluczonego środka)

$(\neg\neg)$ — reguła podwójnego zaprzeczenia

Reguły wnioskowania w notacji sekwentowej IV

Niektóre z wymienionych wyżej reguł były znane już w starożytności.

$(\to E)$ — modus ponendo ponens (łac. sposób (tryb) potwierdzający przez potwierdzenie), krócej modus ponens; reguła odrywania.
$(\bot E)$ — ex falso (sequitur) quodlibet; z fałszu (wynika) cokolwiek.
(RAA) — reductio ad absurdum; reguła sprowadzenia do niedorzeczności.
(TND) — tertium non datur; reguła wykluczonego środka.
$(\neg\neg)$ — reguła podwójnego zaprzeczenia.

Z konstruktywnego punktu widzenia RAA pozwala na wyciągnięcie mocnych wniosków ze słabych przesłanek. Np. w $\neg(\varphi \land \psi) \vdash \neg\varphi \lor \neg\psi$ przesłanka jest słaba (coś nie ma dowodu), natomiast wniosek jest silny (konstruktywny dowód zawiera informację, który z członów alternatywy został udowodniony).

Prawo symplifikacji: $\vdash \varphi \to \psi \to \varphi$

Notacja sekwentowa.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \vdash p}\,(Ass)}{p, q \vdash p}\,(W)}{p \vdash q \to p}\,(\to I)}{\vdash p \to q \to p}\,(\to I)$$

Prawo sylogizmu hipotetycznego (przechodniość implikacji):

$\vdash (\varphi \to \psi) \to (\psi \to \rho) \to \varphi \to \rho$

Notacja sekwentowa.

$$
\dfrac{\dfrac{}{\psi \to \rho \vdash \psi \to \rho}\,(Ass) \qquad \dfrac{\dfrac{}{\varphi \to \psi \vdash \varphi \to \psi}\,(Ass) \qquad \dfrac{}{\varphi \vdash \varphi}\,(Ass)}{\varphi \to \psi, \varphi \vdash \psi}\,(\to E)}{\dfrac{\psi \to \rho, \varphi \to \psi, \varphi \vdash \rho}{\dfrac{\psi \to \rho, \varphi \to \psi \vdash \varphi \to \rho}{\dfrac{\varphi \to \psi \vdash (\psi \to \rho) \to \varphi \to \rho}{\vdash (\varphi \to \psi) \to (\psi \to \rho) \to \varphi \to \rho}\,(\to I)}\,(\to I)}\,(\to I)}\,(\to E)
$$

Prawo importacji: $\vdash (\varphi \to \psi \to \rho) \to (\varphi \wedge \psi \to \rho)$

Notacja sekwentowa.

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{(Ass)}
\UnaryInfC{$p \to q \to r \vdash p \to q \to r$}
\AxiomC{}
\RightLabel{(Ass)}
\UnaryInfC{$p \wedge q \vdash p \wedge q$}
\RightLabel{$(\wedge E)$}
\UnaryInfC{$p \wedge q \vdash p$}
\RightLabel{$(\to E)$}
\BinaryInfC{$p \to q \to r, p \wedge q \vdash q \to r$}
\AxiomC{}
\RightLabel{(Ass)}
\UnaryInfC{$p \wedge q \vdash p \wedge q$}
\RightLabel{$(\wedge E)$}
\UnaryInfC{$p \wedge q \vdash q$}
\RightLabel{$(\to E)$}
\BinaryInfC{$p \to q \to r, p \wedge q \vdash r$}
\RightLabel{$(\to I)$}
\UnaryInfC{$p \to q \to r \vdash p \wedge q \to r$}
\RightLabel{$(\to I)$}
\UnaryInfC{$\vdash (p \to q \to r) \to (p \wedge q \to r)$}
\end{prooftree}
$$

Przemienność alternatywy: $\vdash (\varphi \vee \psi) \to (\psi \vee \varphi)$

Notacja sekwentowa.

$$\dfrac{\dfrac{}{p \vee q \vdash p \vee q}(Ass) \qquad \dfrac{\dfrac{}{p \vdash p}(Ass)}{p \vdash q \vee p}(\vee I) \qquad \dfrac{\dfrac{}{q \vdash q}(Ass)}{q \vdash q \vee p}(\vee I)}{\dfrac{p \vee q \vdash q \vee p}{\vdash (p \vee q) \to (q \vee p)}(\to I)}(\vee E)$$

Reguły wnioskowania w notacji założeniowej I

reguły wprowadzania	reguły eliminacji
$\dfrac{\varphi \qquad \psi}{\varphi \wedge \psi}\,(\wedge I)$	$\dfrac{\varphi \wedge \psi}{\varphi}\,(\wedge E_1) \qquad \dfrac{\varphi \wedge \psi}{\psi}\,(\wedge E_2)$
$\dfrac{\varphi}{\varphi \vee \psi}\,(\vee I_1) \qquad \dfrac{\psi}{\varphi \vee \psi}\,(\vee I_2)$	$\dfrac{\varphi \vee \psi \qquad \begin{array}{c}[\varphi]^n\\ \vdots\\ \rho\end{array} \qquad \begin{array}{c}[\psi]^n\\ \vdots\\ \rho\end{array}}{\rho}\,{}_n(\vee E)$
$\dfrac{}{\top}\,(\top I)$	brak
brak	$\dfrac{\bot}{\varphi}\,(\bot E)$

Reguły wnioskowania w notacji założeniowej II

reguły wprowadzania	reguły eliminacji
$$\dfrac{\begin{array}{c}[\varphi]^n \\ \vdots \\ \psi\end{array}}{\varphi \to \psi}\ {}_n(\to I)$$	$$\dfrac{\varphi \to \psi \qquad \varphi}{\psi}\ (\to E)$$
$$\dfrac{\begin{array}{c}[\varphi]^n \\ \vdots \\ \bot\end{array}}{\neg\varphi}\ {}_n(\neg I)$$	$$\dfrac{\neg\varphi \qquad \varphi}{\bot}\ (\neg E)$$

Reguły wnioskowania w notacji założeniowej III

reguły wprowadzania	reguły eliminacji
$$\dfrac{\begin{matrix}[\varphi]^n & & [\psi]^n \\ \vdots & & \vdots \\ \psi & & \varphi\end{matrix}}{\varphi \leftrightarrow \psi}\ {}_n(\leftrightarrow I)$$	$$\dfrac{\varphi \leftrightarrow \psi \qquad \varphi}{\psi}\ (\leftrightarrow E_1) \qquad \dfrac{\varphi \leftrightarrow \psi \qquad \psi}{\varphi}\ (\leftrightarrow E_2)$$

dla logiki klasycznej

$$\dfrac{\begin{matrix}[\neg\varphi]^n \\ \vdots \\ \bot\end{matrix}}{\varphi}\ {}_n(RAA) \qquad \text{lub} \qquad \dfrac{\neg\neg\varphi}{\varphi}\ (\neg\neg) \qquad \text{lub} \qquad \dfrac{}{\varphi \vee \neg\varphi}\ (TND)$$

Prawo symplifikacji: $\vdash \varphi \to \psi \to \varphi$

Notacja założeniowa.

$$\dfrac{\dfrac{[p]^1}{q \to p}\,(\to I)}{p \to q \to p}\,{}_1(\to I)$$

Uwaga. W notacji założeniowej możliwe jest użycie reguły $(\to I)$ bez zamykania żadnego założenia.

Prawo sylogizmu hipotetycznego (przechodniość implikacji):

$\vdash (\varphi \to \psi) \to (\psi \to \rho) \to \varphi \to \rho$

Notacja założeniowa.

$$\dfrac{\dfrac{\dfrac{\dfrac{[\psi \to \rho]^1 \qquad \dfrac{[\varphi \to \psi]^2 \qquad [\varphi]^3}{\psi}\,(\to E)}{\rho}\,(\to E)}{\varphi \to \rho}\,{}_3(\to I)}{(\psi \to \rho) \to \varphi \to \rho}\,{}_1(\to I)}{(\varphi \to \psi) \to (\psi \to \rho) \to \varphi \to \rho}\,{}_2(\to I)$$

Prawo importacji: $\vdash (\varphi \to \psi \to \rho) \to (\varphi \wedge \psi \to \rho)$

Notacja założeniowa.

$$
\begin{prooftree}
\AxiomC{$[p \to q \to r]^1$}
\AxiomC{$[p \wedge q]^2$}
\RightLabel{$(\wedge E)$}
\UnaryInfC{p}
\RightLabel{$(\to E)$}
\BinaryInfC{$q \to r$}
\AxiomC{$[p \wedge q]^2$}
\RightLabel{$(\wedge E)$}
\UnaryInfC{q}
\RightLabel{$(\to E)$}
\BinaryInfC{r}
\RightLabel{${}_2(\to I)$}
\UnaryInfC{$p \wedge q \to r$}
\RightLabel{${}_1(\to I)$}
\UnaryInfC{$(p \to q \to r) \to (p \wedge q \to r)$}
\end{prooftree}
$$

Przemienność alternatywy: $\vdash (\varphi \vee \psi) \to (\psi \vee \varphi)$

Notacja założeniowa.

$$\dfrac{\dfrac{[p \vee q]^1 \qquad \dfrac{[p]^2}{q \vee p}\,(\vee I) \qquad \dfrac{[q]^2}{q \vee p}\,(\vee I)}{q \vee p}\,{}_2(\vee E)}{(p \vee q) \to (q \vee p)}\,{}_1(\to I)$$

Konsekwencja syntaktyczna

Niech Γ będzie zbiorem formuł, zaś φ formułą.

- Mówimy, że φ jest *konsekwencją syntaktyczną* zbioru Γ, lub jest *wywodliwa* (*wyprowadzalna*, ang. derivable) ze zbioru Γ, co zapisujemy symbolicznie $\Gamma \vdash \varphi$, jeśli istnieje wywód (derywacja) formuły φ ze zbioru Γ.
  Zwykle skracamy $\{\psi_1, \ldots, \psi_n\} \vdash \varphi$ do $\psi_1, \ldots, \psi_n \vdash \varphi$, oraz $\Gamma \cup \{\psi\} \vdash \varphi$ do $\Gamma, \psi \vdash \varphi$, a także $\emptyset \vdash \varphi$ do $\vdash \varphi$.
- Jeśli $\vdash \varphi$ to φ jest *twierdzeniem* (tezą) rozważanego systemu formalnego.
- *Zbiór formuł* Γ *jest sprzeczny* (ang. inconsistent), jeśli dla każdego φ zachodzi $\Gamma \vdash \varphi$, tzn. jeśli każda formuła jest twierdzeniem. W przeciwnym razie *zbiór* Γ *jest niesprzeczny* (ang. consistent).

Definicja. *Podstawieniem* (ang. substitution) formuły ψ za zmienną zdaniową p nazywamy odwzorowanie, które formule φ przyporządkowuje formułę $\varphi[\psi/p]$ powstałą w wyniku wstawienia formuły ψ w miejsce każdego wystąpienia zmiennej zdaniowej p w formule φ. Zdefiniujemy to odwzorowanie formalnie przez rekursję po strukturze formuły φ.

$$q[\psi/p] \stackrel{\text{def}}{=} \begin{cases} \psi, & \text{gdy } q = p \\ q, & \text{gdy } q \neq p \end{cases}$$

$$\Box[\psi/p] \stackrel{\text{def}}{=} \Box \quad (\Box \in \{\bot, \top\})$$

$$(\neg\varphi)[\psi/p] \stackrel{\text{def}}{=} (\neg\varphi[\psi/p])$$

$$(\varphi_1 \Box \varphi_2)[\psi/p] \stackrel{\text{def}}{=} (\varphi_1[\psi/p] \Box \varphi_2[\psi/p]) \quad (\Box \in \{\wedge, \vee, \rightarrow, \leftrightarrow\})$$

Twierdzenie (o podstawianiu). (ang. substitution theorem)

(a) Jeśli $\models \varphi$ to $\models \varphi[\psi/p]$.

(b) Jeśli $\vdash \varphi$ to $\vdash \varphi[\psi/p]$.

Przykład. Udowodniliśmy, że formuła $(p \rightarrow q \rightarrow r) \rightarrow (p \wedge q \rightarrow r)$ jest tezą rachunku zdań. Na podstawie powyższego twierdzenia tezą rachunku zdań jest każda formuła o postaci $(\varphi \rightarrow \psi \rightarrow \rho) \rightarrow (\varphi \wedge \psi \rightarrow \rho)$ dla dowolnych φ, ψ, ρ.

Tezy implikacyjne a reguły wtórne

Twierdzenie. Niech formuła o postaci $\varphi_1 \to \ldots \to \varphi_n \to \psi$ będzie tezą rachunku zdań. Poniższa reguła jest wówczas regułą wtórną.

$$\frac{\varphi_1 \qquad \ldots \qquad \varphi_n}{\psi}\ (\textit{nazwa reguły})$$

Dowód. Jeśli w pewnym wywodzie występują wszystkie przesłanki $\varphi_1, \ldots, \varphi_n$, to przez n-krotne zastosowanie reguły $(\to E)$ otrzymamy w wywodzie wniosek ψ. ■

Przykład. Ponieważ prawo importacji $(\varphi \to \psi \to \rho) \to (\varphi \land \psi \to \rho)$ jest tezą rachunku zdań, to do systemu możemy dołączyć regułę wtórną $(Import)$:

$$\frac{\varphi \to \psi \to \rho}{\varphi \land \psi \to \rho}\ (Import)$$

Dowody (założeniowe) wprost i nie wprost

- Dowód wprost formuły $\varphi \to \psi$.
  Zakładamy, że zachodzi φ. Przy tym założeniu dowodzimy ψ i stosujemy regułę $(\to I)$. Prawo importacji udowodniliśmy wprost.
- Dowód nie wprost (apagogiczny, przez sprowadzenie do niedorzeczności) formuły ψ.
  Zakładamy, że zachodzi $\neg\psi$. Przy tym założeniu dowodzimy $\perp$ i stosujemy regułę (RAA).

Wywód w stylu Fitcha

- Przedstawianie wywodów w postaci drzew dobrze reprezentuje ich strukturę, możliwa jest jednak linearna prezentacja wywodów. W celu pokazania struktury wywodów Jaśkowski początkowo używał prostokątów ("pudełek"). F.B.Fitch, W.Craig, L.Borkowski, J.Słupecki w swoich notacjach wykorzystali idee Jaśkowskiego.
- Zamiast wywodów w postaci drzew można używać notacji Fitcha. Pojawia się tam pojęcie *dowodu podporządkowanego* (pobocznego, ang. subordinate proof) oraz wprowadzona jest pomocnicza *reguła repetycji* (ang. reiteration), pozwalająca na powtórzenie w dowodzie podporządkowanym wcześniejszych formuł z dowodu głównego. Reguła repetycji (R) odpowiada prawu repetycji $\varphi \to \varphi$.
- Wywód (derywacja) w stylu Fitcha składa się z numerowanych wierszy, zawierających formuły wraz z uzasadnieniami. Każda formuła jest albo założeniem, rozpoczynającym nowy dowód poboczny (na ogół bez uzasadnienia), albo formułą wyprowadzoną (zawsze z uzasadnieniem).

Prawo symplifikacji: $\vdash \varphi \to \psi \to \varphi$
Wywód w stylu Fitcha

1	p	założenie
2	q	założenie
3	p	(R), 1
4	$q \to p$	$(\to I)$, 2–3
5	$p \to q \to p$	$(\to I)$, 1–4

Prawo importacji: $\vdash (\varphi \to \psi \to \rho) \to (\varphi \wedge \psi \to \rho)$

Wywód w stylu Fitcha

1	$p \to q \to r$	założenie
2	$p \wedge q$	założenie
3	p	$(\wedge E)$, 2
4	$p \to q \to r$	(R), 1
5	$q \to r$	$(\to E)$, 4, 3
6	q	$(\wedge E)$, 2
7	r	$(\to E)$, 5, 6
8	$p \wedge q \to r$	$(\to I)$, 2–7
9	$(p \to q \to r) \to (p \wedge q \to r)$	$(\to I)$, 1–8

Przemienność alternatywy: $\vdash (\varphi \lor \psi) \to (\psi \lor \varphi)$
Wywód w stylu Fitcha

1	$\quad \mid p \lor q$	założenie
2	$\quad \mid \quad \mid p$	założenie
3	$\quad \mid \quad \mid q \lor p$	$(\lor I)$, 2
4	$\quad \mid \quad \mid q$	założenie
5	$\quad \mid \quad \mid q \lor p$	$(\lor I)$, 4
6	$\quad \mid q \lor p$	$(\lor E)$, 1, 2–3, 4–5
7	$(p \lor q) \to (q \lor p)$	$(\to I)$, 1–6

Prawo De Morgana: $\neg(\varphi \vee \psi) \vdash \neg\varphi \wedge \neg\psi$

$$
\dfrac{
\dfrac{
\dfrac{\neg(p \vee q) \qquad \dfrac{[p]^1}{p \vee q}\,(\vee I)}{\bot}\,(\neg E)
}{\neg p}\,{}_1(\neg I)
\qquad
\dfrac{
\dfrac{\neg(p \vee q) \qquad \dfrac{[q]^2}{p \vee q}\,(\vee I)}{\bot}\,(\neg E)
}{\neg q}\,{}_2(\neg I)
}{\neg p \wedge \neg q}\,(\wedge I)
$$

To jest kolejny przykład na dowód wprost. Niezamknięte założenie możemy potraktować jako przesłankę wtórnej (wyprowadzonej) reguły wnioskowania $(\neg\vee)$.

$$
\dfrac{\neg(\varphi \vee \psi)}{\neg\varphi \wedge \neg\psi}\,(\neg\vee)
$$

Prawo De Morgana: $\neg(\varphi \lor \psi) \vdash \neg\varphi \land \neg\psi$. Wywód w stylu Fitcha

1	$\neg(p \lor q)$	przesłanka
2	$\quad p$	
3	$\quad p \lor q$	$(\lor I)$, 2
4	$\quad \neg(p \lor q)$	(R), 1
5	$\quad \bot$	$(\neg E)$, 4, 3
6	$\neg p$	$(\neg I)$, 2–5
7	$\quad q$	
8	$\quad p \lor q$	$(\lor I)$, 7
9	$\quad \neg(p \lor q)$	(R), 1
10	$\quad \bot$	$(\neg E)$, 9, 8
11	$\neg q$	$(\neg I)$, 7–10
12	$\neg p \land \neg q$	$(\land I)$, 6, 11

Prawo De Morgana: $\vdash \neg(\varphi \wedge \psi) \to \neg\varphi \vee \neg\psi$

$$\mathcal{D} = \dfrac{\dfrac{[\neg(\neg p \vee \neg q)]^2 \qquad \dfrac{[\neg q]^4}{\neg p \vee \neg q}\,(\vee I)}{\bot}\,(\neg E)}{q}\,{}_4(RAA)$$

$$\dfrac{\dfrac{\dfrac{[\neg(p \wedge q)]^1 \qquad \dfrac{\dfrac{\dfrac{[\neg(\neg p \vee \neg q)]^2 \qquad \dfrac{[\neg p]^3}{\neg p \vee \neg q}\,(\vee I)}{\bot}\,(\neg E)}{p}\,{}_3(RAA) \qquad \mathcal{D}}{p \wedge q}\,(\wedge I)}{\bot}\,(\neg E)}{\neg p \vee \neg q}\,{}_2(RAA)}{\neg(p \wedge q) \to \neg p \vee \neg q}\,{}_1(\to I)$$

Tu stosowaliśmy (RAA), więc jest to dowód nie wprost. Na podstawie twierdzenia o związku tez z regułami wtórnymi do systemu możemy dodać regułę

$$\dfrac{\neg(\varphi \wedge \psi)}{\neg\varphi \vee \neg\psi}\,(\neg\wedge)$$

Prawo De Morgana: $\vdash \neg(\varphi \land \psi) \to \neg\varphi \lor \neg\psi$.

Inny (krótszy) dowód nie wprost, wykorzystujący regułę wtórną $(\neg\lor)$.

1	$\neg(p \land q)$	
2	$\neg(\neg p \lor \neg q)$	
3	$\neg\neg p \land \neg\neg q)$	$(\neg\lor)$, 2
4	$\neg\neg p$	$(\land E)$, 3
5	p	$(\neg\neg)$, 4
6	$\neg\neg q$	$(\land E)$, 3
7	q	$(\neg\neg)$, 6
8	$p \land q$	$(\land I)$, 5, 7
9	$\neg(p \land q)$	(R), 1
10	$\bot$	$(\neg E)$, 9, 8
11	$\neg p \lor \neg q$	(RAA), 2–10
12	$\neg(p \land q) \to \neg p \lor \neg q$	$(\to I)$, 1–11

Transpozycja (kontrapozycja): $\neg\psi \to \neg\varphi \vdash \varphi \to \psi$

Wykorzystywany jest dowód nie wprost.

$$\cfrac{\cfrac{\cfrac{\cfrac{\neg\psi \to \neg\varphi \qquad [\neg\psi]^2}{\neg\varphi}\,(\to E) \qquad [\varphi]^1}{\bot}\,(\neg E)}{\psi}\,{}_2(RAA)}{\varphi \to \psi}\,{}_1(\to I)$$

Możemy do systemu dołączyć regułę wtórną:

$$\frac{\neg\psi \to \neg\varphi}{\varphi \to \psi}\,(Transp)$$

Reguła ta jest często stosowana przy dowodach nie wprost.

$\vdash \neg\neg(p \vee \neg p)$

W logice konstruktywnej $\nvdash p \vee \neg p$.

$$\dfrac{\dfrac{}{\neg(p \vee \neg p) \vdash \neg(p \vee \neg p)}\,(Ass) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\neg(p \vee \neg p) \vdash \neg(p \vee \neg p)}\,(Ass) \qquad \dfrac{\dfrac{}{p \vdash p}\,(Ass)}{p \vdash p \vee \neg p}\,(\vee I)}{\neg(p \vee \neg p), p \vdash \bot}\,(\neg E)}{\neg(p \vee \neg p) \vdash \neg p}\,(\neg I)}{\neg(p \vee \neg p) \vdash p \vee \neg p}\,(\vee I)}{\dfrac{\neg(p \vee \neg p) \vdash \bot}{\vdash \neg\neg(p \vee \neg p)}\,(\neg I)}\,(\neg E)$$

Teorie aksjomatyczne

Definicja. Zbiór formuł $\mathcal{T}$ nazywamy *teorią* wtw, gdy jest on zamknięty ze względu na konsekwencję syntaktyczną, tzn. jeśli $\mathcal{T} \vdash \varphi$, to $\varphi \in \mathcal{T}$. Elementy zbioru $\mathcal{T}$ nazywamy twierdzeniami(tezami). Niech Γ będzie zbiorem formuł. $\mathcal{T}(\Gamma) = \{\varphi \mid \Gamma \vdash \varphi\}$ nazywamy teorią zbioru formuł Γ. Formuły ze zbioru Γ nazywamy *aksjomatami pozalogicznymi (swoistymi, specyficznymi)* teorii, a o teorii $\mathcal{T}(\Gamma)$ mówimy, że jest *teorią aksjomatyczną* (lub *aksjomatyzowalną*).

Własności teorii aksjomatycznych

Niech będzie dana teoria $\mathcal{T}(\Gamma)$.

- **Niesprzeczność** (ang. consistency). Teoria $\mathcal{T}$ jest niesprzeczna wtw, gdy zbiór formuł $\mathcal{T}$ jest niesprzeczny.
- **Zupełność.** Każda formuła φ jest albo twierdzeniem teorii, tzn. $\Gamma \vdash \varphi$, albo po dołączeniu do aksjomatów teorii prowadzi do sprzeczności teorii.
- **Poprawność, adekwatność** (ang. soundness). Jeśli $\Gamma \vdash \varphi$ to $\Gamma \models \varphi$.
- **Pełność** (ang. completeness). Jeśli $\Gamma \models \varphi$ to $\Gamma \vdash \varphi$.
- **Rozstrzygalność** (ang. decidability). Teoria $\mathcal{T}$ jest rozstrzygalna wtw, gdy istnieje algorytm, który dla dowolnej formuły zamkniętej φ pozwala stwierdzić, czy $\Gamma \vdash \varphi$, czy też $\Gamma \nvdash \varphi$.

Dla $\Gamma = \emptyset$ poprawność mówi, że każde twierdzenie jest zdaniem prawdziwym, natomiast pełność mówi, że każde zdanie prawdziwe można udowodnić (jest twierdzeniem).

Przykład teorii aksjomatyzowalnej

Zespół ekspertów przygotował następującą analizę sytuacji gospodarczej Loglandii.

Jeśli inwestycje pozostaną na tym samym poziomie, to wzrosną wydatki budżetowe lub wzrośnie bezrobocie. Jeśli wydatki budżetowe nie wzrosną, to podatki zostaną obniżone. Jeśli podatki zostaną obniżone i inwestycje pozostaną na tym samym poziomie, to bezrobocie nie wzrośnie.

Możemy przedstawić ten opis wycinka rzeczywistości w postaci teorii. Wprowadźmy następujące oznaczenia.

$p \stackrel{\text{def}}{=}$ *inwestycje pozostaną na tym samym poziomie*

$q \stackrel{\text{def}}{=}$ *wzrosną wydatki budżetowe*

$r \stackrel{\text{def}}{=}$ *wzrośnie bezrobocie*

$s \stackrel{\text{def}}{=}$ *podatki zostaną obniżone*

Zbiór Γ aksjomatów swoistych teorii $\mathcal{SGL}(\Gamma)$ jest następujący:

$\Gamma = \{p \to q \vee r, \neg q \to s, s \wedge p \to \neg r\}$

Własności rachunku zdań

(Meta)Twierdzenie.
Rachunek zdań jest niesprzeczny, zupełny, poprawny, pełny i rozstrzygalny.

A, α	alfa	N, ν	ni
B, β	beta	Ξ, ξ	ksi
Γ, γ	gamma	O, o	omikron
Δ, δ, ∂	delta	Π, π, ϖ	pi
E, ϵ, ε	epsilon	P, ρ, ϱ	ro
Z, ζ	dzeta	$\Sigma, \sigma, \varsigma$	sigma
H, η	eta	T, τ	tau
$\Theta, \theta, \vartheta$	teta	Υ, υ	ypsilon
I, ι	jota	Φ, ϕ, φ	fi
K, κ	kappa	X, χ	chi
Λ, λ	lambda	Ψ, ψ	psi
M, μ	mi	Ω, ω	omega