Funkcjonalna pełność

- Funkcja prawdziwościowa: dowolna funkcja o sygnaturze:

  $$\mathrm{Log}^n \to \mathrm{Log}$$

- Zbiór spójników logicznych jest *funkcjonalnie pełny* jeśli za ich pomocą można wyrazić dowolną funkcję prawdziwościową.

- Np. zbiór $\{\neg, \wedge, \vee\}$ jest funkcjonalnie pełny

- Funkcjonalnie pełny zbiór jest *minimalny* jeśli każdy jego właściwy podzbiór nie jest funkcjonalnie pełny.

System dowodzenia Hilberta

System dowodzenia H składa się z dwóch elementów:

- zbioru *aksjomatów* (zbioru formuł uznawanych za prawdziwe)
- zbioru *reguł inferencji* (lub *wnioskowania*), czyli zasad transformowania jednych formuł w inne.

Aksjomaty

1. $x \Rightarrow (y \Rightarrow x)$ prawo symplifikacji,
2. $(x \Rightarrow (y \Rightarrow z)) \Rightarrow ((x \Rightarrow y) \Rightarrow (x \Rightarrow z))$ prawo Fregego,
3. $\neg x \Rightarrow (x \Rightarrow y)$ prawo Dunsa Scotusa,
4. $(\neg x \Rightarrow x) \Rightarrow x$ prawo Claviusa,

Uwaga 1 Aksjomaty 2, 3, 4 stanowią zestaw aksjomatów J. Łukasiewicza klasycznego RZ.

Uwaga 2 W przypadku używania stałych logicznych **true** oraz **false** mamy dodatkowy aksjomat:

true

i dodatkową definicję:

true = ¬ **false**

Definicje

1. $X \wedge Y = \neg(X \Rightarrow \neg Y)$
2. $X \vee Y = (\neg X \Rightarrow Y)$
3. $(X \Leftrightarrow Y) = ((X \Rightarrow Y) \wedge (Y \Rightarrow X))$

Definicje pozwalają na tekstowe zastąpienie w dowolnej formule dowolnej jej części (podformuły) równoważnej tekstowo z jedną ze stron definicji przez drugą ze stron tej samej definicji.

Reguła podstawienia

$$\frac{X}{X[Y/a]}$$

gdzie X, Y są dowolnymi formułami, zaś a zmienną zdaniową. X[Y/a] oznacza formułę, która powstaje z formuły X przez tekstowe zastąpienie kadego wystąpienia zmiennej a przez formułę Y.

Reguła odrywania (Modus ponens)

$$\frac{X \Rightarrow Y, X}{Y}$$

Dowodem formuły X w systemie H nazywa się ciąg formuł

$X_1, X_2, \ldots, X_n$

taki, że $X_n \equiv X$, zaś X_i albo jest aksjomatem albo jest wnioskiem z reguły odrywania na podstawie przesłanek ze zbioru $X_1, \ldots, X_{i-1}$.

Formułę, która ma dowód nazywa się *twierdzeniem*.

Przykład Ciąg formuł

$X \Rightarrow (Y \Rightarrow X)$ -- aksjomat 1

$(X \Rightarrow (Y \Rightarrow X)) \Rightarrow ((X \Rightarrow Y) \Rightarrow (X \Rightarrow X))$ -- aksjomat 2

$(X \Rightarrow Y) \Rightarrow (X \Rightarrow X)$ -- reguła odrywania

jest dowodem formuły $(X \Rightarrow Y) \Rightarrow (X \Rightarrow X)$.

Przykład wskazuje na uciążliwości w prowadzeniu dowodów bardziej złożonych formuł. Ponadto, nie nasuwa ten przykład wskazówek dotyczących taktyki prowadzenia dowodów. System Hilberta jest trudno algorytmizowalny.

Własności metalogiczne

Rachunek zdań RZ jest *teorią formalną*, tzn. układem:

RZ = (L , A , R),

gdzie L jest jezykiem teorii, A , R - zbiorem aksjomatów i reguł teorii.

RZ jest teorią *rozstrzygalną*, to znaczy, że istnieje efektywna (mechaniczna) procedura (algorytm), która w skończonej liczbie kroków stwierdza, czy dana formula jest tautologią czy nie. Istnieje kilka takich sposobów rozstrzygania. Metoda związana bezpośrednio z definicją tautologii jest metoda zero-jedynkowa wyliczania logicznej wartości formuły dla wszystkich możliwych wartościowań jej zmiennych.

Ponieważ liczba takich wartościowań jest skończona zatem otrzymuje się niezawodną odpowiedź na pytanie o to, czy formula jest tautologią.

Mówimy, że teoria jest *niesprzeczna* jeżeli nie istnieje formuła taka, że ona sama oraz jej negacja stanowią twierdzenia teorii. RZ jest, w tak określonym sensie, teorią niesprzeczną.

Przykład

Następująca teoria jest sprzeczna:

$$T = (L,A,R),$$

gdzie L jest takim samym językiem jak dla rachunku zdań, zbiór aksjomatów A składa się z następujących aksjomatów:

1. $X \Rightarrow X$
2. $((X \Rightarrow \mathbf{false}) \Rightarrow \mathbf{false}) \Rightarrow X$
3. $\neg\mathbf{false} \Leftrightarrow \mathbf{true}$
4. $\mathbf{true}$

i z następującej reguły:

$$\frac{X}{Y}$$

Sprzeczność tej teorii wynika z tego, że w niej każda formuła Y i ¬Y jest prawdziwe. Aby to pokazać wystarczy skorzystać z reguły dowodzenia i aksjomatu 4: pod X podstawimy **true**.

RZ jest teorią *semantycznie niesprzeczną* - wyraża to twierdzenie o niesprzeczności:

> *Jeżeli formuła jest dowodliwa w RZ (tzn. istnieje dla niej dowód), to jest tautologią.*

Zachodzi także twierdzenie odwrotne - twierdzenie o *semantycznej zupełności* RZ:

> *Każda tautologia RZ jest dowodliwa*.

Mówimy, że system RZ jest *funkcjonalnie zupełny*, jeżeli da się w nim wyrazić wszystkie możliwe funkcje prawdziwościowe o dowolnej liczbie argumentow. RZ w podanej postaci jest funkcjonalnie zupełny, chociaż nie jest *systemem minimalnym*. Łatwo sprawdzić, że systemem minimalnym jest na przykład zbiór spójników:

$\neg$, $\vee$,

$\neg$, $\wedge$,

$\Rightarrow$, **false**,

RACHUNEK KWANTYFIKATORÓW

1. Język

- *Rachunek kwantyfikatorów* (RK) jest uogólnieniem rachunku zdań. Język RK jest nadzbiorem języka RZ.

  - Jest on zdefiniowany jako zbiór napisów dwóch kategorii - termów i formuł

- Alfabet składa się z następujących kategorii leksykalnych:
  (a) symbole *stałych logicznych* **true**, **false**;
  (b) zbiór symboli *zmiennych dziedzinowych*, oznaczanych dalej symbolami x, y, ...
  (c) zbiór symboli *stałych dziedzinowych*;
  (d) zbiór symboli *funkcyjnych* n-argumentowych (n = 1,2,...), oznaczanych dalej symbolami f,g,... ;
  (e) zbiór symboli *predykatów* n-argumentowych (n = 2,3,...), oznaczanych dalej symbolami p,q,... ;
  (f) symbole *spójników logicznych*:
      implikacji $\Rightarrow$, *koniunkcji* $\wedge$, *alternatywy* $\vee$, *negacji* $\neg$, *równoważności* $\Leftrightarrow$;
  (g) symbole *kwantyfikatorów*: $\forall$, $\exists$;
  (h) symbole *pomocnicze*: ( ) ,

***Uwaga*:**

Przedstawiony wyżej zbiór jednostek leksykalnych może - bez utraty ogólności - być pomniejszony o niektóre symbole. Na przykład nie jest konieczne używanie symboli stałych logicznych, wszystkich symboli spójników logicznych (wystarczy spośród nich wybrać adekwatny podzbiór symboli), a także wystarczy posługiwać się symbolem tylko jednego kwantyfikatora. Języki RK zdefiniowane na bazie różnych alfabetów mogą być równoważne w sensie siły ekspresji (wyrażalności).

Reguły formowania (*reguły składni*) definiują dwie klasy napisów. Pierwszą klasą są ***termy***. Zbiór termów TERM jest definiowany indukcyjnie jako najmniejszy zbiór spełniający następujące warunki:

(a) stałe i zmienne dziedzinowe są termami;

(b) jeżeli $t_1,...,t_k$ ($k = 1,2,...$) są termami, a f jest symbolem funkcyjnym k-argumentowym, to $f(t_1,...,t_k)$ jest termem.

Term, który nie zawiera zmiennych dziedzinowych nazywa się *termem stałym*.

Drugą klasą napisów są *formuły*. Zbiór formuł FORM jest definiowany jako najmniejszy zbiór spełniający następujące warunki:

(a) stałe logiczne są formułami;

(b) jeżeli $t_1,...,t_k$ (k = 1,2,...) są termami, zaś p jest symbolem k-argumentowego predykatu, to $p(t_1,...,t_k)$ jest formułą;

(c) jeżeli X1, X2 są formułami, to formułami są także:

$$X\Rightarrow Y,\ X\wedge Y,\ X\vee Y,\ \neg X,\ X\Leftrightarrow Y,\ (X).$$

(d) jeżeli X jest formułą, zaś x jest zmienną dziedzinową, to formułami są:

$$\exists x.X \text{ oraz } \forall x.X$$

Formuły spełniające podane wyżej warunki (a) i (b) nazywa się formułami *atomowymi*.

***Uwaga*:**

W celu unikania dużej liczby nawiasów w formułach, często ustala się priorytety użycia (wiązania) spójników logicznych. I tak, przyjmuje się, że najsilniej wiąże negacja, dalej koniunkcja, dysjunkcja, implikacja i równoważność.

Pojęcia:

- Formuła X występująca po kwantyfikatorze w formule $\exists x.X$ lub $\forall x.X$ nazywa się *zasięgiem kwantyfikatora*, a symbol x występujący bezpośrednio za symbolem kwantyfikatorów nazywa się *wskaźnikiem związania*.

- Zmienna dziedzinowa x może występować tekstowo w wielu miejscach formuły. Każde takie pojawienie się zmiennej nazywa się *wystąpieniem zmiennej*.
- Wystąpienie zmiennej w danej formule może być *wolne* albo *związane*.
- Wystapienie zmiennej w danej formule nazywa się *wystąpieniem wolnym*, jeżeli wystąpienie to nie znajduje się w zasięgu żadnego kwantyfikatora, natomiast w przypadku przeciwnym - nazywa się *wystąpieniem związanym*.

Formuła która zawiera wolne wystąpienia zmiennych nazywa się formułą *otwartą*, a formuła nie zawierająca wolnych wystąpień - formułą *zamkniętą*, czyli *zdaniem*.

Podstawienie

Jeżeli x jest zmienną dziedzinową, t jest termem, oraz X - formułą, to zapis:

$$X[t/x]$$

nazywany *podstawieniem termu za zmienną*, będzie oznaczać formułę, która powstała z formuły X, w taki sposób, że każde wolne wystąpienie zmiennej x w formule X jest zastąpione tekstowo termem t.

<u>Warunek:</u> Od operacji podstawienia wymaga się, aby w termie t nie występowały takie zmienne, które po podstawieniu stały by się związane w formule X.

Zdefiniowany język cechuje to, że z kwantyfikatorami są powiązane jedynie zmienne dziedzinowe. Stąd, język ten nazywa się *językiem kwantyfikatorów pierwszego rzędu*. W logice rozpatruje się także systemy dopuszczające powiązanie przez kwantyfikatory innych obiektów.

Na przykład *rachunek kwantyfikatorów drugiego rzędu* dopuszcza powiązanie przez kwantyfikatory zmiennych predykatowych. Dalej ograniczymy się wyłącznie do rachunku kwantyfikatorów pierwszego rzędu.

2. Semantyka

Rachunek kwantyfikatorów, stanowiąc uogólnienie rachunku zdań, przejmuje znaczenie przypisywane spójnikom logicznym zgodnie ze standardową interpretacją RZ. Nowymi elementami, które wymagają uzupełniającej interpretacji są symbole funkcyjne oraz predykatywne.

Niech I oznacza *rozszerzenie poprzednio wprowadzonej standardowej interpretacji* RZ. Interpretacja I będzie teraz tym nowym symbolom przyporządkowywac pewne funkcje i relacje z wybranych dziedzin interpretacji. W przypadku RZ dziedzina interpretacji jest tylko jeden zbior

$$\mathrm{Log} = \{0 ,1\}.$$

Dziedzina interpretacji jest w tym przypadku jednorodzajowa. Natomiast w przypadku RK tak nie jest - dziedzina interpretacji może składać się z wielu rożnych zbiorów wartości. W tym przypadku mówimy, że dziedzina jest wielorodzajowa.

Wielorodzajowa dziedzina wraz ze zbiorem funkcji i relacji stanowiących interpretacje wyznacza pewien system relacyjny.

Pojęcie systemu relacyjnego (definiowane już poprzednio) jest podstawowe dla zrozumienia semantyki RK. Systemem relacyjnym SR jest struktura o postaci:

$$SR = (D_1,...,D_m; \{F_1,...,F_n\}; \{P_1,...,P_k\}).$$

+ $D_1,...,D_m$ są nośnikami systemu, czyli pewnymi zbiorami wartości;

+ $F_1,...,F_n$ są funkcjami, których argumentami mogą być wartości pewnych wybranych nośników, a wartości należa do jednego wybranego nośnika, czyli dla każdego i = 1,...,n sygnatura F_i jest postaci:

$$F_i : D_{i1} \times ... \times D_{ij} \rightarrow D_{i0}$$

gdzie i1,...,ij jest pewnym skończonej długości ciągiem elementów ze zbioru indeksów {1,...,m}. Ciag ten może byc pusty, co oznacza, że funkcja nie posiada argumentów, czyli jest stałą - ustaloną wartościa ze zbioru D_{i0}.

+ $P_1,...,P_k$ są relacjami, a więc dla j = 1,...,k, sygnatura relacji P_i ma postać:

$$Pi \subseteq D_{i1} \times ... \times D_{ij}$$

gdzie - jak poprzednio - i1,...,ij jest pewnym skończonej długości ciągiem elementów ze zbioru indeksów {1,...,m}.

Punktem wyjściowym do definiowania interpretacji jest wybór pewnego systemu relacyjnego SR. Interpretacja I ustala przyporządkowania:

(a) symbolom stałych dziedzinowych pewne funkcje zeroargumentowe; dla symbolu stałej C będziemy oznaczać taką funkcje zeroargumentową przez C_I;

(b) symbolom funkcyjnym - pewne funkcje z SR o odpowiedniej liczbie argumentów; dla symbolu f będziemy oznaczać taką funkcję przez f_I;

(c) symbolom predykatów - pewne relacje z SR o odpowiedniej liczbie argumentów; dla symbolu predykatu p będziemy oznaczać taką relację przez p_I .

Dalszy tok definiowania semantyki RK przebiega analogicznie do RZ. Polega to na rozszerzeniu interpretacji na dowolne termy i formuły. Pomocniczym elementem jest wartościowanie zmiennych dziedzinowych. Pojęcie wartościowania definiuje się następująco.

Niech Var będzie zbiorem zmiennych dziedzinowych, $D_1 \cup ... \cup D_m$ będzie sumą nośników systemu relacyjnego SR. *Wartościowanie zmiennych* jest funkcją v o sygnaturze:

$$v : Var \to D_1 \cup ... \cup D_m$$

Mając interpretację definiujemy pojęcie *wartości termu*. Jeżeli t jest termem, I - interpretacją, v - wartościowaniem zmiennych dziedzinowych, to *wartością termu* t *w interpretacji* I *przy wartościowaniu* v będziemy oznaczać przez $t_I(v)$.

(a) jeżeli term jest stałą C, to jego wartością w interpretacji I, przy wartościowaniu v, oznaczaną $C_I(v)$, jest C_I;

(b) jeżeli term jest zmienną dziedzinową x, to jego wartością w interpretacji I, przy wartościowaniu v, oznaczaną $x_I(v)$ jest v(x);

(c) jeżeli term jest postaci $f(t_1,...,t_k)$, to jego wartością w interpretacji I, przy wartościowaniu v, oznaczaną $f(t_1,...,t_k)_I(v)$, jest $f_I((t_1)_I(v),..., (t_k)_I(v))$;

Uwaga Zauważmy, że wartość termów stałych, przy ustalonej interpretacji I, nie zależy od wartościowania v.

Definiujemy teraz pojęcie *spełniania*, czyli *prawdziwości* formuły X w interpretacji I przy wartościowaniu v, co - jak poprzednio w RZ - oznaczamy:

$\models X_I(v)$.

Definicja ta jest rozszerzeniem odpowiedniej definicji dla RZ przez dołączenie następujących zasad:

(a) Jeżeli formuła X jest formułą atomową o postaci $p(t_1,...,t_n)$, gdzie p jest predykatem a $t_1,...,t_n$ - termami, to

$\models X_I(v)$

wtedy i tylko wtedy, gdy $<(t_1)_I(v),...,(t_n)_I(v)> \in p_I$.

(b) Jeżeli formuła jest postaci

$X \Rightarrow Y$, $X \wedge Y$, $X \vee Y$, $\neg X$, $X \Leftrightarrow Y$, (X),

to

$\models (X \vee Y)_I(v)$ wtt $\models X_I(v)$ lub $\models Y_I(v)$

(itd. jak dla rachunku zdań)

(c) Jeżeli formuła jest postaci

$\exists x.X$

to

$\models (\exists x.X)_I(v)$ wtt istnieje wartościowanie v', które od wartościowania v różni się co najwyżej wartością zmiennej x, takie że $\models X_I(v')$

(d) Jeżeli formuła jest postaci

$\forall x.X$

to

$\models (\forall x.X)_I(v)$ wtt dla dowolnego wartościowania v',
które od wartościowania v różni się co
najwyżej wartością zmiennej x,
zachodzi $\models X_I(v')$.

Uwaga Związek pomiędzy wartościowaniami v oraz v' można ująć w sposób następujący: $v'(y) = v(y)$ dla $y \neq x$.

Pojęcia ***modelu*** oraz ***tautologii***, wprowadzone w RZ, przenoszą się do RK:

- Formułę X, która spełnia interpretację I dla dowolnego wartościowania v będziemy zapisywać w postaci:

  $\models X_I$

a interpretację I nazywa się *modelem* formuły X. Mówimy też, że formuła X *jest* ***spełnialna*** *w interpretacji* I.

- Formułę X, która spełnia dowolną interpretację dla dowolnego wartościowania (jest prawdziwa dla dowolnego wartościowania w danej interpretacji) nazywa się ***tauologią*** i oznacza w postaci:

  $\models X$

Dwie formuły są ***równoważne w danej interpretacji*** wtedy i tylko wtedy, gdy dla dowolnego wartościowania są jednocześnie spełnione albo niespełnione.

Przykład

1. *Algebra* - *arytmetyka liczb całkowitych* - *przykład podzbioru języka RK.*

Potrzebny alfabet:

(a) symbole *stałych logicznych* **true**, **false** - brak;

(b) zbiór symboli *zmiennych dziedzinowych* - zbiór identyfikatorów;

Gramatyka generująca zbiór zmiennych - (notacja BNF)

<litera> ::= x | y | z

<cyfra> ::= 0 | ... | 9

<ciąg cyfr> ::= <cyfra> | <ciąg cyfr> <cyfr>

<zmienna> ::= <litera> | <litera> <ciąg cyfr>

(c) zbiór symboli *stałych dziedzinowych* - zero, jeden;

(d) zbiór symboli *funkcyjnych*

- dwuargumentowe add, sub, mult, div,
- jednoargumentowy alt;

(e) zbiór symboli *predykatów*: eq, less;

(f) symbole *spójników logicznych* - and, or, not;

(g) symbole *kwantyfikatorów*: ∀ ∃ - brak;

(h) symbole *pomocnicze*: ( ) ,

Termy:

(a) zmienne (arytmetyczne) oraz ‘zero’, ‘jeden’ - są termami;

(b) jeżeli t_1, t_2 są termami, to termami są:

$add(t_1,t_2)$, $sub(t_1,t_2)$, $mult(t_1,t_2)$, $div(t_1,t_2)$

- zapis prefiksowy funktorów binarnych

t_1 add t_2, t_1 sub t_2, t_1 mult t_2, t_1 div t_2

- zapis infiksowy.

Formuły:

(a) jeżeli t_1,t_2 są termami, to

$eq(t_1,t_2)$, $less(t_1,t_2)$

są formułami;

(b) jeżeli X, Y są formułami, to formułami są także:

X **and** Y, X**or**Y, not(X), (X).

Dziedziny interpretacji - zbiór liczb całkowitych INT oraz zbiór wartości logicznych LOG = {p,f}.

Interpretacja I ustala przyporządkowania:

(a) symbolom stałych dziedzinowych:

zero $\longmapsto$ $zero_I = 0 \in$ INT

jeden $\longmapsto$ $jeden_I = 1 \in$ INT

(symbol '=' oznacza równość elementów w zbiorze INT)

(b) symbole funkcyjne

add $\longmapsto$ $+ : INT^2 \to INT$

sub $\longmapsto$ $- : INT^2 \to INT$

mult $\longmapsto$ $* : INT^2 \to INT$

div $\longmapsto$ $/ : INT^2 \to INT$

alt $\longmapsto$ $- : INT \to INT$ (jednoargumentowy funktor)

(c) symbole predykatów

eq $= : INT^2 \to LOG$

less $< : INT^2 \to LOG$

Semantyka (interpretacja) termów $t_I(v)$:

(a) zmienne x ma interpretację $x_I(v) = v(x)$;

(b) stałe

(c) termy postaci $add(x,y)_I(v) = add_I(x_I(v),y_I(v)) = v(x) + v(y)$.