Kilka słów o logice, zbiorach i indukcji

Marcin Michalski, WMAT PWr

Październik 2022

Niniejsza notatka służy przybliżeniu treści, które pojawią się na pierwszym wykładzie, który odbędzie się niestety po pierwszych ćwiczeniach. Spróbujemy krótko i jasno omówić sobie tytułowe tematy, by wstrzelić się w klimat listy 1.

Trochę logiki

Klasyczny rachunek zdań

Klasyczny rachunek zdań (krótko: KRZ), to podstawowy system formalny, który zajmuje się stwierdzeniami przyjmującymi jedną z dwóch wartości logicznych (prawda i fałsz). Można nim modelować proste stwierdzenia z języka naturalnego jak np. "świeci Słońce". Stwierdzenia te, zwane formułami lub zdaniami, można łączyć w dłuższe formuły za pomocą spójników logicznych, np, "jeśli świeci Słońce, to jest ładna pogoda" w KRK miałoby postać $\varphi \to \psi$, gdzie φ to zdanie "świeci Słońce", a ψ to "jest ładna pogoda". Formalnie język KRZ składa się z

(i) symboli stałych $\top$ i $\bot$, które są stałymi interpretowanymi zawsze jako prawda i fałsz;

(ii) symboli formuł atomowych $p_0, p_1, p_2, \ldots$, które można interpretować jako prawdziwe bądź fałszywe;

(iii) spójników logicznych, jak negacja $\neg$, alternatywa $\vee$, koniunkcja $\wedge$, implikacja $\to$, równoważność $\leftrightarrow$, etc.

(iv) symboli dodatkowych, jak wszelkiego rodzaju nawiasy w celu poprawienia czytelności formuł.

Często zamiast posługiwać się symbolami p_k, gdzie k jest dowolną liczbą naturalną, będziemy używać p, q, r, s dla niezbyt długich formuł.

Formuły

Symbole języka KRZ można łączyć w napisy, ale nie każde połączenie symboli w napis będzie miało dla nas sens. Poniżej mamy przepis na to, co jest poprawną formułą.

Definicja 1.

(i) Symbole stałych i formuł atomowych są formułami;

(ii) Jeśli φ, ψ są formułami, to również formułami są $\neg\varphi$, $\varphi\Box\psi$, gdzie $\Box$ to dowolny dwuargumentowy spójnik logiczny;

(iii) Żaden inny napis nie jest formułą, jeśli nie powstał w powyższy sposób w skończonej liczbie kroków.

W ten sposób np. formułą jest $(\bot \vee p_0) \leftrightarrow \neg p_{23}$, ponieważ $p_{23}, p_0, \bot$ są formułami, skąd $(\bot \vee p_0)$ i $\neg p_{23}$ są formułami i ostatecznie cały napis.

Wartościowanie formuł

Następnym krokiem jest wspomniana interpretacja formuł jako prawdziwych lub fałszywych. Do tego służą wartościowania. Oznaczmy wartość logiczną fałsz przez $\mathbb{0}$ i wartość prawda przez $\mathbb{1}$.

Definicja 2. *Wartościowaniem nazywamy funkcję v działającą na symbolach stałych i symbolach formuł atomowych o własnościach*

(i) $v(\bot) = \mathbb{0}$ i $v(\top) = \mathbb{1}$;

(ii) dla każdej formuły atomowej p zachodzi $v(p) = \mathbb{0}$ lub $v(p) = \mathbb{1}$;

Własności *(i)* i *(ii)* są jasne i oddają to, co zasygnalizowaliśmy wcześniej. Chcielibyśmy jednak móc interpretować dowolnie skomplikowane formuły, a nie tylko stałe i atomowe. Istotnie, każde wartościowanie rozszerza się rozsądnie na wszystkie formuły, zachowując przy tym sens spójników. Poniżej jest tabelka ze wszystkimi wartościowaniami dla standardowych spójników.

p	q	$p \vee q$	$p \wedge q$	$p \rightarrow q$	$p \leftrightarrow q$	$\neg p$
$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$

Stosując konsekwentnie powyższe wartościowania dla podstawowych spójników możemy wyznaczyć wartościowania każdej formuły (choć może to być dość żmudne zadanie).

Tautologie

Skupimy się teraz na pewnym specjalnym typie formuł.

Definicja 3. *Formułę φ nazywamy tautologią, jeśli wartość logiczna φ wynosi $\mathbb{1}$ dla każdego wartościowania.*

Trywialnym przykładem tautologii jest $\top$. Istnieje wiele klasycznych tautologii i notatka byłaby zdecydowanie zbyt długa, gdyby spróbować je wszystkie zanalizować (garść tautologii do udowodnienia jest na liście 1). Zwróćmy jednak uwagę na ten ważny aspekt tautologii, który przyda nam się w dalszej pracy. Otóż dostarczają nam one solidnych podstaw do dowodzenia prawdziwości matematycznych stwierdzeń. Twierdzenia matematyczne mają konstrukcję "*założenia* $\rightarrow$ *teza*" i dowody wprost tych twierdzeń to po prostu skończone ciągi implikacji od założeń do tezy. Czasami jednak wygodnie jest przeprowadzać dowody *nie wprost*, tzn. pokazać, że przy założeniu przesłanek i nieprawdziwości tezy otrzymujemy sprzeczność. Sprawdźmy zatem, że schemat dowodu nie wprost jest poprawny.

Przykład 1. *Schemat dowodu nie wprost ma postać*

$$\Big(p \wedge \neg q) \rightarrow \bot\Big).$$

Pokażemy, że zdanie to jest równoważne wynikaniu tezy z przesłanek, tzn.

$$(p \rightarrow q) \leftrightarrow \Big(p \wedge \neg q) \rightarrow \bot\Big).$$

Rozpatrzmy w tabelce wszystkie istotne (tzn. te o różnych wartościach symboli atomowych występujących w formule) możliwe wartościowania symboli p, q.

p	q	$\neg q$	$\bot$	$p \wedge \neg q$	$p \rightarrow q$	$(p \wedge \neg q) \rightarrow \bot$	$(p \rightarrow q) \leftrightarrow \Big(p \wedge \neg q) \rightarrow \bot\Big)$
$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$

W kolejnych kolumnach zapisujemy pomocniczo wartości kolejnych formuł wchodzących w skład całej wartościowanej formuły. W ostatniej kolumnie mamy same $\mathbb{1}$*, co oznacza, że formuła istotnie jest tautologią.*

Kilka słów o zbiorach

W teorii mnogości[1] zbiór i relacja należenia do zbioru $\in$[2] to pojęcia pierwotne, zatem przyjmujemy, że intuicyjnie rozumiemy, co się za tymi pojęciami kryje. Na poważnie natomiast można się zająć ich własnościami. Część z tych własności przyjmujemy jako założenie w formie aksjomatów. Standardowa aksjomatyka ZFC gwarantuje np. istnienie zbioru pustego, par nieuporządkowanych $\{x, y\}$ (czyli zbiorów zawierających dokładnie 2 elementy - x i y), pozwala na porównywanie zbiorów wg ich zawartości[3], a także sprawia, że istotne dla nas operacje na zbiorach mają sens. Zanim jednak sobie te operacje omówimy, wzbogacimy nieco nasz język o kwantyfikatory.

[1] Mnogość to staroświeckie, ale bardzo piękne, określenie zbioru.

[2] $x \in A$ czytamy "x należy do A" lub "x jest elementem A".

[3] tzn. dla zbiorów A i B mamy $A = B$ jeśli $x \in A \leftrightarrow x \in B$ dla dowolnego x.

Kwantyfikatory

Zacznijmy od rozszerzenia naszego pojęcia formuły. Niech Ω będzie niepustym zbiorem.

Definicja 4. *Przyporządkowanie φ nazywamy funkcją zdaniową, jeśli każdemu elementowi $x \in \Omega$ przyporządkowuje wartość logiczną $\varphi(x) \in \{\mathbb{0}, \mathbb{1}\}$.*

Funkcją zdaniową jest np. $\varphi(x) =$ "$x > 0$" dla $\Omega = \mathbb{N}$. Zauważmy, że o ile w KRK mieliśmy do czynienia tylko z prostym wartościowaniem formuł atomowych, teraz korzystamy również ze struktury związaną z Ω. Jeden z aksjomatów, tzw. aksjomat wycinania pozwala na wyodrębnianie elementów danego zbioru za pomocą funkcji zdaniowych.

Aksjomat 1 (wycinania)**.** *Jeśli A jest zbiorem, a φ funkcją zdaniową o zmiennej z A to wtedy istnieje zbiór B, który zawiera tyle te elementy A, które spełniają φ. Zbiór ten oznaczamy przez $\{x \in A : \varphi(x)\}$.*

Możemy teraz wygodnie zdefiniować kwantyfikatory.

Definicja 5. *Symbol $\forall$ nazywamy kwantyfikatorem uniwersalnym. Jeśli φ jest funkcją zdaniową nad Ω, to napis $(\forall x)\varphi(x)$ czytamy "dla każdego $x \in \Omega$ zachodzi $\varphi(x)$" i oznacza, że $\{x \in \Omega : \varphi(x)\} = \Omega$.*

Symbol $\exists$ nazywamy kwantyfikatorem egzystencjalnym. Napis $(\exists x)\varphi(x)$ czytamy "istnieje $x \in \Omega$, że zachodzi $\varphi(x)$" i oznacza, że $\{x \in \Omega : \varphi(x)\} \neq \emptyset$.

Na pierwszy rzut oka wydaje się to skomplikowane, ale w gruncie rzeczy takie podejście wiele upraszcza. Np. aksjomat wycinania moglibyśmy sformułować w jednej linijce

$$(\forall A)(\exists B)(\forall x)(x \in B \leftrightarrow \varphi(x)).^{4}$$

Zauważmy też związek pomiędzy kwantyfikatorem uniwersalnym, a egzystencjalnym (de facto prawo de Morgana)

$$\neg((\forall x)\varphi(x)) \leftrightarrow (\exists x)(\neg\varphi(x)).$$

Od teraz będziemy posługiwać się kwantyfikatorami dość swobodnie dla zwięzłości i precyzji wypowiedzi.

Operacje na zbiorach

Definicja 6. *Niech A, B będą zbiorami. Wtedy*

(i) Zbiór $A \cup B$ nazywamy sumą zbiorów A i B, jest on scharakteryzowany przez formułę

$$(\forall x)((x \in A \cup B) \leftrightarrow (x \in A \vee x \in B));$$

(ii) Zbiór $A \cap B$ nazywamy przekrojem zbiorów A i B jest on scharakteryzowany przez formułę

$$(\forall x)((x \in A \cap B) \leftrightarrow (x \in A \wedge x \in B));$$

[4] Tutaj Ω to rodzina wszystkich zbiorów, ale nie zbiór wszystkich zbiorów, bo takowy nie istnieje.

(iii) *Zbiór $A\backslash B$ nazywamy różnicą zbiorów A i B jest ona scharakteryzowana przez formułę*

$$(\forall x)((x \in A\backslash B) \leftrightarrow (x \in A \wedge x \notin B));$$

(iv) *Zbiór $A^c = \Omega\backslash A$ nazywamy dopełnieniem zbioru A, gdzie Ω oznacza zbiór, do którego ograniczamy nasze rozważania.*

Przykład 2. *Niech rozważaną przestrzenią będzie prosta rzeczywista $\mathbb{R}$, $A = [0, 2]$ i $B = (1, 3)$. Wtedy $A \cup B = [0, 3)$, $A \cap B = (1, 2]$, $A\backslash B = [0, 1]$, $A^c = (-\infty, 0) \cup (2, \infty)$.*

Przykład 3. *Sprawdzimy, że zachodzi następująca tożsamość w rachunku zbiorów*

$$A\backslash(B \cup C) = (A\backslash B)\backslash C.$$

Jeden sposób, to ustalenie dowolnie x i oznaczenie zdań $x \in A$, $x \in B$, $x \in C$ np. odpowiednio przez p, q, r i sprawdzenie, powyższa tożsamość dla tego ustalonego x tłumaczy się na

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

po czym zrobić tabelkę 0-1. *Drugi sposób, to sprawdzenie, czy przynależność dowolnego x do zbioru po jednej ze stron równości prowadzi do przynależności do zbioru po drugiej stronie. I tak np.*

$$\begin{aligned} x \in A\backslash(B \cup C) &\equiv [5] x \in A \wedge \neg(x \in B \cup C) \equiv x \in A \wedge \neg(x \in B \vee x \in C) \equiv \\ &\equiv x \in A \wedge (x \notin B \wedge x \notin C) \equiv (x \in A \wedge x \notin B) \wedge x \notin C \equiv x \in (A\backslash B)\backslash C. \square \end{aligned}$$

Zauważmy, że skorzystaliśmy z prawa de Morgana oraz łączności spójnika $\wedge$.

Sekcję o zbiorach zakończymy zdefiniowaniem ralacji zawierania

Definicja 7. *Mówimy, że zbiór A zawiera się w B, oznaczenie: $A \subseteq B$, jeśli $(\forall x)(x \in A \rightarrow x \in B)$.*

Jest jasne, że $A \subseteq A$, czy $\emptyset \subseteq A$ dla każdego zbioru A. Ponadto relację zawierania możne zdefiniować za pomocą operacji na zbiorach podanych wcześniej

Fakt 1. *Niech A i B będą zbiorami. Następujące stwierdzenia są równoważne*

(i) $A \subseteq B$;

(ii) $A \cup B = B$;

(iii) $A \cap B = A$;

(iv) $A\backslash B = \emptyset$.

Dowód zostawimy jako ćwiczenie.

Zasada indukcji matematycznej

Niech φ będzie formułą zależną od zmiennej naturalnej $n \in \mathbb{N}$. Sformułowanie zasday indukcji matematycznej jest następujące.

Twierdzenie 1 (zasada indukcji matematycznej)**.**

$$\Big(\varphi(0) \wedge (\forall n \in \mathbb{N})(\varphi(n) \to \varphi(n+1))\Big) \to (\forall n \in \mathbb{N})\varphi(n).$$

Intuicyjnie można rozumieć to tak: jeśli wiemy, że potrafimy wejści na pierwszy schodek, a następnie z każdego innego schodka potrafimy wejść na następny, to potrafimy wejść na każdy. Twierdzenie to można zostawić bez dowodu, ponieważ w zasadzie zasada indukcji to jeden z aksjomatów charakteryzujących liczby naturalne (w arytmetyce Peana). Można również się pokusić o konstrukcję liczb naturalnych w języku teorii mnogości (tzw. model von Neumanna) lub skorzystać z równoważności z dobrym uporządkowaniem $\mathbb{N}$. Zostawimy obie opcje jako ćwiczenia dla zainteresowanych.

Zasadę indukcji można sformułować pozornie silniej (choć równoważnie) w następujący sposób.

Twierdzenie 2 (zasada indukcji zupełnej)**.**

$$\Big(\varphi(0) \wedge (\forall n \in \mathbb{N})(\varphi(0) \wedge \varphi(1) \wedge \ldots \varphi(n) \to \varphi(n+1))\Big) \to (\forall n \in \mathbb{N})\varphi(n).$$

Obie wersje indukcji można "zacząć" od pewnego $n_0 > 0$ zamiast od 0.

Zobaczmy indukcję w akcji.

Przykład 4. *Udowodnimy, że* $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$. *Dla* $n = 0$ *mamy* $\sum_{k=0}^{0} 2^k = 2^0 = 1 = 2^1 - 1$, *zatem się zgadza. Załóżmy teraz, że mamy już tezę dla pewnego* $n \in \mathbb{N}$. *Zobaczmy jak się sprawy mają dla* $n+1$

$$\sum_{k=0}^{n+1} 2^k = \sum_{k=0}^{n} 2^k + 2^{n+1} = {}^{6}2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1,$$

co chcieliśmy udowodnić. Stąd, na mocy ZIM mamy tezę.

[6] Tu korzystamy z założenia indukcyjnego