Rozdział 1

Rachunek zdań

Klasyczny rachunek zdań.

1.1 Formuły

Definicja 1.1.1 (Formuła logiki zdaniowej) *Formułą nazywamy:*

1. *pojedynczą zmienną - zmienne oznaczamy zazywczaj jednoliterowymi symbolami alfabetu łacińskiego, np.* a, b, c, p, q, r*, itp., czasem z indeksami dolnymi lub górnymi:* $p_1, p_{87}, q^{15}, q_2^1$*, itp.;*

2. *napis* $(\phi \diamond \psi)$ *gdzie* ϕ *oraz* ψ *są formułami a spójnik* $\diamond \in \{\Rightarrow, \wedge, \vee, ...\}$*. Pełen zbiór dostepnych spójników logicznych pojawi się dalej;*

3. $(\neg\phi)$ *jeśli* ϕ *jest formułą;*

4. *nic innego nie jest formułą.*

Powyższa definicja mówi, że formułami nazywamy te napisy, które dają się skonstruować ze zmiennych zdaniowych przy pomocy spójników wraz z poprawnym nawiasowaniem! Zgodnie z powyższą definicją nie jest formułą napis $p \Rightarrow q$ - formalnie, powinien to być $(p \Rightarrow q)$, chociaż w matematyce często pomija sie oczywiste nawiasy. Przyjmuje się, że operacje wykonuje się od lewej do prawej, natomiast ciągi implikacji $p \implies q \implies p$ nawiasuje się od prawej strony: $(p \implies (q \implies p))$.

1.1.1 Nie-przykłady

Poniższe napisy nie są formułami

1. $p \Rightarrow\Rightarrow q$ (dwa spójniki pod rząd),
2. $\neg \implies \neg$ (spójniki nic nie łączą),
3. napis postaci: to nie jest formuła, (same zmienne, niepołączone żadnymi spójnikami!)

1.1.2 Przykłady

Poniższe napisy są formułami

1. $(p \Rightarrow (r \Rightarrow q))$,
2. $\neg\neg\neg q$ (to samo co $\neg(\neg(\neg q))$ - formuła jest budowana po kolei, zaczynając od q (punkt 1 definicji), po czym stosujemy 3 razy punkt 3 definicji),
3. $(p \Rightarrow \neg q)$ (to samo co $(p \implies (\neq q))$, $(\neq q)$ jest formułą, zgodnie z punktami 1 i 3, można do niej i p zastosować punkt 2).

1.2 Interpretacja

Niech $\mathbb{B} = \{0, 1\}$, gdzie 0 to wyrózniony element zwany *fałszem* a 1 to element zwany *prawdą*. Spójniki $\wedge$, $\vee$ i $\neg$ interpretujemy nastepująco:

- $\neg 1 = 0$, $\neg 0 = 1$;
- $0 \vee 0 = 0$, $0 \vee 1 = 1$, $1 \vee 0 = 1$, $1 \vee 1 = 1$;
- $0 \wedge 0 = 0$, $0 \wedge 1 = 0$, $1 \wedge 0 = 0$, $1 \wedge 1 = 1$;

Podobnie możemy zrobić z innymi spójnikami, ale to odłożymy nieco na później.

Definicja 1.2.1 Wartościowaniem *zbioru zmiennych* $\{p_1, \ldots, p_k\} = X$ *nazywamy dowolne przypisanie tym zmiennym wartości z* $\mathbb{B}$*, tzn. dowolną funkcję* $v : X \to \mathbb{B}$.

Wartościowanie możemy rozszerzyć na dowolne formuły składające się ze zmiennych ze zbioru X *i spójników* $\neg, \wedge, \vee$ *(i innych), w naturalny sposób używając interpretacji spójników wprowadzonej poprzednio: jeżeli* $\phi = p_k$ *to* $v(\phi) = v(p_k)$*, jeżeli* $\phi = (\neg\psi)$ *to* $v(\phi) = \neg(v(\psi))$ *oraz jeżeli* $\phi = \psi \diamond \xi$ *to* $v(\phi) = v(\psi) \diamond v(\xi)$.

W ten sposób możemy nieformalnie (na razie) zapisać $v : \{$ *zbiór formuł nad* $X\} \to \mathbb{B}$.

(Formalnie należałoby zdefiniować porządnie co to jest $\{$ *zbiór formuł nad* $X\}$*).*

1.2.1 Przykłady

Jeśli $v(p) = 0, v(q) = 1, v(r) = 0$. Wtedy

- formuła $q \wedge p$ jest wartościowana na 0 (zapiszemy, że $v(q \wedge p) = 0$),
- $v(r \vee (q \vee p)) = 1$,
- $v(\neg p \wedge r) = 0$.

1.2.2 Zadania

1. Jeśli $v(p) = 1, v(q) = 1, v(r) = 1$, to jakie wartościowania przyjmą formuły z przykładu?
2. dla każdej z formuł z przykłądu znajdź wartościowanie, dla którego formuła jest prawdziwa.
3. czy da się znaleźć wartościowanie, przy którym wszystkie formuły z przykładu są jednoczesnie prawdziwe?
4. ile jest mozliwych róznych wartosciowań zbioru n zmiennych?
5. Czy da się znaleźć wartościowanie $v(p)$, dla którego $v(p \vee \neg p) = 0$?

Dla uproszczenia zbiór zmiennych występujących w zadanej formule ϕ będziemy oznaczać przez $Var(\phi)$.

Definicja 1.2.2 *Niech będzie dana formuła ϕ. Jeżeli dla każdego wartościowania v zmiennych $Var(\phi)$ mamy $v(\Phi) = 1$ wtedy ϕ nazywamy* tautologią.

Przykład: formuła $p \vee \neg p$ z ostatniego zadania jest tautologią.

1.3 Inne spójniki

Zanim przejdziemy do zadań z tautologii, przyjżymy się jeszcze innym spójnikom. Załóżmy, że mamy dwie zmienne p, q. Zastanówmy się, ile jest różnych funkcji $\mathbb{B} \times \mathbb{B} \to \mathbb{B}$? Z poprzednich zajęć wiemy, że jest ich dokładnie 16. Można je przedstawić w nastepującej tabeli (źródło: wazniak.mimuw.edu.pl):

Numer funkcji	$p = 0$ $q = 0$	$p = 0$ $q = 1$	$p = 1$ $q = 0$	$p = 1$ $q = 1$		
0	0	0	0	0		F
1	0	0	0	1		$\wedge$
2	0	0	1	0		$\neg(p \Rightarrow q)$
3	0	0	1	1		p
4	0	1	0	0		$\neg(q \Rightarrow p)$
5	0	1	0	1		q
6	0	1	1	0		XOR
7	0	1	1	1		$\vee$
8	1	0	0	0		NOR
9	1	0	0	1		$\Leftrightarrow$
10	1	0	1	0		$\neg q$
11	1	0	1	1		$q \Rightarrow p$
12	1	1	0	0		$\neg p$
13	1	1	0	1		$p \Rightarrow q$
14	1	1	1	0		$NAND$
15	1	1	1	1		T

po prawej stronie widzimy zwyczajowe oznaczenia odpowiadających im operatorów. Operatory F i T są w praktyce 0-argumentowe - są stałymi 0 i 1, wartość tych operatorów nie zależy od wartości zmiennych p, q. Widzimy też, że niektóre z nich zależą tylo od jednej ze zmiennych np. $\neg q$ nie zalezy od wartości p. Operatory XOR, NOR i $NAND$ znane są zapewne programistom i osobom zajmującym się elektroniką. Natomiast operatory 13 (oraz symetrycznie 11) i 9 mają duże znaczenie dla matematyków (np. w formułowaniu twierdzeń).

Poniższa definicja jest nieco techniczna, ale pokazuje

Definicja 1.3.1 *Dla dowolnej formuły ϕ zawierającą k zmiennych można zdefiniować jednoznacznie funkcję $f : \mathbb{B}^k \to \mathbb{B}$, poprzez:*

$$f(v(p_1), v(p_2), \ldots, v(p_k)) = v(\phi) \quad \forall v \text{ - \textit{wartościowanie}} \tag{1.1}$$

Weźmy teraz dowolną funkcję $f : \mathbb{B}^k \to \mathbb{B}$, $k > 2$ i zapytajmy, czy dla tej funkcji istnieje formuła, która ją definiuje? Okazuje się, że tak i każdą taką funkcję da się przedstawić jako formułę zlożoną z k zmiennych połączonych spójnikami z tabeli! Co więcej: Dla każdej funkcji f istnieje formuła ϕ, która ją definiuje złożona ze zmiennych i spójników $\{\neg, \wedge, \vee\}$ (Patrz Twierdzenie 1.3.1).

Powyższe stwierdzenia sugerują pewne pytania:

- czy każda funkcja jednoznacznie wyznacza formułę która ją generuje?
- czy istnieją inne zbiory spójników, które generują wszystkie funkcje?
- jaki jest najmnejszy zbiór spójników, które generują wszystkie funkje? Czy jest on jedyny?

Zanim odpowiemy, zdefiniujemy:

Definicja 1.3.2 *Formuły ϕ oraz ψ są równoważne (oznaczamy ten fakt przez $\phi \equiv \psi$) wtedy i tylko wtedy, gdy dla każdego wartościowania v zachodzi $v(\psi) = v(\phi)$.*

Przykłady: (do sprawdzenia we własnym zakresie!)

1. $\neg\neg p \equiv p$,
2. $\phi \vee \psi \equiv \neg\phi \Rightarrow \psi$,
3. $\phi \wedge \psi \equiv \neg(\phi \Rightarrow \neg\psi)$.

Zadanie: pokaż, że jesli zastąpimy w powyższym $\equiv$ przez $\iff$, to otrzymana formuła będzie tautologią.

Zadanie: Pokazać, że nastepujące formuły są tautologiami:

1. prawo wyłączonego środka: $p \vee (\neg p)$;
2. prawo sprzeczności: $\neg(p \wedge (\neg p))$;
3. prawo podwójnej negacji: $p \iff \neg(\neg p)$;
4. I prawo de Morgana: $(\neg(p \wedge q)) \iff ((\neg p) \vee (\neg q))$;
5. II prawo de Morgana: $(\neg(p \vee q)) \iff ((\neg p) \wedge (\neg q))$;
6. prawo odrywania: $(p \wedge (p \Rightarrow q)) \Rightarrow q$;
7. prawo negacji implikacji: $(\neg(p \Rightarrow q)) \iff (p \wedge (\neg q))$;
8. rozdzielność koniunkcji względem alternatywy: $(p \wedge (q \vee r)) \iff ((p \wedge q) \vee (p \wedge r))$;
9. rozdzielność alternatywy względem koniunkcji: $(p \vee (q \wedge r)) \iff ((p \vee q) \wedge (p \vee r))$;
10. $p \Rightarrow q \iff \neg q \Rightarrow \neg p$ (prawo kontrapozycji);
11. $(p \iff q) \iff ((p \Rightarrow q) \wedge (q \Rightarrow p))$;

Teraz wróćmy do pytania o reprezentacje funkcji logicznych za pomocą spójników.

Definicja 1.3.3 *Skończony zbiór funkcji boolowskich Γ nazywamy funkcjonalnie pełnym, jeśli każdą funkcję boolowską da się zdefiniować przy pomocy formuły zbudowanej wyłącznie ze spójników odpowiadających funkcjom ze zbioru Γ.*

Przypominamy, że:

Twierdzenie 1.3.1 $\Gamma = \{\neg, \wedge, \vee\}$ *jest funkcjonalnie pełny.*

Zadanie**: udowodnić Twierdzenie 1.3.1.

Podpowiedź: każda funkcja $f : \mathbb{B}^k \to \mathbb{B}$ ma tylko skończenie wiele wartościowiań swoich zmiennych (ile?). Dla niektórych z nich $v(f) = 1$ a dla innych $v(f) = 0$. Czy da się w takim razie „stablicować” wszystkie wartościowania za pomocą formuły zawierającej tylko spójniki z Γ?

Przykład: $\Gamma = \{\neg, \Rightarrow\}$ jest funkcjonalnie pełny.

Dowód: prawdziwa jest następująca równoważność: $\neg(p \Rightarrow \neg q) \equiv p \wedge q$ - wystarczy zastosować prawo negacji implikacji i podwójnej negacji. Natomiast z negacji implikacji dostajemy, że $\neg(\neg p \Rightarrow q) \equiv \neg p \wedge \neg q$. Nastepnie, z II prawa de Morgana dostajemy, że $\neg p \wedge \neg q \equiv \neg(p \vee q)$, czyli $\neg(\neg p \Rightarrow q) \equiv \neg(p \vee q)$ Stąd $(\neg p \Rightarrow q) \equiv (p \vee q)$ (stosując negację „po obu stronach” równości). Widzimy, że dowolną formułę zawierającą tylko $\neg, \vee, \wedge$ da się „przepisać” zamieniając spójniki na odpowiednio $\neg, (\neg p \Rightarrow q), \neg(p \Rightarrow \neg q)$.

Zadania: Pokazać, że:

1. $\Gamma = \{\neg, \vee\}$ jest funkcjonalnie pełny;
2. $\Gamma = \{\neg, \wedge\}$ jest funkcjonalnie pełny;
3. $\Gamma = \{NAND\}$ jest funkcjonalnie pełny;
4. $\Gamma = \{NOR\}$ jest funkcjonalnie pełny;
5. (*) $\Gamma = \{\wedge\}$ NIE JEST funkcjonalnie pełny;
6. (*) $\Gamma = \{\vee\}$ NIE JEST funkcjonalnie pełny;
7. (*) $\Gamma = \{XOR\}$ NIE JEST funkcjonalnie pełny;

1.4 Zdania logiczne

Logika powstała po to, aby umozliwić precyzyjne formułowanie zdań i orzekanie o tym czy te zdania sa prawdziwe czy tez fałszywe, a także po to, aby z pewnych zdań (założeń) wnioskować o prawdziwości innych zdań (wniosków) - o prowadzeniu i poprawności dowodów.

W matematyce zakładamy, że każdemu zdaniu można przypisać wartośc prawda lub fałsz - nie ma odcieni szarości, nie możemy powiedzieć np. że to zdanie jest w 80% prawdziwe.

Niektóre zdania orzekają o posiadaniu lub nie jakiejś wlasności przez pewne obiekty. Zdania takie nazywamy predykatami, np. „x jest liczbą pierwszą”,

„x jest równe 2, „x jest nieparzyste”. Za pomocą poznanych spójników, możemy tworzyć zdania złozone, np. „**jeżeli** x jest liczbą pierwszą **to** x jest równe 2 **lub** x jest nieparzyste”.

W języku spójników, jesli oznaczymy kolejne zdania jako $p(x)$, $d(x)$, $n(x)$, to zdanie możemy zapisać formułą:

$$p(x) \Rightarrow d(x) \vee n(x)$$

odpowiadająca temu zdaniu formuła to:

$$a \Rightarrow (b \vee c)$$

Dla ustalonego x zdanie może być prawdziwe lub fałszywe.

Zastanówmy się, czy zdanie:

$$(p(x) \wedge (p(x) \Rightarrow (d(x) \vee n(x)))) \Rightarrow d(x) \vee n(x)$$

jest **zawsze prawdziwe**? Okazuje się, że tak - odpowiada ono prawu odrywania (prosze zobaczyć!). Gdy obie przesłanki po lewej stronie są prawdziwe, to i koniunkcja jest prawdziwa. Skoro całe prawo jest tautologią, a jest implikacją, to musi być, że i prawa strona jest prawdziwa.

W ten sposób stworzyliśmy *Regułę Dowodzenia*, która pozwala na wysnuwanie wniosków o jednych formułach, przy założeniu że inne są prawdziwe. Tę konretną regułę nazywamy *modus ponens* i zapisujemy

$$\phi, \phi \Rightarrow \psi \models \psi \tag{1.2}$$

(inny zapis na zajęciach).

Inna nieco mniej znana reguła to *modus tollens*:

$$\neg\psi, \phi \Rightarrow \psi \models \neg\phi \tag{1.3}$$

Ogólny zapis reguł dowodzenia to:

$$A_1, A_2, \ldots, A_n \models B \tag{1.4}$$

A odpowiadające im formuły to:

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow B \tag{1.5}$$

Reguła jest nazywana *niezawodną*, jeżeli z prawdziwych przesłanek wynikaja prawdziwe wnioski, lub inaczej, kiedy odpowiednia formuła jest tautologią klasycznego rachunku zdań.

Można łatwo sprawdzić, że zarówno modus tollens jak i pones mają formuły, które są tautologiami.

Teraz mozna się zastanawiać: co to jest dowód, co to jest zdanie prawdziwe, co to jest twierdzenie?

Matematycy zaproponowali aby wyróżnić pewne formuły i uznać je za prawdziwe (aksjomaty) oraz wyrównić pewne reguły dowodzenia, a nastepnie zapytać, jakie inne formuły da się dowieść, korzystając jedynie z założeń aksjomatów i dostepnych reguł. Taki zbiór reguł i aksjomatów nazwano *systemem*.

Dowód formuły B w systemie to ciąg formuł $A_1, A_2, \ldots, A_n = B$, takich, że A_i jest

1. aksjomatem, albo
2. istnieją formuły A_{j_k}, $j_k < i$, takie, że $A_{j_1}, A_{j_n} \models A_i$ jest regułą w systemie.

Formułę nazywamy *twierdzeniem*, jeśli ma dowód.

Przykładowo, wybierzmy następujące aksjomaty (Aksjomaty klasycznego rachunku zdań):

1. $\phi \Rightarrow (\psi \Rightarrow \phi)$ (aksjomat K),
2. $(\phi \Rightarrow (\nu \Rightarrow \psi)) \Rightarrow ((\phi \Rightarrow \nu) \Rightarrow (\phi \Rightarrow \psi))$ (aksjomat S),
3. $(\neg\phi \Rightarrow \psi) \Rightarrow ((\neg\phi \Rightarrow \neg\psi) \Rightarrow \phi)$ (schemat dowodu niewprost)

Oraz regułę modus ponens. Uwaga: w aksjomatach $\phi, \psi\nu$, itp. to dowolne inne formuły, możemy w te meijsca wstawić dowolne napisy z rachunku zdań, ale tak, że jesli w jednym miejscu zamieniamy ϕ np. na $a \Rightarrow b$, to musimy wszędzie za ϕ wstawić ten napis. Np. Aksjomat K z powyższym podstawieniem przyjmie postać $(a \Rightarrow b) \Rightarrow (\psi \Rightarrow (a \Rightarrow b))$.

W tym systemie tym można podac dowód formuły $\phi \Rightarrow \phi$ lub $\phi \vee \neg\phi$ (drugą nalezy sprowadzić do postaci, która zawiera tylko negacje i implikacje).

Przykład: dowód że $\phi \Rightarrow \phi$:

1. $(\phi \Rightarrow ((\xi \Rightarrow \phi) \Rightarrow \phi)) \Rightarrow ((\phi \Rightarrow (\xi \Rightarrow \phi)) \Rightarrow (\phi \Rightarrow \phi))$ (aksjomat S)

   - podstawiamy $\nu = (\xi \Rightarrow \phi)$ oraz $\psi = \phi$ w Aksjomacie S. Ponieważ jest to Aksjomat S („wygląda jak on”), to wiemy, że jest prawdziwy - Aksjomat S jest prawdziwy, jako tautologia, dla dowolnych wartościowań swoich pod-formuł, więc to się nie zmieni, jeśli podstawimy dowolne formuły, nieważne jak by się wartościowały. Dalej będę tylko pisał, że dany punkt to Aksjomat (K, S, lub 3).

2. $(\phi \Rightarrow ((\xi \Rightarrow \phi) \Rightarrow \phi))$ (Aksjomat K)

3. $((\phi \Rightarrow (\xi \Rightarrow \phi)) \Rightarrow (\phi \Rightarrow \phi))$ (modus ponens z 1 i 2)

   - Widzimy, że podpunkt 2 występuje jako pierwsza część implikacji oznaczonej czerwoną strzałką w podpunkcie 1. Ponieważ podpunkt 2 jest aksjomatem, stosujemy modus ponens:

   $1, 2 \models 3$

4. $((\phi \Rightarrow (\xi \Rightarrow \phi))$ (Aksjomat K)

5. $\phi \Rightarrow \phi$ $(3, 4 \models 5)$

■

W skrócie, pomijając komentarze:

1. $(\phi \Rightarrow ((\xi \Rightarrow \phi) \Rightarrow \phi)) \Rightarrow ((\phi \Rightarrow (\xi \Rightarrow \phi)) \Rightarrow (\phi \Rightarrow \phi))$

2. $(\phi \Rightarrow ((\xi \Rightarrow \phi) \Rightarrow \phi))$

3. $((\phi \Rightarrow (\xi \Rightarrow \phi)) \Rightarrow (\phi \Rightarrow \phi))$

4. $((\phi \Rightarrow (\xi \Rightarrow \phi))$

5. $\phi \Rightarrow \phi$

■

Widać, że dowody formalne mogą być konfundujące i nie prowadzić do głębszego zrozumienia problemu. W szczególności trzeba „wpaść” od jakiej formuły zacząć, aby proces odrywania mógł być kontynuowany aż do formuły, którą chcemy dowieść.

1.5 Twierdzenie Posta

Pytanie jest takie: czym jest zbiór wszystkich formuł, które da się dowieść w podanym systemie? Okazuje się, że

Twierdzenie 1.5.1 (Post) *Formuła jest tautologią wtedy i tylko wtedy gdy jest twierdzeniem klasycznego rachunku zdań!*

Wniosek 1.5.1.1 *W klasycznym rachunku zdań można automatycznie dowodzić twierdzenia.*

Dowód: każda formuła ma skończona ilość zmiennych, dajmy na to $m \in \mathbb{N}$. Wystarczy rozpatrzeć wszystkie wartościowania zmiennych (jest ich 2^m) i sprawdzić, czy formuła dla każdego wartościuje się na 1. Jeśli tak, to formuła jest tautologią, a więc w myśl Twierdzenia Posta jest twierdzeniem klasycznego rachunku zdań. ■

UWAGA: Formalny dowód z reguły modus ponens i aksjomatów może wcale nie być dla niej prosty!

Prosze zauważyć, że reguła modus ponens, podaje nam sposób na tworzenie *formalnych* dowodów matematycznych, przez stosowanie ciągu logicznych wynikań. Jest to dedukcja w stylu Sherlocka Holmesa :)

Na dalszych zajęciach poznamy więcej sposobów dowodzenia różnych twierdzeń. To co warto zapamiętać, to to, że matematyka daje nam ścisłe i formalne narzędzia wykazywania, które czasem można nawet sprawdzić automatycznie! (Np. w rachunku zdań, mając pełny formalny dowód, łatwo jest sprawdzić, czy każda formuła pasuje do schematu aksjomatu lub czy jest poprawnym zastosowaniem reguły modus ponens).

1.5.1 Zadania

1. Udowodnić formalnie następujące formuły:

   (a) $\phi \vee \neg\phi$

   (b) $\neg(\phi \wedge \neg\phi)$

   (c) $((\neg\phi) \Rightarrow \neg(\psi \Rightarrow \neg\phi)) \Rightarrow \phi$

   (aby zobaczyć podpowiedź, nalezy kliknąć w dymek)

   Podpowiedź 1:

   Podpowiedź 2:

2. Podpunkt 1(c) udowodnić metodą tabelki.

3. Pokazać, że formuła z podpunktu 1(c) jest równoważna formule odpowiadającej zasadzie *modus tollens*

   Podpowiedź: