Witold Bołt
Taduesz Andrzej Kadłubowski

Logika matematyczna

wersja 0.94 (1 września 2005)

Spis treści

Wstęp

Opracowanie „Logika matematematyczna”, powstało w oparciu o wykład prowadzony w semestrze letnim roku akademickiego 2004/2005, na wydziale Mat–Fiz–Inf Uniwersytetu Gdańskiego, przez prof. dr hab. Ireneusza Recława dla II roku informatyki. Autorzy opracowania w żaden sposób nie zamierzali naruszyć praw autorskich lub jakichkolwiek innych, należących do wykładowcy (lub kogokolwiek innego).

Opracowanie to jest udostępnione w stanie „jak jest”, tzn. autorzy dołożyli starań, by opracowanie to było przyzwoite i rzetelne, jednak nie mogą udzielić żadnej gwarancji. W szczególności nie gwarantują merytorycznej poprawności, zgodności z treścią wykładu, użyteczności do jakichkolwiek celów, czy w końcu sensowności matematycznej zawartych tu treści. W przypadku znalezienie jakichkolwiek błędów, niejasności lub fragmentów które są zupełnie niezrozumiałe, prosimy o kontakt na adres e–mail: `houp@tlen.pl`, lub `tkadlubo@manta.math.univ.gda.pl`. Aktualną wersje skryptu można zawsze znaleźć na stronie: `http://manta.univ.gda.pl/~wbolt/logic/`.

1 Systemy relacyjne

Cała logika matematyczna o jakiej będziemy tutaj mówić, zajmuje się opisem i badaniem różnych, tzw. systemów relacyjnych. Zaczniemy więc od zdefiniowania tego pojęcia.

Definicja 1.1 (system relacyjny)**.** Systemem relacyjnym $\mathbb{A}$ nazywamy uporządkowany układ zbiorów:

$$\mathbb{A} = \langle \mathcal{A}, \{r_i^{\mathbb{A}}\}_{i\in I}, \{f_j^{\mathbb{A}}\}_{j\in J}, \{c_k^{\mathbb{A}}\}_{k\in K} \rangle,$$

gdzie: $\mathcal{A}$ to pewien niepusty zbiór[1], $\{r_i^{\mathbb{A}}\}_{i\in I}$ to zbiór relacji określonych na zbiorze $\mathcal{A}$, $\{f_j^{\mathbb{A}}\}_{j\in J}$ to zbiór funkcji: $\mathcal{A}^{n_j} \to \mathcal{A}$, natomiast zbiór $\{c_k^{\mathbb{A}}\}_{k\in K}$ to zbiór wyróżnionych stałych należących do $\mathcal{A}$.

Zbiory relacji, funkcji i stałych, o których mowa w powyższej definicji, mogą być puste.

Przykład 1.2. Oto kilka przykładów systemów relacyjnych:

- $\langle \mathbb{R}, \leqslant \rangle$, czyli zbiór liniowo uporządkowanych liczb rzeczywistych,
- $\langle \mathbb{R}, +, *, 0, 1 \rangle$, czyli ciało liczb rzeczywistych,
- $\langle \text{świat matematyczny}, \in \rangle$.

Aby móc opisywać systemy relacyjne, musimy w jakiś sposób je charakteryzować. Wprowadzamy więc pojęcie typu systemu relacyjnego.

Definicja 1.3 (typ systemu relacyjnego)**.** Typ systemu relacyjnego, to uporządkowana trójka funkcji, postaci:

$$\tau = (\tau_1, \tau_2, \tau_3),$$

gdzie: $\tau_1(i)$ to liczba argumentów i-tej relacji w systemie relacyjnym, $\tau_2(j)$ to liczba argumentów j-tej funkcji w systemie relacyjnym, $\tau_3(k)$ jest równe zero, dla każdego $k \in K$, dzięki τ_3 dostajemy wiec tylko informację ile jest stałych w danym systemie.

[1]Zdaniem niektórych, w tym prof. Mostowskiego, dodanie warunku $\mathcal{A} \neq \emptyset$ więcej szkodzi, niż pomaga.

2 Język, termy i formuły

2.1 Język

Definicja 2.1 (język)**.** Językiem $\mathscr{L}$ typu τ nazywamy uporządkowaną piątkę zbiorów symboli:

$$\mathscr{L}(\tau) = \langle R, F, C, X, S \rangle,$$

gdzie:

- zbiór R to zbiór symboli relacyjnych: $R = \{r_i : i \in I\}$,
- zbiór F to zbiór symboli funkcyjnych: $F = \{f_j : j \in J\}$,
- zbiór C to zbiór symboli stałych: $C = \{c_k : k \in K\}$,
- zbiór X to zbiór symboli zmiennych: $X = \{x_n : n \in \mathbb{N}\}$ (uwaga: jest to zawsze zbiór nieskończony!),
- zbiór S to zbiór symboli logicznych: $S = \{\neg, \rightarrow, \forall, =, (,)\}$.

Język należy rozumieć jako zbiór symboli, które nie muszą mieć jakiegokolwiek znaczenia - jest to po prostu coś z czego składać będziemy jakieś napisy, które dopiero, gdy będą miały jakiś model, nabiorą znaczenia. Napisy, które dalej nazywać będziemy formułami, budujemy z mniejszych „klocków”, które nazywać będziemy termami. Poniżej podajemy definicję zbioru wszystkich termów języka $\mathscr{L}$.

2.2 Termy i wartościowanie

Definicja 2.2 (zbiór termów)**.** Zbiór wszystkich termów oznaczamy przez T_m. Jest on postaci:

$$T_m = \bigcup_n T_{m_n},$$

gdzie $T_{m_0} = X \cup C$, $T_{m_{n+1}} = T_{m_n} \cup \{f_j(t_1, \ldots, t_{n_j}) : j \in J, t_1, \ldots, t_{n_j} \in T_{m_k}, k \leqslant n\}$.

Zgodnie z tą definicją, termami są zmienne i stałe z języka $\mathscr{L}$, oraz wszystkie symbole funkcji „liczone” na wcześniej zdefiniowanych termach. Zauważmy, że symbole relacyjne nie są termami!

Definicja 2.3 (podstawienie)**.** Podstawieniem (lub inaczej wartościowaniem) nazywamy dowolną funkcję $p\colon X \to \mathcal{A}$.

Aby zdefiniować wartość termu, musimy rozszerzyć funkcję p tak aby jej dziedziną był zbiór T_m. Przyjmujemy więc dodatkowo: $p(c_k) = c_k^{\mathbb{A}}$ dla każdego $k \in K$, oraz $p(f_j(t_1, \ldots, t_{n_j})) = f_j^{\mathbb{A}}(p(t_1), \ldots, p(t_{n_j}))$ dla każdego $j \in J$. W ten sposób możemy wyliczyć wartość dowolnego termu t. Wartość tą oznaczamy przez $p(t)$ lub $t[p]$.

2.3 Formuły

Podobnie jak w przypadku termów, zdefiniujemy zbiór wszystkich formuł.

Definicja 2.4 (zbiór formuł)**.** Zbiór wszystkich formuł języka $\mathscr{L}$, który określamy przez F_m, jest zbiorem postaci: $F_m = \bigcup_n F_{m_n}$, gdzie $F_{m_0} = \{t_1 = t_2, r_i(t_1, \ldots, t_{n_i}) : t_1, \ldots, t_{n_i} \in T_m, i \in I\}$, $F_{m_{n+1}} = F_{m_n} \cup \{(F \to G), (\neg F), (\forall_x F) : F, G \in F_{m_n}\}$.

Zbiór F_{m_0} z powyższej definicji, zawiera tak zwane formuły atomowe. Jak łatwo można zauważyć, w definicji tej zakładamy, że wszystkie formuły powstają wyłącznie z formuł atomowych, implikacji, negacji i kwantyfikatora ogólnego. Często w dowodach twierdzeń metamatematycznych trzeba rozpatrzyć wszystkie możliwości łączenia formuł prostszych w bardziej skomplikowane. Właśnie dlatego tylko tyle sposobów na konstruowanie nowych formuł w powyższej definicji się znalazło — lepiej mieć mniej możliwości.

Oczywiście w praktyce stosuje się również inne spójniki i operatory logiczne niż te z naszej definicji. Można udowodnić, że ten zestaw, który wybraliśmy wystarczy, aby skonstruować wszystkie inne spójniki logiczne. Należy wiedzieć, że gdy używamy innych symboli do konstruowania formuł, to traktujemy je jedynie jako skróty pojęć z powyższej definicji.:

- Zapis $F \vee G$ należy rozumieć jako $\neg F \to G$.
- Zapis $F \wedge G$ odpowiada zapisowi $\neg(F \to \neg G)$.
- Zapis $F \iff G$ to tak naprawdę $(F \to G) \wedge (G \to F)$, czyli w myśl poprzedniego napisu $\neg((F \to G) \to \neg(G \to F))$.
- Zapis $\exists_x F$ zastępujemy natomiast przez $\neg\forall_x \neg F$.

2.4 Zmienne wolne, związane i zdania

Nieformalnie można powiedzieć, że zmienne wolne to takie które nie są „związane” żadnym kwantyfikatorem[2]. Na przykład w formule $\forall_x x + y < x$, zmienna y jest zmienną wolną, natomiast x jest zmienną związaną. W związku z tym, że w termach nie występują kwantyfikatory, przyjmuje się, że wszystkie zmienne w termie są wolne. Zbiór wszystkich zmiennych wolnych termu bądź formuły oznaczamy odpowiednio przez $V(t)$ lub $V(F)$. Zmiennymi wolnymi formuły, zależnie od jej postaci, są:

- $V(t_1 = t_2) = V(t_1) \cup V(t_2)$,
- $V(r_i(t_1, \ldots, t_{n_i})) = V(t_1) \cup \ldots \cup V(t_{n_i})$,
- $V(F \to G) = V(F) \cup V(G)$,
- $V(\neg F) = V(F)$,
- $V(\forall_x F) = V(F) \backslash \{x\}$.

Bardzo często rozważać będziemy formuły w których nie ma zmiennych wolnych. Ze względu na swoją wagę i powszechność, takie formuły mają swoją własną nazwę.

Definicja 2.5 (zdanie)**.** Formułę F nazywamy zdaniem, jeśli $V(F) = \emptyset$.

2.5 Prawdziwość formuły w systemie relacyjnym

Definicja spełniania formuły w systemie relacyjnym, przy danym podstawieniu, musi obejmować wszystkie możliwe postaci formuły F. W definicji będziemy używać oznaczenia $\mathbb{A} \models F[p]$, które należy czytać „formuła F jest spełniona w modelu $\mathbb{A}$ przy podstawieniu p”.

Obok definicji wartościowania termów jest to tak naprawdę jedyne miejsce, gdzie warstwa języka $\mathscr{L}$ styka się z prawdziwymi obiektami matematycznymi. Formuły to tylko ustawianie literek obok siebie, dopiero tutaj przypisujemy im znaczenie.

[2]Uwaga: pojęcie zmiennej wolnej i związanej jest tutaj potraktowane bardzo nieformalnie, gdyż mogą zdażyć się formuły w których zmienna jest wolna w jednym miejscu formuł, a związana w innym – tzn. gdy zasięg jakiegoś kwantyfikatora jest ograniczony przez nawiasy. W takim przypadku ogólnie przyjmujemy, że zmienna jest wolna. Tak czy inaczej, aby pozbyć się takich problemów, zawsze możemy założyć, że na samym początku zamieniamy oznaczenia zmiennych które mogłby powodować kontrowersje – mamy do dyzpozycji nieskończenie wiele symboli zmiennych, więc nie ma z tym problemu.

Definicja 2.6 (spełnianie formuły w systemie relacyjnym)**.** Zależnie od postaci formuły F definiujemy kiedy $A \models F[p]$.

- Mówimy, że $\mathbb{A} \models (t_1 = t_2)[p]$, jeśli wartości tych dwóch termów są sobie równe, czyli $t_1[p] = t_2[p]$.
- Mówimy, że $\mathbb{A} \models r_i(t_1, \ldots, t_n)[p]$, jeśli zachodzi pomiędzy wartościami tych termów relacja $r_i^{\mathbb{A}}(t_1[p], \ldots, t_n[p])$.
- Mówimy, że $\mathbb{A} \models (F \to G)[p]$, jeśli $\mathbb{A} \models F[p]$ implikuje $\mathbb{A} \models G[p]$.
- Mówimy, że $\mathbb{A} \models (\neg F)[p]$, jeśli nieprawda, że $\mathbb{A} \models F[p]$.
- Mówimy, że $\mathbb{A} \models (\forall_x F)[p]$, jeśli dla każdego elementu $a \in \mathcal{A}$ zachodzi $\mathbb{A} \models F[p(a/x)]$, gdzie $p(a/x)(y) = \begin{cases} a & y = x \\ p(y) & y \neq x \end{cases}$.

3 Izomorfizmy systemów relacyjnych

Definicja 3.1 (izomorfizm systemów relacyjnych[3])**.** Niech $\mathbb{A}$ i $\mathbb{B}$ będą systemami relacyjnymi tych samych typów. Funkcja $h\colon \mathbb{A} \to \mathbb{B}$ jest izomorfizmem, jeśli:

1. h jest bijekcją, tzn. jest różnowartościowa i „na”,
2. dla każdego $i \in I$ zachodzi $r_i^{\mathbb{A}}(x_1, \ldots, x_k) \equiv r_i^{\mathbb{B}}(h(x_1), \ldots, h(x_k))$,
3. dla każdego $j \in J$ zachodzi $h(f_j^{\mathbb{A}}(x_1, \ldots, x_n)) = f_j^{\mathbb{B}}(h(x_1), \ldots, h(x_k))$,
4. dla każdego $k \in K$ zachodzi $h(c_k^{\mathbb{A}}) = c_k^{\mathbb{B}}$.

Twierdzenie 3.2. *Niech $\mathbb{A}$ i $\mathbb{B}$ systemy relacyjne tych samych typów, oraz $h\colon \mathbb{A} \to \mathbb{B}$ izomorfizm. Niech p będzie dowolnym podstawieniem. Wtedy, dla każdej formuły F, zachodzi:*

$$\mathbb{A} \models F[p] \equiv \mathbb{B} \models F[h \circ p].$$

A gdy F jest zdaniem, zachodzi:

$$\mathbb{A} \models F \equiv \mathbb{B} \models F.$$

Dowód: Aby podać dowód tegoż twierdzenia, najpierw udowodnimy lemat.

Lemat 3.3. *Dla dowolnego termu t, podstawienia p i izomorfizmu h, zachodzi: $h(t[p]) = t[h \circ p]$.*

Dowód lematu: Dowód będzie indukcyjny w zależności od najmniejszego indeksu n takiego, że $t \in T_{m_n}$. Pierwszy krok to $t \in T_{m_0}$. Czyli t jest albo zmienną albo stałą. Jeśli $t = x_m \in X$, to $h(x_m[p]) = h(p(x_m)) = h \circ p(x_m) = x_m[h \circ p]$. Jeśli natomiast $t = c \in C$, to $h(c[p]) = h(c^{\mathbb{A}}) = c^{\mathbb{B}}$. Stała oczywiście nie zależy od podstawienia, więc możemy napisać $c^{\mathbb{B}} = c[h \circ p]$. Pierwszy krok indukcji mamy w ten sposób za sobą. Załóżmy więc, że jeśli term t należy do T_{m_n} to lemat jest prawdziwy. Zastanówmy się co się dzieje, jeśli term t należy do $T_{m_{n+1}}$. Jest on wtedy na pewno postaci $f(t_1, \ldots, t_n)$, gdzie dla termów $t_1, \ldots, t_n$ możemy korzystać z założenia indukcyjnego. Mamy więc

$$h(f(t_1, \ldots, t_n)[p]) = h(f^{\mathbb{A}}(t_1[p], \ldots, t_n[p])) =$$

Z definicji izomorfizmu mamy dalej:

$$= f^{\mathbb{B}}(h(t_1[p]), \ldots, h(t_n[p])) =$$

[3]To zagadnienie nie zostało zawarte w spisie zagadnień na egzamin pisemny z Logiki.

Korzystając z założenia indukcyjnego mamy:

$$= f^{\mathbb{B}}(t_1[h \circ p], \ldots, t_n[h \circ p]) =$$

No a z definicji wartościowania termu mamy:

$$= f(t_1, \ldots, t_n)[h \circ p]. \quad \Box$$

W ten sposób udowodniliśmy nasz lemat. Przejdźmy do dowodu właściwego twierdzenia. Przeprowadzimy dowód indukcyjny ze względu na postać i rozbudowanie formuły, to znaczy ze względu na n – indeks F_{m_m} do którego należy F. W pierwszym kroku indukcyjnym rozważamy formuły F z F_{m_0}. Wobec tego, F może być postaci $t_1 = t_2$ lub $r(t_1, \ldots, t_n)$.

- Niech F będzie postaci: $t_1 = t_2$. Wówczas $A \models F[p]$ jest spełnione wtedy i tylko wtedy, gdy $t_1[p] = t_2[p]$. Korzystając z definicji izomorfizmu h możemy napisać równoważnie: $h(t_1[p]) = h(t_2[p])$. No ale zgodnie z udowodnionym lematem, jest to równoważne: $t_1[h \circ p] = t_2[h \circ p]$, co z godnie z definicją spełniania równości, jest równoważne warunkowi: $\mathbb{B} \models (t_1 = t_2)[h \circ p]$.
- Niech F będzie postaci: $r(t_1, \ldots, r_n)$. Wtedy $A \models F[p]$ jest spełnione tylko i wyłącznie, gdy $r^{\mathbb{A}}(t_1[p], \ldots, t_n[p])$. Korzystając z definicji h mamy: $r^{\mathbb{B}}(h(t_1[p]), \ldots, h(t_n[p]))$, co na mocy lematu daje nam: $r^{\mathbb{B}}(t_1[h \circ p], \ldots, t_n[h \circ p])$. Z definicji spełniania formuły, dostajemy: $\mathbb{B} \models r(t_1, \ldots, r_n)[h \circ p]$.

W ten sposób zakończyliśmy pierwszy krok indukcyjny. Załóżmy więc, że twierdzenie jest poprawne dla formuł F, które należą do F_{m_n} dla pewnego n. Pokażemy, że wynika z tego również jego prawdziwość dla $G \in F_{m_{n+1}}$. Ograniczymy się do przypadku, gdy G jest postaci $\forall_x F$ (pozostałe przypadki przebiegają bowiem analogicznie): $\mathbb{A} \models (\forall_x F)[p]$ zachodzi wtedy i tylko wtedy, gdy dla każdego $a \in \mathcal{A}$ zachodzi $\mathbb{A} \models F[p(a/x)]$. Korzystając z założenia indukcyjnego, warunek ten jest równoważny warunkowi: dla każdego $a \in \mathcal{A}$ zachodzi $\mathbb{B} \models F[(h \circ p(a/x))]$. To natomiast możemy równoważnie przestawić w postaci: dla każdego $a \in \mathcal{A}$ zachodzi $\mathbb{B} \models F[(h \circ p)(h(a)/x)]$. No a z tego, że h jest bijekcją, możemy również napisać: dla każdego $b \in \mathcal{B}$ zachodzi $\mathbb{B} \models F[(h \circ p)(b/x)]$, co znaczy dokładnie $\mathbb{B} \models (\forall_x F)[h \circ p]$. $\Box$

Wniosek 3.4. Jeśli $\mathbb{A}$ oraz $\mathbb{B}$ są izomorficzne, to są w nich prawdziwe te same zdania.

4 Teoria i model

4.1 Pojęcie teorii i modelu

Zakładamy, że mamy dany język $\mathscr{L}(\tau)$.

Definicja 4.1 (teoria)**.** Teorią nazywamy dowolny zbiór zdań, będący podzbiorem zbioru formuł F_m języka $\mathscr{L}$. Zazwyczaj ten zbiór oznaczmy literą T.

Definicja 4.2 (model)**.** Modelem teorii T nazywamy dowolny system relacyjny $\mathbb{A}$ typu τ, taki że dla każdego zdania $F \in T$ zachodzi:

$$\mathbb{A} \models F.$$

Zauważmy, że w powyższych definicjach zakładaliśmy, że teoria jest zbiorem zdań, a nie ogólnie formuł. Często jednak rozszerzamy tę definicje, tak aby teoria była ogólnie zbiorem formuł.

Definicja 4.3 (teoria i model – rozszerzone dla formuł)**.** Teorią T nazywamy dowolny zbiór formuł, będący podzbiorem zbioru F_m języka $\mathscr{L}$. Modelem takiej teorii T nazywamy dowolny system relacyjny $\mathbb{A}$ wraz z podstawieniem p, jeśli dla każdej formuły $F \in T$ zachodzi:

$$\mathbb{A} \models F[p].$$

Mówimy wówczas, że modelem jest para $\langle \mathbb{A}, p \rangle$.

Uwaga 4.4. O elementach zbioru T często mówimy, iż są to aksjomaty teorii T.

W dalszych rozważaniach za definicję teorii i modelu, przyjmujemy wersje rozszerzone dla formuł.

4.2 Przykłady teorii i ich modeli

Przykład 4.5 (teoria ciał)**.** Rozpatrzmy teorię ciał. Nasz język zawiera dwa symbole stałych 0, 1 oraz dwa symbole działań dwuargumentowych: $+$ i $*$. Aksjomaty teorii ciał to:

$$\forall_{x,y,z}((x + y) + z = x + (y + z))$$
$$\forall_{x,y,z}((x * y) * z = x * (y * z))$$
$$\forall_{x,y} x + y = y + x$$
$$\forall_{x,y} x * y = y * x$$
$$\forall_x x + 0 = x$$
$$\forall_x x * 1 = x$$
$$\forall_x \exists_y x + y = 0$$
$$\forall_{x \neq 0} \exists_y x * y = 1$$
$$\forall_{x,y,z} x * (y + z) = x * y + x * z$$

Przykład 4.6 (modele teorii ciał)**.** Modelami teorii ciał, są na przykład:

1. $\langle \mathbb{Q}, 0, 1, +, * \rangle$, czyli ciało liczb wymiernych ze standardowymi działaniami.
2. $\langle \mathbb{R}, 0, 1, +, * \rangle$, czyli podobne ciało liczb rzeczywistych.
3. $\langle \mathbb{Z}_p, 0, 1, +, * \rangle$, czyli ciało reszt modulo p, gdzie p jest liczbą pierwszą, a wszystkie działania są „modulo p".

Przykład 4.7 (teoria porządków częściowych i liniowych)**.** Rozparzmy teorię porządków częściowych. Język zawiera jedynie jeden symbol relacyjny $\{\leqslant\}$. Aksjomatami teorii porządków częściowych są:

$$\forall_x x \leqslant x$$
$$\forall_x \forall_y \forall_z (x \leqslant y \land y \leqslant z \to x \leqslant z)$$
$$\forall_x \forall_y (x \leqslant y \land y \leqslant x \to x = y)$$

W tym samym języku możemy wyrazić również teorię porządków liniowych. Do podanych wyżej aksjomatów należy wówczas dodać jeszcze:

$$\forall_x \forall_y (x \leqslant y \lor y \leqslant x).$$

Przykład 4.8 (modele teorii porządków częściowych i liniowych)**.** Rozważmy modele:

1. $\langle \mathbb{R}, \leqslant \rangle$, czyli zbiór liczb rzeczywistych ze standardową relacją „mniejszy–równy", jest modelem zarówno dla teorii porządków częściowych, jak i liniowych.
2. $\langle P(\mathbb{N}), \subset \rangle$, czyli zbiór wszystkich podzbiorów liczb naturalnych z relacją bycia podzbiorem, jest modelem dla teorii porządków częściowych. Nie jest to jednak model dla teorii porządków liniowych.

Przykład 4.9 (teoria mnogości)**.** Teoria mnogości (która oznaczać będziemy dalej ZFC[4])

[4] Zermelo-Frankel set theory with the axiom of Choice.

jest bardzo ważna i dość specyficzna, gdyż logika korzysta z niej również jako z tzw. metateorii – czyli teorii w której uprawiamy logikę matematyczną. Można uznać, że teoria mnogości jest to podstawowa teoria całej matematyki. Do jej opisu używamy języka z jednym tylko symbolem relacyjnym $\{\in\}$ – relacją należenia. Oto aksjomaty teorii mnogości (nie wszystkie będą zapisane formalnie):

1. Ekstensjonalność: zbiory są równe, jeśli mają te same elementy.
2. Istnieje zbiór pusty, tzn.
$$\exists_x \forall_y \neg(y \in x).$$
Zbiór pusty oznaczamy dalej jako $\emptyset$.
3. Aksjomat pary: istnieje zbiór $\{x, y\}$ dla dowolnych x i y.
4. Aksjomat sumy: istnieje $\bigcup x$ dla dowolnego x.
5. Aksjomat zbioru potęgowego[5]: istnieje zbiór $P(x)$ dla dowolnego x.
6. Aksjomat nieskończoności: istniej zbiór A taki, że $\emptyset \in A$, oraz jeśli jakiś x należy do A to również $x \cup \{x\}$ należy do A, co formalnie można zapisać:
$$x \in A \to x \cup \{x\} \in A.$$
Zbiór A można sobie wyobrazić jako zbiór postaci:
$$A = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots\}.$$
Najmniejszym takim zbiorem A jest zbiór liczby naturalnych $\mathbb{N}$ – czyli do zdefiniowania zbioru liczb naturalnych nie potrzebujemy żadnych liczb, wystarczy nam tylko zbiór pusty.
7. Aksjomat wyboru: z każdej rodziny zbiorów niepustych, parami rozłącznych, można wybrać tzw. „selektor", czyli zbiór, który ma po jednym punkcie wspólnym z każdym ze zbiorów rodziny.
8. Aksjomat ufundowania: w każdym zbiorze istnieje element z nim rozłączny, czyli:
$$\forall_x \exists_y y \in x \wedge y \cap x = \emptyset.$$
Wyklucza to sytuację $x \in x$.
9. Aksjomat wyróżniania: jeśli Z jest pewnym zbiorem, oraz $\varphi(x)$ pewną formułą, to istnieje zbiór $\{x : x \in Z \wedge \varphi(x)\}$. Zapis ten należy traktować jako schemat aksjomatu, opisujący nieskończenie wiele aksjomatów – dla każdej możliwej formuły φ jest to inny aksjomat.
10. Aksjomat zastępowania[6]: jeśli dla pewnej formuły $F(x, y)$ spełniony jest warunek, że dla każego $x \in X$ istnieje $y \in Y$ taki, że $F(x, y)$, to dla każdego zbioru $A \subset X$ istnieje zbiór $B \subset Y$, którego elementami są te i tylko te elementy y, dla których przy pewnym $x \in A$, zachodzi $F(x, y)$.

Uwaga 4.10 (model teorii mnogości)**.** Nie można udowodnić, że istnieje model teorii mnogości. Być może, można udowodnić, że taki model nie istnieje.

[5]Zbiór potęgowy to zbiór wszystkich podzbiorów danego zbioru. Zbiór ten oznaczamy również przez 2^X.
[6]Na wykładzie aksjomat ten został inaczej sformułowany, w tym opracowaniu podano jednak sformułowanie bardziej zrozumiałe dla autora – znalezione na stronie: `http://www.mif.pg.gda.pl/kmd/ami/cz2.pdf`.

5 Aksjomaty logiki, definicja dowodu

Poniżej zebrano schematy aksjomatów logiki. Ogólnie aksjomatów jest nieskończenie wiele. Podajemy je jednak w skończenie wielu schematach. Język jakim się posługujemy opisując logikę nie pozwala nam tak naprawdę używać kwantyfikatora „dla każdej formuły”. Dlatego też wszelkie aksjomaty zawierające w sobie „dowolną formułę F”, należy rozumieć jako schemat z którego powstaje nieskończenie wiele aksjomatów przez podstawianie każdej możliwej formuły w miejsce F.

Aksjomaty logiki:

- Aksjomaty rachunku zdań. Dla dowolnych formuł F, G, H mamy:

$$F \to (G \to F),$$

$$F \to (G \to H) \to ((F \to G) \to (F \to H)),$$

$$(\neg G \to \neg F) \to (F \to G).$$

- Aksjomaty podstawienia:

$$\forall_x F \to F(t/x),$$

gdzie $F(t/x)$ to podstawienie właściwe[7].

- Aksjomat o rozdzielczości:

$$\forall_x (F \to G) \to (\forall_x F \to \forall_x G).$$

- Jeśli x nie jest zmienną wolną w F, to zachodzi:

$$F \to \forall_x F.$$

- Aksjomaty równości[8] . Dla dowolnych termów t_1, t_2, t_3:

$$t_1 = t_1,$$

$$t_1 = t_2 \to t_2 = t_1,$$

$$t_1 = t_2 \to (t_2 = t_3 \to t_1 = t_3),$$

$$t_1 = s_1 \to (\ldots \to (t_n = s_n \to$$

$$(r(t_1, \ldots, t_n) \to r(s_1, \ldots, s_n)) \ldots),$$

$$t_1 = s_1 \to (\ldots \to (t_n = s_n \to$$

$$(f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)) \ldots).$$

Uwaga 5.1. Do wszystkich aksjomatów logiki można dopisać dowolną liczbę kwantyfikatorów ogólnych.

Poza aksjomatami logiki, które oznaczać będziemy przez *Log* używać też będziemy reguły wnioskowania zwanej „regułą odrywania” lub „*modus ponens*”. Reguła ta mówi, że jeśli formuły $F \to G$ oraz F uznaliśmy za prawdziwe, formułę G też powinniśmy uznać za prawdziwą. Korzystając z tej reguły będziemy budować dowody twierdzeń logiki.

Definicja 5.2 (dowód)**.** Dowodem formuły F w oparciu o teorię T nazywamy dowolny skończony ciąg formuł $F_1, \ldots, F_n$, taki, że $F_n = F$, a każda inna formuła tego ciągu jest albo aksjomatem (tzn. należy do $Log \cup T$) albo powstała z reguły odrywania z poprzednich wyrazów ciągu.

Z definicji dowodu nie wynika wcale, że powinien on mieć jakiś większy sens czy porządek. Wszystko się dzieje w warstwie syntaktycznej, nie wnikamy w matematyczne znaczenie, lecz tylko interesuje nas wygląd napisów. Dowód logiczny może być całkiem „nielogiczny”, wystarczy tylko by spełniał warunki definicji i już jest poprawnym dowodem.

Wniosek 5.3. Jeśli formuła F ma jakiś dowód w oparciu o T, to ma nieskończenie wiele różnych dowodów.

[7] Podstawienie jest właściwe, kiedy wszystkie zmienne z termu t który podstawiamy w miejsce x są wolne w formule F.

[8] Relacja równości jest tak specyficzna, że bardzo często traktuje się ją jako coś dodatkowego, niezależnego od systemu relacyjnego. Równie dobrze moglibyśmy po prostu dodać do zbioru relacji jeszcze jedną relację $= (t_1, t_2)$, i punkt o równości wyrzucić z tej definicji. Nie robimy tego trochę dla wygody, a pewnie też trochę ze względów historycznych, a pewnie jeszcze i innych subtelności, których studenci nie są sobie w stanie wyobrazić.

Definicja 5.4. Twierdzenie teorii T, to formuła, która ma dowód w oparciu o teorię T.

Jeśli formuła F ma dowód w oparciu o teorię T, piszemy $T \vdash F$. Jeśli jakaś formuła F ma dowód w każdej teorii, to znaczy jeśli wynika z aksjomatów logiki, piszemy $\vdash F$. Formuły F o których możemy napisać $\vdash F$, nazywamy twierdzeniami logiki.

Uwaga 5.5. Od tej pory wszystkie twierdzenia logiki będziemy traktować w miarę na równi z aksjomatami logiki. Dla uproszczenia, gdy w dowodzie będziemy chcieli wykorzystać jakieś twierdzenie logiki, to będziemy pomijali fragment polegający na dowodzie tego twierdzenia.

Twierdzenie 5.6. *Jeśli w T da się udowodnić formułę F, to istnieje skończony podzbiór $T_0 \subset T$, taki, że $T_0 \vdash F$.*

Dowód: Skoro w T da się udowodnić formułę F to istnieje jakiś dowód. Niech dowodem tym będzie ciąg $F_1, \ldots, F_n$. Możemy zbudować teorię T_0, korzystając z wyrazów tego ciągu, a dokładniej:

$$T_0 = \{F_i : F_i \text{ jest aksjomatem}\}.$$

Takie T_0 jest na pewno zbiorem skończonym, na pewno jest podzbiorem T i na pewno zachodzi $T_0 \vdash F$. $\square$

5.1 Przykłady twierdzeń logiki

Podamy dwa przykłady twierdzeń logiki w raz z ich formalnymi dowodami rozumianymi w kontekście naszej definicji dowodu.

Fakt 5.7. *Dla dowolnej formuły F mamy: $\vdash F \to F$.*

Dowód: Żeby wyraźniej pokazać, iż dowód logiczny może być zupełnie nie jasny i niezrozumiały, podamy najpierw po prostu ciąg formuł który będzie już kompletnym dowodem – bez żadnych komentarzy. Następnie każdy wyraz ciągu opatrzymy stosownym komentarzem, jednak z formalnego punktu widzenia komentarz ten jest zbędny. Oto pełny dowód naszego faktu:

$$F \to ((F \to F) \to F)$$

$$(F \to ((F \to F) \to F)) \to ((F \to (F \to F)) \to (F \to F))$$

$$(F \to (F \to F)) \to (F \to F)$$

$$F \to (F \to F)$$

$$F \to F \quad \square$$

Dowód ten, mimo że kompletny i poprawny, dla większości czytelników może okazać się nieco niezrozumiały (dla autorów również). Dlatego teraz każdą linijkę dodatkowo opatrzono komentarzem.

Korzystamy z aksjomatu $F \to (G \to F)$, gdzie za G podstawiamy $F \to F$:

$$F \to ((F \to F) \to F)$$

Drugi aksjomat rachunku zdań:

$$(F \to ((F \to F) \to F)) \to ((F \to (F \to F)) \to (F \to F))$$

Tą formułę otrzymujemy z dwóch poprzednich, korzystając z reguły odrywania.

$$(F \to (F \to F)) \to (F \to F)$$

Ponownie korzystamy z aksjomatu $F \to (G \to F)$, gdzie za G podstawiamy F.

$$F \to (F \to F)$$

Z reguły odrywania otrzymujemy formułę (korzystając z dwóch poprzednich linijek), która kończy dowód – jest właśnie tą formułą którą chcieliśmy udowodnić:

$$F \to F \quad \Box$$

Fakt 5.8. *Niech $F(x)$ będzie formułą w której nie występuje zmienna y. Wtedy:*

$$\{\forall_x F(x)\} \vdash \forall_y F(y/x).$$

Dowód:

1. Korzystamy z aksjomatu:
$$\forall_x F(x) \to F(y/x)$$

2. Aksjomaty możemy „domykać” kwantyfikatorami ogólnymi:
$$\forall_y \left(\forall_x F(x) \to F(y/x)\right)$$

3. Korzystamy z aksjomatu o rozdzielczości:
$$\forall_y \left(\forall_x F(x) \to F(y/x)\right) \to \left(\forall_y \forall_x F(x) \to \forall_y F(y/x)\right)$$

4. Z reguły odrywania mamy:
$$\forall_y \forall_x F(x) \to \forall_y F(y/x)$$

5. Zapisujemy kolejny aksjomat:
$$\forall_x F(x) \to \forall_y \forall_x F(x)$$

6. Zapisujemy aksjomat naszej teorii, którą założyliśmy w treści twierdzenia:
$$\forall_x F(x)$$

7. Z reguły odrywania dostajemy:
$$\forall_y \forall_x F(x)$$

8. Ponownie z reguły odrywania, mamy:
$$\forall_y F(y/x) \quad \Box$$

5.2 Zbiór konsekwencji teorii T

Kiedy znamy już aksjomaty logiki, z których korzystamy przy dowodzeniu twierdzeń, możemy podać konstrukcję zbioru konsekwencji danej teorii.

Definicja 5.9 (zbiór konsekwencji teorii T)**.** Zbiór konsekwencji teorii T, który oznaczamy T^*, to zbiór postaci:

$$T^* = \bigcup_n T_n,$$

gdzie $T_0 = Log \cup T$, $T_{n+1} = T_n \cup \{G : \exists_F (F \in T_n \land F \to G \in T_n)\}$.

Zbiór T^* również jest pewną teorią (zgodnie z definicją teorii jako dowolnego podzbioru zbioru formuł). Co więcej zachodzą następujące fakty.

Fakt 5.10. *Dla dowolnej teorii T, mamy:*

$$T^* = T^{**}.$$

Innymi słowy, jeśli $T^* \vdash F$, to $T \vdash F$.

Dowód: Niech $F_1, F_2, \cdots, F_n$ będzie dowodem F w T^*. Każdy element F^* z definicji ma dowód w F. Ciąg będący dowodem formuły F w T otrzymamy, gdy zamiast każdego formuły ciągu F_i nie otrzymanej w wyniku użycia reguły odrywania, lecz będącej aksjomatem teorii T^* podstawimy dowód tejże formuły. □

Fakt 5.11. *Formuła F należy do zbioru T^* wtedy i tylko wtedy, gdy ma dowód w oparciu o T.*

Dowód: Implikacja „$\Leftarrow$": Przeprowadzimy dowód indukcyjny ze względu na długość dowodu formuły F. Pierwszy krok indukcyjny jest spełniony, bo gdy długość dowodu wynosi jeden, to znaczy, że F musi być aksjomatem, czyli należeć do T a co za tym idzie do T^*. Załóżmy, więc że jeśli dowód jest długości n to twierdzenie jest spełnione. Zobaczymy co dzieje się, gdy F ma dowód długości $n+1$. Niech dowodem tym będzie: $F_1, \ldots, F_n, F_{n+1}$. Zauważmy, że na mocy założenia indukcyjnego, wszystkie wyrazy od F_1 do F_n muszą należeć do T^*. Co więcej istnieje takie k, że wszystkie te wyrazy należą do T_k. Rozparzmy dwa przypadki w zależności od postaci F_{n+1}. Jeśli F_{n+1} jest aksjomatem (a może tak być), to na pewno należy do T czyli tym bardziej do T^*. Jeśli F_{n+1} nie jest aksjomatem, to musiało powstać z reguły odrywania. Wśród formuł $F_1, \ldots, F_n$ muszą więc istnieć formuły $F_i = G \to F_{n+1}$ oraz $F_j = G$, które należą do T_k. Zgodnie z definicją zbioru T^*, F_{n+1} należy w takim razie na pewno do T_{k+1}, czyli do T^*. Na mocy twierdzenia o indukcji matematycznej, udowodniliśmy jedną część naszego twierdzenia.

Implikacja „$\Rightarrow$": Musimy pokazać, że jeśli F należy do T^* to ma dowód. Przeprowadzimy dowód indukcyjny ze względu na n takie, że $F \in T_n$ oraz $F \notin T_{n-1}$. Pierwszy krok indukcyjny jest spełniony, ze względu na to, że jeśli $F \in T_0$ to dowodem F jest po prostu samo F. Załóżmy więc, że twierdzenie jest prawdziwe dla formuł które należą do T_n. Pokażemy, że jest też dobre dla tych, które należą do T_{n+1} a nie należą do T_n. Jeśli formuła F należy do T_{n+1} to istnieją formuły $G \to F$ oraz G, które należą do T_n. Zgodnie z założeniem indukcyjnym, mają one swoje dowody. Niech $H_1, \ldots, H_m$ będzie dowodem $G \to F$, oraz $G_1, \ldots, G_k$ będzie dowodem G. Wówczas ciąg: $H_1, \ldots, H_m, G_1, \ldots, G_k, F$ jest dowodem F w oparciu o T. □

Twierdzenie 5.12. *Jeśli $F \in T^*$, to F jest prawdziwe w każdym modelu teorii T.*

Dowód: Przeprowadzimy indukcję ze względu na indeks n zbiorów T_n taki, że $F \in T_{n+1} \backslash T_n$. Jeśli F należy do T_0, to jest aksjomatem logiki lub aksjomatem teorii T, więc na pewno jest spełnione w każdym modelu tej teorii. Załóżmy więc, że twierdzenie jest prawdziwe dla formuł które należą do T_n. Pokażemy że również dla formuł należących do $T_{n+1} \backslash T_n$ jest poprawne. Niech F będzie taką formułą. Wtedy na pewno istnieją formuły G i $G \to F$, które należą do T_n. Zgodnie z założeniem indukcyjnym w każdym modelu $\mathbb{A}$ teorii T zachodzi: $\mathbb{A} \models G[p]$ oraz $\mathbb{A} \models (G \to F)[p]$. Zgodnie z definicją spełniania symbolu „$\to$", skoro w $\mathbb{A}$ jest spełnione zarówno $G[p]$ jak i $(G \to F)[p]$, musi też być spełnione $F[p]$. □

Uwaga 5.13. Odwrotne twierdzenie jest również prawdziwe. Jest ono omówione później.

6 Twierdzenie o dedukcji

Twierdzenie 6.1 (o dedukcji)**.** *Niech T – dowolna teoria, F, G – formuły. Wtedy zachodzi: $T \cup \{F\} \vdash G$ wtedy i tylko wtedy, gdy $T \vdash (F \to G)$.*

Dowód: Wynikanie „$\Leftarrow$": Niech ciąg $F_1, \ldots, F_n$ będzie dowodem zdania $F \to G$ w T. Oczywiście F_n musi być równe $F \to G$. Wówczas ciąg $F_1, \ldots, F_{n-1}, F \to G, F, G$ jest dowodem zdania G w teorii $T \cup \{F\}$.
Wynikanie „$\Rightarrow$": Zakładamy, że $T \cup \{F\} \vdash G$, co znaczy, że G należy do zbioru konsekwencji $(T \cup \{F\})^*$. No a to znaczy, że $G \in \bigcup_n (T \cup \{F\})_n$. Dalsza część dowodu to indukcja, względem n. Musimy rozpatrzeć wiele przypadków, zależnie od tego w którym $(T \cup \{F\})_n$ znajduje się G.

I Niech $G \in (T \cup \{F\})_0$, czyli $G \in Log \cup T \cup \{F\}$. Rozpatrzymy oddzielnie dwa przypadki:

  (a) Jeśli $G \in Log \cup T$, wówczas zachodzi $T \vdash G \to (F \to G)$ (zgodnie z aksjomatem logiki). Ciąg: $G \to (F \to G), G, F \to G$ jest więc dowodem zdania $F \to G$ w oparciu o T.

  (b) Jeśli $G = F$ to też jest „dobrze" bo w każdej teorii da się udowodnić, że $F \to F$.

II Załóżmy, że jeśli $H \in (T \cup \{F\})_n$ to zachodzi $T \vdash F \to H$. Pokażemy, że z tego wynika, że jeśli $G \in (T \cup \{F\})_{n+1}$ to $T \vdash F \to G$. Wiemy na pewno, że G powstało z reguły odrywania, tak więc istnieje jakieś H_1, takie, że: $H_1 \in (T \cup \{F\})_n$ oraz $H_1 \to G \in (T \cup \{F\})_n$. Z założenia indukcyjnego mamy więc, że $T \vdash F \to H_1$ oraz $T \vdash F \to (H_1 \to G)$. Niech więc teraz ciąg $K_1, \ldots, K_n$ będzie dowodem $F \to H_1$, natomiast $J_1, \ldots, J_m$ będzie dowodem $F \to (H_1 \to G)$. Wtedy ciąg:

$$K_1, \ldots, K_n, J_1, \ldots, J_m, (F \to (H_1 \to G)) \to ((F \to H_1) \to (F \to G)),$$

$$(F \to H_1) \to (F \to G), F \to G$$

jest dowodem zdania $F \to G$ w oparciu o T, innymi słowy: $T \vdash F \to G$.

Na mocy zasady indukcji matematycznej, twierdzenie o dedukcji jest prawdziwe dla dowolnego zdania G. □

Wniosek 6.2. Jeśli $T \cup \{\neg G\} \vdash \neg F$ to $T \vdash F \to G$.

Dowód wniosku: Z tw. o dedukcji otrzymujemy, że $T \vdash \neg G \to \neg F$. Niech $F_1, \ldots, F_n$ będzie dowodem zdania $\neg G \to \neg F$ w oparciu o T. Wtedy ciąg: $F_1, \ldots, F_n, (\neg G \to \neg F) \to (F \to G), F \to G$ jest dowodem $F \to G$ w oparciu o T. □

7 Twierdzenie Lindenbauma, zdania nierozstrzygalne

7.1 Pojęcie sprzeczności i niesprzeczności

Definicja 7.1. Teoria T jest sprzeczna, jeśli istnieje taka formuła F, że zarazem $T \vdash F$ i $T \vdash \neg F$.

Fakt 7.2. *W teorii sprzecznej da się udowodnić wszystko, czyli $\forall_{G \in \mathrm{F_m}} T \vdash G$.*

Dowód: Nie będzie dowodu ultra-formalnego. Jeżeli mamy dowody F i $\neg F$, to możemy z nich zrobić dowód $F \wedge \neg F$, co jest zawsze fałszem. Potem dokładamy $(F \wedge \neg F) \to G$, która to implikacja jest twierdzeniem logiki, bo ma fałszywy poprzednik, więc jest zawsze prawdziwa. Potem stosujemy regułę odrywania i dostajemy G.

Definicja 7.3. Teoria niesprzeczna to teoria, która nie jest sprzeczna.

Fakt 7.4. *Jeśli teoria ma model, to jest ona niesprzeczna.*

Dowód: W modelu o wszystkim możemy powiedzieć, czy jest prawdą, czy nie. W teorii sprzecznej da się udowodnić wszystko, więc wszystko należy uznać za prawdę, bo do tego dowody służą. Model nie może spełniać wszystkich zdań. Zawsze mamy albo $\mathbb{M} \models \psi$, albo $\mathbb{M} \models \neg\psi$. Oba na raz nie mają sensu wobec definicji prawdziwości zdań w modelu. $\square$

Fakt 7.5. *Teoria jest niesprzeczna, jeśli każda jej skończona podteoria jest niesprzeczna. Innymi słowy: jeśli istnieje skończona podteoria sprzeczna, to cała teoria jest sprzeczna.*

Szkic dowodu, albo komentarz Sprzeczność zawsze objawia się w skończonym zbiorze aksjomatów. Chodzi o to, że jeżeli teoria T jest sprzeczna, to bierzemy dowolną formułę F i robimy dowód $F_1, F_2, \cdots, F_n$ formuły F i dowód $G_1, G_2, \cdots, G_m$ formuły $\neg F$. Zarówno ciąg F_i, jak i G_j są skończone, korzystają więc ze skończonej ilości aksjomatów z teorii T. Więc mamy skończoną podteorię $T \cap (\{F_i\} \cup \{G_j\})$, która zawiera wszystko, czego potrzebujemy, by przeprowadzić dowód zarówno F, jak i $\neg F$, jest więc sprzeczna. $\square$

Fakt 7.6. *Jeśli teoria T jest niesprzeczna, to zbiór konsekwencji T^* jest również niesprzeczny.*

Twierdzenie 7.7 (reductio ad absurdum[9])**.** $T \cup \{\neg F\}$ *jest sprzeczna wtedy i tylko wtedy, gdy* $T \vdash F$.

Dowód: Implikacja „$\Rightarrow$" : Albo T jest sprzeczna sama w sobie, wtedy na mocy definicji sprzeczności dowód $T \vdash F$ istnieje. Jeżeli T jest niesprzeczna, zaś dołożenie do niej jednego aksjomatu $\neg F$ tą niesprzeczność popsuje, to na pewno $T \vdash F$.

Implikacja „$\Leftarrow$": Albo T jest sprzeczna sama w sobie, więc powiększona o jeden aksjomat tym bardziej — wtedy implikacja jest zawsze prawdziwa, bo ma następnik prawdziwy. Jeżeli T jest niesprzeczna i istnieje dowód $T \vdash F$, to po powiększeniu teorii o dodatkowy aksjomat to tym bardziej mamy $T \cup \{\neg F\} \vdash F$, co jest jawną oznaką sprzeczności. $\square$

Przykład 7.8 (teorie sprzeczne i niesprzeczne)**.** Przykładem najprostszej teorii sprzecznej może być teoria $\{F, \neg F\}$, gdzie F to dowolna formuła.

Przykładem teorii niesprzecznej może być teoria grup. Teoria ta jest niesprzeczna, ponieważ istnieje model – istnieją przecież grupy w matematyce.

7.2 Pojęcie rozstrzygalności

Definicja 7.9. Mówimy, że formuła F jest rozstrzygalna w teorii T, jeżeli $T \vdash F$ albo $T \vdash \neg F$.

Przykład 7.10. Istnieją zarówno grupy przemienne, jak i nieprzemienne, czego teoria grup nie rozstrzyga, co opiszemy formalnie. Aksjomaty teorii grup to:

$$\forall_{x,y,z}((x + y) + z = x + (y + z))$$

$$\forall_x(x + e = e + x = x)$$

$$\forall_x \exists_z (x + z = e)$$

Istnieje model $\langle \mathbb{Z}, + \rangle$, w którym też jest prawdziwe dodatkowe zdanie:

$$\forall_{x,y}((x + y) = (y + x))$$

Istnieje jednak model $\langle S_n, \circ \rangle$, czyli permutacje zbioru n-elementowego z operacją składania w roli działania „+", w którym to dodatkowe zdanie nie jest spełnione.

[9] Z łac. *reduction ad absurdum* znaczy sprowadzenie do niedorzeczności. Twierdzenie to używane jest właśnie do konstruowania dowodów „przez zaprzecznie".

7.3 Pojęcie zupełności

Definicja 7.11 (zupełny zbiór twierdzeń)**.** Mówimy, że niesprzeczny zbiór formuł T jest zupełny, jeżeli dla każdej formuły F albo zachodzi $F \in T$ albo $\neg F \in T$.

Definicja 7.12 (zupełny zbiór aksjomatów)**.** Mówimy, że zbiór aksjomatów T jest zupełnym zbiorem aksjomatów, jeśli zbiór T^* jest zupełny.

7.4 Twierdzenie Lindenbauma

Twierdzenie 7.13 (Lindenbauma)**.** *Każdą teorię niesprzeczną T można rozszerzyć do teorii zupełnej T'.*

Dowód: Dowód będzie uproszczony tylko dla języków przeliczalnych, czyli gdy $|\mathscr{L}| = \aleph_0$. Wtedy też $|F_m| = \aleph_0$, czyli można formuły ustawić w ciąg: $F_m = \{F_n : n \in \mathbb{N}\}$. Należy przeprowadzić indukcję po tym ciągu.

(1) (a) Jeśli $T \cup \{\neg F_0\}$ jest sprzeczna, to wtedy $T \vdash F_0$, więc $T \cup \{F_0\} \subset T^*$ będzie niesprzeczny. $T \cup \{F_0\}$ oznaczmy jako ${T_0}'$.

(b) Jeśli $T \cup \{\neg F_0\}$ jest niesprzeczna, to po prostu przyjmujemy ${T_0}' := T \cup \{\neg F_0\}$.

Czyli możemy rozbudować teorię T tak, by rozstrzygała również F_0, a przy tym nadal była niesprzeczna.

(2) Możemy dokładnie tak samo, w oparciu o niesprzeczną teorię ${T_n}'$ zbudować ${T_{n+1}}'$, która będzie nadal niesprzeczna, a przy tym będzie rozstrzygała również F_{n+1}.

Przy pomocy indukcji matematycznej możemy w ten sposób rozstrzygnąć wszystkie F_i. Dostajemy teorię T' rozstrzygającą wszystkie formuły:

$$T' = \bigcup_i {T_i}'.$$

Takie T' jest niesprzeczne, dlatego, że ciąg teorii T_i jest wstępujący, tzn. $\forall_{i,j}(i < j) T_i \subset T_j$, przy czym każdy element tego ciągu jest niesprzeczny. To jest trochę tak, jakby brać granicę w nieskończoności, ale granica to pojęcie z analizy matematycznej, tutaj go nie mamy, ale suma teorio-mnogościowa nam w zupełności wystarczy.

Dowód dla języków dowolnie dużej mocy opiera się na lemacie Kuratowskiego–Zorna. □

8 Twierdzenie o pełności oraz twierdzenie o zwartości

8.1 Twierdzenie Gödla o pełności

Twierdzenie 8.1 (Gödla o pełności)**.** *Każda teoria niesprzeczna T ma model.*

Szkic dowodu: Niech T będzie teorią pewnego języka $\mathscr{L}$. Chcemy zbudować model dla teorii T. Zbudujemy go z termów języka będącego rozszerzeniem $\mathscr{L}$. Dowód bazuje na rozszerzeniu teorii T do teorii T', oraz języka $\mathscr{L}$ do języka $\mathscr{L}'$, tak aby spełniony był warunek: *dla każdej formuły F i zmiennej x istnieje stała c taka, że formuła $\exists_x F \to F(c/x)$ należy do T'*. Potrzebować będziemy więc dodatkowych stałych w języku. Budujemy język $\mathscr{L}_1$ z języka $\mathscr{L}$ dokładając tam odpowiednio dużo stałych $c(F, x)$ (dla każdej formuły i zmiennej potrzebujemy stałą - czyli stałe te zależą od formuły F i zmiennej x; będzie ich tyle ile wszystkich formuł z T i zmiennych z $\mathscr{L}$). Budujemy też teorię T_1 na bazie teorii T dorzucając właśnie odpowiednie formuły. Mamy więc:

$$T_1 = T \cup \{\exists_x F \to F(c(F, x)/x) : x \in X, F \in F_m\}.$$

Należałoby udowodnić, że T_1 jest również niesprzeczna - dowód pomijamy.

Powyższe postępwanie możemy powtarzać w nieskończoność budując kolejne teorie T_n na bazie teorii T_{n-1} oraz języki $\mathscr{L}_n$ na bazie $\mathscr{L}_{n-1}$. Ostatecznie, przyjmując, że $L = L_0$ oraz $T = T_0$ mamy:

$$T' = \bigcup_n T_n, \quad L' = \bigcup_n L_n.$$

Teorię T' rozszerzamy do teorii zupełnej, która rozstrzyga wszystkie formuły (możemy to zrobić na mocy twierdzenia Lindenbauma). Dla takiej teorii T' zbudujemy model. Model ten będziemy budować z termów. Aby to zrobić, zdefiniujemy relację równoważności termów. Relacja określimy bardzo intuicyjnie:

$$t_1 \sim t_2 \quad \text{wtedy i tylko wtedy gdy forumła: } t_1 = t_2 \in T'.$$

Relacja $\sim$ mówi więc, że dwa termy są w relacji równoważności, jeśli w teorii T', rzeczywiście jest formuła mówiąc, że te dwa termy są równe (dość oczywiste, prawda?). Ze względu na to, że T' jest zupełna, to dla każdych dwóch termów t_1 i t_2 w T' jest zdanie $t_1 = t_2$ lub $t_1 \neq t_2$, więc relacja jest dobrze zdefiniowana.

Nasz model $\mathbb{A}$ będzie oparty na zbiorze postaci:

$$\mathcal{A} = \{[t]_\sim : t \in T_m\}.$$

Czyli zbiór $\mathcal{A}$ jest zbiorem wszystkich klas abstrakcji relacji $\sim$. Musimy jeszcze, aby dokładnie zdefiniować model $\mathbb{A}$ podać definicje relacji, funkcji i stałych w zbiorze $\mathcal{A}$ oraz definicję podstawienia:

- Dla każdego symbolu relacyjnego r z języka $\mathscr{L}'$, definiujemy relację $r^{\mathbb{A}}$:

  $$r^{\mathbb{A}}([t_1], \ldots, [t_n]) \text{ zachodzi, wtedy i tylko wtedy, gdy } r(t_1, \ldots, t_n) \in T'.$$

- Dla każdego symbolu funkcyjnego f z języka $\mathscr{L}'$, definiujemy funkcję $f^{\mathbb{A}}$:

  $$f^{\mathbb{A}}([t_1], \ldots, [t_n]) = [f(t_1), \ldots, f(t_n)].$$

- Dla każdego symbolu stałej c z języka $\mathscr{L}'$, definiujemy stałą $c^{\mathbb{A}}$:

  $$c^{\mathbb{A}} = [c].$$

- Definiujemy też podstawienie $p : X \to \mathcal{A}$:

  $$p(x) = [x].$$

Model $\langle \mathbb{A}, p \rangle$ jest modelem teorii T'. Jest on również modelem teorii T, co należałoby jeszcze pokazać (dowód pomijamy). $\square$

Uwaga 8.2. Model $\mathbb{A}$ z dowodu jest mocy co najwyżej równej mocy języka. Jeśli więc język $\mathscr{L}$ jest przeliczalny, to również model jest przeliczalny.

8.2 Wnioski z twierdzenia Gödla o pełności

Wniosek 8.3. Jeśli ZFC (teoria mnogości) jest niesprzeczna, to ma model przeliczalny.

Wniosek 8.4. Niech $T = \{F : \mathbb{R} \models F\}$ – zbiór wszystkich zdań spełnionych w zbiorze liczb rzeczywistych. Istnieje jakiś model $\mathbb{A}$ dla teorii T który jest przeliczalny. Innymi słowy istnieje przeliczalny zbiór który spełnia wszystkie te same zdania co zbiór liczb rzeczywistych.

Wniosek 8.5. Jeśli zdanie F jest spełnione w każdym modelu teorii T to da się je udowodnić w oparciu o teorię T.

Dowód wniosku: Załóżmy przeciwnie, że $\neg(T \vdash F)$. Wówczas teoria $T \cup \{\neg F\}$ jest niesprzeczna. No ale wtedy istnieje model dla $T \cup \{\neg F\}$. Czyli istnieje model teorii T w którym nie zachodzi F, co jest sprzeczne z założeniem, że F jest spełnione w każdym modelu teorii T. $\square$

8.3 Twierdzenie Gödla o zwartości

Twierdzenie 8.6 (Gödla o zwartości)**.** *Jeśli każda skończona podteoria teorii T ma model, to również cała teoria T ma model.*

Dowód: Jeśli każda skończona podteoria ma model, to znaczy że jest niesprzeczna, w związku z czym cała teoria T jest niesprzeczna. Zgodnie z twierdzeniem o pełności, teoria T musi więc mieć model. □

9 Arytmetyka Peano

9.1 Aksjomaty arytmetyki Peano

(1)
$$\forall_x \forall_y x + y = y + x$$

(2)
$$\forall_x \forall_y x \cdot y = y \cdot x$$

(3)
$$\forall_x \forall_y \forall_z (x + y) + z = x + (y + z)$$

(4)
$$\forall_x \forall_y \forall_z (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

(5)
$$\forall_x \forall_y \forall_z x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

(6)
$$\forall_x x + \Delta_0 = x$$

(7)
$$\forall_x x \cdot \Delta_1 = x$$

(8)
$$\forall_x \forall_y \forall_z x + y = x + z \to y = z$$

(9) Każda liczba różna od zera jest następnikiem:
$$\forall_x x \neq \Delta_0 \to \exists_y y + \Delta_1 = x.$$

(10) Zasada indukcji matematycznej. Podamy tu schemat aksjomatu opisujący nieskończenie wiele aksjomatów – oddzielny dla każdej formuły. Niech F będzie formułą a x zmienną:
$$(F(\Delta_0/x) \wedge \forall_x (F(x) \to F(x + \Delta_1/x))) \to$$
$$\to \forall_x F(x)$$

9.2 Standardowy model arytmetyki Peano

Standardowym modelem arytmetyki Peano jest $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$, przy czym oczywiście liczba 0 odpowiada symbolowi Δ_0, liczba 1 symbolowi Δ_1, standardowe działanie dodawania symbolowi $+$, oraz standardowe działanie mnożenia symbolowi $\cdot$. Istnieją jednak niestandardowe modele arytmetyki Peano.

9.3 Niestandardowe modele arytmetyki Peano

Podamy konstrukcję niestandardowego modelu arytmetyki Peano. Niech symbolowi Δ_0 odpowiada liczba 0, symbolowi Δ_1 liczba 1. A symbolom Δ_{n+1} odpowiednio $\Delta_n + \Delta_1$.

Niech F_n to będą formuły postaci: $\exists_y x = \Delta_n + y$, co w skrócie można by zapisać $x \geqslant \Delta_n$, gdybyśmy mieli relację większy równy (ale nie mamy). Niech T będzie zbiorem wszystkich zdań które są spełnione w arytmetyce Peano (w liczbach $\mathbb{N}$):

$$T = \{F : \mathbb{N} \models F \wedge F \text{ jest zdaniem}\}.$$

Niech teoria T' będzie postaci:

$$T' = T \cup \{F_n : n \in \mathbb{N}\}.$$

Niech T_0 będzie skończoną podteorią T'. Wówczas na pewno T_0 jest postaci:

$$T_0 = (T_0 \cap T) \cup \{F_{n_1}, \ldots, F_{n_k}\}.$$

Modelem dla teorii T_0 są liczby naturalne z podstawieniem p takim, że element $p(x)$ jest większy od liczb n_i dla każdego i od 1 do k. W związku z tym, że T_0 ma model, również T' musi mieć model. Niech tym modelem będzie $\langle \mathbb{A}, p\rangle$. Zauważmy jednak, że w tym modelu element $p(x)$ musi być większy od wszystkich elementów Δ_i tego modelu, bo dla każdego i $\mathbb{A} \models F_i$. Modelem $\mathbb{A}$ nie może więc być zbiór liczb naturalnych, gdyż tam nie ma takiego elementu. Taki model jest niestandardowym modelem arytmetyki Peano. Spełnia te same zdania co model $\langle \mathbb{N}, +, \cdot, 0, 1\rangle$. Zauważmy też, że na mocy aksjomatu 9 ten dodatkowy element ma swoje następniki, poprzedniki pewnie też. Pojawia się więc dużo więcej dodatkowych elementów, niż tylko ten jeden.

Uwaga 9.1. Niestandardowy model arytmetyki Peano, którego konstrukcje podano wyżej, może być przeliczalny.

9.4 Zupełność i definiowalność a arytmetyka Peano i ZFC

Aksjomaty matematyki, które określamy często przez ZFC stanowią niezupełny zbiór aksjomatów, gdyż istnieje chociażby hipoteza continuum CH[10], która jest niezależna od aksjomatów. Nie jest to jednak jedyne niezależne zdanie, tzn. nie da się tak uzupełnić ZFC aby był to zbiór zupełny. [11] Podobnie jest z arytmetyką Peano. Co więcej zachodzą poniższe fakty (podajemy je bez dowodów).

Twierdzenie 9.2 (Gödla)**.** *Każde „definiowalne” rozszerzenie arytmetyki Peano lub ZFC jest niezupełne.*

Twierdzenie 9.3 (Tarskiego o niedefiniowalności prawdy)**.** *Niech T będzie rozszerzeniem arytmetyki Peano (lub ZFC) oraz $\mathbb{A}$ niech będzie modelem teorii T. Wówczas zbiór $\{F : \mathbb{A} \models F\}$ jest niedefiniowalny w $\mathbb{A}$.*

Twierdzenie 9.4 (Gödla)**.** *W ZFC nie można udowodnić, że ZFC jest niesprzeczny o ile jest niesprzeczny.*

[10] Hipoteza ta mówi, że nie ma żadnej liczby kardynalnej pomiędzy $\aleph_0$ a $\mathfrak{C}$. Przyjęcie tej hipotezy lub jej zaprzeczenia jako aksjomatu nie powoduje żadnej sprzeczności, czyli z już przyjętych założeń nic na ten temat nie wiadomo.

[11] Uwaga: Twierdzenie Lindenbauma mówi, że takie uzupełnienie istnieje, ale absolutnie nie mówi nam nic o tym, jak je zdefiniować.

10 Twierdzenia Skolema–Löwenheima i inne twierdzenia o mocach modeli

Twierdzenie 10.1. *Jeśli teoria T ma modele skończone, dowolnie duże, to ma model nieskończony.*

Dowód: Niech zdania F_n będą zdaniami *„istnieje co najmniej n różnych elementów”*[12]. Niech $T' = T \cup \{F_n : n \in \mathbb{N}\}$. Każda skończona podteoria T' ma model, ponieważ wśród zdań z tej podteorii da się znaleźć F_i gdzie i jest największe, więc wystarczy wziąć model teorii T który ma przynajmniej i elementów (a zgodnie z założeniami twierdzenia taki model istnieje). Skoro każda skończona podteoria T' ma model, to na mocy tw. o zwartości, teoria T' ma model. Model ten musi być nieskończony. Co więcej jest to również model teorii T. □

Twierdzenie 10.2 (Skolema–Löwenheima)**.** *Jeśli teoria T ma model nieskończony, to ma również model dowolnej mocy większej równej od mocy języka.*

Dowód: Pokażemy jak skonstruować model dowolnej mocy większej równej mocy języka. Niech zbiór I będzie zbiorem szukanej mocy. Zdefiniujmy stałe $\{C_i : i \in I\}$ i dodajmy je do języka. Niech $T = \{F : \mathbb{A} \models F\}$. Stwórzmy teorię $T' = T \cup \{\neg(C_i = C_j) : i, j \in I \wedge i \neq j\}$. Teoria T' ma model, bo każda skończona podteoria T' ma model tym modelem jest $\mathbb{A}$. A skoro T' ma model to w modelu tym musi być co najmniej tyle stałych ile moc I. Model teorii T' jest również modelem teorii T. □

Wniosek 10.3. Jeśli istnieje model nieskończony, to istnieją przynajmniej dwa modele nieizomorficzne.

Przykład 10.4. Niech $T = \{F : \mathbb{R} \models F\}$ – teoria składająca się ze wszystkich zdań spełnionych w zbiorze liczb rzeczywistych. Zgodnie z twierdzeniem Skolema–Löwenheima istnieje na przykład model mocy $2^{\mathfrak{c}}$ dla takiej teorii T. Innymi słowy istnieje zbiór mocy $2^{\mathfrak{c}}$ o własnościach liczb rzeczywistych.

Uwaga 10.5. Z dowodu tw. Gödla o pełności, wynika również fakt na temat mocy modelu. Model który się tam pojawia jest co najwyżej mocy języka. Ma to duże znaczenie, gdyż zazwyczaj używamy przeliczalnych języków – istnieją więc wtedy modele przeliczalne. (Więcej znajdziesz w odpowiedniej uwadze po twierdzeniu o pełności.)

A Przykłady zadań

Zadanie 1. Pokazać, że formuła:

$$\exists_x \forall_y \exists_z [F(y,z) \to F(x,z)] \to [F(x,x) \to F(y,x)]$$

a) jest spełniona w każdym modelu skończonym,

b) nie jest tautologią – wskazać model nieskończony, w którym nie jest spełniona.

Zadanie 2. Niech w języku będą dostępna dwa symbole funkcyjne $\{+, \cdot\}$ oraz dwie stałe $\{0, 1\}$.

a) Podaj aksjomatykę ciał o charakterystyce[13] 0.

[12] Można podać konstrukcję takiego zdania. Na przykład zdanie F_3 ma postać: $\exists_x \exists_y \exists_z (x \neq y) \wedge (y \neq z) \wedge (x \neq z)$. Oczywiście dla dużych n zdania te są dość długie.

[13] Charakterystyka ciała $\mathbb{K}$ oznaczana symbolicznie $\chi(\mathbb{K})$ to najmniejsza liczba „jedynek” z tego ciała, która po „dodaniu” da w tym ciele „zero”. Jeśli przez „dodawanie jedynek” nie da się osiągnąć zera, przyjmujemy, że charakterystyka równa się zero.

b) Udowodnij, iż teoria ta (z punktu poprzedniego) nie jest skończenie aksjomatyzowana.

c) Pokazać, że jeśli φ jest zdaniem tego języka, to: jeśli zdanie to jest spełnione w każdym ciele $\mathbb{K}$ o charakterystyce $\chi(\mathbb{K}) = 0$, to istnieje taka stała k, iż zdanie to jest spełnione we wszystkich ciałach o charakterystyce większej od k.

Zadanie 3. Mając dowody $F \to G$ oraz $G \to H$, dowieść $F \to H$, gdzie F, G, H to pewne formuły.

Zadanie 4. Dane są struktury:

1. $\langle \mathbb{Z}, +, 0 \rangle$, $\langle \mathbb{R}, +, 0 \rangle$.
2. $\langle \mathbb{Z}, +, 0 \rangle$, $\langle \mathbb{Q}, +, 0 \rangle$.

Rozstrzygnąć czy struktury te są:

a) izomorficzne (jeśli tak to podań izomorfizm, jeśli nie, to wykazać, ze go nie ma),

b) mają te same zbiory zdań w nich prawdziwych (jeśli tak, to to wykazać, jeśli nie, to podać zdanie rozróżniające).

Rozwiązanie: Zaczniemy od pokazania, że w $\langle \mathbb{Z}, +, 0 \rangle$ nie są spełnione te same zdania co w $\langle \mathbb{R}, +, 0 \rangle$ i $\langle \mathbb{Q}, +, 0 \rangle$. Rozważmy bowiem zdanie:

$$\forall_x \exists_y y + y = x,$$

co słownie można by zapisać: „dla każdej liczby istnieje jej połowa”, lub po prostu „dzielnie przez dwa jest wykonalne zawsze”. Oczywiście w zbiorze liczb całkowitych tak nie jest, bo na przykład dla $x = 3$ nie istnieje żaden y należący do $\mathbb{Z}$, który spełniałby $y+y = x$. Czyli punkt *b*) mamy w ten sposób rozwiązany. Okazuje się jednak, że to wystarcza również na dowód, że struktury te nie mogą być izomorficzne, bo gdyby były to, zgodnie z udowodnionym w tym opracowaniu twierdzeniem, musiałby być w nich spełnione te same zdania.

Dla zestawu pierwszego można podać również inne uzasadnienie, że struktury nie są izomorficzne. Wiadomo bowiem, że zbiory $\mathbb{Z}$ oraz $\mathbb{R}$ nie są równoliczne, czyli nie istnieje żadna bijekcja $\mathbb{Z} \to \mathbb{R}$, a co za tym idzie nie może być mowy o izomorfizmie (który musi być bijekcją w myśl definicji).

Zadanie 5. Wykazać niezależność podanych zdań od aksjomatów teorii porządków częściowych (TPC). Zdania do rozstrzygnięcia to:

a) $\exists_x \forall_y p(x, y)$

b) $\forall_x \exists_y p(x, y) \land \neg p(y, x)$

Rozwiązanie: Dla każdego ze zdań wystarczy podać dwa modele TPC: jeden w którym dane zdanie jest spełnione, a drugi w którym nie jest spełnione.

Dla punktu *a*) mogą to być $\langle \mathbb{N}, \leqslant \rangle$, w którym zdanie jest prawdziwe (istnieje jeden x taki, że wszystkie inne elementa są od niego mniejsze bądź równe - jest to oczywiście 0), oraz $\langle \mathbb{R}, \leqslant \rangle$, w którym to zdanie jest fałszywe (bo nie istnieje element najmniejszy).

Dla punktu *b*) modelem w którym zdanie jest prawdziwe może być również $\langle \mathbb{N}, \leqslant \rangle$, ponieważ dla każdej liczby naturalnej, istnieje liczba która jest od niej większa i która zarazem nie jest mniejsza równa od niej. Modelem w którym zdanie to nie jest spełnione może być za to model $\langle P(\mathbb{N}), \subseteq \rangle$, czyli zbiór wszystkich podzbiorów liczb naturalnych z relacją bycia podzbiorem. Zauważmy bowiem, że dla $x = \mathbb{N}$, który jest oczywiście elementem $P(\mathbb{N})$, nie istnieje taki zbiór który jednoczenie zawierałby się w $P(\mathbb{N})$, zawierał całe $\mathbb{N}$ i sam nie zawierał się w $\mathbb{N}$.

W obu przypadkach widzimy więc, że zdania są niezależne od aksjomatów TPC. W niektórych modelach są spełnione, w innych nie, czyli zależą od doboru modelu, a nie od teorii jako takiej.

B Klasyczny rachunek zdań

W tym dodatku zawarto aksjomaty klasycznego rachunku oraz przykłady zadań wraz z rozwiązaniami.

B.1 Oznaczenia i terminologia

W klasycznym rachunku zdań wszystkie zmienne są wolne, nie występuje bowiem pojęcie kwantyfikatora. Stąd nie ma rozgraniczenia na zdania i formuły. Teoretycznie, gdybyśmy chcieli trzymać się poprzednich definicji (z rachunku predykatów) musielibyśmy mówić tylko o formułach klasycznego rachunku zdań, jednak przyjęło się, że można o niech również mówić zdania.

Definicje zbiorów zupełnych, niesprzecznych, dowodu, spełniania itp., są niemależe identyczne jak w rachunku predykatów, z tą różnicą, że formuły są tutaj dużo prostszej postaci (nie ma predykatów ani kwantyfikatorów, a jedynie spójniki logiczne). Intuicyjny sens tych wszystkich pojęć pozostaje jednak niezmieniony, tak więc pomijamy wszelkie definicje.

B.2 Aksjomatyka klasycznego rachunku zdań

Możliwe są różne układy systemu aksjomatów. Prezentujemy tutaj jeden z możliwych, nie koniecznie najlepszy, jednak na pewno poprawny. Poniższe zapisy to schematy aksjomatów, których jest nieskończenie wiele. Symbole F, G, H oznaczają dowolne formuły klasycznego rachunku zdań.

1. Reguła symplifikacji:
$$F \to (G \to F)$$

2. Reguła Fregego:
$$[F \to (G \to H)] \to [(F \to G) \to (F \to H)]$$

3. Reguła Claviusa:
$$(\neg F \to F) \to F$$

4. Reguła Dunsa Scotusa:
$$\neg F \to (F \to G)$$

Wszystkie tautologie klasycznego rachunku zdań, można udowodnić w oparciu o ten zestaw aksjomatów i znaną już z rachunku predykatów, regułę odrywania.

B.3 Przykłady zadań

Zadanie 6. Niech zbiór A zawiera wszystkie te zdania klasycznego rachunku zdań, które są prawdziwe przy pewnym, ustalonym, wartościowaniu (tj. podstawieniu) w. Niech też zbiór B zawiera wszystkie te zdania klasycznego rachunku zdań, które przy tym samym podstawieniu są fałszywe. Sprawdzić czy zbiory A i B są zupełne i niesprzeczne.

Rozwiązanie: Zauważmy najpierw, że zbiory A i B na pewno są zupełne. Załóżmy bowiem, że tak nie jest, tzn. na przykład, że zbiór A jest niezupełny. Znaczyło by to, że istnieje jakaś formuła φ klasycznego rachunku zdań, która nie należy do A, oraz $\neg\varphi$ nie należy do tegoż zbioru. Zauważmy jednak, że przy podstawieniu w albo φ jest prawidziwa, albo $\neg\varphi$ jest prawidziwa, wobec czego albo pierwsza, albo druga musi należeć do A. Dowód, że B jest zupełny, jest identyczny.

Zastanówmy się teraz, czy zbiory te są niesprzeczne. Zaczniemy od pokazania, że zbiór B jest sprzeczny. Zauważmy, że do zbioru B należą w szczególności również, wszystkie zaprzecznia tautologii, czyli formuły które są fałszywe przy każdym podstawieniu. No ale z drugiej strony tautologie są uniwersalne. Tak więc, jeśli φ jest tautologią klasycznego rachunku zdań, to na pewno $B \vdash \varphi$ oraz $B \vdash \neg\varphi$. No a to dokładnie znaczy, że zbiór B jest sprzeczny. Zajmijmy się więc zbiorem A.

Zbiór A zawiera wszystkie formuły, które są prawdziwe przy pewnym podstawieniu. Udowodnimy indukcyjnie twierdzenie, że jeśli jakaś formuła φ daje się udowodnić w A, to na pewno $\neg\varphi$ nie da się udowodnić w A, a dokładniej pokażemy, że nie istnieje dowód formuły $\neg\varphi$ jeśli istnieje dowód φ w oparciu o A. Na początku zauważmy, że jeśli φ jest prawdziwa przy podstawieniu w to należy po prostu do A, więc sama jest swoim dowodem. Jeśli φ jest fałszywa przy podstawieniu w, to za to $\neg\varphi$ jest prawidziwa i możemy „odwrócić" sytuację. Zakładamy więc, że φ jest prawdziwa przy podstawieniu w (co czynimy bez utraty ogólności). Jeśli istniałby dowód formuły $\neg\varphi$ w oparciu o A to przynajmniej raz musiałaby zostać użyta reguła odrywania. Indukcję przeprowadzimy więc po liczbie użyć reguły odrywania w dowodzie i pokażemy że można używać jej nieskończenie wiele razy, ale to i tak nie pomoże. Pierwszy krok indukcji mamy już właściwie za sobą, bo wiemy, że dla zera jest dobrze. Możemy jednak jeszcze pokazać, że jak zastosujemy tylko raz regułę odrywania, to nic to nie pomoże. Gdyby $\neg\varphi$ dało się uzyskać stosując raz regułę odrywania, to musiałaby istnieć jakaś formuła F, taka, że zarówno F jaki i $F \to \neg\varphi$ dają się wywieść bez stosowania reguły odrywania. No ale to znaczy, że zarówno F jak i $F \to \neg\varphi$ musiałby należeć do A, co jest niemożliwe (gdyby $F \to \neg\varphi$ było prawdziwe przy podstawieniu w, to F musiałoby być fałszywe, więc nie mogłoby należeć do A i odwrotnie, gdyby A należało to, ta druga formuła nie mogłaby należeć). Załóżmy więc, że przy użyciu n razy reguły odrywania nie da się otrzymać $\neg\varphi$ z A. Pokażemy że reguła odrywania zastosowana jeszcze raz nic nie pomoże. Załóżmy, że budujemy dowód $\neg\varphi$ i użyliśmy w nim już n razy regułę odrywania. Chcielibyśmy użyć ją ponownie. W dowodzie tym musiałaby istnieć formuła F oraz $F \to \neg\varphi$, które albo należą do F albo powstały z reguły odrywania zastosowanej co najwyżej n razy (ale razem – tzn. łączna liczba reguł odrywania musi wynosić n – co szczerze mówić nie wiele zmienia). W związku z tym, zdania F oraz $F \to \neg\varphi$ nie mogą być (zgodnie z założeniem indukcyjnym) fałszywe przy podstawieniu w. Nie jest to jednak możliwe, bo przecież $\neg\varphi$ jest przy podstawianiu w fałszywe, czyli gdyby F było prawdziwe, bo $F \to \neg\varphi$ byłoby fałszywe i na odwrót. Czyli dwie formuły F oraz $F \to \neg\varphi$ nie mogą istnieć. Czyli zastosowanie reguły odrywania po raz $n+1$ nic nie pomoże. Tak więc na mocy zasady indukcji matematycznej, możemy regułę odrywania stosować bez końca, a i tak nie pomoże nam to w uzyskaniu formuły $\neg\varphi$. Co za tym idzie zbiór A jest niesprzeczny. Co ciekawe, w ten sposób pokazaliśmy też, że ów zbiór A jest równy A^*, tzn. nie da się z niego wywieść nic więcej poza to co sam zawiera.