6. Rachunek predykatów z symbolami funkcyjnymi

Rozważamy teraz język KRP, w którym występują symbole funkcyjne. W najbardziej ogólnym przypadku, mamy przeliczalną liczbę symboli funkcyjnych n-argumentowych dla każdej liczby naturalnej n.

Zakładamy też, że język ten zawiera również predykat identyczności, scharakteryzowany w podrozdziale III.5. W pewnych ujęciach, wygodne jest także używanie *operatora deskrypcyjnego* $\iota(x)$; wyrażenie $\iota(x)A(x)$ (gdzie $A(x)$ jest formułą języka KRP o zmiennej wolnej x) czytamy: *jedyne* x *takie, że* $A(x)$. Operator ten podobny jest składniowo do kwantyfikatorów. W niniejszym ujęciu nie będzie nam on potrzebny.

Jeśli $t, t_1, \ldots, t_n$ są termami, a F jest n-argumentowym symbolem funkcyjnym, to wyrażenie postaci:

$$F(t_1, \ldots, t_n) = t$$

czytamy *wartość funkcji (oznaczanej symbolem)* F *dla argumentów (oznaczanych symbolami)* $t_1, \ldots, t_n$ *równa jest (obiektowi oznaczanemu przez term)* t.

6.1. Definicje

Funkcje należą do niezbędnika każdego matematyka. Również we wszelkich naukach empirycznych, w których stosuje się opisy *ilościowe*, niezbędne jest używanie funkcji. Wreszcie, także w empirycznych naukach Humanistycznych posługiwanie się funkcjami jest codziennością.

Pojęcie funkcji

Nie będziemy przytaczać tu wszystkich definicji związanych z prawidłowym operowaniem pojęciem funkcji. Słuchaczki niniejszego kursu wysłuchały kursu *Wstęp do matematyki*, gdzie podano stosowną terminologię, definicje oraz twierdzenia. Przypomnijmy jedynie podstawową definicję. Jeśli $f \subseteq X^n \times Y$ jest relacją, to mówimy, że f jest n-argumentową funkcją ze zbioru X^n w zbiór Y i zapisujemy ten fakt jako $f : X^n \to Y$, gdy:

$$\forall x_1 \in X \ldots \forall x_n \in X \exists y \in Y \quad (x_1, \ldots, x_n, y) \in f$$

$$\forall x_1 \in X \ldots \forall x_n \in X \forall y_1 \in Y \forall y_2 \in Y \quad (((x_1, \ldots, x_n, y_1) \in f \wedge (x_1, \ldots, x_n, y_2) \in f) \to y_1 = y_2).$$

W zgodzie z powszechnie przyjętymi konwencjami, gdy $f : X^n \to Y$ oraz $(x_1, \ldots, x_n, y) \in f$, to piszemy $f(x_1, \ldots, x_n) = y$ i mówimy, że y jest wartością funkcji f dla argumentów $x_1, \ldots, x_n$.

Pewne dalsze definicje niezbędne dla rozumienia wykładu przypomniane zostaną w trakcie omawiania kolejnych przykładów.

Pojęcie termu

Przypomnijmy, że definicja *termu* języka KRP jest indukcyjna:

(i) wszystkie zmienne indywiduowe x_n oraz wszystkie stałe indywiduowe a_k są termami;

(ii) jeśli $t_1, \ldots, t_{n_j}$ są dowolnymi termami, a $f_j^{n_j}$ jest symbolem funkcyjnym n_j-argumentowym, to wyrażenie $f_j^{n_j}(t_1, \ldots, t_{n_j})$ jest termem;

(iii) nie ma innych termów (języka KRP) prócz zmiennych indywiduowych i stałych indywiduowych oraz tych termów, które można skonstruować wedle reguły (ii).

Reguły MDS dla kwantyfikatorów w języku KRP z symbolami funkcyjnymi

Reguły MDS dla formuł z kwantyfikatorami różnią się od tych sformułowanych w III.1.1. jedynie tym, że zamiast o stałych indywiduowych mówimy w nich o termach.

Przypominamy, że term t jest *podstawialny* za zmienną x w formule A, gdy po zastąpieniu wszystkich wolnych wystąpień x w A przez t żadna zmienna, która była wolna w t nie stanie się związana.

Poniższe reguły określają, jaką formułę należy dopisać do tworzonej gałęzi, jeśli na gałęzi tej wystąpiła formuła danej postaci. Przypominamy, że $A(t/x)$ oznacza formułę otrzymaną z formuły o zmiennej wolnej x przez zastąpienie wszystkich wolnych wystąpień tej zmiennej termem t.

Reguły rozkładu formuł dotyczące kwantyfikatorów mają postać następującą:

- ***Reguła dla formuł generalnie skwantyfikowanych:***

$$R(\forall) \qquad \begin{array}{c} \forall x\, A(x) \\ | \\ A(t/x) \end{array}$$

dla każdego termu t podstawialnego za x w $A(x)$.

- ***Reguła dla formuł egzystencjalnie skwantyfikowanych:***

$$R(\exists) \qquad \begin{array}{c} \exists x\, A(x) \\ | \\ A(t/x) \end{array}$$

dla nowego termu t podstawialnego za x w $A(x)$ nie występującego dotąd na rozważanej gałęzi.

- ***Reguła dla negacji formuł generalnie skwantyfikowanych:***

$$R(\neg\forall) \qquad \begin{array}{c} \neg\forall x\, A(x) \\ | \\ \neg A(t/x) \end{array}$$

dla nowego termu t podstawialnego za x w $A(x)$ nie występującego dotąd na rozważanej gałęzi.

- ***Reguła dla negacji formuł egzystencjalnie skwantyfikowanych:***

$$R(\neg\exists) \qquad \begin{array}{c} \neg\exists x\, A(x) \\ | \\ \neg A(t/x) \end{array}$$

dla każdego termu t podstawialnego za x w $A(x)$.

Uwaga o notacji. W tym podrozdziale drzewa semantyczne zapisywać będziemy również w postaci ***ciągów***. Wiadomo, że elementy drzewa nierozwojowego (rzędu skończonego) można w sposób jednoznaczny ponumerować tak, aby dało się je ustawić w ciąg.[1] Wybierzemy jedną z takich możliwości. Opisana ona będzie w sposób nieformalny, w trakcie omawiania kolejnych przykładów.

---

[1] O różnych własnościach drzew, a w szczególności, o ich kodowaniach, piszemy w rozdziale I skryptu.

6.2. Przykłady

Przejdźmy do prezentacji przykładów ilustrujących działanie metody drzew semantycznych w KRP z symbolami funkcyjnymi. Będą one dotyczyły nie tylko takich samych zagadnień, jak rozpatrywane w podrozdziałach III.2.–III.5.: semantycznej niesprzeczności, tautologiczności oraz wynikania logicznego, lecz również pewnych nowych problemów. W omawianych przykładach odwoływać się będziemy do często rozważanych w matematyce struktur. Czytelniczki nie powinny być jednak z tego powodu przejęte grozą — wprowadzane pojęcia opatrzone będą nie tylko definicjami, lecz również komentarzami.

PRZYKŁAD III.6.1: PIERWSZY — TABLICZKI DODAWANIA I MNOŻENIA.

Dodawania i mnożenia liczb naturalnych uczysz się w wieku kilku lat. Chociaż, gdy się chwilę zastanowisz, to być może dopadnie cię refleksja: skąd właściwie wiesz, jaki jest wynik wykonywania tych operacji (tj. dodawania i mnożenia) na liczbach naturalnych? Prawdopodobnie, nauczono cię tabliczek dodawania i mnożenia podobnie jak naucza się wierszyków, „na pamięć". Stosowano przy tym różne heurystyki; np. rysunki jabłuszek, kotków, monet, itp. No i teraz umiesz dodawać i mnożyć. Czyżby jednak ta ***wiedza***[2] miała uzasadnienie wyłącznie w owych dogmatycznych rysunkach? To temat na zajęcia z filozofii matematyki lub, ogólniej, z filozofii nauki. Te zajęcia dotyczą tylko elementarza logicznego, a więc nie znajdziesz w nich wyczerpującej odpowiedzi na tego typu pytania metafizyczne. Ograniczymy się do stwierdzenia, że arytmetykę można zbudować na bazie aksjomatycznej, jako teorię pierwszego rzędu (a więc teorię w języku KRP, z predykatem identyczności oraz symbolami funkcyjnymi).

Tabliczki dodawania i mnożenia zbudować można w ARYTMETYCE ROBINSONA. Jest to system aksjomatyczny w języku KRP z identycznością oraz następującymi symbolami funkcyjnymi:

σ — jednoargumentowy symbol funkcyjny; wyrażenie $\sigma(t)$, gdzie t jest dowolnym termem, czytamy: *następnik* t;

$\oplus$ — dwuargumentowy symbol funkcyjny; wyrażenie $\oplus(t_1, t_2)$, gdzie t_1, t_2 są dowolnymi termami, czytamy: *suma* t_1 i t_2;

$\otimes$ — dwuargumentowy symbol funkcyjny; wyrażenie $\otimes(t_1, t_2)$, gdzie t_1, t_2 są dowolnymi termami, czytamy: *iloczyn* t_1 i t_2.

Nadto, w języku Arytmetyki Robinsona używamy stałej indywiduowej $\bigcirc$. Jest to symbol, który czytamy: *zero*.

AKSJOMATY.

Aksjomaty dotyczące jedynie predykatu identyczności:

$\forall x \ (x = x)$

$\forall x \forall y \ (x = y \rightarrow y = x)$

$\forall x \forall y \forall z \ ((x = y \wedge y = z) \rightarrow x = z)$.

Uwaga. Ta grupa aksjomatów występuje we wszystkich teoriach, w których używamy predykatu identyczności. Nie będziemy jej powtarzać w następnych przykładach, należy jednak pamiętać, że zawsze z nich korzystamy. Nadto, warto też pamiętać, że ani te aksjomaty, ani inne, w których występuje symbol = identyczności nie gwarantują, że denotacja tego symbolu jest „prawdziwą" równością =. Dla pełnej poprawności, powinniśmy używać innego symbolu dla predykatu identyczności w języku przedmiotowym (np.: $\doteq$), a innego dla relacji identyczności = (por. uwagi na początku podrozdziału III.5.). Nie robimy tego, ufając, iż Czytelniczki są już oswojone z różnicą między językiem przedmiotowym i metajęzykiem i że życzliwie, ze zrozumieniem tolerują tego typu drobne świństewka notacyjne.

---

[2] Wiedza = uzasadnione, prawdziwe przekonanie.

Aksjomaty identyczności dla symboli $\bigcirc$, σ, $\oplus$ oraz $\otimes$:

$\forall x \forall y\ (x = y \rightarrow \sigma(x) = \sigma(y))$

$\forall x \forall y \forall z\ (x = y \rightarrow \oplus(x, z) = \oplus(y, z))$

$\forall x \forall y \forall z\ (x = y \rightarrow \oplus(z, x) = \oplus(z, y))$

$\forall x \forall y \forall z\ (x = y \rightarrow \otimes(x, z) = \otimes(y, z))$

$\forall x \forall y \forall z\ (x = y \rightarrow \otimes(z, x) = \otimes(z, y))$.

Aksjomaty specyficzne systemu Arytmetyki Robinsona:

A_1: $\forall x \forall y\ (x \neq y \rightarrow \sigma(x) \neq \sigma(y))$

A_2: $\forall x\ (\bigcirc \neq \sigma(x))$

A_3: $\forall x\ (x \neq \bigcirc \rightarrow \exists y\ (x = \sigma(y)))$

A_4: $\forall x\ (\oplus(x, \bigcirc) = x)$

A_5: $\forall x \forall y\ (\oplus(x, \sigma(y)) = \sigma(\oplus(x, y)))$

A_6: $\forall x\ (\otimes(x, \bigcirc) = \bigcirc)$

A_7: $\forall x \forall y\ (\otimes(x, \sigma(y)) = \oplus(\otimes(x, y), x))$.

Modelem zamierzonym dla tych aksjomatów jest struktura, której uniwersum jest zbiór wszystkich[3] liczb naturalnych, a denotacjami poszczególnych terminów pozalogicznych są:

- symbolu $\bigcirc$ — liczba zero;
- symbolu σ — operacja następnika;
- symbolu $\oplus$ — operacja dodawania;
- symbolu $\otimes$ — operacja mnożenia.

Co „mówią” poszczególne aksjomaty (o owej interpretacji zamierzonej)? Oto możliwe odczyty Humanistyczne:

A_1: Różne liczby naturalne mają różne następniki.

A_2: Zero nie jest następnikiem żadnej liczby.

A_3: Każda liczba różna od zera jest następnikiem jakiejś liczby.

A_4: Wynik dodania zera do dowolnej liczby jest tą liczbą.

A_5: Suma: pierwszej liczby oraz następnika drugiej równa jest następnikowi sumy liczb: pierwszej oraz drugiej.

A_6: Wynik przemnożenia dowolnej liczby przez zero jest zerem.

A_7: Iloczyn: pierwszej liczby oraz następnika drugiej równy jest sumie: iloczynu liczb pierwszej i drugiej oraz pierwszej liczby.

---

[3] I tylko! Jak jednak wiadomo, nasze zamierzenia mogą okazać się zbyt śmiałe. Tak jest zarówno w tym przypadku, jak i w przypadku Arytmetyki Peana (zob. przykład III.6.5.).

Jeśli aksjomaty te wydają ci się oczywiste, to witaj we Wspólnocie Intelektualnej Ludzkości! Nie są chyba znani osobnicy, którym zdania te wydawałyby się fałszywe, przy podanej powyżej interpretacji zamierzonej. Powstaje naturalnie pytanie: czy z tych aksjomatów ***wynikają***[4] DOKŁADNIE WSZYSTKIE prawdy arytmetyczne? Odpowiedzi na to, wydawałoby się proste, pytanie dostarczają ważne twierdzenia metalogiczne (o których usłyszysz na roku III, na wykładzie dotyczącym *Funkcji Rekurencyjnych*). Odpowiedź jest negatywna; chociaż każde zdanie wyprowadzalne z aksjomatów jest prawdziwe w zamierzonej interpretacji, to jednak nie wszystkie zdania prawdziwe w tej interpretacji są wyprowadzalne z aksjomatów. Ma to też związek z *nierozstrzygalnością* KRP (o której piszemy w rozdziale IV tego skryptu).

Pierwsze trzy z powyższych aksjomatów mają gwarantować, że uniwersum interpretacji zamierzonej jest poprawnie utworzoną kolejką: na początku jest zero, potem następnik zera (czyli jedynka), potem następnik następnika zera (czyli następnik jedynki, a więc dwójka), i tak dalej. Za każdą liczbą naturalną jest dokładnie jedna liczba większa od niej o jeden, a od każdej liczby naturalnej jest tylko *skończenie*[5] wiele „kroków wstecz", do zera.

Aksjomaty A_4 oraz A_5 charakteryzują dodawanie, natomiast A_6 oraz A_7 ustalają własności mnożenia. Nie obawiaj się: w charakterystykach tych ***nie*** popełnia się błędnego koła.

Pokażemy teraz, jak uzyskiwać dowody prostych prawd arytmetycznych przy użyciu metody drzew semantycznych.

Oto dowód, iż $\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\sigma(\sigma(\sigma(\bigcirc))))$, czyli że dwa i dwa jest cztery:

1.	$\forall x \ \oplus(x, \bigcirc) = x$	aksjomat A_4
2.	$\forall x \forall y \ \oplus(x, \sigma(y)) = \sigma(\oplus(x, y))$	aksjomat A_5
3.	$\neg(\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\sigma(\sigma(\sigma(\bigcirc)))))$	założenie dowodu nie wprost
4.	$\oplus(\sigma(\sigma(\bigcirc)), \bigcirc) = \sigma(\sigma(\bigcirc))$	reguła $R(\forall)$ dla termu $\sigma(\sigma(\bigcirc))$ w A_4
5.	$\forall y \ \oplus(\sigma(\sigma(\bigcirc)), \sigma(y)) = \sigma(\oplus(\sigma(\sigma(\bigcirc)), y))$	reguła $R(\forall)$ dla termu $\sigma(\sigma(\bigcirc))$ w A_5
6.	$\oplus(\sigma(\sigma(\bigcirc)), \sigma(\bigcirc)) = \sigma(\oplus(\sigma(\sigma(\bigcirc)), \bigcirc))$	reguła $R(\forall)$ dla termu $\bigcirc$ w 5.
7.	$\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\oplus(\sigma(\sigma(\bigcirc)), \sigma(\bigcirc)))$	reguła $R(\forall)$ dla termu $\sigma(\bigcirc)$ w 5.
8.	$\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\oplus(\sigma(\sigma(\bigcirc)), \bigcirc))$	6. i 7., reguły dla identyczności
9.	$\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\sigma(\sigma(\sigma(\bigcirc))))$	4. i 8., reguły dla identyczności
10.	$\times_{3,9}$	SPRZECZNOŚĆ: $3, 9$.

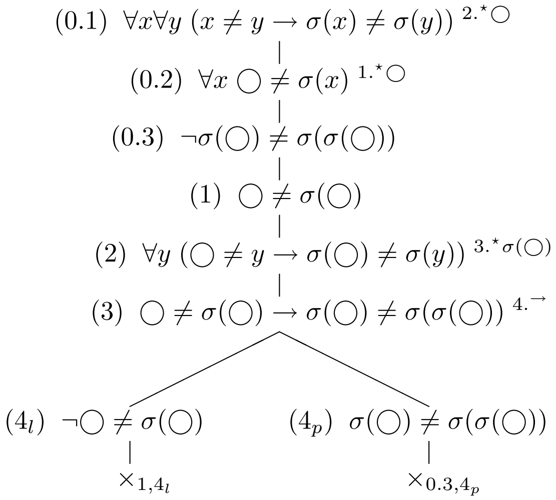
W Arytmetyce Robinsona łatwo dowodzi się wszelakich *konkretnych* faktów arytmetycznych, np.: $\bigcirc \neq \sigma(\bigcirc)$, $\sigma(\bigcirc) \neq \sigma(\sigma(\bigcirc))$, itp. Natomiast nie są w niej dowodliwe liczne zdania generalnie skwantyfikowane, jak np. $\forall x \ (x \neq \sigma(x))$. Przykładowe dowody zdań tego drugiego rodzaju podajemy w przykładzie III.6.5., dotyczącym Arytmetyki Peana oraz zasady indukcji matematycznej.

Pokażmy jeszcze jeden dowód w Arytmetyce Robinsona: udowodnimy mianowicie, że z aksjomatów A_1 oraz A_2 wynika logicznie nierówność $\sigma(\bigcirc) \neq \sigma(\sigma(\bigcirc))$, tj. iż jeden jest różne od dwa. Budujemy drzewo semantyczne, w którego pniu umieszczamy A_1 oraz A_2, a także $\neg\sigma(\bigcirc) \neq \sigma(\sigma(\bigcirc))$.

---

[4] Przy interpretacji symbolu = jako relacji identyczności.

[5] Uwaga: pojęcia *skończoności* nie można wyrazić w języku pierwszego rzędu; ten intuicyjny komentarz czyniony jest w metajęzyku.



Wszystkie gałęzie drzewa są zamknięte. Wykluczyliśmy zatem możliwość, by A_1 oraz A_2 były prawdziwe i jednocześnie nierówność $\sigma(\bigcirc) \neq \sigma(\sigma(\bigcirc))$ była fałszywa. Tak więc, $\sigma(\bigcirc) \neq \sigma(\sigma(\bigcirc))$ wynika logicznie z A_1 oraz A_2.

PRZYKŁAD III.6.2: DRUGI — GRUPY.

Lubisz tańczyć, prawda? Przypuśćmy więc, że stajesz na parkiecie (nieważne: trzeźwa, czy nie), wykonujesz ulubiony taniec i wracasz do baru. Czy jesteś pewna, że nadal jesteś tą samą osobą? Ponieważ abstrahujemy od twojego zespołu przekonań (osądów, emocji, itp.), więc zadamy nieco inne pytanie: czy jesteś pewna, że do baru wróciło to samo ciało, ten sam, za przeproszeniem, obiekt fizyczny? Zakładamy dodatkowo, że w trakcie tańca nie uległaś rozerwaniu (czyli, że wracasz do baru w jednym kawałku), nie rozciągnęłaś się ani nie skurczyłaś oraz że nie uczyniono w tobie żadnych dodatkowych otworów.[6]

Pytanie nasze sprowadza się do tego, czy ruchy podczas tańca pozostawią taką, za przeproszeniem, bryłę, jaką jesteś, niezmienioną. Jeszcze jedno założenie, które być może wyda ci się nietrafne, ale które w istocie jest niewinne: zakładamy, że w tańcu jesteś bryłą sztywną.[7]

Zgodzisz się, że przy tych założeniach taniec sprowadza się do ***przesunięć*** oraz ***obrotów*** brył sztywnych. A stąd już niewielki (taneczny) krok w kierunku TEORII GRUP.

* * *

Aksjomaty teorii grup można sformułować w różnych językach, tzn. można na różne sposoby dobrać zestaw stałych pozalogicznych. Podamy trzy takie możliwości.

TEORIA GRUP: PIERWSZA AKSJOMATYKA.

Język teorii grup jest w tym przypadku językiem KRP z identycznością oraz:

- jednym dwuargumentowym symbolem funkcyjnym $\boxdot$, nazywającym *działanie* w grupie.

AKSJOMATY:

Aksjomaty identyczności dla symbolu $\boxdot$, czyli formuły:

$\forall x \forall y \forall z\, (x = y \rightarrow \boxdot(x, z) = \boxdot(y, z))$

$\forall x \forall y \forall z\, (x = y \rightarrow \boxdot(z, x) = \boxdot(z, y))$.

---

[6] Ani nie zatkano już istniejących. Upraszam, aby tych założeń nie traktować jako obscenicznych: to są zwykłe warunki natury topologicznej.

[7] Niewinność tego założenia polega na tym, że nawet jeśli w tańcu dziko podrygujesz i wykręcasz się na wszelakie sposoby, to jednak pozostajesz ***sumą*** brył sztywnych.

Aksjomaty specyficzne teorii grup:

G^1_1: $\forall x \forall y\ (\boxdot(x, \boxdot(y, z)) = \boxdot(\boxdot(x, y), z))$

G^1_2: $\forall x \forall y \exists z\ (\boxdot(x, z) = y)$

G^1_3: $\forall x \forall y \exists z\ (\boxdot(z, x) = y)$.

Warunek *przemienności* działania $\boxdot$, tj.:

$$(A) \quad \forall x \forall y\ (\boxdot(x, y) = \boxdot(y, x))$$

nie jest logiczną konsekwencją aksjomatów teorii grup. Te układy postaci $\langle G, \boxdot_G \rangle$, dla których G jest dowolnym zbiorem, a $\boxdot_G$ działaniem w zbiorze G takim, że zachodzą aksjomaty teorii grup oraz warunek (A) nazywamy *grupami przemiennymi* (albo *abelowymi*).

Jako ćwiczenie proponujemy próbę wykazania, że istotnie warunek (A) nie wynika logicznie z aksjomatów teorii grup. Wskazówka: budujemy drzewo semantyczne, w którego pniu umieszczamy aksjomaty G^1_1, G^2_1, G^3_1 oraz negację warunku (A). Gdyby to drzewo okazało się zamknięte, to (A) byłoby logiczną konsekwencją G^1_1, G^2_1 oraz G^3_1.

TEORIA GRUP: DRUGA AKSJOMATYKA.

W tym przypadku używany język to język KRP z identycznością oraz:

- jednym dwuargumentowym symbolem funkcyjnym $\boxdot$, nazywającym *działanie* w grupie;
- jedną stałą indywiduową ε nazywającą element *neutralny* (względem działania) w grupie.

AKSJOMATY TEORII GRUP W TYM JĘZYKU:

Aksjomaty identyczności dla symboli $\boxdot$ oraz ε są takie same, jak w poprzednim przypadku:

$\forall x \forall y \forall z\ (x = y \rightarrow \boxdot(x, z) = \boxdot(y, z))$

$\forall x \forall y \forall z\ (x = y \rightarrow \boxdot(z, x) = \boxdot(z, y))$.

Aksjomaty specyficzne:

G^2_1: $\forall x \forall y\ \boxdot\ (x, \boxdot(y, z)) = \boxdot(\boxdot(x, y), z)$

G^2_2: $\forall x\ (\boxdot(x, \varepsilon) = x)$

G^2_3: $\forall x\ (\boxdot(\varepsilon, x) = x)$

G^2_4: $\forall x \exists y\ (\boxdot(x, y) = \varepsilon)$

G^2_5: $\forall x \exists y\ (\boxdot(y, x) = \varepsilon)$.

Dowód jedyności elementu neutralnego, tj. zdania:

$$(G^2_6) \quad \forall z (\forall x\ (\boxdot(x, z) = x \wedge \boxdot(z, x) = x) \rightarrow \varepsilon = z).$$

1.	$\forall x\ (\boxdot(x,\varepsilon) = x)$	aksjomat G_2^2
2.	$\forall x\ (\boxdot(\varepsilon,x) = x)$	aksjomat G_3^2
3.	$\neg\forall z(\forall x\ (\boxdot(x,z) = x \wedge \boxdot(z,x) = x) \rightarrow \varepsilon = z)$	negacja G_6^2 (założenie dowodu nie wprost)
4.	$\neg(\forall x\ (\boxdot(x,a) = x \wedge \boxdot(a,x) = x) \rightarrow \varepsilon = a)$	$R(\neg\forall)$, 3
5_g. 5_d.	$\forall x\ (\boxdot(x,a) = x \wedge \boxdot(a,x) = x)$ $\neg\varepsilon = a$	$R(\neg \rightarrow)$, 4
6.	$\boxdot(a,\varepsilon) = a$	$R(\forall)$ dla a, 1
7.	$\boxdot(\varepsilon,a) = a$	$R(\forall)$ dla a, 2
8.	$\boxdot(\varepsilon,a) = \varepsilon \wedge \boxdot(a,\varepsilon) = \varepsilon$	$R(\forall)$ dla ε, 5_g
9_g. 9_d.	$\boxdot(\varepsilon,a) = \varepsilon$ $\boxdot(a,\varepsilon) = \varepsilon$	$R(\wedge)$, 8
10.	$\varepsilon = a$	$R(=)$, 9_g, 7
11.	$\times_{5_d,10}$	SPRZECZNOŚĆ: $5_d, 10$.

TEORIA GRUP: TRZECIA AKSJOMATYKA.

W tym przypadku używany język to język KRP z identycznością oraz:

- jednym dwuargumentowym symbolem funkcyjnym $\boxdot$, nazywającym *działanie* w grupie;
- jedną stałą indywiduową ε nazywającą element *neutralny* (względem działania) w grupie;
- jednym jednoargumentowym symbolem funkcyjnym $\circledcirc$ nazywającym element *odwrotny* (względem swojego argumentu).

AKSJOMATY:

Aksjomaty identyczności dla symboli $\boxdot$, $\circledcirc$ oraz ε:

$\forall x\forall y\forall z\ (x = y \rightarrow \boxdot(x,z) = \boxdot(y,z))$

$\forall x\forall y\forall z\ (x = y \rightarrow \boxdot(z,x) = \boxdot(z,y))$

$\forall x\forall y\ (x = y \rightarrow \circledcirc(x) = \circledcirc(y))$.

Aksjomaty specyficzne:

G_1^3: $\forall x\forall y\forall z\ (\boxdot(x,\boxdot(y,z)) = \boxdot(\boxdot(x,y),z))$

G_2^3: $\forall x\ (\boxdot(x,\varepsilon) = x)$

G_3^3: $\forall x\ (\boxdot(x,\circledcirc(x)) = \varepsilon)$.

Dowód prawa skracania, tj. zdania:

$$(G_4^3) \quad \forall x\forall y\forall z\ (\boxdot(x,z) = \boxdot(y,z) \rightarrow x = y).$$

1.	$\forall x \forall y \forall z\ (\boxdot(x, \boxdot(y,z)) = \boxdot(\boxdot(x,y),z))$	aksjomat G_1^3
2.	$\forall x\ (\boxdot(x,\varepsilon) = x)$	aksjomat G_2^3
3.	$\forall x\ (\boxdot(x,\circledcirc(x)) = \varepsilon)$	aksjomat G_3^3
4.	$\neg\forall x \forall y \forall z\ (\boxdot(x,z) = \boxdot(y,z) \rightarrow x = y)$	negacja G_4^3 (założenie dowodu nie wprost)
5.	$\neg\forall y \forall z\ (\boxdot(a_1,z) = \boxdot(y,z) \rightarrow a_1 = y)$	$R(\neg\forall)$ dla a_1, 4
6.	$\neg\forall z\ (\boxdot(a_1,z) = \boxdot(a_2,z) \rightarrow a_1 = a_2)$	$R(\neg\forall)$ dla a_2, 5
7.	$\neg(\boxdot(a_1,a_3) = \boxdot(a_2,a_3) \rightarrow a_1 = a_2)$	$R(\neg\forall)$ dla a_3, 6
8_g. 8_d.	$\boxdot(a_1,a_3) = \boxdot(a_2,a_3)$ $a_1 \neq a_2$	$R(\neg \rightarrow)$, 7
9.	$\forall y \forall z\ (\boxdot(a_1, \boxdot(y,z)) = \boxdot(\boxdot(a_1,y),z))$	$R(\forall)$ dla a_1, 1
10.	$\forall z\ \boxdot\ (a_1, \boxdot(a_3,z)) = \boxdot(\boxdot(a_1,a_3),z)$	$R(\forall)$ dla a_3, 9
11.	$\boxdot(a_1, \boxdot(a_3,\circledcirc(a_3))) = \boxdot(\boxdot(a_1,a_3),\circledcirc(a_3))$	$R(\forall)$ dla $\circledcirc(a_3)$, 10
12.	$\boxdot(a_1, \boxdot(a_3,\circledcirc(a_3))) = \boxdot(\boxdot(a_2,a_3),\circledcirc(a_3))$	$R(=)$ 11, 8_g
13.	$\forall y \forall z\ (\boxdot(a_2, \boxdot(y,z)) = \boxdot(\boxdot(a_2,y),z))$	$R(\forall)$ dla a_2, 1
14.	$\forall z\ (\boxdot(a_2, \boxdot(a_3,z)) = \boxdot(\boxdot(a_2,a_3),z)$	$R(\forall))$ dla a_3, 13
15.	$\boxdot(a_2, \boxdot(a_3,\circledcirc(a_3))) = \boxdot(\boxdot(a_2,a_3),\circledcirc(a_3))$	$R(\forall)$ dla $\circledcirc(a_3)$, 14
16.	$\boxdot(a_3,\circledcirc(a_3)) = \varepsilon$	$R(\forall)$ dla a_3, 3
17.	$\boxdot(a_1, \boxdot(a_3,\circledcirc(a_3))) = \boxdot(a_2, \boxdot(a_3,\circledcirc(a_3)))$	$R(=)$, 12, 15
18.	$\boxdot(a_1,\varepsilon) = \boxdot(a_2,\varepsilon)$	$R(=)$, 16,17
19.	$\boxdot(a_2,\varepsilon) = a_2$	$R(\forall)$ dla a_2, 2
20.	$\boxdot(a_3,\varepsilon) = a_3$	$R(\forall)$ dla a_3, 2
21.	$a_1 = \boxdot(a_2,\varepsilon)$	$R(=)$, 19, 18
22.	$a_1 = a_2$	$R(=)$, 20, 21
23.	$\times_{8_d,22}$	Sprzeczność: $8_d, 22$.

Dowód zdania:

$$(G_5^3)\quad \forall x\ (\boxdot(x,\varepsilon) = \boxdot(\varepsilon,x)).$$

1.	$\forall x \forall y \forall z\ (\boxdot(x, \boxdot(y,z)) = \boxdot(\boxdot(x,y),z))$	aksjomat G_1^3
2.	$\forall x\ (\boxdot(x,\varepsilon) = x)$	aksjomat G_2^3
3.	$\forall x\ (\boxdot(x,\circledcirc(x)) = \varepsilon)$	aksjomat G_3^3
4.	$\forall x \forall y \forall z\ (\boxdot(x,z) = \boxdot(y,z) \rightarrow x = y)$	twierdzenie G_4^3
5.	$\neg\forall x\ (\boxdot(x,\varepsilon) = \boxdot(\varepsilon,x))$	negacja G_5^3 (założenie dowodu nie wprost)
6.	$\boxdot(a,\varepsilon) \neq \boxdot(\varepsilon,a)$	$R(\forall)$ dla a, 5
7.	$\forall y \forall z\ (\boxdot(\varepsilon, \boxdot(y,z)) = \boxdot(\boxdot(\varepsilon,y),z))$	$R(\forall)$ dla ε, 1
8.	$\forall z\ (\boxdot(\varepsilon, \boxdot(a,z)) = \boxdot(\boxdot(\varepsilon,a),z))$	$R(\forall)$ dla a, 7
9.	$\boxdot(\varepsilon, \boxdot(a,\circledcirc(a))) = \boxdot(\boxdot(\varepsilon,a),\circledcirc(a))$	$R(\forall)$ dla $\circledcirc(a)$, 8
10.	$\boxdot(a,\circledcirc(a)) = \varepsilon$	$R(\forall)$ dla a, 3
11.	$\boxdot(\varepsilon,\varepsilon) = \varepsilon$	$R(\forall)$ dla ε, 2
12.	$\boxdot(\varepsilon,\varepsilon) = \boxdot(\boxdot(\varepsilon,a),\circledcirc(a))$	$R(=)$, 9, 10
13.	$\varepsilon = \boxdot(\boxdot(\varepsilon,a),\circledcirc(a))$	$R(=)$, 11, 12
14.	$\boxdot(a,\circledcirc(a)) = \boxdot(\boxdot(\varepsilon,a),\circledcirc(a))$	$R(=)$, 10, 13
15.	$\forall y \forall z\ (\boxdot(a,z) = \boxdot(y,z) \rightarrow a = y$	$R(\forall))$ dla a, 4
16.	$\forall z\ (\boxdot(a,z) = \boxdot(\boxdot(\varepsilon,a),z) \rightarrow a = \boxdot(\varepsilon,a))$	$R(\forall)$ dla $\boxdot(\varepsilon,a)$, 15
17.	$\boxdot(a,\circledcirc(a)) = \boxdot(\boxdot(\varepsilon,a),\circledcirc(a)) \rightarrow a = \boxdot(\varepsilon,a)$	$R(\forall)$ dla $\circledcirc(a)$, 16
18_l.	$\boxdot(a,\circledcirc(a)) \neq \boxdot(\boxdot(\varepsilon,a),\circledcirc(a))$	$R(\rightarrow)$, 17
$18_l.1.$	$\times_{14,18_l}$	Sprzeczność: $14, 18_l$.
18_p.	$a = \boxdot(\varepsilon,a)$	$R(\rightarrow)$, 17
$18_p.1.$	$\boxdot(a,\varepsilon) = a$	$R(\forall)$ dla a, 2
$18_p.2.$	$\boxdot(a,\varepsilon) = \boxdot(\varepsilon,a)$	$R(=)$, 18_p., $18_p.1$.
$18_p.3.$	$\times_{6,18_p.2.}$	Sprzeczność: $6, 18_p.2$.

Dowód zdania:

$$(G_6^3) \quad \forall y \forall x\ (\boxdot(x,y) = x \rightarrow y = \varepsilon).$$

1.	$\forall x\ (\boxdot(x,\varepsilon) = x)$	aksjomat G_2^3
2.	$\forall x\ (\boxdot(x,\varepsilon) = \boxdot(\varepsilon,x))$	twierdzenie G_5^3
3.	$\neg\forall y \forall x\ (\boxdot(x,y) = x \rightarrow y = \varepsilon)$	negacja G_6^3 (założenie dowodu nie wprost)
4.	$\neg\forall x\ (\boxdot(x,a) = x \rightarrow a = \varepsilon)$	$R(\forall)$ dla a, 3
5_g.	$\forall x\ \boxdot\ (x,a) = x$	$R(\neg \rightarrow)$, 4
5_d.	$a \neq \varepsilon$	
6.	$\boxdot(\varepsilon,a) = \varepsilon$	$R(\forall)$ dla ε, 5_g
7.	$\boxdot(a,\varepsilon) = \boxdot(\varepsilon,a)$	$R(\forall)$ dla a, 2
8.	$\boxdot(a,\varepsilon) = \varepsilon$	$R(=)$, 6,7
9.	$\boxdot(a,\varepsilon) = a$	$R(\forall)$ dla a, 1
10.	$a = \varepsilon$	$R(=)$, 8,9
11.	$\times_{5_d,10}$	SPRZECZNOŚĆ: $5_d, 10$.

Przykłady grup.

- Zbiór liczb całkowitych z działaniem dodawania oraz zerem jako elementem neutralnym tworzy grupę.
- Zbiór liczb rzeczywistych różnych od zera z działaniem mnożenia oraz jedynką jako elementem neutralnym tworzy grupę.
- Zbiór wszystkich wzajemnie jednoznacznych odwzorowań danego zbioru na siebie tworzy grupę. Działaniem jest tu złożenie funkcji, a elementem neutralnym funkcja identycznościowa.

PRZYKŁAD III.6.3: TRZECI — ALGEBRY BOOLE'A.

Znajdowanie analogii między różnymi twierdzeniami to szczególna umiejętność.[8] Możesz posiąść tę umiejętność, nawet na (stosunkowo niskim) poziomie elementarza logicznego. Z pewnością zauważyłaś, że jest odpowiedniość między pewnymi prawami KRZ a niektórymi prawami rachunku zbiorów.

Podobnie jak w przypadku teorii grup, również dla teorii algebr Boole'a podać można różne (równoważne) aksjomatyki. Ograniczymy się do dwóch.

TEORIA ALGEBR BOOLE'A: PIERWSZA AKSJOMATYKA.

Język teorii algebr Boole'a jest językiem KRP z identycznością oraz:

- symbolem funkcyjnym dwuargumentowym $\boxplus$, nazywającą *kres górny* (swoich argumentów);
- symbolem funkcyjnym dwuargumentowym $\boxtimes$, nazywającą *kres dolny* (swoich argumentów);
- symbolem funkcyjnym jednoargumentowym $\boxminus$, nazywającą *dopełnienie* (swojego argumentu);

AKSJOMATY:

Aksjomaty identyczności dla symboli $\boxplus$, $\boxtimes$, $\boxminus$, $\triangledown$ oraz $\vartriangle$:

$$\forall x \forall y \forall z\ (x = y \rightarrow \boxplus(x,z) = \boxplus(y,z))$$

$$\forall x \forall y \forall z\ (x = y \rightarrow \boxtimes(x,z) = \boxtimes(y,z))$$

---

[8] Jeszcze ciekawsza jest umiejętność znajdowania analogii między różnymi analogiami, jak twierdzą matematycy.

$\forall x \forall y \forall z \; (x = y \rightarrow \boxplus(z, x) = \boxplus(z, y))$

$\forall x \forall y \forall z \; (x = y \rightarrow \boxtimes(z, x) = \boxtimes(z, y))$

$\forall x \forall y \; (x = y \rightarrow \boxminus(x) = \boxminus(y))$.

Aksjomaty specyficzne teorii algebr Boole'a:

B^1_1: $\forall x \forall y \; (\boxplus(x, y) = \boxplus(y, x))$

B^1_2: $\forall x \forall y \; (\boxtimes(x, y) = \boxtimes(y, x))$

B^1_3: $\forall x \forall y \forall z \; (\boxplus(x, \boxplus(y, z)) = \boxplus(\boxplus(x, y), z))$

B^1_4: $\forall x \forall y \forall z \; (\boxtimes(x, \boxtimes(y, z)) = \boxtimes(\boxtimes(x, y), z))$

B^1_5: $\forall x \forall y \; (\boxplus(\boxtimes(x, y), y) = y)$

B^1_6: $\forall x \forall y \; (\boxtimes(\boxplus(x, y), y) = y)$

B^1_7: $\forall x \forall y \forall z \; (\boxplus(x, \boxtimes(y, z)) = \boxtimes(\boxplus(x, y), \boxplus(x, z)))$

B^1_8: $\forall x \forall y \forall z \; (\boxtimes(x, \boxplus(y, z)) = \boxplus(\boxtimes(x, y), \boxtimes(x, z)))$

B^1_9: $\forall x \forall y \; (\boxplus(\boxtimes(x, \boxminus(x)), y) = y)$

B^1_{10}: $\forall x \forall y \; (\boxtimes(\boxplus(x, \boxminus(x)), y) = y)$.

Prostymi konsekwencjami tych aksjomatów są np.:

- $\forall x \; (\boxplus(x, x) = x)$
- $\forall x \; (\boxtimes(x, x) = x)$
- $\forall x \forall y \; ((\boxplus(x, y) = \boxplus(x, \boxminus(x)) \wedge \boxtimes(x, y) = \boxtimes(x, \boxtimes(x))) \rightarrow y = \boxminus(x))$.

Niech ich wyprowadzenia będą ćwiczeniem dla czytelniczek. Jako wskazówkę podajemy ciąg równości dla pierwszych dwóch rozważanych wyżej przypadków:

$$x = \boxplus(x, \boxtimes(x, y)) = \boxtimes(\boxplus(x, x), \boxplus(x, y)) = \boxplus(\boxtimes(x, \boxplus(x, y)), \boxtimes(x, \boxplus(x, y))) = \boxplus(x, x)$$

$$x = \boxtimes(x, \boxplus(x, y)) = \boxplus(\boxtimes(x, x), \boxtimes(x, y)) = \boxtimes(\boxplus(x, \boxtimes(x, y)), \boxplus(x, \boxtimes(x, y))) = \boxtimes(x, x).$$

Teoria algebr Boole'a: druga aksjomatyka.

Język teorii algebr Boole'a jest językiem KRP z identycznością oraz:

- symbolem funkcyjnym dwuargumentowym $\boxplus$, nazywającą *kres górny* (swoich argumentów);
- symbolem funkcyjnym dwuargumentowym $\boxtimes$, nazywającą *kres dolny* (swoich argumentów);
- symbolem funkcyjnym jednoargumentowym $\boxminus$, nazywającą *dopełnienie* (swojego argumentu);
- stałą indywiduową $\triangledown$, nazywającą *jedynkę* (element największy) algebry;
- stałą indywiduową $\vartriangle$, nazywającą *zero* (element najmniejszy) algebry.

Aksjomaty:

Aksjomaty identyczności dla symboli $\boxplus$, $\boxtimes$, $\boxminus$, $\triangledown$ oraz $\vartriangle$:

$\forall x \forall y \forall z\ (x = y \rightarrow \boxplus(x, z) = \boxplus(y, z))$

$\forall x \forall y \forall z\ (x = y \rightarrow \boxtimes(x, z) = \boxtimes(y, z))$

$\forall x \forall y \forall z\ (x = y \rightarrow \boxplus(z, x) = \boxplus(z, y))$

$\forall x \forall y \forall z\ (x = y \rightarrow \boxtimes(z, x) = \boxtimes(z, y))$

$\forall x \forall y\ (x = y \rightarrow \boxminus(x) = \boxminus(y))$.

Uwaga. Naprawdę potrzebne są tylko dwa pierwsze z tych aksjomatów. Pozostałe można wyprowadzić z innych aksjomatów teorii algebr Boole'a.

Aksjomaty specyficzne teorii algebr Boole'a:

B_2^1: $\forall x\ (\boxplus(x, \vartriangle) = x)$

B_2^2: $\forall x\ (\boxtimes(x, \triangledown) = x)$

B_2^3: $\forall x\ (\boxplus(x, \boxminus(x)) = \triangledown)$

B_2^4: $\forall x\ (\boxtimes(x, \boxminus(x)) = \vartriangle)$

B_2^5: $\forall x \forall y\ (\boxplus(x, y) = \boxplus(y, x))$

B_2^6: $\forall x \forall y\ (\boxtimes(x, y) = \boxtimes(y, x))$

B_2^7: $\forall x \forall y \forall z\ (\boxplus(x, \boxtimes(y, z)) = \boxtimes(\boxplus(x, y), \boxplus(x, z)))$

B_2^8: $\forall x \forall y \forall z\ (\boxtimes(x, \boxplus(y, z)) = \boxplus(\boxtimes(x, y), \boxtimes(x, z)))$.

Definicja algebr Boole'a przez częściowe porządki.

Niech U będzie dowolnym zbiorem uporządkowanym częściowo przez relację $\prec$. Przypominamy, że dla dowolnego zbioru $A \subseteq U$:

- element $a \in A$ nazywamy *elementem maksymalnym* w A, jeśli zachodzi implikacja:
  $\forall x\ ((x \in a \wedge x \prec a) \rightarrow x = a)$;
- element $a \in A$ nazywamy *elementem minimalnym* w A, jeśli zachodzi implikacja:
  $\forall x\ ((x \in a \wedge a \prec x) \rightarrow x = a)$;
- element $a \in A$ nazywamy *elementem największym* w A, jeśli $x \prec a$ dla wszystkich $x \in A$;
- element $a \in A$ nazywamy *elementem najmniejszym* w A, jeśli $a \prec x$ dla wszystkich $x \in A$;
- element $a \in U$ jest *kresem górnym* zbioru A, jeśli $x \prec a$ dla wszystkich $x \in A$;
- element $a \in U$ jest *kresem dolnym* zbioru A, jeśli $a \prec x$ dla wszystkich $x \in A$;
- element $a \in U$ jest *najmniejszym kresem górnym* zbioru A, jeśli a jest elementem najmniejszym zbioru wszystkich kresów górnych zbioru A;
- element $a \in U$ jest *największym kresem dolnym* zbioru A, jeśli a jest elementem największym zbioru wszystkich kresów dolnych zbioru A.

Mówimy, że $\langle U, \prec\rangle$ jest ***kratą***, jeśli dla dowolnych elementów $x, y \in U$ istnieją: najmniejszy kres górny oraz największy kres dolny zbioru $\{x, y\}$. Ponieważ elementy te są wyznaczone jednoznacznie, więc możemy przyjąć oznaczenia:

- $\boxtimes(x, y)$ — dla największego kresu dolnego zbioru $\{x, y\}$;
- $\boxplus(x, y)$ — dla najmniejszego kresu górnego zbioru $\{x, y\}$.

Krata $\langle U, \prec\rangle$ jest ***dystrybutywna***, jeśli dla dowolnych $x, y, z \in U$ zachodzą warunki:

- $\forall x \forall y \forall z \ \boxplus(x, \boxtimes(y, z)) = \boxtimes(\boxplus(x, y), \boxplus(x, z))$
- $\forall x \forall y \forall z \ \boxtimes(x, \boxplus(y, z)) = \boxplus(\boxtimes(x, y), \boxtimes(x, z))$.

Kratę dystrybutywną $\langle U, \prec\rangle$ nazywamy ***algebrą Boole'a***, jeśli dla dowolnego elementu $x \in U$ istnieje jego *dopełnienie*, tj. element $\boxminus(x)$ spełniający warunki:

- $\forall x \forall y \ \boxplus(\boxtimes(x, \boxminus(x)), y) = y$
- $\forall x \forall y \ \boxtimes(\boxplus(x, \boxminus(x)), y) = y$.

Z każdego z podanych wyżej układów aksjomatów dla teorii algebr Boole'a można wywieść wszystkie warunki charakteryzujące algebry Boole'a jako określone przed chwilą struktury uporządkowane, a także na odwrót: z charakterystyki porządkowej algebr Boole'a można wyprowadzić każdą z omawianych wcześniej aksjomatyk.

Uwaga o standardowej notacji. Dla operacji w algebrach Boole'a używa się zwykle standardowych oznaczeń:

- $\cup$ — dla kresu górnego (także: $\vee$);
- $\cap$ — dla kresu dolnego (także: $\wedge$);
- $-$ — dla operacji dopełnienia.

Powyżej celowo nie używaliśmy standardowej notacji. Niech będzie prostym ćwiczeniem dla czytelniczek zapisanie podanych aksjomatyk teorii algebr Boole'a w notacjach standardowych. Wykonanie tego ćwiczenia nagrodzone zostanie iluminacją: stwierdzisz, że przecież gdzieś już to widziałaś!

Przykłady algebr Boole'a.

- Wszystkie ***podzbiory dowolnego zbioru*** U wraz z operacjami teoriomnogościowymi: sumy (kres górny), iloczynu (kres dolny), dopełnienia (do U), zbiorem U jako jedynką oraz zbiorem pustym $\emptyset$ jako zerem tworzą algebrę Boole'a.
- **Algebra wartości logicznych.** Tabliczki prawdziwościowe funktorów odpowiadających spójnikom zdaniowym pokazują, że w zbiorze wartości logicznych $\{0, 1\}$ można wprowadzić strukturę algebry Boole'a. Zerem tej algebry jest 0, jej jedynką jest 1. Kres dolny odpowiada koniunkcji, kres górny alternatywie (nierozłącznej), a operacja dopełnienia odpowiada negacji.
- **Algebra zdarzeń.** Przestrzeń zdarzeń jest algebrą Boole'a. Jest to, rzecz jasna, szczególny przypadek pierwszego z rozważanych przykładów. Zdarzenia są zbiorami (zdarzeń elementarnych), a koniunkcji i alternatywie zdarzeń odpowiadają operacje teoriomnogościowe na zbiorach zdarzeń elementarnych; zdarzeniu przeciwnemu do danego zdarzenia odpowiada dopełnienie teoriomnogościowe tego zdarzenia.

- **Kraty pojęć.** Ten przykład wykorzystuje kilka pojęć algebraicznych, których tu nie objaśniamy. Jest on przeznaczony dla tych czytelniczek, które są już trochę oswojone z algebrą, lub też takich, które — zżerane zdrową ambicją — zechcą odnaleźć owe pojęcia w jakimś podręczniku. Dodajmy, że algebry z tego przykładu mają ciekawe zastosowania, także lingwistyczne — np. w opisie zależności semantycznych w leksykonie.

Kontekstem nazwiemy dowolny układ postaci (G, M, I), gdzie G (ogół rozważanych obiektów) i M (ogół rozważanych cech) są zbiorami, a I relacją o dziedzinie G oraz przeciwdziedzinie M. Wyrażenie gIm czytajmy: obiekt g ma cechę m. Można czynić dalsze założenia o tego typu układach; w tym miejscu przywoływanie ich jest nieistotne. Zdefiniujmy dwa operatory na rodzinach zbiorów obiektów i cech:

$\rhd(A) = \{m \in M\ :\ (\forall g)\ [g \in A \to gIm]\}$

$\lhd(B) = \{g \in G\ :\ (\forall m)\ [m \in B \to gIm]\}$

Para $(\rhd, \lhd)$ jest odpowiedniością Galois. Dla dowolnego kontekstu (G, M, I) nazwiemy *pojęciem formalnym* tego kontekstu każdą parę (A, B) taką, że:

$A \subseteq G,\ B \subseteq M,\ \rhd(A) = B,\ \lhd(B) = A.$

Ekstensją pojęcia formalnego (A, B) jest A, jego *intensją* jest B. Rodzinę wszystkich pojęć formalnych kontekstu (G, M, I) oznaczmy przez $\mathfrak{B}(G, M, I)$. Rodzina ta jest częściowo uporządkowana przez relację $\prec$:

$(A_1, B_1) \prec (A_2, B_2)$ wtedy i tylko wtedy, gdy $A_1 \subseteq A_2$.[9]

Podstawowe dla rozważanej problematyki twierdzenie wysłowić można następująco (zob. Bernhard Ganter, Rudolf Wille *Formal Concept Analysis. Mathematical Foundations.* Springer Verlag, Berlin Heidelberg New York, 1999, str. 20; upraszczam nieco notację; wszystkie potrzebne do zrozumienia twierdzenia pojęcia znaleźć można w dowolnym solidnym podręczniku teorii krat; stosujemy też standardowe niedomówienia algebraiczne):

Twierdzenie.

Krata pojęć $\mathfrak{B}(G, M, I)$ jest kratą zupełną, w której kresy zdefiniowane są równościami:

$$\bigwedge_{t \in T} (A_t, B_t) = (\bigcap_{t \in T} A_t, \rhd(\lhd(\bigcup_{t \in T} B_t)))$$

$$\bigvee_{t \in T} (A_t, B_t) = (\lhd(\rhd(\bigcup_{t \in T} A_t)), \bigcap_{t \in T} B_t).$$

Krata zupełna $\boldsymbol{V}$ jest izomorficzna z $\mathfrak{B}(G, M, I)$ wtedy i tylko wtedy, gdy istnieją odwzorowania $\gamma : G \to V$ oraz $\mu : M \to V$ takie, że $\gamma(G)$ jest supremum-gęsty w $\boldsymbol{V}$, $\mu(M)$ jest infimum-gęsty w $\boldsymbol{V}$ oraz gIm jest równoważne z $\gamma g \leqslant \mu m$ dla wszystkich $g \in G$ i wszystkich $m \in M$. W szczególności, $\boldsymbol{V} \cong \mathfrak{B}(V, V, \leqslant)$. Mamy tu oczywiście: $\boldsymbol{V} = (V, \leqslant)$.

PRZYKŁAD III.6.4: CZWARTY — ELEMENTARNE WŁASNOŚCI FUNKCJI.

Ten przykład podobny jest do rozważanego wcześniej (w podrozdziale III.5.) przykładu TO, CO TYGRYSY LUBIĄ NAJBARDZIEJ. Nie rozważamy tu żadnej teorii aksjomatycznej. Rozpatrzymy natomiast kilka prostych przykładów dowodów metodą drzew semantycznych faktów dotyczących funkcji w ogólności. Tak więc, jedynymi założeniami, które czynimy (oprócz aksjomatów identyczności) są definicyjne warunki dla funkcji.

Przypomnijmy: jeśli $f \subseteq X^n \times Y$ jest relacją, to mówimy, że f jest n-argumentową funkcją ze zbioru X^n w zbiór Y i zapisujemy ten fakt jako $f : X^n \to Y$, gdy:

$$\forall x_1 \in X \ldots \forall x_n \in X \exists y \in Y\ \ (x_1, \ldots, x_n, y) \in f$$

$$\forall x_1 \in X \ldots \forall x_n \in X \forall y_1 \in Y \forall y_2 \in Y\ \ (((x_1, \ldots, x_n, y_1) \in f \wedge (x_1, \ldots, x_n, y_2) \in f) \to y_1 = y_2).$$

Gdy $f : X^n \to Y$ oraz $(x_1, \ldots, x_n, y) \in f$, to piszemy $f(x_1, \ldots, x_n) = y$ i mówimy, że y jest wartością funkcji f dla argumentów $x_1, \ldots, x_n$. W rozważanych wcześniej przypadkach grup oraz algebr Boole'a mieliśmy $X = Y$, tzn. rozważane funkcje były operacjami w jakimś ustalonym zbiorze.

---

[9] Co jest równoważne temu, że $B_2 \subseteq B_1$.

Uwaga. Ponieważ funkcje są *zbiorami* (par uporządkowanych), więc w języku, w którym mówimy o funkcjach używamy teoriomnogościowego predykatu $\in$, nazywającego relację *należenia* (elementu do zbioru).

Niżej podajemy aksjomatykę teorii mnogości ZF (Zermelo-Fraenkla). Jest to teoria w języku KRP z identycznością. Jedyną stałą pozalogiczną tej teorii jest dwuargumentowy predykat $\in$. Formułę $x \in y$ czytamy: x jest elementem y.

AKSJOMATY TEORII MNOGOŚCI ZF.

Aksjomat ekstensjonalności:

$$\forall x \forall y\ (\forall z\ (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

Ten aksjomat stwierdza, że każdy zbiór jest jednoznacznie wyznaczony poprzez swoje elementy.

Aksjomat pary:

$$\forall x \forall y \exists z \forall u\ (u \in z \leftrightarrow u = x \vee u = y)$$

To aksjomat gwarantujący istnienie pary nieuporządkowanej.

Aksjomat sumy:

$$\forall x \exists y \forall z\ (z \in y \leftrightarrow \exists u\ (z \in u \wedge u \in x))$$

Aksjomat ten gwarantuje istnienie sumy dowolnej rodziny zbiorów.

Aksjomat zbioru potęgowego:

$$\forall x \exists y \forall z\ (z \in y \leftrightarrow \forall u (u \in z \rightarrow u \in x))$$

Na mocy tego aksjomatu, dla dowolnego zbioru istnieje zbiór złożony dokładnie ze wszystkich jego podzbiorów.

Schemat wyróżniania:

$$\forall x_1 \forall x_2 \ldots \forall x_n \forall y \exists u\ (u \in z \leftrightarrow u \in y \wedge \varphi(u, x_1, x_2, \ldots, x_n))$$

gdzie φ jest formułą języka teorii mnogości ZF taką, że z nie jest zmienną wolną w φ, zaś $x_1, x_2, \ldots, x_n$ są zmiennymi wolnymi formuły φ innymi niż u.

Schemat wyróżniania pozwala z elementów danego wprzódy zbioru utworzyć jego podzbiór, złożony z tych elementów, które mają jakąś własność, wyrażalną w języku (pierwszego rzędu) teorii mnogości.

Mamy tu do czynienia nie z jednym aksjomatem, ale właśnie ze *schematem* nieskończenie wielu aksjomatów.

Aksjomat nieskończoności:

$$\exists x\ (\exists y\ (y \in x \wedge \neg \exists z\ (z \in y)) \wedge \forall y\ (y \in x \rightarrow \forall z (\forall u\ (u \in z \leftrightarrow u = y) \rightarrow z \in x)))$$

Ten aksjomat stwierdza istnienie (co najmniej jednego) zbioru nieskończonego. Uwaga: to jedyny aksjomat egzystencjalny w tej teorii mnogości.

Schemat zastępowania:

$$\forall u (\forall x \forall y \forall z\ (x \in u \wedge \varphi(x, y) \wedge \varphi(x, z) \rightarrow y = z) \rightarrow \exists w \forall v\ (v \in w \leftrightarrow \exists x\ (x \in u \wedge \varphi(x, v))))$$

Schemat ten gwarantuje, intuicyjnie mówiąc, że obraz dowolnego zbioru względem jakiejkolwiek funkcji (opisywalnej formułą języka teorii mnogości) także jest zbiorem.

Tu również mamy do czynienia nie z jednym aksjomatem, ale ze *schematem* nieskończenie wielu aksjomatów.

Aksjomat ufundowania:

$$\forall x (\exists u\ (u \in x) \rightarrow \exists y (y \in x \wedge \forall z\ (z \in y \rightarrow \neg z \in x)))$$

Aksjomat ufundowania wyklucza istnienie nieskończonych $\in$-zstępujących ciągów zbiorów, tj. takich ciągów $\langle x_1, x_2, x_3, x_4, \ldots \rangle$, że:

$$x_2 \in x_1,\ x_3 \in x_2,\ x_4 \in x_3, \ldots$$

Gdy do tego systemu dołączyć ***Aksjomat wyboru***:

$\forall x((\forall y\ (y \in x \rightarrow \exists z\ (z \in y)) \wedge \forall y \forall u\ (y \in x \wedge u \in x \rightarrow y = u \vee \neg \exists v\ (v \in y \wedge v \in u))) \rightarrow \exists w(\forall y\ (y \in x \rightarrow \exists z\ (z \in y \wedge z \in w \wedge \forall v\ (v \in y \wedge v \in w \rightarrow v = z)))))$

to otrzymamy system teorii mnogości nazywany ZFC.

Uwaga. Do aksjomatyki teorii ZF należą także *aksjomaty dla identyczności*:

- $\forall x\ (x = x)$
- $\forall x \forall y\ (x = y \rightarrow y = x)$
- $\forall x \forall y \forall z\ (x = y \wedge y = z \rightarrow x = z)$;
- $\forall x \forall y \forall z\ ((x = y \wedge x \in z \rightarrow y \in z))$;
- $\forall x \forall y \forall z\ ((x = y \wedge z \in x \rightarrow z \in y))$.

Uwaga. Używane tu (np. w schematach wyróżniania i zastępowania) terminy: *nieskończony* i *przeliczalny* należą do *metajęzyka*.

Fundamentalne znaczenie teorii mnogości dla współczesnej matematyki polega m.in. na tym, że wszystkie konstrukcje matematyczne wyrazić można za pomocą pojęcia zbioru oraz relacji należenia elementu do zbioru.

* * *

Przykład III.6.4.1.

Niech teraz f będzie funkcją z X w Y, niech $A \subseteq Y$, $B \subseteq Y$ oraz $A \subseteq B$. Wtedy:

$$f^{-1}[A] \subseteq f^{-1}[B].$$

Przypominamy (wiadomości ze szkoły lub z kursu Wstęp do Matematyki dla studentek pierwszego roku JiNoI), że stosujemy następujące oznaczenia.

Jeśli $f : X \longrightarrow Y$, $A \subseteq X$, $B \subseteq Y$, to:

$$f[A] = \{y \in Y :\ \exists x \in A\ f(x) = y\}$$

$$f^{-1}[B] = \{x \in X :\ \exists y \in B\ f(x) = y\}.$$

Zbiór $f[A]$ nazywamy *obrazem* zbioru A względem funkcji f, a $f^{-1}[B]$ *przeciwobrazem* zbioru B względem funkcji f.

Mamy zatem pokazać, że jeśli $f : X \longrightarrow Y$ oraz $A \subseteq B \subseteq Y$, to $f^{-1}[A] \subseteq f^{-1}[B]$.

Dla dowodu tej implikacji metodą drzew semantycznych należy:

- zapisać wszystkie założenia; w tym przypadku będą to formuły stwierdzające, że:
  - f jest funkcją z X w Y;
  - A jest zawarty w Y;
  - B jest zawarty w Y;
  - A jest zawarty w B;

- zapisać zaprzeczenie tezy, tj. formułę:
  $\neg\forall x(\exists y\,(y \in A \wedge y = f(x)) \to \exists y\,(y \in B \wedge y = f(x)))$
- zbudować drzewo semantyczne, w którego pniu umieszczono wszystkie wymienione wyżej formuły.

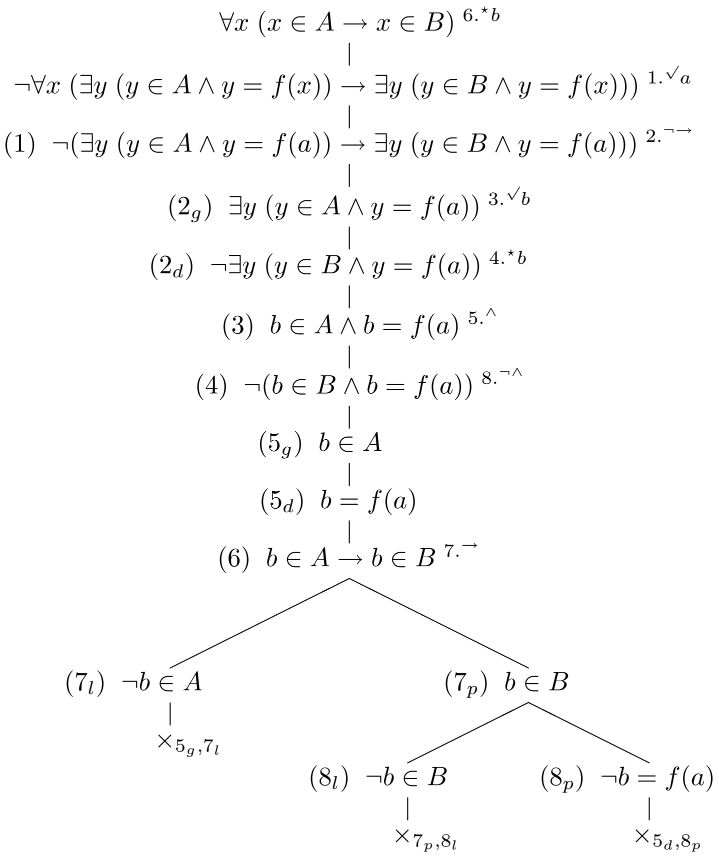
Jeśli drzewo semantyczne zbudowane z powyższych formuł (umieszczonych w jego pniu) będzie zamknięte, to teza zostanie udowodniona.

Tak się akurat składa, że do zakończenia rozważanego dowodu (czyli do zamknięcia wszystkich gałęzi rozważanego drzewa) wystarczy uwzględnienie jedynie dwóch z wymienionych wyżej formuł, a mianowicie:

$$\forall x\,(x \in A \to x \in B)$$

$$\neg\forall x(\exists y\,(y \in A \wedge y = f(x)) \to \exists y\,(y \in B \wedge y = f(x))).$$

Oto stosowne drzewo:



Zauważmy, że do zamknięcia wszystkich gałęzi tego drzewa nie tylko nie były potrzebne informacje, że f jest funkcją, ale także reguły dotyczące predykatu identyczności.

PRZYKŁAD III.6.4.2.

Niech (w jakimś uniwersum złożonym ze zbiorów) dane będą:

- dwuargumentowa funkcja $\triangle$,
- dwuargumentowa relacja $\prec$.

Wartość funkcji $\triangle$ dla argumentów x oraz y oznaczać będziemy przez $x \triangle y$.

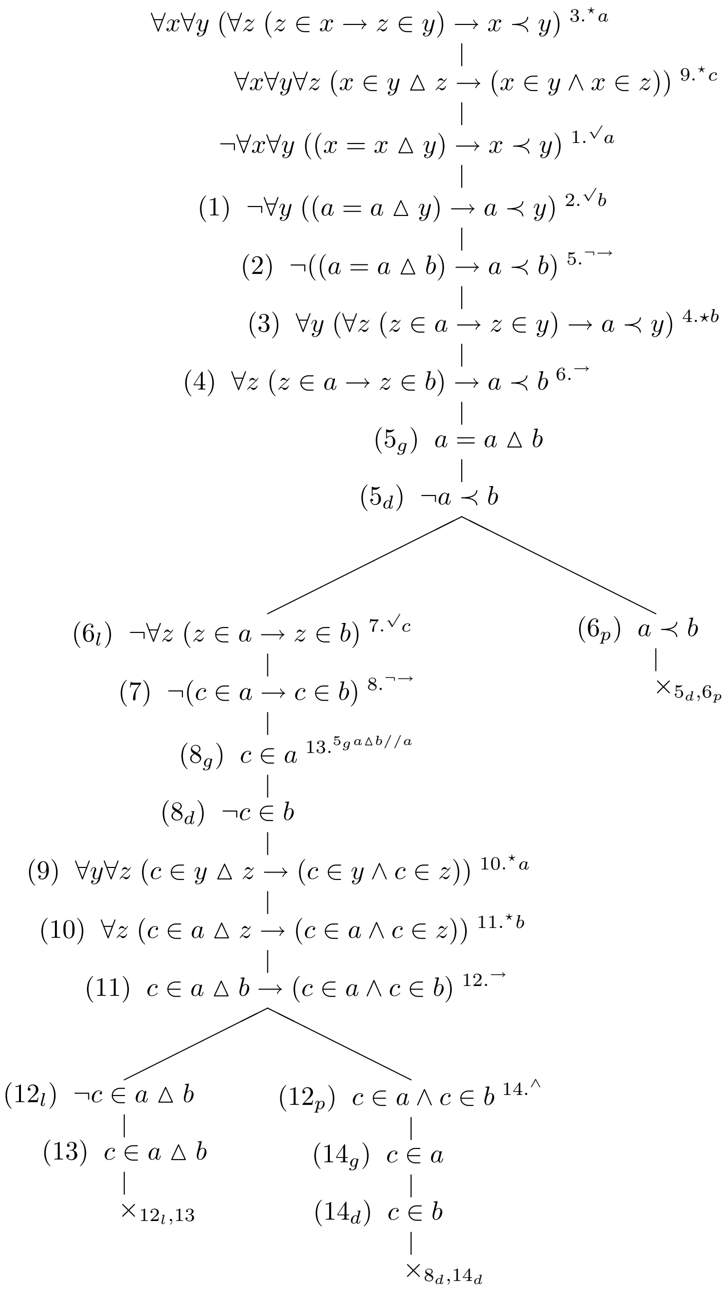
Załóżmy, że $\triangle$ i $\prec$ spełniają warunki:

- (a) $\forall x \forall y\, (\forall z\, (z \in x \rightarrow z \in y) \rightarrow x \prec y)$
- (b) $\forall x \forall y \forall z\, ((x \in y \vartriangle z \rightarrow (x \in y \wedge x \in z))$.

Pokażemy, że wtedy:

$$(c) \quad \forall x \forall y\, ((x = x \vartriangle y) \rightarrow x \prec y).$$

Budujemy drzewo, w którego pniu umieszczamy warunki (1) i (2) oraz zaprzeczenie warunku (3):



Wszystkie gałęzie drzewa są zamknięte, a więc udowodniliśmy, że (c) wynika logicznie z (a) oraz (b).

Przykład III.6.4.3.

Udowodnimy, że dla dowolnych funkcji f, g oraz h:

$$(✠)\quad \forall x \forall y\ ((x = y \wedge f(y) = g(y)) \rightarrow (h(f(x)) = h(g(y)))).$$

Oczywiście, milcząco zakładamy tu, że dziedziny i przeciwdziedziny rozważanych funkcji są dobrze określone.

Budujemy drzewo semantyczne, w którego korzeniu umieszczamy zaprzeczenie warunku (✠). Założenia, iż f, g oraz h są funkcjami będą wykorzystywane w regułach identyczności (podstawiania termów).

$$\begin{array}{c}
\neg\forall x\forall y\ ((x = y \wedge f(y) = g(y)) \rightarrow h(f(x)) = h(g(y)))\ ^{1.\surd a} \\
| \\
(1)\ \neg\forall y\ ((a = y \wedge f(y) = g(y)) \rightarrow h(f(a)) = h(g(y)))\ ^{2.\surd b} \\
| \\
(2)\ \neg((a = b \wedge f(b) = g(b)) \rightarrow h(f(a)) = h(g(b)))\ ^{3.\neg\rightarrow} \\
| \\
(3_g)\ a = b \wedge f(b) = g(b)\ ^{4.\wedge} \\
| \\
(3_d)\ \neg h(f(a)) = h(g(b))\ ^{5.4_g a//b} \\
| \\
(4_g)\ a = b \\
| \\
(4_d)\ f(b) = g(b)\ ^{6.4_g a//b} \\
| \\
(5)\ \neg h(f(a)) = h(g(a))\ ^{7.6 f(a)//g(a)} \\
| \\
(6)\ f(a) = g(a) \\
| \\
(7)\ \neg h(f(a)) = h(f(a)) \\
| \\
\times_7
\end{array}$$

Otrzymujemy drzewo zamknięte, a zatem udowodniliśmy warunek (✠).

* * *

PRZYKŁAD III.6.5: PIĄTY — INDUKCJA MATEMATYCZNA.

Rozszerzymy teraz system arytmetyki Robinsona poprzez dodanie do jego aksjomatów ***schematu*** aksjomatów, zwanego ***zasadą indukcji***. Otrzymany w ten sposób system nazywa się ARYTMETYKĄ PEANA.

Stałe pozalogiczne Arytmetyki Peana są takie same, jak w Arytmetyce Robinsona:

σ — jednoargumentowy symbol funkcyjny; wyrażenie $\sigma(t)$, gdzie t jest dowolnym termem, czytamy: *następnik t*;

$\oplus$ — dwuargumentowy symbol funkcyjny; wyrażenie $\oplus(t_1, t_2)$, gdzie t_1, t_2 są dowolnymi termami, czytamy: *suma* t_1 i t_2;

$\otimes$ — dwuargumentowy symbol funkcyjny; wyrażenie $\otimes(t_1, t_2)$, gdzie t_1, t_2 są dowolnymi termami, czytamy: *iloczyn* t_1 i t_2;

$\bigcirc$ — stała indywiduowa; symbol $\bigcirc$ czytamy: *zero*.

AKSJOMATYKA ARYTMETYKI PEANA:

Aksjomaty identyczności dla symboli $\bigcirc$, σ, $\oplus$ oraz $\otimes$ są takie same, jak w Arytmetyce Robinsona.

Aksjomaty specyficzne Arytmetyki Peana:

P_1: $\forall x \forall y\ (x \neq y \rightarrow \sigma(x) \neq \sigma(y))$

P_2: $\forall x\ (\bigcirc \neq \sigma(x))$

P_3: $\forall x\ (x \neq \bigcirc \rightarrow \exists y\ (x = \sigma(y)))$

P_4: $\forall x\ (\oplus(x, \bigcirc) = x)$

P_5: $\forall x \forall y\ (\oplus(x, \sigma(y)) = \sigma(\oplus(x, y)))$

P_6: $\forall x\ (\otimes(x, \bigcirc) = \bigcirc)$

P_7: $\forall x \forall y\ (\otimes(x, \sigma(y)) = \oplus(\otimes(x, y), x))$

P_8: $(A(\bigcirc) \wedge \forall x\ (A(x) \rightarrow A(\sigma(x)))) \rightarrow \forall x\ A(x)$
(dla dowolnej formuły A, o jednej zmiennej wolnej, języka Arytmetyki Peana).

P_8 nie jest jednym aksjomatem, lecz schematem (przeliczalnie wielu) aksjomatów. P_8 nazywamy *zasadą indukcji.*

Pokażemy, jak z zasady indukcji wywieść jeden z aksjomatów arytmetyki Robinsona, a mianowicie aksjomat:

$$A_3:\ \ \forall x\ (x \neq \bigcirc \rightarrow \exists y\ (x = \sigma(y))).$$

Niech $F(x)$ będzie formułą $x \neq \bigcirc \rightarrow \exists y\ (x = \sigma(y))$.

Schemat indukcji zastosowany do formuły $F(x)$ ma postać:

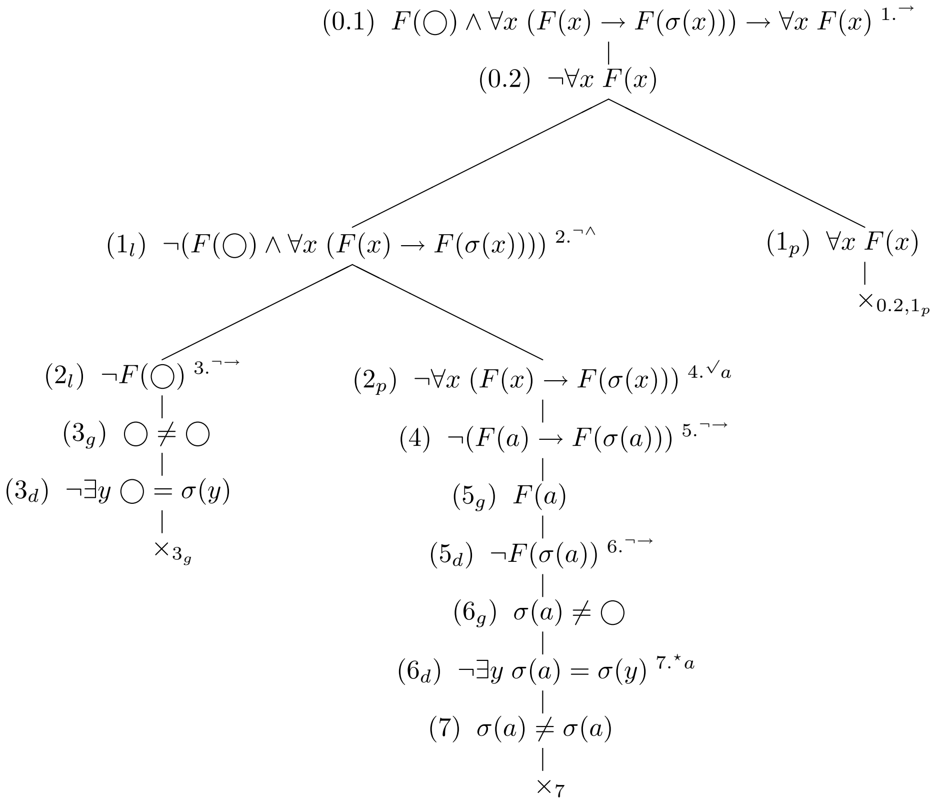
$$(F(\bigcirc) \wedge \forall x\ (F(x) \rightarrow F(\sigma(x)))\ \rightarrow)\forall x\ F(x).$$

Aby wykazać, że A_3 wynika logicznie z aksjomatu indukcji wystarczy wykluczyć, że jednocześnie:

- aksjomat indukcji (dla formuły $F(x)$) jest prawdziwy;
- aksjomat A_3 jest fałszywy.

Trzeba więc pokazać, że drzewo semantyczne, w którego pniu umieszczamy aksjomat indukcji oraz zaprzeczenie aksjomatu A_3 ma wszystkie gałęzie zamknięte.

Budujemy drzewo:



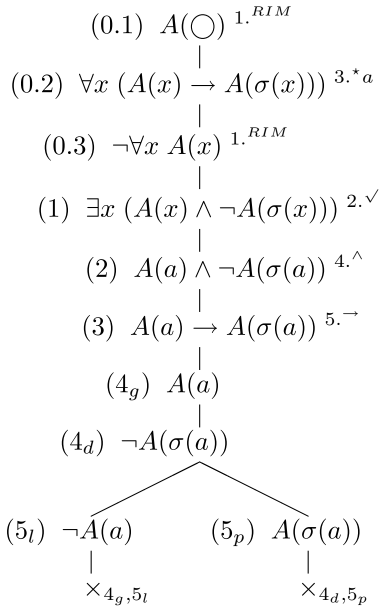
Wszystkie gałęzie drzewa są zamknięte. Tak więc, pokazaliśmy, że A_3 wynika logicznie z aksjomatu indukcji.

Rozważmy następującą regułę wnioskowania:

$$\frac{\begin{array}{c} A(\bigcirc) \\ \neg\forall x\, A(x) \end{array}}{\exists x\, (A(x) \land \neg A(\sigma(x)))}$$

gdzie $A(x)$ jest dowolną formułą języka Arytmetyki Peana z jedną zmienną wolną. Nazwiemy ją ***regułą indukcji matematycznej*** (w skrócie: RIM).

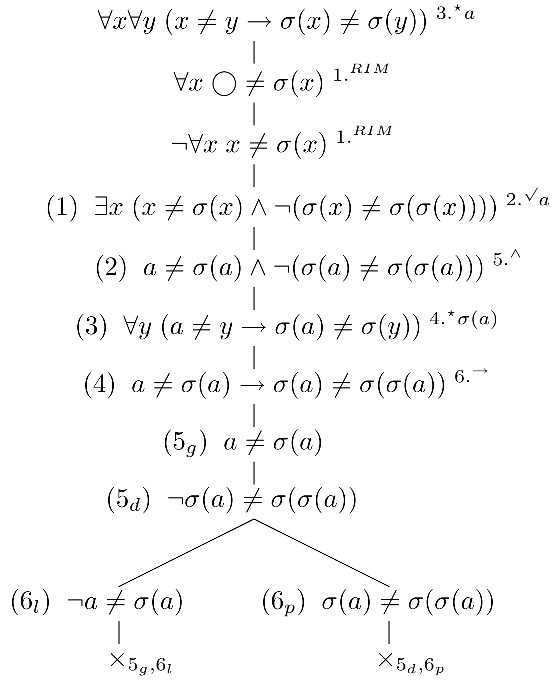
Jeśli do aksjomatów P_1–P_7 dołączyć regułę RIM, to można udowodnić — co samo w sobie nie jest zaskakujące — zasadę indukcji P_8. W tym celu wystarczy dowieść, że z przesłanek $A(\bigcirc)$ oraz $\forall x\, (A(x) \to A(\sigma(x)))$ wynika logicznie wniosek $\forall x\, A(x)$, dla dowolnej formuły $A(x)$ języka Arytmetyki Peana z jedną zmienną wolną. Budujemy więc drzewo, w którego pniu umieszczamy powyższe przesłanki oraz zaprzeczony wniosek:



Formuła o numerze (1) jest tu wnioskiem z przesłanek o numerach (0.1) oraz (0.3) wedle reguły RIM.

Wszystkie gałęzie drzewa są zamknięte, a zatem dowiedliśmy, że zasada indukcji P_8 może zostać wyprowadzona z reguły indukcji RIM.

Rozważmy jeszcze jedno zastosowanie reguły indukcji RIM. Jak już wspomniano, w Arytmetyce Robinsona nie można udowodnić, że $\forall x\, x \neq \sigma(x)$. Pokażemy, że zdanie to można udowodnić z aksjomatów A_1 oraz A_2 Arytmetyki Robinsona oraz reguły RIM. Budujemy drzewo, w którego pniu umieszczamy A_1, A_2 oraz $\neg\forall x\, x \neq \sigma(x)$. Formułą $A(y)$, która wystąpi w przesłankach reguły RIM jest formuła $\forall x\,(y \neq \sigma(x))$.



Wszystkie gałęzie drzewa są zamknięte, a zatem z A_1 oraz A_2 wynika logicznie wniosek $\forall x\, x \neq \sigma(x)$.

* * *

Uwaga. Przykłady III.6.1. oraz III.6.5. różnią się od przykładów III.6.2. oraz III.6.3. pod następującym względem:

- teorie arytmetyczne budowane były w celu charakterystyki ***jednego*** modelu zamierzonego — uniwersum „prawdziwych" liczb naturalnych wraz z określonymi na nich operacjami; podobnie rzecz się ma np. z teoriami geometrycznymi;
- teorie algebraiczne (wymienione tu: teoria grup, teoria algebr Boole'a, a także liczne inne, np.: teoria pierścieni, teoria ciał, teoria krat, teoria półgrup, itd.) budowane były w celu charakterystyki obszernej klasy ***różnych*** modeli, spełniających tylko wspólne aksjomaty bardzo ogólnej natury.

O pewnych zależnościach między możliwością *kategorycznego* (tj. jednoznacznego, z dokładnością do izomorfizmu) opisu struktur matematycznych a ufnością w stosowany aparat inferencyjny (tj. np. w *pełność* używanego systemu logicznego) piszemy w rozdziale IV.

* * *

6.3. Prefiksowe postacie normalne i skolemizacja

W KRZ każda formuła jest inferencyjnie równoważna pewnej formule w koniunkcyjnej postaci normalnej (KPN), a także pewnej formule w alternatywnej postaci normalnej (APN). Fakt ten może być wykorzystany w dowodzie twierdzenia o pełności KRZ, ma także inne zastosowania.

W KRP również dysponujemy metodą sprowadzania dowolnej formuły języka tego rachunku do pewnej standardowej postaci normalnej. Pokażemy mianowicie, że dowolna formuła języka KRP jest równoważna formule, która rozpoczyna się ciągiem kwantyfikatorów, po którym następuje formuła bez kwantyfikatorów. Nadto, pokażemy, że poprzez wprowadzenie nowych symboli funkcyjnych można wyeliminować wszystkie kwantyfikatory egzystencjalne z owego ciągu.

Mówimy, że formuły A i B języka KRP są ***inferencyjnie równoważne***, gdy drzewo semantyczne formuły $\neg(A \equiv B)$ jest zamknięte.

Mówimy, że formuły A i B języka KRP są ***równospełnialne***, gdy zbiór $\{A\}$ jest semantycznie niesprzeczny wtedy i tylko wtedy, gdy zbiór $\{B\}$ jest semantycznie niesprzeczny.

Mówimy, że formuła A języka KRP jest w ***prefiksowej postaci normalnej***, gdy jest ona postaci $Q_1x_1 \ldots Q_nx_n\ B$, gdzie B jest formułą bez kwantyfikatorów, a każdy symbol Q_i jest jednym z kwantyfikatorów: $\forall$ lub $\exists$. Jeśli w dodatku B jest w KPN, to mówimy, że A jest w ***koniunkcyjnej prefiksowej postaci normalnej***. Ciąg $Q_1x_1 \ldots Q_nx_n$ nazywamy ***prefiksem*** formuły A, a formułę B jej ***matrycą***.

Przez ***formułę uniwersalną*** rozumiemy każdą formułę w prefiksowej postaci normalnej, w której prefiksie występują jedynie kwantyfikatory generalne.

W następującym Lemacie przywołuje się równoważności, na mocy których możemy przekształcać dowolną formułę języka KRP w odpowiadającą jej (inferencyjnie równoważną) formułę w prefiksowej postaci normalnej. Intuicyjnie mówiąc, Lemat ten daje wskazówki, jak „wyciągać" kwantyfikatory z formuły do jej prefiksu (z zachowaniem inferencyjnej równoważności).

LEMAT 6.3.1. Dla dowolnego ciągu kwantyfikatorów $\overrightarrow{Qx} = Q_1x_1 \ldots Q_nx_n$ oraz dowolnych formuł A i B zachodzą następujące równoważności:

$\overrightarrow{Qx}\neg\forall yA \equiv \overrightarrow{Qx}\exists y\neg A$.
$\overrightarrow{Qx}\neg\exists yA \equiv \overrightarrow{Qx}\forall y\neg A$.
$\overrightarrow{Qx}(\forall yA \vee B) \equiv \overrightarrow{Qx}\forall z(A(z/y) \vee B)$.
$\overrightarrow{Qx}(A \wedge \forall yB) \equiv \overrightarrow{Qx}\forall z(A \wedge B(z/y))$.
$\overrightarrow{Qx}(\exists yA \wedge B) \equiv \overrightarrow{Qx}\exists z(A(z/y) \wedge B)$.
$\overrightarrow{Qx}(A \wedge \exists yB) \equiv \overrightarrow{Qx}\exists z(A \wedge B(z/y))$.
$\overrightarrow{Qx}(\forall yA \vee B) \equiv \overrightarrow{Qx}\forall z(A(z/y) \vee B)$.
$\overrightarrow{Qx}(A \vee \forall yB) \equiv \overrightarrow{Qx}\forall z(A \vee B(z/y))$.

$\overrightarrow{Qx}(\exists yA \vee B) \equiv \overrightarrow{Qx}\exists z(A(z/y) \vee B)$.
$\overrightarrow{Qx}(A \vee \exists yB) \equiv \overrightarrow{Qx}\exists z(A \vee B(z/y))$.
$\overrightarrow{Qx}(\forall yA \to B) \equiv \overrightarrow{Qx}\exists z(A(z/y) \to B)$.
$\overrightarrow{Qx}(A \to \forall yB) \equiv \overrightarrow{Qx}\forall z(A \to B(z/y))$.
$\overrightarrow{Qx}(\exists yA \to B) \equiv \overrightarrow{Qx}\forall z(A(z/y) \to B)$.
$\overrightarrow{Qx}(A \to \exists yB) \equiv \overrightarrow{Qx}\exists z(A \vee B(z/y))$.

We wszystkich tych równoważnościach z jest zmienną nie występującą po lewej stronie równoważności.

Dowód. Pozostawiamy czytelniczkom jako ćwiczenie pokazanie, że drzewa semantyczne negacji wszystkich powyższych równoważności są zamknięte.

Uwaga. Będziemy traktować spójnik równoważności materialnej $\equiv$ jako skrót definicyjny. Inaczej mówiąc, każdą formułę postaci $A \equiv B$ zapisujemy jako $(A \to B) \wedge (B \to A)$.

Twierdzenie 6.3.2. Dla dowolnej formuły A języka KRP istnieje równoważna jej formuła A' w prefiksowej postaci normalnej, o tych samych zmiennych wolnych co A. Każdą taką formułę A' nazywamy ***prefiksową postacią normalną*** formuły A.

Dowód. Przez indukcję po budowie formuły A. W krokach indukcyjnych należy skorzystać z lematu 6.3.1. Szczegóły pozostawiamy czytelniczkom.

Lemat 6.3.3. Dla dowolnego zdania $A = \forall x_1 \dots \forall x_n \exists yB$ języka KRP sygnatury σ zdanie

$$A' = \forall x_1 \dots \forall x_n B(f(\forall x_1, \dots, x_n))$$

gdzie f jest nowym symbolem funkcyjnym spoza σ, jest równospełnialne z A.

Dowód. Niech $\sigma' = \sigma \cup \{f\}$. Jeśli $\mathfrak{M}'$ jest strukturą sygnatury σ' i $\mathfrak{M}' \models A'$, to dla struktury $\mathfrak{M}$ otrzymanej z $\mathfrak{M}'$ przez opuszczenie interpretacji symbolu f zachodzi $\mathfrak{M} \models A$. Z drugiej strony, jeśli $\mathfrak{M}$ jest strukturą sygnatury σ i $\mathfrak{M} \models A$, to możemy rozszerzyć $\mathfrak{M}$ do struktury $\mathfrak{M}'$ przez zdefiniowanie denotacji $\Delta_{\mathfrak{M}'}(f)$ w taki sposób, aby dla wszystkich $\Delta_{\mathfrak{M}'}(a_1), \dots, \Delta_{\mathfrak{M}'}(a_n) \in \mathit{dom}(\mathfrak{M}') = \mathit{dom}(\mathfrak{M})$ zachodziło $\mathfrak{M} \models A(f(a_1, \dots, a_n)/y)$. Wtedy także $\mathfrak{M}' \models A'$.

Twierdzenie 6.3.4. Dla dowolnego zdania A języka KRP sygnatury σ istnieje formuła uniwersalna A' w języku KRP sygnatury σ rozszerzonej o nowe symbole funkcyjne taka, że A oraz A' są równospełnialne.

Dowód. Na mocy Twierdzenia 6.3.2. wystarczy założyć, że A jest w koniunkcyjnej postaci normalnej. Niech $y_1, \dots y_n$ będą wszystkimi zmiennymi egzystencjalnie skwantyfikowanymi w A (w porządku ich wystąpienia w prefiksie A). Dla każdego $\leqslant i \leqslant n$ niech $x_1, \dots, x_{n_i}$ będą wszystkimi zmiennymi generalnie skwantyfikowanymi poprzedzającymi y_i w prefiksie A. Rozszerzamy sygnaturę σ przez dodanie dla każdego $\leqslant i \leqslant n$ nowego n_i symbolu funkcyjnego f_i. Formułę A' otrzymujemy z formuły A przez usunięcie z prefiksu A wszystkich kwantyfikatorów egzystencjalnych oraz zastąpienie wszystkich wystąpień y_i przez $f_i(x_1, \dots, x_{n_i})$. Dla wykazania, że A' jest równospełnialna z A wystarczy n razy zastosować Lemat 6.3.3.

Każdą formułę A' spełniającą tezę powyższego twierdzenia nazywamy ***skolemową postacią normalną*** formuły A.

Na mocy powyższego twierdzenia tworzenie drzew semantycznych dla (negacji) dowolnych formuł języka KRP można sprowadzić do tworzenia drzew semantycznych dla (negacji) formuł uniwersalnych. Zobaczymy w dwóch następnych podrozdziałach, jakie fakt ten ma znaczenie.

Przykłady. 6.3.5.

Rozważmy dwie formuły:

- (1) $\forall x \exists y P(x, y) \vee \neg \exists x \forall y Q(x, y)$
- (2) $\forall x \forall y (\exists z (P(x, z) \wedge P(y, z)) \to \exists u Q(x, y, u))$.

Formułę w prefiksowej postaci normalnej równoważną inferencyjnie z (1) możemy znaleźć np. w następujący sposób:

$\forall x \exists y P(x,y) \vee \neg \exists x \forall y Q(x,y)$
$\forall u (\exists y P(u,y) \vee \neg \exists x \forall y Q(x,y))$
$\forall u \exists v (P(u,v) \vee \neg \exists x \forall y Q(x,y))$
$\forall u \exists v (P(u,v) \vee \forall x \neg \forall y Q(x,y))$
$\forall u \exists v (P(u,v) \vee \forall x \exists y \neg Q(x,y))$
$\forall u \exists v \forall w (P(u,v) \vee \exists y \neg Q(w,y))$
$\forall u \exists v \forall w \exists z (P(u,v) \vee \neg Q(w,z))$.

Formułę w prefiksowej postaci normalnej równoważną inferencyjnie z (2) możemy znaleźć np. w następujący sposób:

$\forall x \forall y (\exists z (P(x,z) \wedge P(y,z)) \rightarrow \exists u Q(x,y,u))$
$\forall x \forall y \forall w ((P(x,w) \wedge P(y,w)) \rightarrow \exists u Q(x,y,u))$
$\forall x \forall y \forall w \exists z ((P(x,w) \wedge P(y,w)) \rightarrow Q(x,y,z))$.

Możliwymi postaciami skolemowymi formuł (1) oraz (2) są np.:

- $(1)'$ $\forall u \forall w (P(u, f(u)) \vee \neg Q(w, g(u,w)))$
- $(2)'$ $\forall x \forall y \forall w ((P(x,w) \wedge P(y,w)) \rightarrow Q(x,y,f(x,y,w)))$.

* * *

Jerzy Pogonowski
Zakład Logiki Stosowanej UAM
www.logic.amu.edu.pl