Logika Matematyczna 18, 19

Jerzy Pogonowski

Zakład Logiki Stosowanej UAM
www.logic.amu.edu.pl
pogon@amu.edu.pl

Metoda TA w KRP (2)

Wprowadzenie

W niniejszej, drugiej prezentacji dotyczącej metody TA w KRP omawiamy:

- prefiksowe postacie normalne formuł i skolemizację
- niektóre twierdzenia metalogiczne dotyczące KRP
- metodę TA w KRP z identycznością
- metodę TA w KRP z symbolami funkcyjnymi.

Do metody TA w KRP powrócimy jeszcze później, po omówieniu konsekwencji rezolucyjnej w KRP oraz pojęcia unifikacji.

TA w KRP a własności metalogiczne KRP

Wykorzystamy metodę TA w dowodach kilku twierdzeń metalogicznych dotyczących KRP.

Najpierw pokażemy, że formuły języka KRP można przekształcać na równoważne im (w ściśle określonym sensie) formuły w tzw. prefiksowych postaciach normalnych.

Przedstawimy też kilka ważnych twierdzeń metalogicznych dotyczących KRP, których dowody otrzymać można przy użyciu metody tablic analitycznych.

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 (tablicowo) formule, która rozpoczyna się ciągiem kwantyfikatorów, po którym następuje formuła bez kwantyfikatorów. Podobne twierdzenie o równoważności inferencyjnej zachodzi dla aksjomatycznego ujęcia KRP (zob. wykłady 20–21). Nadto, pokażemy, że poprzez wprowadzenie nowych symboli funkcyjnych można wyeliminować wszystkie kwantyfikatory egzystencjalne z owego ciągu.

Prefiksowe postacie normalne i skolemizacja

Mówimy, że formuły α i β języka KRP są ***inferencyjnie równoważne***, gdy tablica analityczna formuły $\neg(\alpha \equiv \beta)$ jest zamknięta.
Mówimy, że formuły α i β języka KRP są ***równospełnialne***, gdy zbiór $\{\alpha\}$ jest semantycznie niesprzeczny wtedy i tylko wtedy, gdy zbiór $\{\beta\}$ jest semantycznie niesprzeczny.

Mówimy, że formuła α języka KRP jest w ***prefiksowej postaci normalnej***, gdy jest ona postaci $Q_1 x_1 \ldots Q_n x_n\ \beta$, gdzie β jest formułą bez kwantyfikatorów, a każdy symbol Q_i jest jednym z kwantyfikatorów: $\forall$ lub $\exists$. Jeśli w dodatku β jest w KPN, to mówimy, że α jest w ***koniunkcyjnej prefiksowej postaci normalnej***. Ciąg $Q_1 x_1 \ldots Q_n x_n$ nazywamy ***prefiksem*** formuły α, a formułę β jej ***matrycą***.

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

Prefiksowe postacie normalne i skolemizacja

Twierdzenie 1.
Dla dowolnego ciągu kwantyfikatorów $\overrightarrow{Qx} = Q_1 x_1 \dots Q_n x_n$ oraz dowolnych formuł α i β zachodzą następujące równoważności:

- $\overrightarrow{Qx}\neg\forall y\alpha \equiv \overrightarrow{Qx}\exists y\neg\alpha$.
- $\overrightarrow{Qx}\neg\exists y\alpha \equiv \overrightarrow{Qx}\forall y\neg\alpha$.
- $\overrightarrow{Qx}(\forall y\alpha \vee \beta) \equiv \overrightarrow{Qx}\forall z(\alpha(y/z) \vee \beta)$.
- $\overrightarrow{Qx}(\alpha \wedge \forall y\beta) \equiv \overrightarrow{Qx}\forall z(\alpha \wedge \beta(y/z))$.
- $\overrightarrow{Qx}(\exists y\alpha \wedge \beta) \equiv \overrightarrow{Qx}\exists z(\alpha(y/z) \wedge \beta)$.
- $\overrightarrow{Qx}(\alpha \wedge \exists y\beta) \equiv \overrightarrow{Qx}\exists z(\alpha \wedge \beta(y/z))$.

Prefiksowe postacie normalne i skolemizacja

- $\overrightarrow{Qx}(\forall y\alpha \vee \beta) \equiv \overrightarrow{Qx}\forall z(\alpha(y/z) \vee \beta)$.
- $\overrightarrow{Qx}(\alpha \vee \forall y\beta) \equiv \overrightarrow{Qx}\forall z(\alpha \vee \beta(y/z))$.
- $\overrightarrow{Qx}(\exists y\alpha \vee \beta) \equiv \overrightarrow{Qx}\exists z(\alpha(y/z) \vee \beta)$.
- $\overrightarrow{Qx}(\alpha \vee \exists y\beta) \equiv \overrightarrow{Qx}\exists z(\alpha \vee \beta(y/z))$.
- $\overrightarrow{Qx}(\forall y\alpha \to \beta) \equiv \overrightarrow{Qx}\exists z(\alpha(y/z) \to \beta)$.
- $\overrightarrow{Qx}(\alpha \to \forall y\beta) \equiv \overrightarrow{Qx}\forall z(\alpha \to \beta(y/z))$.
- $\overrightarrow{Qx}(\exists y\alpha \to \beta) \equiv \overrightarrow{Qx}\forall z(\alpha(y/z) \to \beta)$.
- $\overrightarrow{Qx}(\alpha \to \exists y\beta) \equiv \overrightarrow{Qx}\exists z(\alpha \vee \beta(y/z))$.

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

Prefiksowe postacie normalne i skolemizacja

Twierdzenie 2.
Dla dowolnej formuły α języka KRP istnieje równoważna jej formuła α' w prefiksowej postaci normalnej, o tych samych zmiennych wolnych co α. Każdą taką formułę α' nazywamy ***prefiksową postacią normalną*** formuły α.

Twierdzenie 3.
Dla dowolnego zdania $\alpha = \forall x_1 \ldots \forall x_n \exists y \beta$ języka KRP sygnatury σ zdanie

$$\alpha' = \forall x_1 \ldots \forall x_n \beta(f(x_1, \ldots, x_n)),$$

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

Prefiksowe postacie normalne i skolemizacja

Twierdzenie 4.
Dla dowolnego zdania α języka KRP sygnatury σ istnieje formuła uniwersalna α' w języku KRP sygnatury σ rozszerzonej o nowe symbole funkcyjne taka, że α oraz α' są równospełnialne.

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

Na mocy powyższego twierdzenia tworzenie tablic analitycznych dla (negacji) dowolnych formuł języka KRP można sprowadzić do tworzenia tablic analitycznych dla (negacji) formuł uniwersalnych.

Przykłady

Formułę w prefiksowej postaci normalnej równoważną inferencyjnie z (1):

- (1) $\forall x \exists y P(x,y) \vee \neg \exists x \forall y Q(x,y)$

możemy znaleźć np. w następujący sposób:

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

Przykłady

Formułę w prefiksowej postaci normalnej równoważną inferencyjnie z (2):

- (2) $\forall x \forall y(\exists z(P(x,z) \wedge P(y,z)) \rightarrow \exists u Q(x,y,u))$

możemy znaleźć np. w następujący sposób:

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

Przykłady

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

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

Zwartość

Twierdzenie 5. ***Twierdzenie o zwartości.***
Zbiór zdań S języka KRP jest spełnialny wtedy i tylko wtedy, gdy każdy skończony podzbiór S jest spełnialny.

Z powyższego twierdzenia wynika, że zbiór zdań S języka KRP **nie** jest spełnialny wtedy i tylko wtedy, gdy ***pewien*** skończony podzbiór S **nie** jest spełnialny.

Twierdzenie Löwenheima-Skolema

Twierdzenie 6. ***Twierdzenie Löwenheima-Skolema.***
Jeśli przeliczalny zbiór zdań S języka KRP jest spełnialny (tj. ma model), to S ma model przeliczalny.

Dowód.
Rozważmy systematyczną tablicę analityczną D z założeń S i o korzeniu $\neg(\alpha \wedge \neg\alpha)$ dla dowolnego wybranego zdania α. Na mocy twierdzenia o trafności metody tablic analitycznych w KRP, D nie może być dowodem tablicowym formuły $\alpha \wedge \neg\alpha$ (gdyż to oznaczałoby, że $\alpha \wedge \neg\alpha$ jest tautologią KRP, co nie jest prawdą). Tablica D nie jest zatem sprzeczna, czyli zawiera gałąź otwartą P. Wtedy struktura $\mathfrak{M}^P$ zdefiniowana w dowodzie twierdzenia o pełności metody TA w KRP jest modelem zbioru S. Ponieważ istnieje przeliczalnie wiele termów bazowych języka KRP, więc $\mathfrak{M}^P$ jest przeliczalnym modelem S.

Twierdzenie Herbranda

Następujące twierdzenie wzmacnia twierdzenie o pełności metody TA w KRP, w tym sensie, że pozwala przechodzić od niespełnialności zbioru formuł uniwersalnych (lub nawet formuł ze zmiennymi wolnymi) języka KRP do niespełnialności pewnego zbioru formuł KRZ.

Twierdzenie 7. ***Twierdzenie Herbranda.***
Niech S będzie zbiorem formuł otwartych języka KRP. Wtedy zachodzi alternatywa:

- (a) S ma model Herbranda;
- (b) S nie jest spełnialny. W szczególności, istnieje skończenie wiele podstawień (termów bazowych za zmienne wolne) formuł z S takich, że koniunkcja formuł otrzymanych w wyniku tych podstawień nie jest spełnialna.

Twierdzenie Herbranda

Warunek (b) powyżej jest równoważny warunkowi:

- (c) Istnieje skończenie wiele podstawień (termów bazowych za zmienne wolne) negacji formuł z S takich, że alternatywa formuł otrzymanych w wyniku tych podstawień jest tautologią KRP. Zauważmy, że w tym przypadku możemy tak dobrać zmienne zdaniowe (z języka KRZ), że odpowiednia alternatywa tych zmiennych jest tautologią KRZ.

Ważnym wnioskiem z twierdzenia Herbranda jest następujące twierdzenie.

Twierdzenie 8.

Jeśli $\alpha(\overrightarrow{x})$ jest formułą bez kwantyfikatorów w języku KRP z co najmniej jedną stałą indywiduową, to $\exists \overrightarrow{x}\ \alpha(\overrightarrow{x})$ jest tautologią wtedy i tylko wtedy, gdy istnieją termy bazowe $\overrightarrow{t_i}$ takie, że alternatywa $\alpha(\overrightarrow{t_1}) \vee \ldots \vee \alpha(\overrightarrow{t_n})$ jest tautologią. [Wyrażenie $\overrightarrow{x}$ oznacza ciąg zmiennych wolnych. Podobnie, wyrażenie $\overrightarrow{t}$ oznacza ciąg termów bazowych.]

Twierdzenie Herbranda

Twierdzenie powyższe można również wzmocnić do twierdzenia następującego.

Twierdzenie 9.
Niech α będzie zdaniem w prefiksowej postaci normalnej (w języku L), a β formułą w prefiksowej postaci normalnej równoważną inferencyjnie (tablicowo) zdaniu $\neg\alpha$ oraz niech $\gamma(\overrightarrow{x})$ będzie otwartą skolemizacją formuły β (w języku L', tworzoną wedle konstrukcji podanej w twierdzeniu 3). Wtedy α jest tautologią wtedy i tylko wtedy, gdy istnieją termy bazowe $\overrightarrow{t_1}, \ldots, \overrightarrow{t_n}$ języka L' takie, że alternatywa $\neg\gamma(\overrightarrow{t_1}) \vee \ldots \vee \neg\gamma(\overrightarrow{t_n})$ jest tautologią.

(Formuła jest otwarta, jeśli zawiera zmienne wolne. W przeciwnym przypadku jest zamknięta.)

Twierdzenie Churcha

Precyzyjne sformułowanie twierdzenia Churcha wymagałoby wprowadzenia całego szeregu pojęć i twierdzeń związanych z matematyczną reprezentacją pojęcia ***obliczalności***. Na to w niniejszym elementarzu nie możemy sobie pozwolić.

W dotychczasowym programie studiów *Językoznawstwa i Informacji Naukowej* przewiduje się (na roku trzecim) osobne konwersatorium ***Funkcje Rekurencyjne***, poświęcone tej problematyce.

W planie studiów *Językoznawstwa i Nauk o Informacji* przewiduje się, również na roku trzecim, kurs ***Algorytmy i Obliczanie***, gdzie także planuje się omawianie tej problematyki.

Twierdzenie Churcha

Metoda tablic analitycznych jest jedynie ***półalgorytmem***, tj.:

- Jeśli α ***jest*** tautologią KRP, to isnieje tablicowy dowód α.
- Jeśli α ***nie jest*** tautologią KRP, to (systematyczna) tablica analityczna dla α może zawierać gałąź, którą należy przedłużać w nieskończoność; w konsekwencji, nie można ***w skończonej liczbie kroków*** wykazać z pomocą tablic analitycznych, że dana formuła ***nie jest*** tautologią KRP.

Powyższe ograniczenie nie dotyczy jedynie metody tablic analitycznych. **Twierdzenie Churcha** stwierdza, że nie istnieje metoda algorytmiczna ustalania, czy dowolna formuła α języka KRP jest, czy też nie jest tautologią tego rachunku.

Twierdzenie Churcha

Nie ma zatem efektywnej metody, tj. wykorzystującej jedynie z góry określone, mechaniczne kroki, która w skończonej liczbie takich kroków pozwoliłaby ***rozstrzygnąć***, dla dowolnej formuły α języka KRP, czy α jest, czy też nie jest tautologią tego rachunku. Rachunek predykatów jest ***nierozstrzygalny***.

Jak dowiemy się z następnych wykładów, istnieją metody syntaktyczne (np. metoda aksjomatyczna) takie, że ogół ***tez*** KRP pokrywa się ze zbiorem wszystkich tautologii KRP. Nie jest to żadna sprzeczność z wypowiedzianym przed chwilą twierdzeniem Churcha. W metodzie aksjomatycznej mówimy, że α jest ***tezą*** KRP, gdy ***istnieje*** dowód α z aksjomatów tego rachunku. I chociaż zbiór aksjomatów jest obliczalny (efektywnie podany), a także reguły wnioskowania są obliczalne, czego konsekwencją jest to, że pojęcie ***dowodu*** również jest obliczalne, to nie istnieje żadna efektywna metoda ograniczenia złożoności (np. długości) dowodu danej tezy.

Twierdzenie Churcha

Tak więc, chociaż wiemy, że dla dowolnej formuły α języka KRP, że:

- α jest tezą KRP wtedy i tylko wtedy, gdy α jest tautologią KRP,

to nie możemy z góry określić długości dowodów tez KRP. I to właśnie kryje się za nierozstrzygalnością KRP.

Więcej na ten temat dowiedzą się ci studenci, którzy dobrną do trzeciego roku studiów, od tych wykładowców, którzy momentu tego dożyją.
Na razie życzmy sobie nawzajem, aby obu stronom udało się ten program zrealizować.

Metoda TA dla KRP z identycznością

Jeśli pracujemy w języku KRP z identycznością, to identyczność jest traktowana w metodzie TA jako ***stała logiczna***. Trzeba zatem podać dodatkowe reguły dotyczące tablic atomowych zawierających predykat identyczności. Ponadto, twierdzenia o trafności oraz o pełności tablic analitycznych dla języka KRP z identycznością wymagają osobnych dowodów.

Identyczność jest relacją równoważności, czyli jest zwrotna, symetryczna oraz przechodnia. Nadto, przedmioty identyczne są nieodróżnialne, ani przez żadną własność, ani poprzez pozostawanie w zależnościach z innymi przedmiotami.

Zauważmy, że bez relacji identyczności praktycznie niewyobrażalne jest uprawianie większości dyscyplin matematycznych — współczesne rozumienie pojęcia ***funkcji***, jednego z najistotniejszych pojęć matematycznych, wykorzystuje relację identyczności.

Identyczność

Dla ***predykatu*** identyczności tradycyjnie używanym symbolem jest $=$ i tradycja ta zostanie tu uszanowana. To, że ***relację*** identyczności oznaczamy tym samym symbolem, nie powinno prowadzić do nieporozumień — z kontekstu zawsze będzie jasno wynikać, czy odnosimy się do predykatu (język), czy do relacji (odniesienie przedmiotowe języka, interpretacje).

Tak więc, identyczność termów t_1 oraz t_2 zapisywać będziemy formułą: $t_1 = t_2$. Formułę $\neg t_1 = t_2$ będziemy (także zgodnie z tradycją), zapisywać też czasem w postaci $t_1 \neq t_2$.

Identyczność

O predykacie identyczności zakłada się następujące aksjomaty:

- (1) $\forall x\ (x = x)$
- (2) $\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n\ ((x_1 = y_1 \wedge \ldots \wedge x_n = y_n) \rightarrow (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)))$
- (3) $\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n\ ((x_1 = y_1 \wedge \ldots \wedge x_n = y_n) \rightarrow (P(x_1, \ldots, x_n) \equiv Q(y_1, \ldots, y_n)))$.

dla wszystkich n-argumentowych symboli funkcyjnych f oraz wszystkich predykatów n-argumentowych, dla wszystkich n.

Zwrotność predykatu identyczności wyraża warunek (1). Własności: symetryczności oraz przechodniości predykatu identyczności, czyli:

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

są konsekwencją powyższych aksjomatów.

Tablice atomowe w języku KRP z identycznością

Tablicami atomowymi są, oprócz wymienionych w definicji TA dla KRP, również wszystkie drzewa postaci:

α $\vert$ $t_1 = t_2$ $\vert$ $\alpha(t_2//t_1)$	α $\vert$ $t_2 = t_1$ $\vert$ $\alpha(t_2//t_1)$

gdzie α jest dowolnym zdaniem języka KRP z identycznością, a t_1 oraz t_2 dowolnymi termami bazowymi tego języka, oraz gdzie $\alpha(t_2//t_1)$ jest formułą powstającą z α poprzez zastąpienie ***pewnych*** wystąpień termu t_1 wystąpieniami termu t_2.

Tablice analityczne w języku KRP z identycznością

Definicja ***tablic analitycznych*** w języku KRP z identycznością jest taka sama, jak definicja TA w KRP, przy czym tablice atomowe są teraz oczywiście rozumiane w sensie definicji podanej powyżej.

- Gałąź P tablicy analitycznej D jest ***sprzeczna***, jeśli:
  - α oraz $\neg\alpha$ występują w P, dla pewnego zdania α, ***lub***
  - $\neg(t = t)$ występuje w P, dla pewnego termu t.
- Tablica D jest ***sprzeczna***, jeśli każda gałąź w D jest sprzeczna.

Wszystkie pozostałe definicje z części (1) (tablice systematyczne, tablice zakończone, dowody tablicowe, itd.) przenoszą się automatycznie na przypadek języka KRP z identycznością.

Reguły tworzenia tablic analitycznych

Reguły dotyczące predykatu identyczności w metodzie tablic analitycznych można sprowadzić np. do następujących dwóch:

- Jeśli t_1 oraz t_2 są dowolnymi termami, α zawiera jakieś wystąpienia termu t_1, to gałąź tablicy zawierającą formuły α oraz $t_1 = t_2$ przedłużamy dodając formułę $\alpha(t_2//t_1)$:

$$R_{12}(=) \qquad \begin{array}{c} \alpha \\ | \\ t_1 = t_2 \\ | \\ \alpha(t_2//t_1) \end{array}$$

gdzie $\alpha(t_2//t_1)$ jest formułą powstającą z α poprzez zastąpienie pewnych wystąpień termu t_1 wystąpieniami termu t_2.

Reguły tworzenia tablic analitycznych

- Jeśli t_1 oraz t_2 są dowolnymi termami, α zawiera jakieś wystąpienia termu t_1, to gałąź drzewa zawierającą formuły α oraz $t_2 = t_1$ przedłużamy dodając formułę $\alpha(t_2//t_1)$:

$$R_{21}(=) \qquad \begin{array}{c} \alpha \\ | \\ t_2 = t_1 \\ | \\ \alpha(t_2//t_1) \end{array}$$

gdzie $\alpha(t_2//t_1)$ jest formułą powstającą z α poprzez zastąpienie pewnych wystąpień termu t_1 wystąpieniami termu t_2.

Umowa notacyjna. Zastosowanie reguły $R_{ij}(=)$ w kroku $^{n.}$ do formuły o numerze (m) z wykorzystaniem identyczności termów t_1 oraz t_2 wyrażonej w formule o numerze (k) zaznaczać będziemy umieszczonym z prawej strony formuły o numerze (m) komentarzem: $^{n.\,k,t_2//t_1}$.

Poprawność metody TA w KRP z identycznością

Chociaż nie możemy zagwarantować środkami czysto syntaktycznymi, że interpretacją predykatu identyczności jest relacja identyczności, to możemy mimo to zagwarantować, że metoda tablic analitycznych w języku KRP z identycznością jest trafna i pełna.

Zachodzi ***Twierdzenie o trafności metody tablic analitycznych w KRP z identycznością*** i jego dowód jest natychmiastowy.

Dla dowodu twierdzenia o pełności metody TA w KRP z identycznością trzeba wprowadzić pojęcie modelu ilorazowego.

Model ilorazowy

Niech $\mathfrak{M}$ będzie strukturą otrzymaną w twierdzeniu o pełności metody TA w KRP (pomijamy indeks odnoszący się do gałęzi, gdyż nie jest on tu istotny), dla systematycznej tablicy analitycznej D ze zbioru założeń S. Przypominamy, że elementami uniwersum $\mathfrak{M}$ są termy bazowe.

Definiujemy relację $\cong$ w uniwersum modelu $\mathfrak{M}$:

- $t_1 \cong t_2$ wtedy i tylko wtedy, gdy $\mathfrak{M} \models t_1 = t_2$.

Wtedy $\cong$ jest relacją równoważności w uniwersum modelu $\mathfrak{M}$. Niech $[t]$ oznacza klasę równoważności termu t względem tej relacji.

Budujemy ***model ilorazowy*** $\mathfrak{M}/_{\cong}$ w sposób następujący:

Model ilorazowy

- uniwersum modelu $\mathfrak{M}/_{\cong}$ to rodzina wszystkich klas równoważności relacji $\cong$.
- $f^{\mathfrak{M}/_{\cong}}([t_1], \ldots, [t_n]) = [f^{\mathfrak{M}}(t_1, \ldots, t_n)]$, dla każdego symbolu funkcyjnego f.
- $\mathfrak{M}/_{\cong} \models R([t_1], \ldots, [t_n])$ wtedy i tylko wtedy, gdy $\mathfrak{M} \models R(t_1, \ldots, t_n)$, dla każdego predykatu (różnego od predykatu identyczności).

W standardowy sposób pokazuje się, że jest to poprawna definicja, tj., że nie zależy ona od wyboru reprezentantów z poszczególnych klas równoważności $\cong$.

Interpretacja predykatu identyczności w modelu $\mathfrak{M}/_{\cong}$ jest relacją identyczności (a nie jakąkolwiek inną relacją równoważności spełniającą aksjomaty identyczności).

Pełność metody TA w KRP z identycznością

Twierdzenie 10. ***Pełność metody tablic analitycznych w KRP z identycznością.***
Dla dowolnego zbioru zdań S zawierającego aksjomaty identyczności zachodzi alternatywa:

- S jest tablicowo sprzeczny.
- Istnieje model dla S, w którym predykat identyczności interpretowany jest jako relacja identyczności.

Twierdzenia o trafności i pełności metody TA w KRP z identycznością gwarantują, że można poprawnie używać tej metody do rozwiązywania takich samych problemów, jak w KRP.

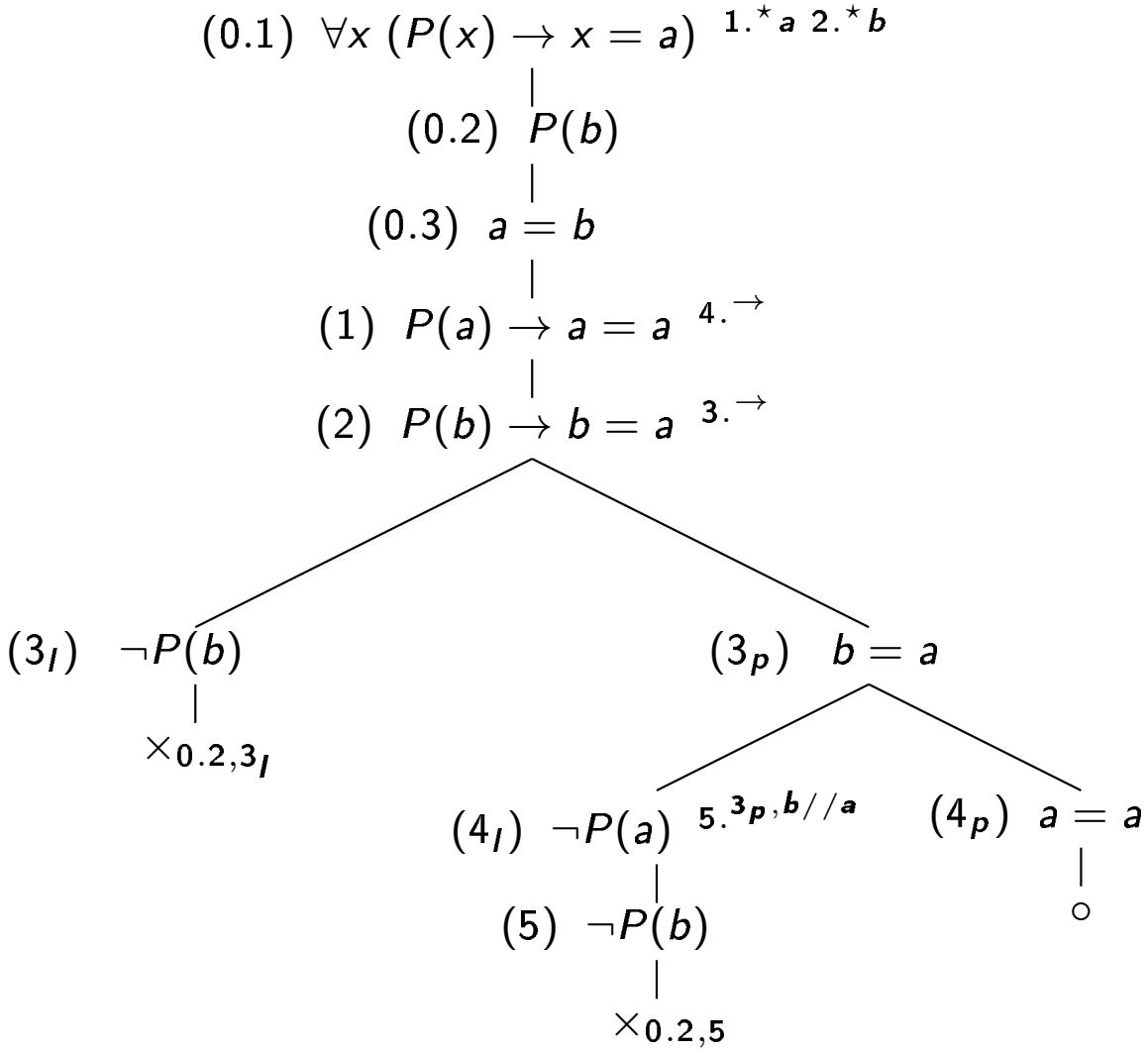
Przykład 1

Pokażemy, że następujące formuły tworzą zbiór semantycznie niesprzeczny:

$$\forall x\,(P(x) \to x = a)$$
$$P(b)$$
$$a = b$$

Przypuszczamy zatem, że podane wyżej formuły są prawdziwe w co najmniej jednej interpretacji. Przypuszczenie to zostanie potwierdzone, o ile tablica analityczna, tj. drzewo, w którego pniu umieszczamy te formuły będzie miało co najmniej jedną gałąź otwartą. Budujemy tablicę:

Przykład 1



Tablica ma gałąź otwartą. Zbiór semantycznie niesprzeczny.

Przykład 2

Pokażemy, że każda relacja, która jest jednocześnie symetryczna oraz antysymetryczna jest zawarta w relacji identyczności.

W tym celu wystarczy pokazać, że następująca reguła wnioskowania jest niezawodna:

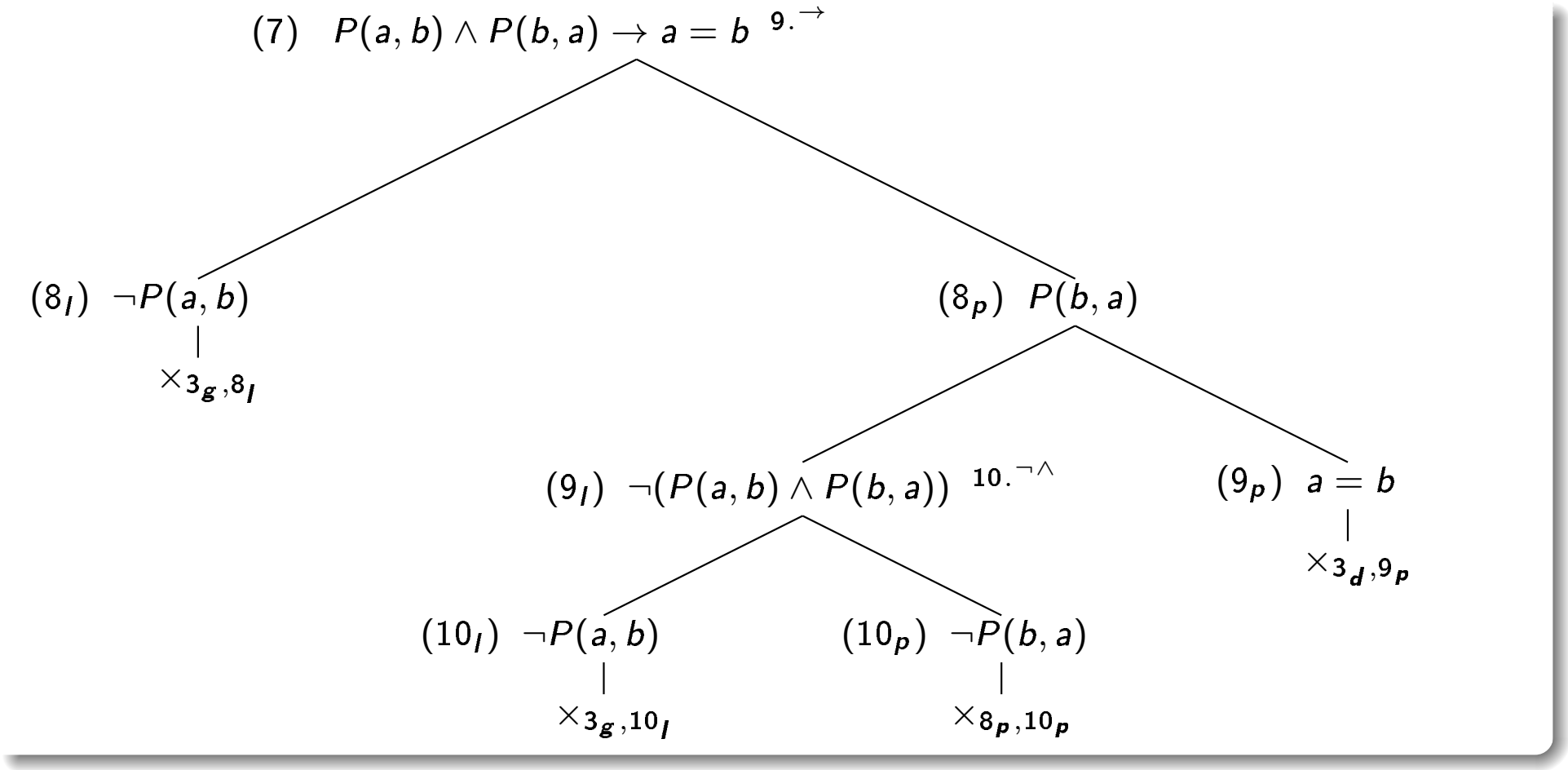
$$\frac{\forall x \forall y\ (P(x,y) \to P(y,x)) \qquad \forall x \forall y\ (P(x,y) \wedge P(y,x) \to x = y)}{\forall x \forall y\ (P(x,y) \to x = y)}$$

Budujemy tablicę analityczną, tj. drzewo, w którego pniu umieszczamy przesłanki oraz zaprzeczenie wniosku badanej reguły [ponieważ tablica nie mieści się na jednym slajdzie, przedstawiamy ją w dwóch częściach]:

Przykład 2

$$(0.1)\ \forall x \forall y\ (P(x,y) \to P(y,x))\ ^{4.\star a}$$
$$\Big|$$
$$(0.2)\ \forall x \forall y\ (P(x,y) \wedge P(y,x) \to x = y)\ ^{6.\star a}$$
$$\Big|$$
$$(0.3)\ \neg \forall x \forall y\ (P(x,y) \to x = y)\ ^{1.\checkmark a}$$
$$\Big|$$
$$(1)\ \neg \forall y\ (P(a,y) \to a = y)\ ^{2.\checkmark b}$$
$$\Big|$$
$$(2)\ \neg (P(a,b) \to a = b)\ ^{3.\neg \to}$$
$$\Big|$$
$$(3_g)\ P(a,b)$$
$$\Big|$$
$$(3_d)\ a \neq b$$
$$\Big|$$
$$(4)\ \forall y\ (P(a,y) \to yPa)\ ^{5.\star b}$$
$$\Big|$$
$$(5)\ P(a,b) \to P(a,b)\ ^{8.\to}$$
$$\Big|$$
$$(6)\ \forall y\ (P(a,y) \wedge P(y,a) \to a = y)\ ^{7.\star b}$$
$$\Big|$$
$$(7)\ P(a,b) \wedge P(b,a) \to a = b\ ^{9.\to}$$

Przykład 2



Tablica zamknięta. Reguła niezawodna.

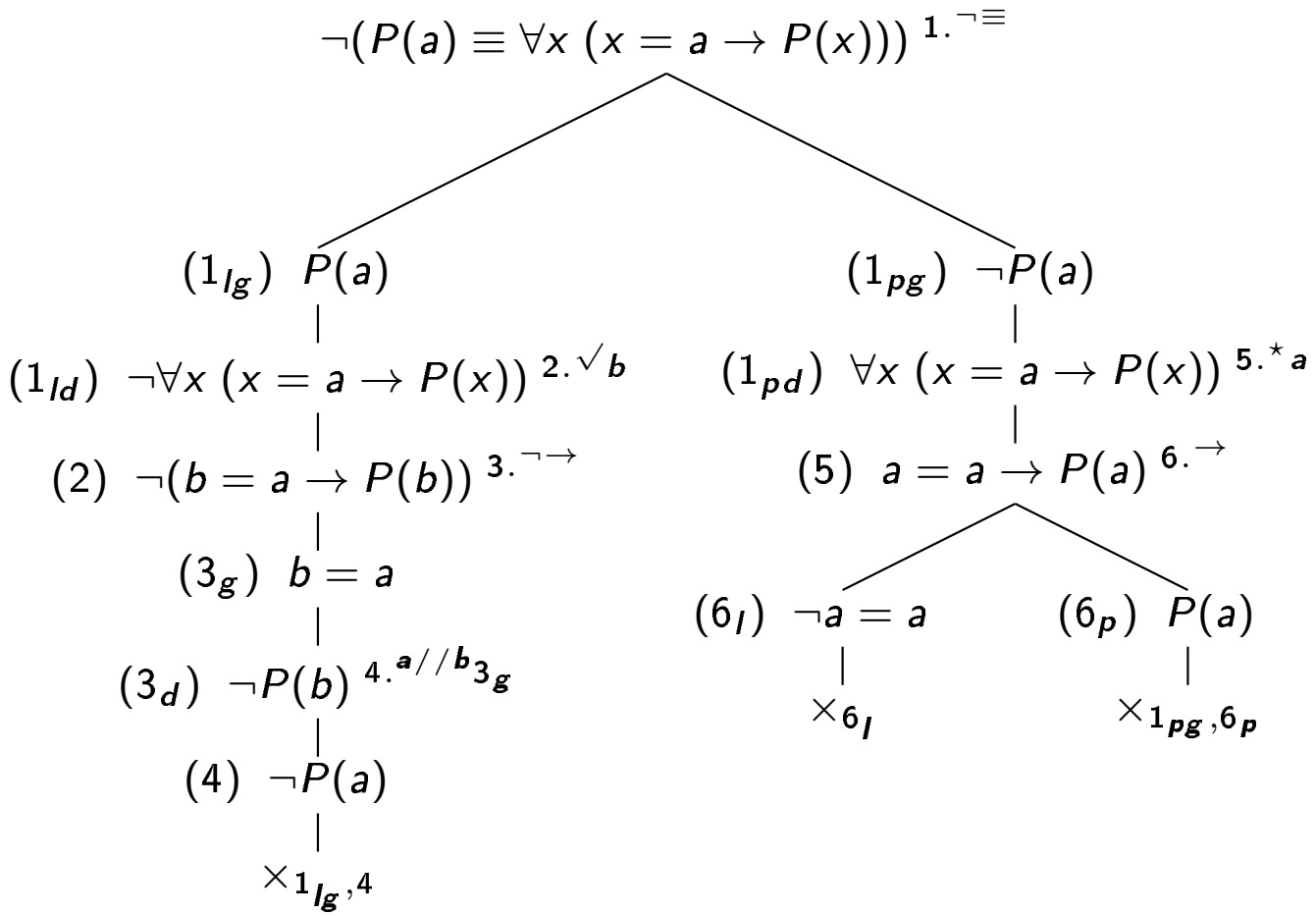
Przykład 3

Pokażemy, że następująca formuła jest tautologią KRP z identycznością:

$$P(a) \equiv \forall x\ (x = a \to P(x))$$

W tym celu wystarczy pokazać, że powyższa formuła ma dowód tablicowy, tj., że tablica analityczna jej negacji ma wszystkie gałęzie zamknięte:

Przykład 3



Tablica sprzeczna. Badana formuła jest tautologią KRP.

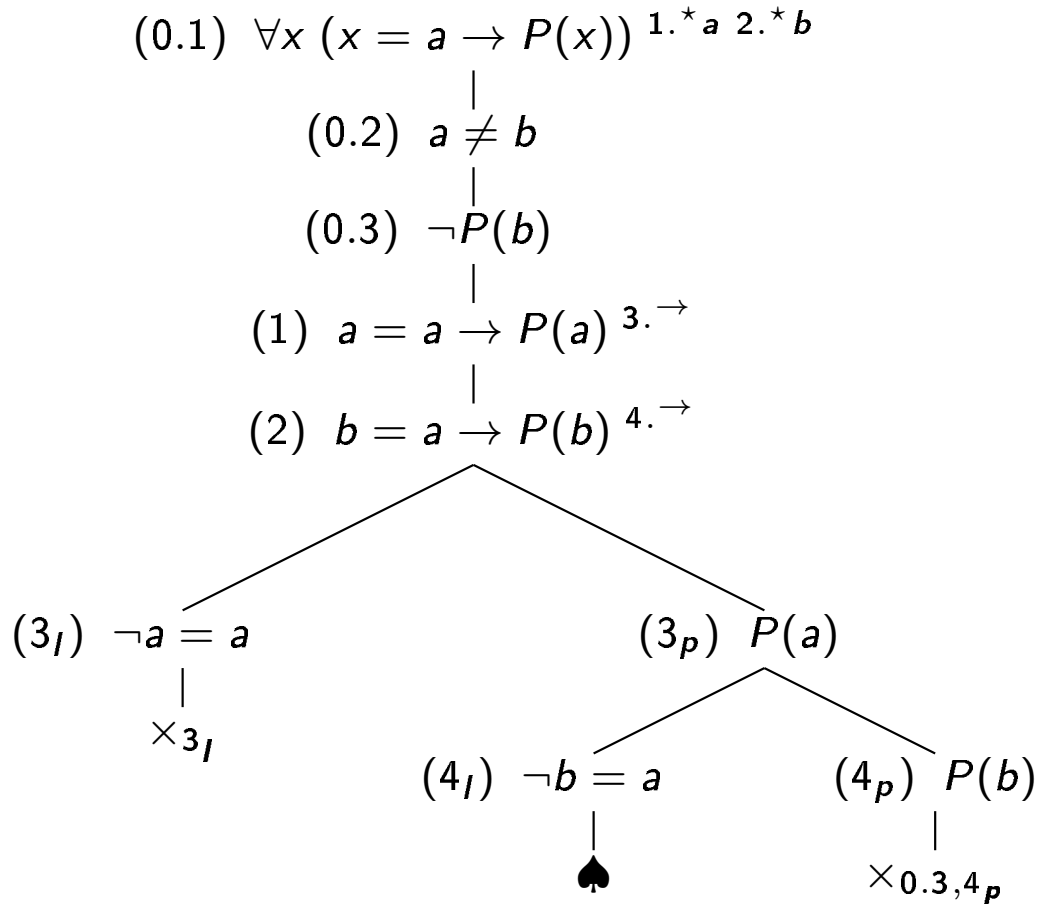
Przykład 4

Ustalimy, czy następująca reguła jest niezawodna:

$$\frac{\forall x(x = a \to P(x)) \qquad a \neq b}{P(b)}$$

Budujemy tablicę analityczną, tj. drzewo, w którego pniu umieszczamy przesłanki oraz zaprzeczony wniosek:

Przykład 4



Tablica ma gałąź otwartą. Badana reguła jest zawodna.

Metoda TA dla KRP z symbolami funkcyjnymi

Dokładniejsze omówienie działania metody TA dla KRP z symbolami funkcyjnymi odkładamy na nieco później. Zajmiemy się tym mianowicie dopiero po wprowadzeniu pojęcia ***unifikacji***, co nastąpi w wykładzie poświęconym konsekwencji ***rezolucyjnej*** w KRP.

Poniżej podajemy jedynie kilka prostych przykładów, w których nie trzeba odwoływać się do pojęcia unifikacji. Niektóre dowody zapisywane będą nie w postaci drzew, ale w postaci tabel, zawierających ponumerowane wiersze dowodu oraz stosowne komentarze dowodowe.

Przykład 4: Własności Funkcji

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

Ponieważ tablica jest sprzeczna, więc stanowi dowód warunku (✠):

Przykład 4: Własności Funkcji

$$\neg\forall x\forall y\,((x = y \wedge f(y) = g(y)) \to h(f(x)) = h(g(y)))\ ^{1.\checkmark a}$$
$$|$$
$$(1)\ \ \neg\forall y\,((a = y \wedge f(y) = g(y)) \to h(f(a)) = h(g(y)))\ ^{2.\checkmark b}$$
$$|$$
$$(2)\ \ \neg((a = b \wedge f(b) = g(b)) \to h(f(a)) = h(g(b)))\ ^{3.\neg\to}$$
$$|$$
$$(3_g)\ \ a = b \wedge f(b) = g(b)\ ^{4.\wedge}$$
$$|$$
$$(3_d)\ \ \neg h(f(a)) = h(g(b))\ ^{5.^{4g.a//b}}$$
$$|$$
$$(4_g)\ \ a = b$$
$$|$$
$$(4_d)\ \ f(b) = g(b)\ ^{6.^{4g.a//b}}$$
$$|$$
$$(5)\ \ \neg h(f(a)) = h(g(a))\ ^{7.^{6.f(a)//g(a)}}$$
$$|$$
$$(6)\ \ f(a) = g(a)$$
$$|$$
$$(7)\ \ \neg h(f(a)) = h(f(a))$$
$$|$$
$$\times_7$$

Arytmetyka Robinsona

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***.

Arytmetyka Robinsona

Aksjomaty dotyczące jedynie predykatu identyczności:

- $\forall x\ (x = x)$
- $\forall x \forall y\ (x = y \to y = x)$
- $\forall x \forall y \forall z\ ((x = y \wedge y = z) \to x = z)$.

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

- $\forall x \forall y\ (x = y \to \sigma(x) = \sigma(y))$
- $\forall x \forall y \forall z\ (x = y \to \oplus(x, z) = \oplus(y, z))$
- $\forall x \forall y \forall z\ (x = y \to \oplus(z, x) = \oplus(z, y))$
- $\forall x \forall y \forall z\ (x = y \to \otimes(x, z) = \otimes(y, z))$
- $\forall x \forall y \forall z\ (x = y \to \otimes(z, x) = \otimes(z, y))$.

Arytmetyka Robinsona

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

Arytmetyka Robinsona

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

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

Arytmetyka Robinsona

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

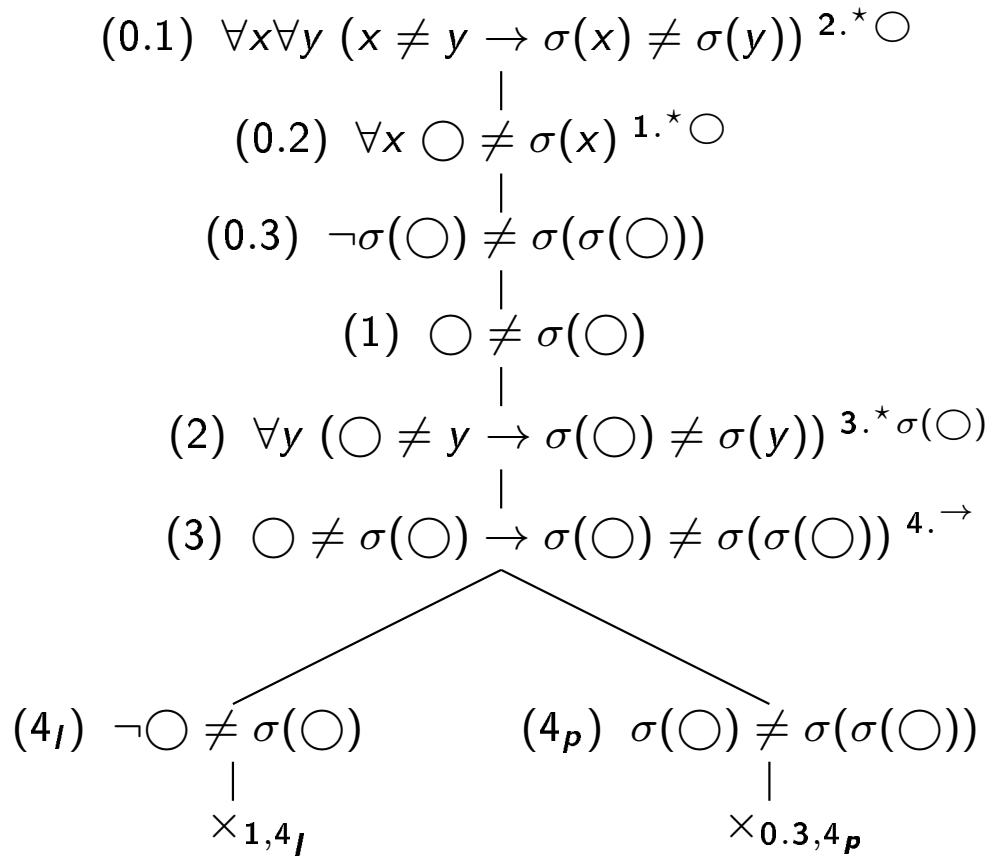
1.	$\forall x \ \oplus(x,\bigcirc) = x$	aksjomat A_4
2.	$\forall x \forall y \ \oplus(x,\sigma(y)) = \sigma(\oplus(x,y))$	aksjomat A_5
3.	$\neg(\oplus(\sigma(\sigma(\bigcirc)),\sigma(\sigma(\bigcirc))) = \sigma(\sigma(\sigma(\sigma(\bigcirc)))))$	z.d.n.
4.	$\oplus(\sigma(\sigma(\bigcirc)),\bigcirc) = \sigma(\sigma(\bigcirc))$	$R(\forall)$ dla $\sigma(\sigma(\bigcirc))$ w A_4
5.	$\forall y \ \oplus(\sigma(\sigma(\bigcirc)),\sigma(y)) = \sigma(\oplus(\sigma(\sigma(\bigcirc)),y))$	$R(\forall)$ dla $\sigma(\sigma(\bigcirc))$ w A_5
6.	$\oplus(\sigma(\sigma(\bigcirc)),\sigma(\bigcirc)) = \sigma(\oplus(\sigma(\sigma(\bigcirc)),\bigcirc))$	$R(\forall)$ dla $\bigcirc$ w 5.
7.	$\oplus(\sigma(\sigma(\bigcirc)),\sigma(\sigma(\bigcirc))) = \sigma(\oplus(\sigma(\sigma(\bigcirc)),\sigma(\bigcirc)))$	$R(\forall)$ dla $\sigma(\bigcirc)$ w 5.
8.	$\oplus(\sigma(\sigma(\bigcirc)),\sigma(\sigma(\bigcirc))) = \sigma(\sigma(\oplus(\sigma(\sigma(\bigcirc)),\bigcirc)))$	6. i 7., reguły dla $=$
9.	$\oplus(\sigma(\sigma(\bigcirc)),\sigma(\sigma(\bigcirc))) = \sigma(\sigma(\sigma(\sigma(\bigcirc))))$	4. i 8., reguły dla $=$
10.	$\times_{3,9}$	Sprzeczność: 3, 9.

Arytmetyka Robinsona

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 podamy za chwilę, omawiając aksjomatykę Arytmetyki Peana.

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 tablicę analityczną, tj. drzewo, w którego pniu umieszczamy A_1 oraz A_2, a także $\neg\sigma(\bigcirc) \neq \sigma(\sigma(\bigcirc))$.

Arytmetyka Robinsona



Tablicowy dowód $\sigma(\bigcirc) \neq \sigma(\sigma(\bigcirc))$.

Arytmetyka Robinsona

Przedstawimy dowody następujących zdań języka Arytmetyki Robinsona:

$$\oplus(\bigcirc, \sigma(\bigcirc)) = \sigma(\bigcirc)$$

$$\otimes(\bigcirc, \sigma(\bigcirc)) = \bigcirc.$$

Dowód $\oplus(\bigcirc, \sigma(\bigcirc)) = \sigma(\bigcirc)$

0.1.	$\forall x\ (\oplus(x, \bigcirc) = x)$	aksjomat A_4
0.2.	$\forall x \forall y\ (\oplus(x, \sigma(y)) = \sigma(\oplus(x, y)))$	aksjomat A_5
0.3.	$\neg(\oplus(\bigcirc, \sigma(\bigcirc)) = \sigma(\bigcirc))$	z.d.n.
1.	$\oplus(\bigcirc, \bigcirc) = \bigcirc$	0.1., $R(\forall)$ dla $\bigcirc$
2.	$\forall y\ (\oplus(\bigcirc, \sigma(y)) = \sigma(\oplus(\bigcirc, y)))$	0.2., $R(\forall)$ dla $\bigcirc$
3.	$\oplus(\bigcirc, \sigma(\bigcirc)) = \sigma(\oplus(\bigcirc, \bigcirc))$	2, $R(\forall)$ dla $\bigcirc$
4.	$\oplus(\bigcirc, \sigma(\bigcirc)) = \sigma(\bigcirc)$	1,3, $R(=)$
5.	$\times_{0.3.,4}$	Sprzeczność.

Dowód $\otimes(\bigcirc, \sigma(\bigcirc)) = \bigcirc$

0.1.	$\forall x\ (\oplus(x, \bigcirc) = x)$	aksjomat A_4
0.2.	$\forall x\ (\otimes(x, \bigcirc) = \bigcirc)$	aksjomat A_6
0.3.	$\forall x \forall y\ (\otimes(x, \sigma(y)) = \oplus(\otimes(x, y), x))$	aksjomat A_7
0.4.	$\neg(\otimes(\bigcirc, \sigma(\bigcirc)) = \bigcirc)$	z.d.n.
1.	$\otimes(\bigcirc, \bigcirc) = \bigcirc$	0.2., $R(\forall)$ dla $\bigcirc$
2.	$\forall y\ (\otimes(\bigcirc, \sigma(y)) = \oplus(\otimes(\bigcirc, y), \bigcirc))$	0.3., $R(\forall)$ dla $\bigcirc$
3.	$\otimes(\bigcirc, \sigma(\bigcirc)) = \oplus(\otimes(\bigcirc, \bigcirc), \bigcirc)$	2, $R(\forall)$ dla $\bigcirc$
4.	$\otimes(\bigcirc, \sigma(\bigcirc)) = \oplus(\bigcirc, \bigcirc)$	1,3, $R(=)$
5.	$\oplus(\bigcirc, \bigcirc) = \bigcirc$	0.1., $R(\forall)$ dla $\bigcirc$
6.	$\otimes(\bigcirc, \sigma(\bigcirc)) = \bigcirc$	4,5, $R(=)$
7.	$\times_{0.4.,6}$	Sprzeczność.

Arytmetyka Peana

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*.

Arytmetyka Peana

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

Aksjomaty specyficzne Arytmetyki Peana:

- P_1: $\forall x \forall y\ (x \neq y \to \sigma(x) \neq \sigma(y))$
- P_2: $\forall x\ (\bigcirc \neq \sigma(x))$
- P_3: $\forall x\ (\oplus(x, \bigcirc) = x)$
- P_4: $\forall x \forall y\ (\oplus(x, \sigma(y)) = \sigma(\oplus(x, y)))$
- P_5: $\forall x\ (\otimes(x, \bigcirc) = \bigcirc)$
- P_6: $\forall x \forall y\ (\otimes(x, \sigma(y)) = \oplus(\otimes(x, y), x))$
- P_7: $(A(\bigcirc) \wedge \forall x\ (A(x) \to A(\sigma(x)))) \to \forall x\ A(x)$
  (dla dowolnej formuły A, o jednej zmiennej wolnej, języka Arytmetyki Peana).

Arytmetyka Peana

P_7 nie jest jednym aksjomatem, lecz schematem (przeliczalnie wielu) aksjomatów. P_7 nazywamy ***zasadą indukcji***.

Rozważmy następującą regułę wnioskowania:

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

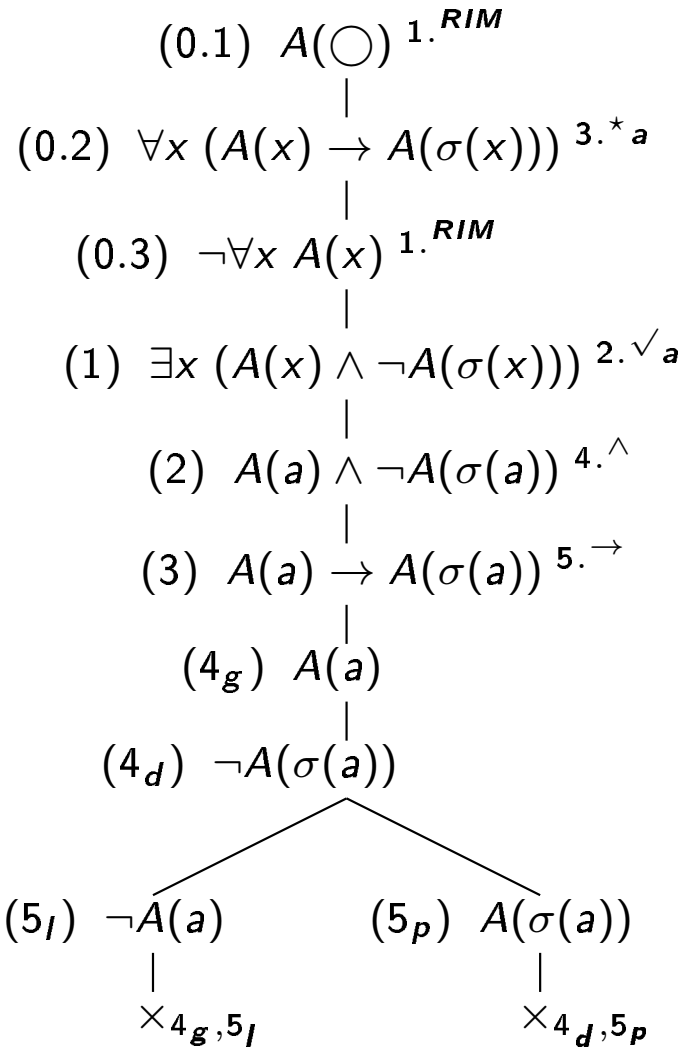
gdzie $A(x)$ jest dowolną formułą języka Arytmetyki Peana z jedną zmienną wolną. Nazwiemy ją ***regułą indukcji matematycznej*** (w skrócie: RIM).

Arytmetyka Peana

Jeśli do aksjomatów P_1–P_6 dołączyć regułę RIM, to można udowodnić — co samo w sobie nie jest zaskakujące — zasadę indukcji P_7. 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 tablicę analityczną, tj. drzewo, w którego pniu umieszczamy powyższe przesłanki oraz zaprzeczony wniosek:

Arytmetyka Peana



Tablica sprzeczna. P_1–P_6 i RIM implikują zasadę indukcji P_7.

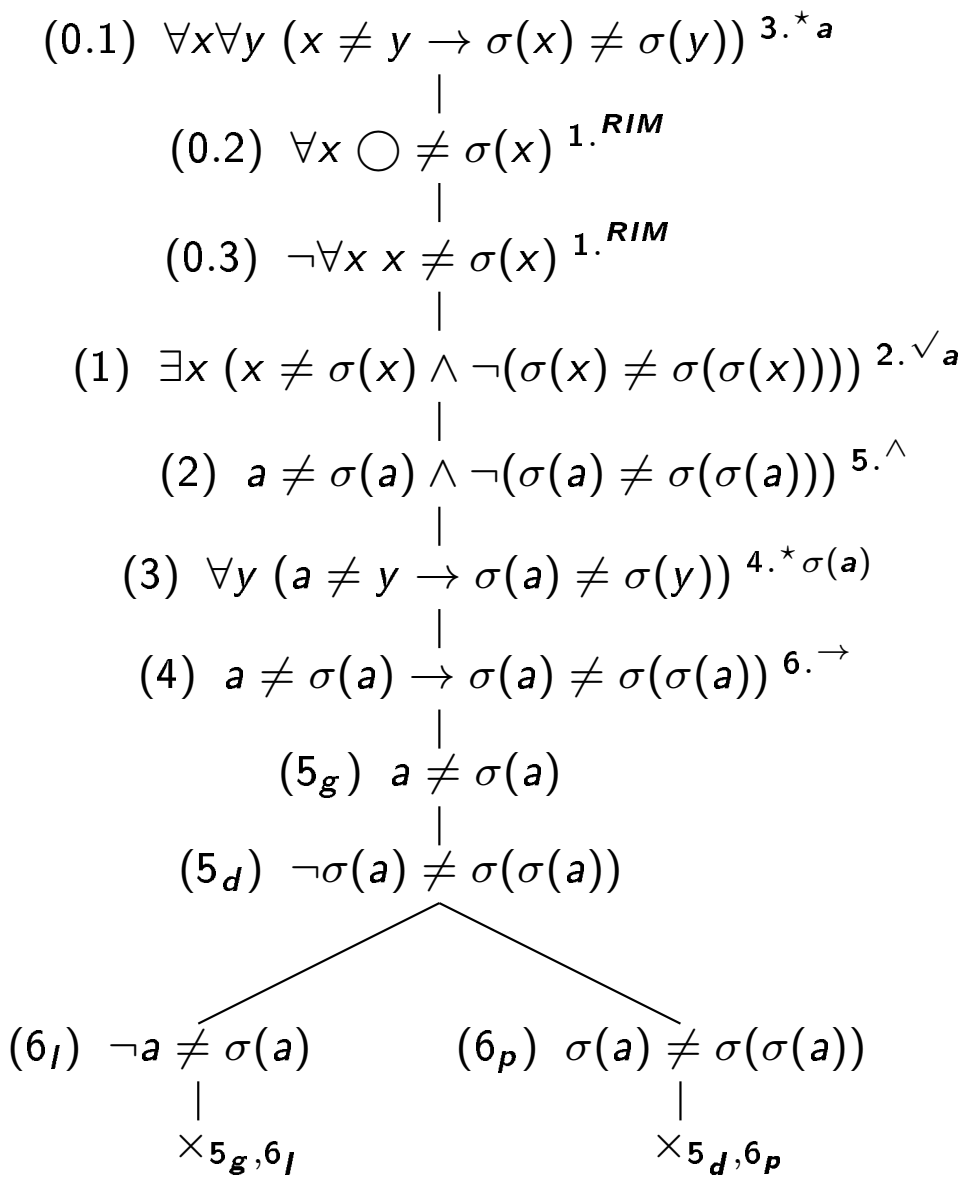
Arytmetyka Peana

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 tablicę analityczną, tj. 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 $\forall x\ (y \neq \sigma(x))$.

Ponieważ ta tablica jest sprzeczna, więc $\forall x\ (x \neq \sigma(x))$ można udowodnić z aksjomatów A_1 oraz A_2 Arytmetyki Robinsona przy pomocy reguły RIM:

Arytmetyka Peana



Algebra: Grupy — Pierwsza Aksjomatyka

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.

Algebra: Grupy — Pierwsza Aksjomatyka

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

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

Uwaga. We wszystkich trzech aksjomatykach dla teorii grup dochodzą jeszcze warunki ustalające, że identyczność jest relacją równoważności.

Aksjomaty specyficzne teorii grup:

- G_1^1: $\forall x \forall y \ (\boxdot(x, \boxdot(y, z)) = \boxdot(\boxdot(x, y), z))$
- G_2^1: $\forall x \forall y \exists z \ (\boxdot(x, z) = y)$
- G_3^1: $\forall x \forall y \exists z \ (\boxdot(z, x) = y)$.

Algebra: Grupy — Pierwsza Aksjomatyka

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 tablicę analityczną, tj. drzewo, w którego pniu umieszczamy aksjomaty G_1^1, G_1^2, G_1^3 oraz negację warunku (A). Tablica nie jest sprzeczna, co oznacza, że (A) nie jest logiczną konsekwencją G_1^1, G_1^2 oraz G_1^3.

Algebra: Grupy — Druga Aksjomatyka

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

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

Algebra: Grupy — Druga Aksjomatyka

Aksjomaty specyficzne:

- G_1^2: $\forall x \forall y \ \boxdot(x, \boxdot(y, z)) = \boxdot(\boxdot(x, y), z)$
- G_2^2: $\forall x \ (\boxdot(x, \varepsilon) = x)$
- G_3^2: $\forall x \ (\boxdot(\varepsilon, x) = x)$
- G_4^2: $\forall x \exists y \ (\boxdot(x, y) = \varepsilon)$
- G_5^2: $\forall x \exists y \ (\boxdot(y, x) = \varepsilon)$.

Dowód jedyności elementu neutralnego, tj. zdania:

$$(G_6^2) \quad \forall z(\forall x \ (\boxdot(x, z) = x \wedge \boxdot(z, x) = x) \rightarrow \varepsilon = z)$$

podajemy w poniższej tabeli:

Algebra: Grupy — Druga Aksjomatyka

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.	$\forall x\ (\boxdot(x,a) = x \wedge \boxdot(a,x) = x)$	$R(\neg\rightarrow)$, 4
5_d.	$\neg\varepsilon = a$	
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.	$\boxdot(\varepsilon,a) = \varepsilon$	$R(\wedge)$, 8
9_d.	$\boxdot(a,\varepsilon) = \varepsilon$	
10.	$\varepsilon = a$	$R(=)$, 9_g, 7
11.	$\times_{5_d,10}$	Sprzeczność: 5_d, 10.

Algebra: Grupy — Trzecia Aksjomatyka

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

- $\forall x \forall y \forall z \, (x = y \to \boxdot(x, z) = \boxdot(y, z))$
- $\forall x \forall y \forall z \, (x = y \to \boxdot(z, x) = \boxdot(z, y))$
- $\forall x \forall y \, (x = y \to \circledcirc(x) = \circledcirc(y))$.

Algebra: Grupy — Trzecia Aksjomatyka

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:

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

podajemy w poniższej tabeli (na dwóch slajdach):

Algebra: Grupy — Trzecia Aksjomatyka

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.	$\neg\forall x \forall y \forall z\ (\boxdot(x, z) = \boxdot(y, z) \to x = y)$	negacja G_4^3 (założenie dowodu nie wprost)
5.	$\neg\forall y \forall z\ (\boxdot(a_1, z) = \boxdot(y, z) \to a_1 = y)$	$R(\neg\forall)$ dla a_1, 4
6.	$\neg\forall z\ (\boxdot(a_1, z) = \boxdot(a_2, z) \to a_1 = a_2)$	$R(\neg\forall)$ dla a_2, 5
7.	$\neg(\boxdot(a_1, a_3) = \boxdot(a_2, a_3) \to a_1 = a_2)$	$R(\neg\forall)$ dla a_3, 6
8_g. 8_d.	$\boxdot(a_1, a_3) = \boxdot(a_2, a_3)$ $a_1 \neq a_2$	$R(\neg \to)$, 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

Algebra: Grupy — Trzecia Aksjomatyka

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:

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

podajemy poniżej (na dwóch slajdach):

Algebra: Grupy — Trzecia Aksjomatyka

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

Algebra: Grupy — Trzecia Aksjomatyka

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.	$\forall y \forall z\ (\boxdot(a, z) = \boxdot(y, z) \to a = y$	$R(\forall)$ dla a, 4
16.	$\forall z\ (\boxdot(a, z) = \boxdot(\boxdot(\varepsilon, a), z) \to a = \boxdot(\varepsilon, a))$	$R(\forall)$ dla $\boxdot(\varepsilon, a)$, 15
17.	$\boxdot(a, \circledcirc(a)) = \boxdot(\boxdot(\varepsilon, a), \circledcirc(a)) \to a = \boxdot(\varepsilon, a)$	$R(\forall)$ dla $\circledcirc(a)$, 16
18_I.	$\boxdot(a, \circledcirc(a)) \neq \boxdot(\boxdot(\varepsilon, a), \circledcirc(a))$	$R(\to)$, 17
$18_I.1.$	$\times_{14, 18_I}$	Sprzeczność: $14, 18_I$.
18_p.	$a = \boxdot(\varepsilon, a)$	$R(\to)$, 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:

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

podajemy poniżej:

Algebra: Grupy — Trzecia Aksjomatyka

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.	$\neg\forall y\forall x\ (\boxdot(x,y) = x \to y = \varepsilon)$	negacja G_6^3 (założenie dowodu nie wprost)
4.	$\neg\forall x\ (\boxdot(x,a) = x \to a = \varepsilon)$	$R(\forall)$ dla a, 3
5_g.	$\forall x\ \boxdot(x,a) = x$	$R(\neg\to)$, 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.

Algebra: Grupy — Przykłady

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.

Koniec

Pokazaliśmy działanie metody tablic analitycznych w KRP. Dowody wszystkich twierdzeń oraz liczne (bardziej złożone) przykłady znajdują się w pliku tabkrp.pdf.

Na kolejnych wykładach omówimy:

- konsekwencję aksjomatyczną w KRP
- konsekwencję założeniową w KRP
- konsekwencję rezolucyjną w KRP.