Wstęp do teorii mnogości i logiki

Jerzy Tiuryn

Wydział Matematyki, Informatyki i Mechaniki
Uniwersytet Warszawski
20 października 1998

Spis treści

I Wstęp do teorii mnogości **3**

1 Zbiory i operacje na zbiorach **4**

2 Relacje **8**

3 Liczby naturalne **11**

4 Funkcje **16**
4.1 Definiowanie funkcji przez indukcję 21

5 Relacje równoważności **25**

6 Teoria mocy **31**
6.1 Zbiory przeliczalne 33
6.2 Zbiory nieprzeliczalne 36
6.3 Porównywanie liczb kardynalnych 37
6.4 Operacje na liczbach kardynalnych 39

7 Częściowe porządki **44**
7.1 Słowa 45
7.2 Drzewa 47
7.3 Drzewa etykietowane 49
7.4 Kresy zbiorów, kraty zupełne 58
7.5 Twierdzenia o punkcie stałym 62
7.6 Lemat Kuratowskiego-Zorna 67

8 Dobre ufundowanie **71**
8.1 Indukcja noetherowska 72
8.2 Dobre porządki 75
8.3 Liczby porządkowe 77
8.4 Twierdzenie Zermelo i dowód lematu Kuratowskiego-Zorna 80

II Wstęp do logiki **84**

9 Elementy algebry uniwersalnej **85**
9.1 Algebra termów 85
9.2 Homomorfizmy 87

9.3 Podalgebry . . . 90
9.4 Kongruencje . . . 92
9.5 Uogólnione produkty algebr . . . 93
9.6 Klasy równościowo definiowalne . . . 94
9.7 Algebry wolne . . . 96

10 Unifikacja **103**
10.1 Algorytm unifikacji . . . 105
10.2 Terminacja algorytmu . . . 106
10.3 Częściowa poprawność algorytmu . . . 107
10.4 Najbardziej ogólny unifikator . . . 110

11 Rachunek zdań **113**
11.1 Składnia . . . 113
11.2 Semantyka . . . 113
11.3 Systemy dowodzenia . . . 115
11.3.1 System hilbertowski . . . 115
11.3.2 System naturalnej dedukcji . . . 121
11.3.3 Gentzenowski rachunek sekwentów . . . 124
11.4 Elementy teorii modeli . . . 127
11.5 Informacja o logice intuicjonistycznej . . . 128

12 Język pierwszego rzędu **133**
12.1 Składnia . . . 133
12.2 Semantyka . . . 134
12.3 Podstawianie termów . . . 136
12.4 Hilbertowski system dowodzenia . . . 138
12.5 Teorie aksjomatyczne . . . 142
12.5.1 Arytmetyka Peano . . . 142
12.5.2 Teoria mnogości Zermelo-Fraenkla . . . 143
12.6 Elementy teorii modeli . . . 145

13 Język drugiego rzędu **154**
13.1 Składnia . . . 154
13.2 Semantyka . . . 155

Wstęp

Informatyka przeżywa obecnie burzliwy rozwój metod formalnych, których stopień komplikacji może być bardzo duży. Dlatego też studenci informatyki powinni zostać do tego przygotowani od samego początku studiów. Niniejszy wykład "*Wstęp do teorii mnogości i logiki*" jest jednym z przedmiotów na pierwszym roku studiów mającym za zadanie zapoznanie studentów z pewnymi działami teorii zbiorów oraz metod formalnych logiki matematycznej mającymi bezpośredni związek z informatyką zarówno teoretyczną jak i praktyczną.

Zakres materiału oraz nacisk na poszczególne działy w tym wykładzie nieco się różni od tradycyjnych wykładów z tej tematyki prowadzonych poprzednio na naszym Wydziale.[1]

Pierwszy semestr tego wykładu poświęcony jest teorii mnogości. Kładę tutaj znacznie większy nacisk na zbiory częściowo uporządkowane ze szczególnym potraktowaniem twierdzeń o punkcie stałym, które znajdują duże zastosowanie we współczesnej informatyce. Dużo podaję przykładów o orientacji informatycznej: słowa, drzewa, drzewa etykietowane. Dobre porządki pojawiają się jako szczególny przypadek relacji dobrze ufundowanych. Liczby porządkowe są tutaj potraktowane bardzo pobieżnie. Zasada indukcji pozaskończonej jest zastąpiona indukcją noetherowską.

Drugi semestr natomiast dotyczy logiki. Przedstawione są tam podstawy algebry uniwersalnej (podstawowe pojęcia, algebry wolne, rozmaitości algebr). Dyskutuję problem unifikacji termów wraz z pełnym dowodem poprawności algorytmu unifikacji. Dzięki temu czytelnik może zapoznać się metodami ścisłego dowodzenia poprawności algorytmów. Również sama unifikacja jest użytecznym narzędziem wykorzystywanym przez wiele działów informatyki, m.in. języki funkcyjne, sztuczna inteligencja, automatyczne wnioskowanie. Następnie omawiam rachunek zdań. Główny nacisk kładę tutaj na różne systemy formalne: system hilbertowski, naturalnej dedukcji i gentzenowski rachunek sekwentów. Podaję też trochę informacji o logice intuicjonistycznej. Oprócz metod formalnych przedstawiam też twierdzenie o zwartości — jedno z podstawowych narzędzi teoriomodelowych. Na zakończenie podaję informacje o logice pierwszego rzędu (hilbertowski system formalny, elementy teorii modeli) i o języku drugiego rzędu.

Obecna, trzecia edycja tego skryptu jest nieznacznie poprawioną i rozszerzoną wersją drugiej edycji, która została wydana w 1997r. Notatki te były przygotowywane w oparciu o wykłady, jakie prowadziłem w latach 1992/93, 93/94 oraz 97/98 dla studentów pierwszego roku informatyki na Wydziale Matematyki, Informatyki i Mechaniki, Uniwersytetu Warszawskiego. Obecne wydanie skryptu zawiera pełne dowody twierdzeń dotyczących wstępu do teorii mnogości oraz oraz większość dowodów w części poświęconej logice. Dłuższe (i zwykle trudniejsze) z tych dowodów nie zmieszczą się na wykładzie z tego przedmiotu. Umieściłem je w skrypcie mając nadzieję, że może zainteresują one niektórych bardziej dociekliwych studentów.

[1] Chodzi o Wydział Matematyki, Informatyki i Mechaniki, Uniwersytetu Warszawskiego.

Chciałbym wyrazić podziękowania dr Damianowi Niwińskiemu, dr Igorowi Walukiewiczowi oraz prof. dr hab. Pawłowi Urzyczynowi za uwagi dotyczące poniższych notatek. Chciałbym też wyrazić wdzieczność mgr Grzegorzowi Grudzińskiemu, mgr Marcinowi Jurdzińskiemu, mgr Robertowi Maronowi i mgr Aleksowi Schubertowi za pomoc techniczną przy przygotowywaniu tych notatek. Oczywiście wszelkie błędy i niedociągnięcia w materiale przedstawionym w tym skrypcie są moją 'zasługą'. Gdyby ktoś chciał się podzielić ze mną swoimi uwagami na temat skryptu, będę wdzięczny za wiadomość przez e-mail na adres: `tiuryn@mimuw.edu.pl`

Warszawa 20.10.98 Jerzy Tiuryn

Literatura

1. Z. Adamowicz, P. Zbierski, *Logika matematyczna*, PWN, Warszawa 1991.
2. K. Kuratowski, A. Mostowski, *Teoria mnogości*, PWN, Warszawa, 1978.
3. H. Rasiowa, *Wstęp do matematyki współczesnej*, PWN, Warszawa, 1971.
4. A. Wojciechowska, *Elementy logiki i teorii mnogości*, PWN, Warszawa, 1979.

Część I

Wstęp do teorii mnogości

1 Zbiory i operacje na zbiorach

Teorię mnogości, czyli teorię zbiorów, buduje się w oparciu o pojęcia pierwotne: *zbiór* oraz związek $\in$ "*być elementem*". Napis $x \in A$ czytamy: " x należy do A". Pojęcia pierwotne oznaczają kategorię pojęć, których się nie definiuje. Ponadto przyjmuje się pewien zestaw własności dotyczących tych pojęć zwanych *aksjomatami*. Aksjomaty są własnościami, które przyjmuje się bez dowodu. Cały taki zestaw nazywa się *aksjomatyczną teorią*. W zależności od tego jakie przyjmuje się pojęcia i własności pierwotne — możemy mieć różne teorie aksjomatyczne dotyczące tego samego działu matematyki. Nasze wprowadzenie do teorii mnogości będzie się opierać na znanej aksjomatyce *Zermelo-Fraenkla*. Nie będziemy jednak w jawny sposób odwoływać się do aksjomatów teorii mnogości. [2]

Do porównywania zbiorów służy następująca zasada *ekstensjonalności*:

$$A = B \text{ wtw, gdy dla każdego } x,\ (x \in A \text{ wtw, gdy } x \in B).$$

Tak więc dwa zbiory są równe wtedy i tylko wtedy, gdy mają te same elementy. Mówimy, że zbiór A jest *zawarty* w zbiorze B (oznaczamy $A \subseteq B$), gdy każdy element zbioru A jest elementem zbioru B. Gdy $A \subseteq B$, to mówimy też, że A jest *podzbiorem* B. Zasadę ekstensjonalności można wyrazić przy pomocy zawierania:

$$A = B \text{ wtw, gdy } A \subseteq B \text{ oraz } B \subseteq A.$$

Ważnym przykładem zbioru jest zbiór nie mający żadnych elementów — *zbiór pusty*. Oznaczamy go przez $\emptyset$. Na mocy zasady ekstensjonalności istnieje co najwyżej jeden zbiór pusty.[3] Zbiory mające skończoną liczbę elementów możemy definiować przez wymienienie tych elementów. Na przykład, zbiór $\{a, b, 0\}$ składa się z trzech elementów: a, b oraz 0, zakładając, że $a, b, 0$ są trzema różnymi obiektami. Jeśli $\varphi(x)$ jest pewną własnością[4] zależną od x oraz A jest zbiorem, to napis $\{x \in A \mid \varphi(x)\}$ oznacza zbiór wszystkich tych elementów x ze zbioru A, które spełniają własność φ.

Następnie zdefiniujemy pewne operacje na zbiorach. Niech A, B będą zbiorami. *Sumą* zbiorów A i B nazywamy zbiór $A \cup B$, którego elementami są te i tylko te obiekty, które są elementami A lub elementami B. *Przecięciem* zbiorów A i B nazywamy zbiór $A \cap B$, którego elementami są te i tylko te obiekty, które są jednocześnie elementami A i B. *Różnicą* zbiorów A i B nazywamy zbiór $A - B$, którego elementami są te elementy zbioru A, które nie należą do B. *Zbiorem potęgowym* zbioru A nazywamy zbiór $P(A)$, którego elementami są wszystkie podzbiory zbioru A.

[2] Zainteresowanego czytelnika odsyłamy do książki K. Kuratowski, A Mostowski "*Teoria Mnogości*", PWN, Warszawa, 1978.

[3] Istnienie zbioru pustego trzeba postulować aksjomatem.

[4] Obecne wprowadzenie jest intuicyjne — nie będziemy formalnie definiować pojęcia własności.

Działania sumy i przecięcia są operacjami dwuargumentowymi. Można łatwo uogólnić te operacje na dowolne rodziny zbiorów. Niech $\mathcal{A}$ będzie rodziną zbiorów. *Sumą* tej rodziny nazwiemy zbiór $\bigcup \mathcal{A}$, taki że dla dowolnego elementu x,

$$x \in \bigcup \mathcal{A} \text{ wtw, gdy istnieje } A \in \mathcal{A}, \text{ taki że } x \in A.$$

Dualnie definiujemy *przecięcie* rodziny $\mathcal{A}$, o ile $\mathcal{A} \neq \emptyset$. Jest to zbiór $\bigcap \mathcal{A}$, taki że dla dowolnego elementu x,

$$x \in \bigcap \mathcal{A} \quad \text{wtw, gdy} \quad \text{dla każdego } A \in \mathcal{A}, \text{ zachodzi } x \in A.$$

Dla przykładu, pokażemy dwie tożsamości algebry zbiorów.

Fakt 1.1

(i) $A - (B \cup C) = (A - B) \cap (A - C)$.

(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Dowód: Dla dowodu równości pokażemy dwa zawierania: $A-(B\cup C) \subseteq (A-B)\cap(A-C)$ oraz $(A-B)\cap(A-C) \subseteq A-(B\cup C)$. Aby pokazać, że $A-(B\cup C) \subseteq (A-B)\cap(A-C)$ należy dowieść, że każdy element zbioru $A-(B\cup C)$ należy do $(A-B)\cap(A-C)$. Weźmy więc dowolny element $x \in A-(B\cup C)$. Oznacza to, że $x \in A$ oraz $x \notin B \cup C$. Zatem $x \notin B$ oraz $x \notin C$. Tak więc $x \in A$ oraz $x \notin B$, czyli $x \in A - B$. Podobnie, $x \in A - C$. Łącznie dostajemy $x \in (A - B) \cap (A - C)$. Wobec dowolności wyboru elementu x udwodniliśmy zawieranie

$$A - (B \cup C) \subseteq (A - B) \cap (A - C). \tag{1}$$

Zawieranie w stronę przeciwną pokazujemy w podobny sposób. Jeśli $x \in (A-B)\cap(A-C)$ to $x \in A$ oraz $x \notin B$ i $x \notin C$. Zatem $x \notin B \cup C$ i dostajemy $x \in A - (B \cup C)$. Wobec dowolności wyboru x mamy dowód zawierania

$$(A - B) \cap (A - C) \subseteq A - (B \cup C). \tag{2}$$

Zawierania (1) i (2) dają dowód pierwszej części Faktu 1.1.

Powyższe rozumowanie można skrócić zauważając, że wszystkie kroki w dowodzie pierwszego zawierania dają się odwrócić, a tym samym dają dowód równości. Zilustrujemy to na przykładzie dowodu drugiej części faktu.

Niech x będzie dowolnym elementem. Wtedy następujące zdania są równoważne.

$$x \in A \cap (B \cup C)$$

$$x \in A \quad \text{oraz } (x \in B \text{ lub } x \in C)$$

$$(x \in A \text{ oraz } x \in B) \text{ lub } (x \in A \text{ oraz } x \in C)$$

$$x \in (A \cap B) \text{ lub } x \in (A \cap C)$$

$$x \in (A \cap B) \cup (A \cap C)$$

Równoważność powyższych pięciu zdań wynika z wprost z definicji operacji $\cap$ i $\cup$ oraz z własności *spójników logicznych* "i" oraz "lub". ■

Poniżej podamy rozwiązania dwóch przykładowych zadań.

Przykład 1.2

(i) Sprawdzimy czy równość $A \cap (B \cup C) = (A \cap B) \cup C$ zachodzi dla dowolnych zbiorów A, B, C. Niech x będzie dowolnym obiektem. Pisząc warunki opisujące należenie x do lewej i do prawej strony powyższej równości łatwo jest stwierdzić, że równoważność nie będzie zachodziła w sytuacji gdy x nie będzie należał do A oraz będzie należał do C. Rzeczywiście, dla zbiorów $A = B = \emptyset$ oraz $C = \{5\}$ powyższa równość nie zachodzi.

(ii) Sprawdzimy dla jakich zbiorów A, B, zachodzi $P(A \cup B) = P(A) \cup P(B)$. Zauważmy, że jeśli istnieją elementy $a \in A - B$ oraz $b \in B - A$, to $\{a, b\} \in P(A \cup B)$, ale $\{a, b\}$ nie należy ani do $P(A)$ ani do $P(B)$. Czyli jeśli $A - B \neq \emptyset$ oraz $B - A \neq \emptyset$, to $P(A \cup B) \neq P(A) \cup P(B)$. Z drugiej strony, jeśli $A - B = \emptyset$ to $A \subseteq B$ i wtedy mamy $P(A) \subseteq P(B)$ oraz $P(A \cup B) = P(B) = P(A) \cup P(B)$. Podobnie pokazujemy równość gdy $B - A = \emptyset$. Zatem $P(A \cup B) = P(A) \cup P(B)$ wtw, gdy $A \subseteq B$ lub $B \subseteq A$.

Chcielibyśmy podkreślić, że aby dowieść że pewna równość jest prawem rachunku zbiorów trzeba ją udowodnić dla dowolnych zbiorów. Natomiast aby pokazać, że pewna równość nie jest prawem rachunku zbiorów wystarczy pokazać, że nie zachodzi ona dla pewnych konkretnych zbiorów. Wystarczy tu podać konkretny zestaw zbiorów, nie siląc się na ogólność. Im prostsze zbiory wybierzemy na kontrprzykład tym lepiej.

Zadania

1.1. Dowieść, że dla dowolnych zbiorów A, B, jeśli $A - B = B - A$, to $A = B$.

1.2. Dowieść, że dla dowolnych zbiorów A, B, jeśli $A \subseteq B$, to $P(A) \subseteq P(B)$.

1.3. Czy dla dowolnych zbiorów A, B zachodzi $P(A \cap B) = P(A) \cap P(B)$?

1.4. Wyznaczyć wszystkie zbiory A, B, C takie, że $(A - C) \cup B = (A \cup B) - C$.

1.5. Niech A będzie rodziną zbiorów. Dowieść, że

$$A \subseteq P(A) \quad \text{wtw, gdy} \quad \bigcup A \subseteq A$$

1.6. Która z implikacji w poniższej równoważności jest prawdziwa dla dowolnej rodziny zbiorów A?

$$P(A) \subseteq A \quad \text{wtw, gdy} \quad A \subseteq \bigcup A$$

1.7. Dowieść, że dla każdego zbioru A zachodzi $\bigcup P(A) = A$.

1.8. Niech A, B będą dowolnymi rodzinami zbiorów. Dowieść, że $\bigcup(A \cup B) = (\bigcup A) \cup (\bigcup B)$. Czy równość $\bigcup(A \cap B) = (\bigcup A) \cap (\bigcup B)$ zachodzi?

1.9. Dowieść, że każdy zbiór jest sumą wszystkich swoich skończonych podzbiorów.

2 Relacje

Parą uporządkowaną o współrzędnych a i b nazywamy obiekt $\langle a, b\rangle$, jednoznacznie wyznaczony przez a, b oraz ich kolejność wystąpienia. Tak więc podstawową cechą pary uporządkowanej wynikającą wprost z powyższej definicji jest następująca własność. Dla dowolnych obiektów a, b, c, d

$$\langle a, b\rangle = \langle c, d\rangle \quad \text{wtw, gdy} \quad a = c \text{ oraz } b = d. \tag{3}$$

Następujące twierdzenie pokazuje, że definicję pary uporządkowanej można oprzeć na konstrukcji teoriomnogościowej.

Fakt 2.1 *Dla dowolnych a, b, c, d,*

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} \text{ wtw, gdy } a = c \text{ oraz } b = d.$$

Dowód: Implikacja z prawej strony w lewą jest oczywista. Załóżmy, że

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}.$$

Jeśli $a = b$, to zbiór $\{\{a\}, \{a, b\}\}$ ma jeden element, a zatem zbiór po prawej stronie równości też musi mieć jeden element czyli $a = b = c = d$.

Załóżmy więc, że $a \neq b$. Wtedy zbiór $\{\{a\}, \{a, b\}\}$ ma dwa elementy. Zatem $c \neq d$. Ponieważ $\{a\}$ jest jedynym jednoelementowym zbiorem po lewej stronie więc musi on być równy jedynemu zbiorowi jednoelementowemu po prawej stronie. Zatem

$$\{a\} = \{c\} \quad \text{oraz} \quad \{a, b\} = \{c, d\},$$

skąd natychmiast otrzymujemy $a = c$ oraz $b = d$. ∎

Konstrukcji spełniających własność (3) jest wiele. Zwykle nie będziemy się odwoływać do konkretnej konstrukcji pary uporządkowanej bowiem zwykle własności pary wynikają już bezpośrednio z (3) i nie zależą od specyficznej konstrukcji. Przykładem własności zależącej od konkretnej konstrukcji pary z powyższego twierdzenia jest $a \in \bigcup\langle a, b\rangle$.

Iloczynem kartezjańskim zbiorów A, B nazywamy zbiór $A \times B$, którego elementami są wszystkie pary uporządkowane $\langle a, b\rangle$, takie że $a \in A$ oraz $b \in B$. Iloczyn $A \times A$ oznaczamy przez A^2. Podzbiory zbioru $A \times B$ nazywamy *relacjami* w $A \times B$. Podzbiory zbioru A^2 nazywamy *relacjami binarnymi* w A. Jeśli $R \subseteq A \times B$ jest relacją to notacja aRb oznacza $\langle a, b\rangle \in R$. Podamy kilka przykładów relacji.

Przykład 2.2

(i) (*Identyczność*) Niech A będzie zbiorem, $I_A = \{\langle a, a\rangle \in A \times A \mid a \in A\}$.

(ii) Niech R oznacza zbiór liczb rzeczywistych. Zwykłe uporządkowanie zbioru R wyznacza relację $\leq = \{\langle r_1, r_2\rangle \in R \times R \mid r_1 \leq r_2\}$.

(iii) Zbiór $P = \{\langle k, m\rangle \in N \times N \mid k = m^2\}$ jest binarną relacją w zbiorze N wszystkich liczb naturalnych.

(iv) Zbiór $Q = \{\langle k, m\rangle \in N \times Z \mid k = m^2\}$ jest relacją w $N \times Z$, gdzie Z oznacza zbiór wszystkich liczb całkowitych.

Niech $n > 0$ będzie liczbą naturalną. Powyższe definicje można łatwo uogólnić na przypadek gdy współrzędnych jest n. Uporządkowaną n-tką o współrzędnych $a_1, \ldots, a_n$ nazwiemy obiekt $\langle a_1, \ldots, a_n\rangle$ wyznaczony jednoznacznie przez swoje współrzędne oraz kolejność ich występowania. Zatem w tym przypadku mamy następującą cechę n-tek uporządkowanych. Dla dowolnych obiektów $a_1, \ldots a_n$ oraz $b_1, \ldots, b_n$,

$$\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle \quad \text{wtw, gdy } \; a_1 = b_1, \ldots, a_n = b_n.$$

Podobnie jak w przypadku par uporządkowanych nie będziemy wnikać w strukturę wewnętrzną n-tek uporządkowanych. Używając konstrukcji pary można n-tkę uporządkowaną zdefiniować na przykład następująco.

$$\langle a_1, \ldots, a_n\rangle = \langle a_1, \langle a_2, \ldots, \langle a_{n-1}, a_n\rangle \ldots\rangle.$$

Iloczynem kartezjańskim zbiorów $A_1, \ldots, A_n$ nazywamy zbiór $A_1 \times A_2 \times \ldots \times A_n$ wszystkich n-tek uporządkowanych $\langle a_1, \ldots, a_n\rangle$ takich, że $a_1 \in A_1, \ldots, a_n \in A_n$. Iloczyn kartezjański n-krotny zbioru A ze sobą oznaczamy przez A^n. Relacją w $A_1 \times A_2 \times \ldots \times A_n$ nazywamy dowolny podzbiór tego zbioru. Relacją *n-argumentową* w zbiorze A nazywamy dowolny podzbiór zbioru A^n.

Niech $R \subseteq A \times B$, oraz $S \subseteq B \times C$ będą relacjami. *Złożeniem* relacji R i S nazwiemy relację[5]

$$SR = \{\langle a, c\rangle \in A \times C \mid \text{istnieje } b \in B \text{ taki, że } \langle a, b\rangle \in R \text{ oraz } \langle b, c\rangle \in S\}.$$

Relacją odwrotną do R nazwiemy relację $R^{-1} \subseteq B \times A$,

$$R^{-1} = \{\langle b, a\rangle \in B \times A \mid \langle a, b\rangle \in R\}.$$

[5]Kolejność relacji występująca w złożeniu jest być może niezgodna z intuicją czytelnika. Taka kolejność jest podyktowana tym, że funkcje są szczególnym przypadkiem relacji, a składanie funkcji historycznie oznacza się właśnie w tej kolejności. Niektórzy autorzy oznaczają złożenie relacji w odwrotnym porządku, tzn. RS. Dla uniknięcia sytuacji, w której będziemy zmuszeni mieć do czynienia z dwoma operacjami składania relacji: jako ogólnych relacji i jako funkcji—zdecydowaliśmy się wprowadzić od początku odwrotną kolejność składania dla dowolnych relacji.

Twierdzenie 2.3 *Niech $R \subseteq A \times B$, $S \subseteq B \times C$, oraz $T \subseteq C \times D$. Wtedy*

(i) $T(SR) = (TS)R$.

(ii) $(SR)^{-1} = R^{-1}S^{-1}$.

Dowód: Udowodnimy najpierw (i). Niech $\langle a, d\rangle \in A \times D$. Zachodzą następujące równoważności.

$$\langle a, d\rangle \in T(SR) \text{ wtw, gdy}$$
$$\text{istnieje } c \in C, \text{ takie że } \langle a, c\rangle \in SR \text{ oraz } \langle c, d\rangle \in T, \text{ wtw, gdy}$$
$$\text{istnieją } c \in C \text{ oraz } b \in B, \text{ takie że } \langle a, b\rangle \in R \text{ oraz } \langle b, c\rangle \in S \text{ oraz } \langle c, d\rangle \in T, \text{ wtw, gdy}$$
$$\text{istnieje } b \in B, \text{ takie że } \langle a, b\rangle \in R \text{ oraz } \langle b, d\rangle \in TS, \text{ wtw, gdy}$$
$$\langle a, d\rangle \in (TS)R$$

Dla dowodu (ii) weźmy dowolną parę $\langle c, a\rangle \in C \times A$. Wtedy

$$\langle c, a\rangle \in (SR)^{-1} \text{ wtw, gdy}$$
$$\langle a, c\rangle \in SR \text{ wtw,gdy}$$
$$\text{istnieje } b \in B \text{ takie, że } \langle a, b\rangle \in R \text{ oraz } \langle b, c\rangle \in S, \text{ wtw, gdy}$$
$$\text{istnieje } b \in B \text{ takie, że } \langle b, a\rangle \in R^{-1} \text{ oraz } \langle c, b\rangle \in S^{-1}, \text{ wtw, gdy}$$
$$\langle c, a\rangle \in R^{-1}S^{-1}$$

■

Zadania

2.1. Dla każdego z poniższych warunków sprawdzić czy istnieje relacja $R \subseteq N \times N$, gdzie N oznacza zbiór liczb naturalnych, spełniająca

a.) $R^{-1} \not\subseteq R$.

b.) $R \neq \emptyset$, $RR = R$ oraz $R \cap I_N = \emptyset$.

c.) $R^{-1} = N^2 - R$.

2.2. Niech $\mathcal{R}$ będzie niepustą rodziną relacji w $A \times B$ i niech $S \subseteq B \times C$. Dowieść

a.) $S(\bigcup \mathcal{R}) = \bigcup\{SR \mid R \in \mathcal{R}\}$.

b.) $S(\bigcap \mathcal{R}) \subseteq \bigcap\{SR \mid R \in \mathcal{R}\}$. Czy zawieranie można zastąpić równością?

c.) $(\bigcup \mathcal{R})^{-1} = \bigcup\{R^{-1} \mid R \in \mathcal{R}\}$.

d.) $(\bigcap \mathcal{R})^{-1} = \bigcap\{R^{-1} \mid R \in \mathcal{R}\}$.

3 Liczby naturalne

Rodzina zbiorów $\mathcal{A}$ jest *induktywna* gdy

- $\emptyset \in \mathcal{A}$,
- dla każdego zbioru $X \in \mathcal{A}$, zbiór $X \cup \{X\}$ należy do $\mathcal{A}$.

Operację, która zbiorowi X przyporządkowuje $X \cup \{X\}$ nazywamy operacją *następnika*. Następnik zbioru X oznaczamy X'. Istnienie zbiorów induktywnych jest postulowane aksjomatem zwanym *aksjomatem nieskończoności*. Aksjomat ten wyraża istnienie zbiorów nieskoćzonych.

Twierdzenie 3.1 *Istnieje najmniejszy zbiór induktywny, tzn. istnieje taki zbiór induktywny $\mathcal{A}_0$, że dla każdego zbioru induktywnego $\mathcal{B}$, zachodzi $\mathcal{A}_0 \subseteq \mathcal{B}$.*

Dowód: Niech $\mathcal{A}$ będzie zbiorem induktywnym i niech

$$\Delta = \{\mathcal{B} \subseteq \mathcal{A} \mid \mathcal{B} \text{ jest zbiorem induktywnym}\}.$$

Ponieważ oczywiście przecięcie dowolnej niepustej rodziny zbiorów induktywnych jest zbiorem induktywnym to $\mathcal{A}_0 = \bigcap \Delta$ jest zbiorem induktywnym. Pokażemy, że jest to najmniejszy zbiór induktywny. Niech $\mathcal{B}$ będzie dowolnym zbiorem induktywnym. Oczywiście $\mathcal{B} \cap \mathcal{A} \in \Delta$. Zatem, z definicji przecięcia,

$$\mathcal{A}_0 \subseteq \mathcal{B} \cap \mathcal{A}.$$

Ponieważ $\mathcal{B} \cap \mathcal{A} \subseteq \mathcal{B}$, to $\mathcal{A}_0 \subseteq \mathcal{B}$. Zatem $\mathcal{A}_0$ jest najmniejszym zbiorem induktywnym. ∎

Najmniejszy zbiór induktywny nazywamy *zbiorem liczb naturalnych* i oznaczamy go przez N. Zbiór N, jak każdy zbiór induktywny, musi zawierać $\emptyset$ – element ten reprezentuje liczbę naturalną 0. Ponadto N jest zamknięty na operację następnika, a zatem zawiera następnik 0 (który jest oczywiście oznaczany przez 1), następnik następnika 0 (czyli następnik 1, oznaczany przez 2), itd.

Twierdzenie 3.2 (Zasada indukcji)
Jeśli $P \subseteq N$ jest zbiorem liczb naturalnych takim, że

- $0 \in P$,
- *dla każdej liczby n, jeśli $n \in P$, to $n' \in P$,*

to P zawiera wszystkie liczby naturalne, tzn. $P = N$.

Dowód: Wynika bezpośrednio z faktu, że N jest najmniejszym zbiorem induktywnym. ∎

Następujące twierdzenie zbiera pewne własności liczb naturalnych, które będą wykorzystywane w dalszych częściach tego wykładu.

Twierdzenie 3.3 *Dla dowolnych liczb* $m, n \in N$,

(i) Jeśli $m \in n$, *to* $m \subseteq n$.

(ii) $n \notin n$.

(iii) Jeśli $m' = n'$, *to* $m = n$.

(iv) Jeśli $m \subseteq n$ *oraz* $m \neq n$, *to* $m \in n$.

(v) Zachodzi: $m \subseteq n$ *lub* $n \subseteq m$.

(vi) Zachodzi dokładnie jedna z możliwości: $m \in n$, $m = n$, $n \in m$.

Dowód: Twierdzenie to będziemy dowodzić przez indukcję. Dla dowodu (i) rozważmy zbiór

$$P = \{n \in N \mid \text{ dla każdego } m \in n,\ m \subseteq n\}.$$

Pokażemy, że P jest zbiorem induktywnym. Oczywiście $0 \in P$. Załóżmy, że $n \in P$. Dla pokazania, że $n' \in P$ weźmy dowolny $m \in n'$. Ponieważ $n' = n \cup \{n\}$, to mamy dwa przypadki do rozpatrzenia. Jeśli $m \in n$ to z założenia indukcyjnego mamy $m \subseteq n$ a zatem $m \subseteq n'$. Jeśli natomiast $m = n$, to oczywiście $m \subseteq n'$. Tak więc w każdym przypadku m jest zawarte w n', co dowodzi że $n' \in P$.

Dla dowodu (ii) rozważmy zbiór

$$P = \{n \in N \mid n \notin n\}.$$

Oczywiście $0 \in P$. Załóżmy, że $n \in P$ i przypuśćmy, że

$$n' \in n \cup \{n\}. \tag{4}$$

Zatem albo $n' \in n$ lub $n' = n$. W pierwszym przypadku, korzystając z (i) otrzymujemy $n \cup \{n\} \subseteq n$ a zatem $n \in n$, co daje sprzeczność z założeniem indukcyjnym. W drugim przypadku bezpośrednio otrzymujemy $n \in n$, co daje ponownie sprzeczność. Tak więc (4) jest niemożliwe, co dowodzi $n' \in P$.

Aby udowodnić (iii) załóżmy, że

$$m \cup \{m\} = n \cup \{n\}.$$

Zatem m musi należeć do prawej strony powyższej równości. Jeśli $m \in n$, to korzystając z (i) mamy $m \subseteq n$. Jeśli natomiast $m = n$, to oczywiście też mamy $m \subseteq n$. Z symetrii założeń wynika, że również $n \subseteq m$. Zatem $m = n$.

Dla dowodu (iv) bierzemy zbiór

$$P = \{n \in N \mid \text{dla każdego } m \subseteq n,\ \text{ jeśli } m \neq n,\ \text{ to } m \in n\}.$$

Oczywiście $0 \in P$ (bo zbiór pusty nie zawiera właściwych podzbiorów). Załóżmy, że $n \in P$ i niech

$$m \subseteq n'. \tag{5}$$

Załóżmy, że m jest właściwym podzbiorem zbioru n'. Pokażemy, że $m \in n'$. Jeśli $n \in m$ to na mocy (i) $n \subseteq m$ więc także $n' \subseteq m$ i z (5) wynika,że $n' = m$, sprzeczność. Mamy więc $n \notin m$. Z (5) otrzymujemy

$$m \subseteq n.$$

Jeśli $m = n$, to oczywiście $m \in n'$. Niech więc $m \neq n$. Ponieważ m jest właściwym podzbiorem n, to z założenia indukcyjnego otrzymujemy $m \in n$, co daje $m \in n'$. To kończy dowód (iv)

Dla dowodu (v) rozważmy zbiór

$$P = \{n \in N \mid \text{ dla każdego } m \in N, \text{ jeśli } n \not\subseteq m \text{ to } m \subseteq n\}.$$

Dla dowodu induktywności zbioru P zauważmy, że $0 \in P$ oraz załóżmy, że $n \in P$. Weźmy dowolny m taki, że

$$n' \not\subseteq m. \tag{6}$$

Z założenia indukcyjnego wynika, że $m \subseteq n$ lub $n \subseteq m$. Jeśli $m \subseteq n$ to oczywiście $m \subseteq n'$ i nie musimy nic robić. Załóżmy więc, że $n \subseteq m$ i $n \neq m$. Z (iv) mamy $n \in m$. Zatem $n' \subseteq m$, co jest sprzeczne z (6). Otrzymana sprzeczność dowodzi, że założony przypadek nie może zajść. Zatem $n' \in P$.

Warunek (vi) wynika bezpośrednio z udowodnionych już punktów. Zachodzenie jednej z wymienionych możliwości wynika z (iv) i (v). Natomiast niemożliwość zajścia jednocześnie dwóch z wymienionych przypadków wynika z (ii) i (i). ∎

W przypadku liczb naturalnych relację zawierania oznacza sie zwyczajowo $\leq$, natomiast relację $\in$ oznacza się $<$. Jeśli $n \in m$, to mówimy, że n jest *mniejsze* od m oraz, że m jest *większe* od n. Następnik liczby n oznaczamy oczywiście przez $n+1$. Liczba naturalna n jest jednocześnie zbiorem wszystkich liczb naturalnych mniejszych od niej, tzn.

$$n = \{k \in N \mid k < n\}.$$

Poniższe twierdzenie mówi o tym, że każdy skończony niepusty zbiór liczb naturalnych ma element największy.

Twierdzenie 3.4 *Dla każdej liczby naturalnej n i dla każdego niepustego zbioru $X \subseteq n$ istnieje $n_0 \in X$ takie, że dla każdego $m \in X$, zachodzi $m \leq n_0$, tzn. n_0 jest największą liczbą w X.*

Dowód: Niech P będzie zbiorem tych wszystkich liczb naturalnych n, że dla każdego niepustego $X \subseteq n$, istnieje $n_0 \in X$ taki, że dla każdego $m \in X$, zachodzi $m \leq n_0$. Pokażemy, że P jest zbiorem induktywnym. Oczywiście $0 \in P$.

Załóżmy, że $n \in P$ i niech $X \subseteq n'$ będzie dowolnym niepustym podzbiorem. Rozważmy dwa przypadki.

Jeśli $n \in X$ to oczywiście szukanym elementem n_0 jest n. Jeśli natomiast $n \notin X$, to $X \subseteq n$ i z założenia indukcyjnego wnioskujemy o istnieniu $n_0 \in X$ o odpowiednich własnościach. ∎

Na zakończenie podamy ważne twierdzenie zwane *zasadą minimum*.

Twierdzenie 3.5 (Zasada minimum)
Każdy niepusty zbiór liczb naturalnych ma liczbę najmniejszą, tzn. jeśli $X \subseteq N$ oraz $X \neq \emptyset$, to istnieje $n_0 \in X$ takie, że dla każdego $m \in X$, $n_0 \leq m$.

Dowód: Niech X będzie niepustym zbiorem liczb naturalnych nie mającym najmniejszego elementu. Niech

$$P = \{n \in N \mid n \cap X = \emptyset\}.$$

Pokażemy, że P jest zbiorem induktywnym. Oczywiście $0 \in P$. Załóżmy, że $n \in P$ oraz, że $n' \cap X \neq \emptyset$. Zatem $n \in X$ oraz dla każdego $m < n$ mamy $m \notin X$. Oznacza to, że n jest najmniejszym elementem X. Otrzymana sprzeczność dowodzi, że $n' \cap X = \emptyset$, a zatem $n' \in P$.

Z zasady indukcji wynika, że $P = N$ a zatem $X = \emptyset$. Otrzymana sprzeczność dowodzi, że X musi mieć element najmniejszy. ∎

Zadania

3.1. Dowieść, że dla każdej liczby naturalnej $n \neq 0$, zachodzi $(\bigcup n)' = n$.

3.2. Dowieść, że $\bigcup N = N$.

3.3. Niech $n > 0$ będzie liczbą naturalną. Ile elementów ma najmniejszy zbiór A spełniający poniższe warunki?

a.) dla $1 \leq i \leq n$, zbiór $\{i\}$ należy do A;

b.) jeśli $X, Y \in A$, to $X \cup Y \in A$.

3.4. Ile elementów ma zbiór $P(n)$, gdzie n jest liczbą naturalną?

3.5. Ile elementów ma zbiór $m \times n$, gdzie m, n są liczbami naturalnymi?

3.6. Dowieść, że dla dowolnej liczby naturalnej $n \geq 2$,

$$A_1 \cup \ldots \cup A_n = (A_1 - A_2) \cup (A_2 - A_3) \cup \ldots (A_{n-1} - A_n) \cup (A_n - A_1) \cup (A_1 \cap \ldots \cap A_n).$$

4 Funkcje

Niech A i B będą zbiorami. *Funkcją* z A do B nazwiemy uporządkowaną trójkę $\langle f, A, B\rangle$, gdzie $f \subseteq A \times B$ jest relacją spełniającą następujące dwa warunki.

$$\text{Dla dowolnych } a \in A \text{ oraz } b_1, b_2 \in B, \text{ jeśli } \langle a, b_1\rangle \in f \text{ oraz } \langle a, b_2\rangle \in f, \text{ to } b_1 = b_2. \tag{7}$$

$$\text{Dla każdego } a \in A \text{ istnieje } b \in B \text{ taki, że } \langle a, b\rangle \in f. \tag{8}$$

W przypadku, gdy $\langle f, A, B\rangle$ jest funkcją z A do B, to mówimy zwykle, że f jest funkcją z A do B i oznaczamy to przez $f : A \to B$. Zauważmy, że funkcja jest zadana nie tylko przez relację f, ale również przez zbiory: A (zwany *dziedziną*) oraz B (zwany *przeciwdziedziną*). W szczególności może tak się zdarzyć, że mamy dwie różne funkcje $f : A \to B$ oraz $g : A \to C$, gdzie $B \neq C$ oraz relacje f i g są równe. Na przykład, $\langle I_A, A, A\rangle$ oraz $\langle I_A, A, B\rangle$, gdzie $A \subseteq B$ jest właściwym podzbiorem, są dwiema różnymi funkcjami (bo się różnią przeciwdziedzną). Tak więc, zgodnie z umową, mamy $I_A : A \to A$ oraz $I_A : A \to B$. Tę drugą funkcję zgrabniej jest oznaczyć, np. $\iota_{A,B} : A \to B$, podkreślając jej zależność od B, chociaż teoriomnogościowo, jako relacje mamy $I_A = \iota_{A,B}$. Będziemy się starali unikać używania niejednoznacznych nazw na funkcje.

Zbiór wszystkich funkcji z A w B oznaczamy symbolem B^A. Każdą trójkę $\langle f, A, B\rangle$ spełniającą (7) nazywamy *funkcją częściową* z A do B. Dziedziną funkcji częściowej f nazywamy zbiór

$$Dom(f) = \{a \in A \mid \text{ istnieje } b \in B \text{ taki, że } \langle a, b\rangle \in f\}.$$

Zauważmy, że jeśli $f \subseteq A \times B$ jest funkcją częściową z A do B, to f jest funkcją z $Dom(f)$ do B. Jeśli $f : A \to B$ oraz $a \in A$, to $f(a)$ oznacza jedyny element ze zbioru B taki, że $\langle a, f(a)\rangle \in f$. Element $f(a)$ jest *wartością* funkcji f na elemencie a.

Zauważmy, że istnieje dokładnie jedna funkcja $f : \emptyset \to A$, gdzie A jest dowolnym zbiorem. Jest to pusta relacja. Natomiast, jeśli $A \neq \emptyset$, to nie ma funkcji z A w $\emptyset$. W tym przypadku pusta relacja jest funkcją częściową, ale nie jest funkcją.

Przykład 4.1

(i) Relacja I_A z przykładu 2.2 (i) jest funkcją z A do A. Relacje $\leq$ oraz Q nie są funkcjami. P jest funkcją częściową z N do N. Dziedziną tej funkcji jest zbiór wszystkich liczb będących kwadratami liczb naturalnych. Relacja P^{-1} jest funkcją z N do N oraz relacja Q^{-1} jest funkcją z Z do N.

(ii) *Indeksowaną rodziną zbiorów* nazywamy dowolną funkcję ze *zbioru indeksów* I do rodziny zbiorów $\mathcal{A}$. Indeksowane rodziny zbiorów zwykle oznacza się przez $\{A_i\}_{i\in I}$. Sumę takiej rodziny oznaczamy przez $\bigcup_{i\in I} A_i$. Podobnie dla przecięć.

(iii) Niech A będzie dowolnym zbiorem. *Słowem* nad alfabetem A nazywamy skończony ciąg elementów zbioru A, czyli funkcję $w : n \to A$, gdzie $n \in N$. Liczba n jest *długością* słowa w, oznaczaną przez $|w|$. A^* oznacza zbiór wszystkich słów nad alfabetem A. Szczególnym słowem nad każdym alfabetem jest *słowo puste*, oznaczane ε, które definiuje się jako (jedyne) słowo długości 0.

Zgodnie z naszą notacją zbiór A^n można rozumieć na dwa sposoby—jako n-krotny iloczyn kartezjański zbioru A lub jako zbiór wszystkich funkcji ze zbioru n do A (czyli słów nad A długości n). Aby uniknąć takiej niejednoznaczności możemy utożsamiać n-tki uporządkowane elementów z A z funkcjami z n do A (w rozdziale dotyczącym relacji sprawę *implementacji* n-tek uporządkowanych pozostawiliśmy otwartą). Przy takim utożsamieniu n-tka $\langle a_1, \ldots, a_n \rangle$ jest reprezentowana przez funkcję $w : n \to A$ taką, że $w(i) = a_{i+1}$, dla $i < n$.

Na zbiorze słów mamy następująco zdefiniowaną operację *składania*. Niech $w : n \to A$ oraz $u : m \to A$ będą słowami. Złożenie słów w oraz u jest słowem $wu : m + n \to A$ zdefiniowanym dla $i < m + n$ następująco.

$$(wu)(i) = \begin{cases} w(i), & \text{jeśli } i < n \\ u(i-n), & \text{jeśli } n \leq i < m+n \end{cases}$$

(iv) Niech A będzie dowolnym zbiorem. *Multizbiorem* nad A nazywamy dowolną funkcję $\mathcal{A} : A \to N$. Mulizbiory tym się różnią od zbiorów, że ich elementy występują z *krotnościami*, tzn. gdy $\mathcal{A}(x) = 4$, to mówimy, że element x występuje w $\mathcal{A}$ z krotnością 4. Elementy występujące z krotnością 0 nie należą do $\mathcal{A}$. Zbiory można oczywiście traktować jako te multizbiory, w których każdy element występuje z krotnością co najwyżej 1. Przez $\mathcal{M}(A)$ bedziemy oznaczać zbiór wszystkich multizbiorów nad A.

Funkcję $f : A \to B$ nazwiemy *różnowartościową*, gdy dla dowolnych $a_1, a_2 \in A$, jeśli $f(a_1) = f(a_2)$, to $a_1 = a_2$. Funkcję f nazwiemy *na* B, jeśli dla każdego $b \in B$ istnieje $a \in A$ taki, że $f(a) = b$. Funkcję, która jest jednocześnie na oraz różnowartościowa nazywamy *bijekcją*.

Przykład 4.2

(i) Identyczność $I_A : A \to A$ jest bijekcją.

(ii) Funkcja $f : R \to R$, zdefiniowana wzorem $f(x) = x^2$ nie jest ani różnowartościowa ani na R.

(iii) Funkcja $f_1 : \{x \in R \mid 0 \leq x\} \to R$, zdefiniowana $f_1(x) = x^2$ jest różnowartościowa, ale nie jest na R. Funkcja f_1 jest *obcięciem* funkcji f do zbioru liczb rzeczywistych niedodatnich.

(iv) Funkcja $f_2 : R \to \{x \in R \mid 0 \leq x\}$, zdefiniowana $f_2(x) = x^2$ jest na, ale nie jest różnowartościowa.

(v) Funkcja $f : N \times N \to N$ zdefiniowana wzorem $f(m,n) = 2^n(2m+1)-1$ jest bijekcją. Rzeczywiście, jeśli $2^{n_1}(2m_1+1)-1 = 2^{n_2}(2m_2+1)-1$, to $2^{n_1}(2m_1+1) = 2^{n_2}(2m_2+1)$. Zatem, z jednoznaczności rozkładu liczb na czynniki pierwsze wynika, że $n_1 = n_2$. Otrzymujemy więc $2m_1 + 1 = 2m_2 + 1$, czyli $m_1 = m_2$, co oznacza, że f jest funkcją różnowartościową. Żeby pokazać,że f jest na, weźmy dowolną liczbę naturalną k. Niech $n \in N$ będzie największą liczbą taką, że 2^n dzieli $k+1$. Zatem $(k+1)/2^n$ jest liczbą nieparzystą. Niech $m = ((k+1)/2^n - 1)/2$. Łatwo sprawdzić, że $f(m,n) = k$. Dowodzi to, że f jest funkcją na N.

Twierdzenie 4.3 *Jeśli $f : A \to B$ oraz $g : B \to C$ są funkcjami, to relacja $gf \subseteq A \times C$ jest funkcją z A do C. Dla $a \in A$, $(gf)(a) = g(f(a))$. Ponadto, jeśli funkcje f, g są obie różnowartościowe lub obie na, to gf jest też różnowartościowa, lub odpowiednio, na.*

Dowód: Niech $a \in A$ będzie dowolnym elementem. Wtedy istnieje $b \in B$ oraz $c \in C$, takie że $\langle a,b\rangle \in f$ oraz $\langle b,c\rangle \in g$. Zatem istnieje $c \in C$ takie, że $\langle a,c\rangle \in gf$. Oznacza to, że

$$(gf)(a) = g(f(a)), \tag{9}$$

o ile pokażemy, że gf jest funkcją.

Dla pokazania jednoznaczności załóżmy, że $\langle a,c_1\rangle \in gf$ oraz $\langle a,c_2\rangle \in gf$. Wtedy istnieją $b_1, b_2 \in B$ takie, że $\langle a,b_1\rangle \in f$, $\langle a,b_2\rangle \in f$, $\langle b_1,c_1\rangle \in g$ oraz $\langle b_2,c_2\rangle \in g$. Ponieważ f jest funkcją to $b_1 = b_2$ a zatem, ponieważ g jest funkcją, to $c_1 = c_2$. Tak więc pokazaliśmy, że złożenie gf jest funkcją.

Jeśli f i g są różnowartościowe oraz $(gf)(a_1) = (gf)(a_2)$, to z różnowartościowości g oraz (9) wynika, że $f(a_1) = f(a_2)$. Zatem, z różnowartościowości f otrzymujemy $a_1 = a_2$, co dowodzi różnowartościowości gf.

Załóżmy, że f i g są na, i niech $c \in C$ będzie dowolnym elementem. Ponieważ g jest na C to istnieje $b \in B$ taki, że $g(b) = c$. Z faktu, że f jest na B otrzymujemy, że istnieje $a \in A$ taki, że $f(a) = b$. Zatem $(gf)(a) = g(f(a)) = g(b) = c$, co dowodzi, że gf jest na C. ■

Niech $f : A \to B$ będzie funkcją. Funkcję $g : B \to A$ nazwiemy *odwrotną* do f jeśli

$$gf = I_A \text{ oraz } fg = I_B.$$

Twierdzenie 4.4 *Niech $f : A \to B$ będzie funkcją. Następujące warunki są równoważne*

(i) f ma funkcję odwrotną,

(ii) f jest bijekcją,

(iii) Relacja odwrotna f^{-1} jest funkcją.

Dowód: Załóżmy (i) i niech $g : B \to A$ będzie funkcją odwrotną do f. Jeśli $f(a_1) = f(a_2)$, to $g(f(a_1)) = g(f(a_2))$. Ponieważ $gf = I_A$ to $a_1 = a_2$. Zatem f jest różnowartościowa. Dla pokazania, że f jest na weźmy dowolny $b \in B$. Niech $a = g(b)$. Wtedy $f(a) = f(g(b)) = b$, ponieważ $fg = I_B$. Zatem f jest bijekcją.

Załóżmy teraz (ii). Pokażemy, że relacja f^{-1} jest funkcją. Weźmy dowolny $b \in B$. Ponieważ f jest na, to istnieje $a \in A$ takie że $f(a) = b$. Oznacza to, że $\langle b, a\rangle \in f^{-1}$. Jeśli natomiast $\langle b, a_1\rangle \in f^{-1}$ oraz $\langle b, a_2\rangle \in f^{-1}$ to mamy $f(a_1) = f(a_2)$ i z różnowartościowości f otrzymujemy $a_1 = a_2$. W ten sposób udowodniliśmy, że f^{-1} jest funkcją.

Na zakończenie dowodu załóżmy (iii). Wówczas dla dowolnego $a \in A$, mamy $\langle a, a\rangle \in f^{-1}f$, bo $\langle a, f(a)\rangle \in f$. Zatem $I_A \subseteq f^{-1}f$. Z drugiej strony, jeśli $\langle a_1, a_2\rangle \in f^{-1}f$, to istnieje $b \in B$, takie że $\langle a_1, b\rangle \in f$ oraz $\langle b, a_2\rangle \in f^{-1}$. Więc $\langle b, a_1\rangle \in f^{-1}$ i ponieważ f^{-1} jest funkcją to $a_1 = a_2$. To dowodzi, że $f^{-1}f = I_A$.

Dowód równości $ff^{-1} = I_B$ jest analogiczny i pozostawiamy go czytelnikowi. ∎

Oczywiście funkcję odwrotną do danej funkcji f oznaczamy f^{-1}.

Niech $f : A \to B$ będzie funkcją i niech $X \subseteq A$. *Obrazem* zbioru X przy przekształceniu f nazwiemy zbiór

$$\vec{f}(X) = \{b \in B \mid \text{ istnieje } a \in X, \text{ taki że } f(a) = b\}.$$

Dla zbioru $Y \subseteq B$, *przeciwobrazem* zbioru Y przy przekształceniu f nazwiemy zbiór

$$\vec{f}^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

Twierdzenie 4.5 *Niech $f : A \to B$ będzie funkcją, niech $\mathcal{X}$ będzie rodziną podzbiorów zbioru A oraz niech $\mathcal{Y}$ będzie rodziną podzbiorów zbioru B. Wtedy*

(i) $\vec{f}(\bigcup \mathcal{X}) = \bigcup\{\vec{f}(X) \mid X \in \mathcal{X}\}$,

(ii) Jeśli $\mathcal{X} \neq \emptyset$, *to* $\vec{f}(\bigcap \mathcal{X}) \subseteq \bigcap\{\vec{f}(X) \mid X \in \mathcal{X}\}$,

(iii) $\vec{f}^{-1}(\bigcup \mathcal{Y}) = \bigcup\{\vec{f}^{-1}(Y) \mid Y \in \mathcal{Y}\}$,

(iv) Jeśli $\mathcal{Y} \neq \emptyset$, *to* $\vec{f}^{-1}(\bigcap \mathcal{Y}) = \bigcap\{\vec{f}^{-1}(Y) \mid Y \in \mathcal{Y}\}$.

Dowód: Udowodnimy (i). Niech $b \in B$ będzie dowolnym elementem. Mamy następujący ciąg równoważności.

$b \in \vec{f}(\bigcup \mathcal{X})$ wtw, gdy
istnieje $a \in \bigcup \mathcal{X}$ takie, że $f(a) = b$ wtw, gdy
istnieje $a \in A$ oraz istnieje $X \in \mathcal{X}$ takie, że $a \in X$ oraz $f(a) = b$ wtw, gdy
istnieje $X \in \mathcal{X}$ oraz istnieje $a \in A$ takie, że $a \in X$ oraz $f(a) = b$ wtw, gdy
istnieje $X \in \mathcal{X}$ takie, że $b \in \vec{f}(X)$ oraz $f(a) = b$ wtw, gdy
$b \in \bigcup\{\vec{f}(X) \mid X \in \mathcal{X}\}$.

Dla dowodu (ii) weźmy dowolny $b \in \vec{f}(\bigcap \mathcal{X})$. Oznacza to, że istnieje $a \in \bigcap \mathcal{X}$ taki, że $f(a) = b$. Zatem dla każdego $X \in \mathcal{X}$ mamy: $a \in X$ oraz $f(a) = b$. Tak więc b należy do każdego obrazu $\vec{f}(X)$, dla X przebiegających $\mathcal{X}$, czyli $b \in \bigcap\{\vec{f}(X) \mid X \in \mathcal{X}\}$, co kończy dowód.

Powyższy dowód można rozpisać na podobne kroki tak jak w poprzednim przypadku. Dostaniemy ciąg równoważności za wyjątkiem jednego przejścia, które jest tylko w jedną stronę (które?).

Natępnie udowodnimy (iii). Niech $a \in A$ będzie dowolnym elementem. Mamy następujący ciąg równoważności.

$a \in \vec{f}^{-1}(\bigcup \mathcal{Y})$ wtw, gdy
$f(a) \in \bigcup \mathcal{Y}$ wtw, gdy
istnieje $Y \in \mathcal{Y}$ takie, że $f(a) \in Y$ wtw, gdy
istnieje $Y \in \mathcal{Y}$ takie, że $a \in \vec{f}^{-1}(Y)$ wtw, gdy
$a \in \bigcup\{\vec{f}^{-1}(Y) \mid Y \in \mathcal{Y}\}$.

Dowód (iv) jest zupełnie analogiczny do powyższego dowodu i dlatego pozostawimy go czytelnikowi. ■

Przykład 4.6 Zawieranie w punkcie (ii) powyższego twierdzenia nie może być zastąpione równością o czym świadczy następujący przykład. Niech f będzie funkcją z Przykładu 4.2 (ii). Niech $A = \{-1\}$ oraz $B = \{1\}$. Wówczas

$$\vec{f}(A \cap B) = \vec{f}(\emptyset) = \emptyset,$$

ale

$$\vec{f}(A) \cap \vec{f}(B) = \{1\}.$$

Dla funkcji różnowartościowych zawieranie w Twierdzeniu 4.5 (ii) można zastąpić równością.

4.1 Definiowanie funkcji przez indukcję

W zbiorze liczb naturalnych możemy definiować funkcje wykorzystując własność zbioru N polegającą na tym, że jest to najmniejszy zbiór zawierający 0 i zamknięty na operację następnika.

Rozważmy następujący przykład.

Przykład 4.7 Chcemy zdefiniować operację dodawania w zbiorze liczb naturalnych opierając się jedynie na operacji następnika. Oczywiście dodawanie $f : N \times N \to N$ jest funkcją spełniającą następujące warunki.

$$f(m,0) = m$$
$$f(m,n') = f(m,n)'.$$

Zauważmy, że powyższe równości można traktować jak opis sposobu na obliczanie dodawania dwóch liczb naturalnych. Pierwsza równość dotyczy sytuacji gdy drugi argument w f jest równy 0, podczas gdy drugie równanie definiuje wynik dodawania m do następnika n odwołując się do wyniku dodawania m do n, a więc do pary argumentów, dla której możemy założyć, że umiemy policzyć wartość. Liczba m w powyższej definicji jest dowolna ale ustalona. Nazywamy ją *parametrem* tej definicji.

Do definiowania funkcji powyższą metodą służy następujące twierdzenie.

Twierdzenie 4.8 (O definiowaniu funkcji przez indukcję)
Niech A i B będą dowolnymi zbiorami takimi, że $B \neq \emptyset$. Niech $g : A \to B$ oraz $h : B \times A \times N \to B$ będą dowolnymi funkcjami. Wtedy istnieje dokładnie jedna funkcja $f : A \times N \to B$ spełniająca następujące warunki dla dowolnego $a \in A$ oraz $n \in N$,

$$f(a,0) = g(a)$$
$$f(a,n') = h(f(a,n),a,n).$$

W powyższym twierdzeniu A jest zbiorem *parametrów*. Dowód Twierdzenia 4.8 będzie podany później – w dziale o punktach stałych.

Tak więc wynika z powyższego twierdzenia, że istnieja dokładnie jedna funkcja f spełniająca równania Przykładu 4.7. Funkcje g i h dla tego przykładu wyglądają następująco: $g = I_N$, $h(x,y,z) = x'$, dla $x,y,z \in N$. Wartość $f(m,n)$ oczywiście oznaczamy przez $m+n$. Podamy jeszcze dwa przykłady definicji indukcyjnych.

Przykład 4.9 Używając operacji dodawania możemy zdefiniować indukcyjnie mnożenie. Jest to (jedyna) funkcja $f : N \times N \to N$ spełniająca równania

$$f(m,0) = 0$$
$$f(m,n') = m + f(m,n).$$

Funkcją g dla tego przykładu jest $g(x) = 0$ dla $x \in N$. Natomiast funkcją h jest $h(x, y, z) = y + x$ dla $x, y, z \in N$.

Przykład 4.10 Zbiór parametrów oczywiście nie musi być zbiorem liczb naturalnych. Poniższy układ równań definiuje operację iteracji $Iter : P(A \times A) \times N \to P(A \times A)$ dowolnej relacji binarnej w A, gdzie A jest dowolnym zbiorem.

Dla $r \subseteq A \times A$ oraz $n \in N$ definiujemy

$$Iter(r, 0) = I_A$$
$$Iter(r, n') = r\ Iter(r, n).$$

Oczywiście $Iter(r, n)$ jest n-krotnym złożeniem relacji r ze sobą. Funkcją $g : P(A \times A) \to P(A \times A)$ jest $g(r) = I_A$, dla $r \in P(A \times A)$. Natomiast funkcją $h : P(A \times A) \times P(A \times A) \times N \to P(A \times A)$ jest zdefiniowana następująco: $h(r_1, r_2, n) = r_2 r_1$, dla $r_1, r_2 \in P(A \times A)$ oraz $n \in N$.

Zdarzają się sytuacje, jak zobaczymy później, w których będziemy definiowali indukcyjnie funkcję odwołując się nie tylko do jej wartości dla liczby poprzedniej, ale uzależniając wynik od wszystkich dotąd obliczonych wartości. W tym celu udowodnimy następujące twierdzenie.

Twierdzenie 4.11 *Niech A i B będą dowolnymi zbiorami takimi, że $B \neq \emptyset$. Niech $g : A \to B$ oraz $h : B^* \times A \times N \to B$ będą dowolnymi funkcjami. Wtedy istnieje dokładnie jedna funkcja $f : A \times N \to B$ spełniająca następujące warunki dla dowolnego $a \in A$ oraz $n \in N$,*

$$f(a, 0) = g(a)$$
$$f(a, n') = h((f(a, 0) \cdots f(a, n)), a, n).$$

W powyższym równaniu $(f(a, 0) \cdots f(a, n))$ jest słowem w B^* o literach $f(a, 0), \ldots, f(a, n)$.

Dowód: Oczywiście istnieje co najwyżej jedna funkcja f spełniająca warunki powyższego twierdzenia. Jeśli f_1 i f_2 są dwiema takimi funkcjami, to bez trudu pokazujemy przez indukcję, że dla dowolnych $n \in N$ oraz $a \in A$,

$$f_1(a, n) = f_2(a, n).$$

Łatwy dowód powyższej równości pozostawimy czytelnikowi.

Dla dowodu istnienia f zastosujemy Twierdzenie 4.8. Niech $\tilde{B} = B^*$ i niech $\tilde{g} : A \to \tilde{B}$ będzie zdefiniowana tak, że $\tilde{g}(a)$ jest słowem jednoliterowym $g(a)$. Dalej, niech $\tilde{h} : \tilde{B} \times A \times N \to \tilde{B}$ będzie funkcją zdefiniowaną następująco

$$\tilde{h}(w, a, n) = w\, h(w, a, n),$$

tzn. do słowa w jest dopisywana litera $h(w, a, n)$.

Niech $\tilde{f} : A \times N \to \tilde{B}$ będzie jedyną funkcją zdefiniowaną indukcyjnie przez warunki

$$\tilde{f}(a,0) = \tilde{g}(a)$$
$$\tilde{f}(a,n') = \tilde{h}(\tilde{f}(a,n),a,n).$$

Niech $\ell : B^* \to B$ będzie funkcją przyporządkowującą dowolnemu niepustemu słowu w ostatnią, tj. najbardziej prawą literę w tym słowie. Ponadto przyjmijmy $\ell(\varepsilon) = b_0$, gdzie $b_0 \in B$ jest dowolnym, ustalonym elementem. Niech $f : A \times N \to B$ będzie funkcją zdefiniowaną następująco

$$f(a,n) = \ell(\tilde{f}(a,n)).$$

Najpierw pokażemy, że

$$\tilde{f}(a,n) = (f(a,0)\cdots f(a,n)). \tag{10}$$

Dowód (10) jest przez indukcję ze względu na n. Dla $n = 0$ mamy

$$\tilde{f}(a,0) = \tilde{g}(a) = (g(a)) = (\ell(\tilde{g}(a))) = (\ell(\tilde{f}(a,0))) = (f(a,0)).$$

Ponadto

$$\tilde{f}(a,n') = \tilde{h}(\tilde{f}(a,n),a,n) = \tilde{f}(a,n)h(\tilde{f}(a,n),a,n)) =$$
$$(f(a,0)\cdots f(a,n))\ell(\tilde{f}(a,n')) = (f(a,0)\cdots f(a,n)f(a,n')).$$

Tak więc pokazaliśmy (10). Pozostaje pokazać, że f spełnia zadane warunki. Oczywiście mamy

$$f(a,0) = \ell(\tilde{f}(a,0)) = \ell(\tilde{g}(a)) = g(a).$$

Ponadto

$$f(a,n') = \ell(\tilde{f}(a,n') = \ell(\tilde{h}(\tilde{f}(a,n),a,n)) =$$
$$\ell(\tilde{f}(a,n)h(\tilde{f}(a,n),a,n)) = h(\tilde{f}(a,n),a,n) =$$
$$h((f(a,0)\cdots f(a,n)),a,n).$$

Ostatnia równość w powyższym ciągu równości wynika z (10). Tak więc f jest żądaną funkcją. ∎

Zadania

4.1. Niech $I \neq \emptyset$. Udowodnić, że dla każdej rodziny indeksowanej $\{A_{i,j}\}_{i\in I, j\in J}$ zachodzi

$$\bigcap_{i\in I}\bigcup_{j\in J} A_{i,j} = \bigcup_{f\in J^I}\bigcap_{i\in I} A_{i,f(i)}$$

4.2. Niech $f : A^A \to P(A)$ będzie taka, że $f(\varphi) = \vec{\varphi}(A)$. Czy f jest różnowartościowa i czy jest na $P(A)$? Przedyskutować odpowiedź w zależności od zbioru A.

4.3. Niech $A \neq \emptyset$ i niech $f : A \to A$. Udowodnić, że dla dowolnego $a \in A$ istnieje najmniejszy zbiór $X \subseteq A$ taki, że $a \in X$ oraz $\vec{f^{-1}}(X) \subseteq X$.

4.4. Niech $f : P(N) \times P(N) \to P(N)$ będzie taka, że $f(A, B) = A \cap B$, dla dowolnych $A, B \subseteq N$. Czy f jest różnowartościowa i czy jest na $P(N)$? Wyznaczyć $\vec{f^{-1}}(\{N\})$. Niech $C \subseteq N$ będzie dowolnym zbiorem. Wyznaczyć $\vec{f}(P(C) \times P(C))$.

4.5. Niech $f : N^N \to P(N)$ będzie taka, że $f(\varphi) = \vec{\varphi^{-1}}(\{1\})$. Czy f jest różnowartościowa i czy jest na $P(N)$? Znaleźć obraz zbioru wszystkich funkcji stałych i przeciwobrazy zbiorów $\{\{5\}\}$ i $\{5\}$.

4.6. Niech $f : A \to B$ i niech $X \subseteq A$ oraz $Y \subseteq B$. Dowieść, że

$$X \subseteq \vec{f^{-1}}(Y) \quad \text{wtw, gdy} \quad \vec{f}(X) \subseteq Y.$$

4.7. Podać przykład takiej funkcji f oraz zbiorów A, B, że $\vec{f^{-1}}(\vec{f}(A)) \neq A$ oraz $\vec{f}(\vec{f^{-1}}(B)) \neq B$.

4.8. Niech $f : A \to B$. Udowodnić, że f jest różnowartościowa wtedy i tylko wtedy, gdy dla każdego zbioru C i dowolnych $g, h : C \to A$, jeśli $fg = fh$, to $g = h$.

4.9. Niech $f : A \to B$. Udowodnić, że f jest na B wtedy i tylko wtedy, gdy dla każdego zbioru C i dowolnych $g, h : B \to C$, jeśli $gf = hf$, to $g = h$.

4.10. Niech $f : P(R) \to P(P(R))$ będzie taka, że $f(A) = P(A)$, dla $A \subseteq R$. Czy f jest różnowartościowa i czy jest na $P(P(R))$? Znaleźć $\vec{f^{-1}}(P(P(Q)))$, gdzie R oznacza zbiór liczb rzeczywistych a Q zbiór liczb wymiernych.

4.11. Dowieść, że funkcja $f : P(A)^B \to P(A \times B)$ taka, że dla $\varphi \in P(A)^B$,

$$f(\varphi) = \{\langle a, b\rangle \in A \times B \mid a \in \varphi(b)\}$$

jest bijekcją.

4.12. Dowieść, że funkcja $g : P(A \times B) \to P(A)^B$ taka, że dla $R \subseteq A \times B$ oraz $b \in B$,

$$g(R)(b) = \{a \in A \mid \langle a, b\rangle \in R\}$$

jest bijekcją. Czy g jest funkcją odwrotną do funkcji f z poprzedniego zadania?

5 Relacje równoważności

Relację $R \subseteq A \times A$ nazwiemy *relacją równoważności* w A gdy spełnia ona następujące trzy warunki.

- (*Zwrotność*) Dla każdego $a \in A$, $\langle a, a\rangle \in R$,
- (*Symetria*) Dla dowolnych $a, b \in A$, jeśli $\langle a, b\rangle \in R$, to $\langle b, a\rangle \in R$,
- (*Przechodniość*) Dla dowolnych $a, b, c \in A$, jeśli $\langle a, b\rangle \in R$, oraz $\langle b, c\rangle \in R$, to $\langle a, c\rangle \in R$.

Niech $R \subseteq A \times A$ będzie relacją równoważności w A i niech $a \in A$. *Klasą abstrakcji* elementu a nazwiemy zbiór

$$[a]_R = \{x \in A \mid \langle a, x\rangle \in R\}.$$

Rodzinę $\mathcal{P}$ podzbiorów zbioru A nazwiemy *podziałem* zbioru A, gdy spełnia ona następujące trzy warunki.

- Każdy zbiór z $\mathcal{P}$ jest niepusty,
- Jeśli $X_1, X_2 \in \mathcal{P}$ oraz $X_1 \cap X_2 \neq \emptyset$, to $X_1 = X_2$,
- $\bigcup \mathcal{P} = A$.

Następujące twierdzenie ustala wzajemną odpowiedniość pomiędzy podziałami danego zbioru a relacjami równoważności w tym zbiorze.

Twierdzenie 5.1 (Zasada abstrakcji)

(i) Klasy abstrakcji dowolnej relacji równoważności w A tworzą podział zbioru A.

(ii) Dla każdego podziału zbioru A istnieje dokładnie jedna relacja równoważności, której klasy abstrakcji wyznaczają ten podział.

Dowód: Udowodnimy najpierw pierwszą część twierdzenia. Niech $R \subseteq A \times A$ będzie relacją równoważności i niech $\mathcal{P} = \{[a]_R \mid a \in A\}$ będzie zbiorem wszystkich klas abstrakcji relacji R. Ponieważ, $a \in [a]_R$, jak wynika to ze zwrotności R, to $[a]_R \neq \emptyset$.

Przypuśćmy, że $c \in [a]_R \cap [b]_R$. Zatem

$$\langle a, c\rangle \in R \text{ oraz } \langle b, c\rangle \in R.$$

Korzystając z symetrii i przechodniości R otrzymujemy

$$\langle a, b\rangle \in R. \tag{11}$$

Niech $x \in [a]_R$ będzie dowolnym elementem. Zatem $\langle a, x\rangle \in R$. Korzystając z (11), symetrii i przechodniości dostajemy $\langle b, x\rangle \in R$, czyli $x \in [b]_R$. Tak więc, $[a]_R \subseteq [b]_R$. Ze względu na symetrię założeń otrzymujemy również $[b]_R \subseteq [a]_R$, co łącznie daje $[a]_R = [b]_R$.

Oczywiście $\bigcup \mathcal{P} \subseteq A$. Ponieważ $a \in [a]_R$, to również $A \subseteq \bigcup \mathcal{P}$. Zatem $\cup\mathcal{P} = A$ i $\mathcal{P}$ jest podziałem.

Dla dowodu drugiej części twierdzenia weźmy dowolny podział $\mathcal{P}$ zbioru A. Niech $\sim_{\mathcal{P}} \subseteq A \times A$ będzie relacją zdefiniowaną następująco

$$\langle a, b\rangle \in \sim_{\mathcal{P}} \quad \text{wtw, gdy istnieje} \quad X \in \mathcal{P} \quad \text{taki, że } a, b \in X.$$

Pokażemy najpierw, że $\sim_{\mathcal{P}}$ jest relacją równoważności. Niech $a \in A$. Ponieważ $A = \bigcup \mathcal{P}$, to istnieje $X \in \mathcal{P}$ taki, że $a \in X$. Zatem $\langle a, a\rangle \in \sim_{\mathcal{P}}$, co dowodzi zwrotności. Relacja $\sim_{\mathcal{P}}$ jest oczywiście symetryczna. Niech $\langle a, b\rangle \in \sim_{\mathcal{P}}$ oraz $\langle b, c\rangle \in \sim_{\mathcal{P}}$. Zatem istnieją $X, Y \in \mathcal{P}$ takie, że $a, b \in X$ oraz $b, c \in Y$. Ponieważ X i Y mają element wspólny, to $X = Y$. Zatem $\langle a, c\rangle \in \sim_{\mathcal{P}}$, co dowodzi przechodniości. Stąd $\sim_{\mathcal{P}}$ jest relacją równoważności.

Niech $\mathcal{P}' = \{[a] \mid a \in A\}$ będzie podziałem wyznaczonym przez $\sim_{\mathcal{P}}$. Dla uproszczenia notacji, w tej części dowodu $[a]$ będzie oznaczało $[a]_{\sim_{\mathcal{P}}}$. Pokażemy, że $\mathcal{P} = \mathcal{P}'$. Niech $X \in \mathcal{P}$. Ponieważ $X \neq \emptyset$, to niech $a \in X$ będzie dowolnym elementem. Pokażemy, że

$$X = [a]. \tag{12}$$

Jeśli $x \in X$, to $\langle a, x\rangle \in \sim_{\mathcal{P}}$, a zatem $x \in [a]$. Na odwrót, jeśli $x \in [a]$, to $\langle a, x\rangle \in \sim_{\mathcal{P}}$, a zatem istnieje $Y \in \mathcal{P}$ taki, że $a, x \in Y$. Ponieważ X i Y mają wspólny element (mianowicie a), to $X = Y$. Czyli $x \in X$, co dowodzi (12). W ten sposób pokazaliśmy, że $\mathcal{P} \subseteq \mathcal{P}'$.

Dla dowodu zawierania $\mathcal{P}' \subseteq \mathcal{P}$ weźmy dowolny $[a] \in \mathcal{P}'$. Niech $X \in \mathcal{P}$ będzie zbiorem zawierającym a. Pokażemy, że

$$X = [a]. \tag{13}$$

Jeśli $x \in X$, to mamy $a, x \in X$, a zatem $\langle a, x\rangle \in \sim_{\mathcal{P}}$, czyli $x \in [a]$. Dowód odwrotnego zawierania jest analogiczny do dowodu zawierania $[a] \subseteq X$ w (12). To kończy dowód (13), a co za tym idzie dowód istnienia relacji równoważności wyznaczającej zadany podział $\mathcal{P}$.

Pozostaje do wykazania jednoznaczność. Przypuśćmy, że R_1 i R_2 są dwiema relacjami równoważności oraz, że

$$\{[a]_{R_1} \mid a \in A\} = \{[a]_{R_2} \mid a \in A\}. \tag{14}$$

Udowodnimy, że

$$R_1 = R_2.$$

Niech $\langle a, b\rangle \in R_1$. Wynika z (14), że istnieje $c \in A$ takie, że $[a]_{R_1} = [c]_{R_2}$. Zatem $a, b \in [c]_{R_2}$, co na mocy symetrii i przechodniości R_2 daje $\langle a, b\rangle \in R_2$. W ten sposób pokazaliśmy zawieranie $R_1 \subseteq R_2$. Ponieważ role R_1 i R_2 są całkowicie symetryczne, to powyższe rozumowanie może być użyte do udowodnienia zawierania w stronę przeciwną. To kończy dowód jednoznaczności, a tym samym całego twierdzenia. ■

Niech R będzie relacją równoważności w zbiorze A. *Zbiorem ilorazowym* A/R nazywamy zbiór wszystkich klas abstrakcji relacji R, tzn.

$$A/R = \{[a]_R \mid a \in A\}.$$

Ze zbiorem ilorazowym A/R jest naturalnie związane przekształcenie kanoniczne $[-]_R : A \to A/R$, które każdemu elementowi $a \in A$ przyporządkowuje klasę abstrakcji $[a]_R$.

Przykład 5.2 Podamy kilka przykładów relacji równoważności. Łatwe dowody, że relacje te są istotnie relacjami równoważności pozostawiamy czytelnikowi.

(i) Niech $L \subseteq A^*$. Na zbiorze słów A^* zdefiniujemy relację $\sim_L$ jak następuje. Dla $u, w \in A^*$, $u \sim_L w$ zachodzi wtw, gdy dla dowolnych słów $x, y \in A^*$ mamy następującą równoważność,

$$xuy \in L \quad \text{wtw, gdy} \quad xwy \in L.$$

Tak więc dwa słowa są w relacji $\sim_L$ gdy ich zachowanie w każdym kontekście jest takie samo ze względu na należenie do L. Relacja ta jest relacją równoważności. Jest to ważna relacja spotykana w teorii języków formalnych. Język L nazywa sie językiem *regularnym* gdy zbiór ilorazowy $A^*/\sim_L$ jest skończony.

(ii) Niech n będzie liczbą naturalną. W zbiorze Z liczb całkowitych definiujemy relację $\equiv_n$ jak następuje,

$$k \equiv_n l \quad \text{wtw, gdy} \quad n|(k-l),$$

tzn., gdy k oraz l mają tę samą resztę z dzielenia przez n. Relacja $\equiv_n$ jest relacją równoważności. Zbiór ilorazowy $Z/\equiv_n$ nazywa się zbiorem liczb całkowitych *modulo* n. Elementy tego zbioru mogą być reprezentowane przez n różnych reszt: $0, 1, \ldots, n-1$.

(iii) Niech zbiór $\mathcal{W}$ będzie najmniejszym zbiorem słów nad alfabetem $N \cup \{+, \times, (,)\}$ (nawiasy "(,)" są tutaj elementami alfabetu) spełniającym następujące warunki

- Dla $n \in N$, $n \in \mathcal{W}$,
- Jeśli $u, w \in \mathcal{W}$, to $(u + w) \in \mathcal{W}$ oraz $(u \times w) \in \mathcal{W}$.

Elementy zbioru $\mathcal{W}$ nazywamy *wyrażeniami*. W zbiorze wyrażeń zdefiniujemy relację $\simeq$ przyjmując, że $u \simeq w$ wtw, gdy wyrażenia u oraz w wyznaczają tę samą liczbę naturalną (przyjmując, że + oznacza dodawanie, a $\times$ oznacza mnożenie). Relacja $\simeq$ jest relacją równoważności.

(iv) Powyższe przykłady relacji równoważności są szczególnym przypadkiem następującego ogólnego schematu. Niech $f : A \to B$ będzie funkcją. *Jądrem* funcji f nazywamy relację $ker(f)$ zdefiniowaną następująco

$$\langle a_1, a_2 \rangle \in ker(f) \text{ wtw, gdy } f(a_1) = f(a_2).$$

Relacja $ker(f)$ jest relacją równoważności.

Relacja z (i) jest jądrem funkcji, która każdemu słowu w przyporządkowuje zbiór wszystkich kontekstów, w których to słowo może się pojawić w L, tzn $f(w) = \{\langle x, y \rangle \in A^* \mid xwy \in L\}$. Relacja z (ii) jest jądrem funkcji przyporządkowującej każdej liczbie całkowitej jej resztę z dzielenia przez n. Wreszcie relacja z przykładu (iii) jest jądrem funkcji przyporządkowującej każdemu wyrażeniu jego wartość.

Na zakończenie tej części podamy przykład konstrukcji używającej zbiorów ilorazowych.

Przykład 5.3 (*Konstrukcja pierścienia liczb całkowitych*)
Pokażemy jak można skonstruować zbiór liczb całkowitych z operacjami dodawania i mnożenia, opierając się na zbiorze liczb naturalnych z operacjami dodawania + i mnożenia $\times$. Liczbę całkowitą k chcemy przedstawić jako parę liczb naturalnych $\langle n, m \rangle$ takich, że ich różnica daje k. Oczywiście to prowadzi do konieczności utożsamienia pewnych par. W zbiorze $N \times N$ zdefiniujemy binarną relację $\sim$,

$$\langle m, n \rangle \sim \langle m', n' \rangle \quad \text{wtw, gdy} \quad m + n' = n + m'.$$

Łatwo jest sprawdzić, że $\sim$ jest relacją równoważności w $N \times N$. Niech $Z = (N \times N)/\sim$. W zbiorze Z wprowadzimy dwie operacje.

$$[\langle m, n \rangle]_\sim \oplus [\langle m', n' \rangle]_\sim = [\langle m + m', n + n' \rangle]_\sim \tag{15}$$

$$[\langle m, n \rangle]_\sim \otimes [\langle m', n' \rangle]_\sim = [\langle (m \times m') + (n \times n'), (m \times n') + (n \times m') \rangle]_\sim. \tag{16}$$

Przy definiowaniu operacji na klasach abstrakcji, tak jak to miało miejsce w (15) i (16), bardzo ważną rzeczą jest pokazanie *poprawności* tych definicji, tzn. pokazanie, że wynik operacji wykonanej na dwóch klasach abstrakcji nie zależy od wyboru reprezentantów tych klas. Poprawność operacji zdefiniowanych w (15) i (16) wynika bezpośrednio z następującego lematu.

Lemat 5.4

(i) Jeśli $\langle m_1, n_1\rangle \sim \langle m_2, n_2\rangle$ *oraz* $\langle m_1', n_1'\rangle \sim \langle m_2', n_2'\rangle$, *to*

$$\langle m_1 + m_1', n_1 + n_1'\rangle \sim \langle m_1 + m_1', n_1 + n_1'\rangle.$$

(ii) Jeśli $\langle m_1, n_1\rangle \sim \langle m_2, n_2\rangle$ *oraz* $\langle m_1', n_1'\rangle \sim \langle m_2', n_2'\rangle$, *to*

$$\langle (m_1\times m_1')+(n_1\times n_1'), (m_1\times n_1')+(n_1\times m_1')\rangle \sim \langle (m_2\times m_2')+(n_2\times n_2'), (m_2\times n_2')+(n_2\times m_2')\rangle.$$

Dowód: Łatwy dowód lematu pozostawimy czytelnikowi jako ćwiczenie. ■

Zadania

5.1. Niech R będzie relacją dwuargumentową w N^N taką, że $\langle f, g\rangle \in R$ wtw, gdy dla każdego $n \in N$, różnica $f(n) - g(n)$ jest liczbą parzystą. Pokazać, że R jest relacją równoważności. Opisać klasę abstrakcji identyczności I_N. Czy zbiór klas abstrakcji R jest nieskończony?

5.2. Niech R_1, R_2 będą relacjami równoważności w A. Czy z tego, że $A/R_1 = A/R_2$ wynika, że $R_1 = R_2$? Pokazać, że zbiór $\{X \subseteq A \mid$ istnieje $a \in A$ takie, że $X = [a]_{R_1} \cap [a]_{R_2}\}$ jest zbiorem klas abstrakcji pewnej relacji równoważności. Jaka to relacja?

5.3. Czy relacje równoważności są zamknięte na następujące operacje?

a.) suma;

b.) przecięcie;

c.) składanie.

5.4. Niech R_1, R_2 będą relacjami równoważności w A.

a.) Dowieść, że $R_1R_2 = A^2$ wtw, gdy $R_2R_1 = A^2$.

b.) Dowieść, że $R_1 \cup R_2$ jest relacją równoważności wtw, gdy $R_1 \cup R_2 = R_1R_2$.

c.) Dowieść, że R_1R_2 jest relacją równoważności wtw, gdy $R_1R_2 = R_2R_1$.

5.5. Dowieść, że dla dowolnej relacji $R \subseteq A^2$ istnieje najmniejsza relacja równoważności w A zawierająca R.

5.6. Niech $\mathcal{R}$ będzie niepustą rodziną relacji równoważności w zbiorze A spełniającą następujący warunek. Dla dowolnych $R_1, R_2 \in \mathcal{R}$, zachodzi $R_1 \subseteq R_2$ lub $R_2 \subseteq R_1$. Dowieść, że $\bigcup \mathcal{R}$ jest relacją równoważności w A.

5.7. Niech R_1, R_2 będą relacjami równoważności w A takimi, że $R_1 \cap R_2 = I_A$ oraz $R_1 R_2 = A^2$. Wskazać bijekcję pomiędzy zbiorami $A/R_1 \times A/R_2$ oraz A.

6 Teoria mocy

Powiemy, że zbiory A, B są *równoliczne* (oznaczamy $A \sim B$), gdy istnieje bijekcja $f : A \to B$.

Przykład 6.1

(i) $N \times N \sim N$, gdzie bijekcją $f : N \times N \to N$ jest funkcja określona w przykładzie 4.2 (5).

(ii) N jest równoliczny ze zbiorem liczb parzystych Par, funkcją ustalającą równoliczność jest $f(n) = 2n$.

(iii) Niech $a < b$ będą dowolnymi liczbami rzeczywistymi, wtedy odcinek otwarty (a, b) jest równoliczny z odcinkiem otwartym $(0, 1)$, gdzie bijekcją $f : (a, b) \to (0, 1)$ jest funkcja $f(x) = \frac{(x-a)}{(b-a)}$.

(iv) Funkcja arctan ustala równoliczność odcinka otwartego $(-\pi/2, \pi/2)$ ze zbiorem wszystkich liczb rzeczywistych.

(v) Dla każdego zbioru A, zbiór potęgowy $P(A)$ jest równoliczny z $\{0, 1\}^A$. Funkcją ustalającą równoliczność jest $\varphi : P(A) \to \{0, 1\}^A$ zdefiniowana następująco. Dla $X \in P(A)$, niech $\varphi(X) : A \to \{0, 1\}$ będzie funkcją *charakterystyczną* zbioru X zdefiniowaną następująco

$$\varphi(X)(a) = \begin{cases} 1, & \text{jeśli } a \in X \\ 0, & \text{jeśli } a \notin X. \end{cases}$$

Pozostawimy czytelnikowi jako ćwiczenie sprawdzenie, że φ jest istotnie bijekcją.

Następujące twierdzenie pokazuje, że $\sim$ zachowuje się jak relacja równoważności.[6]

Fakt 6.2 *Dla dowolnych zbiorów A, B, C,*

(i) $A \sim A$.

(ii) Jeśli $A \sim B$, *to* $B \sim A$.

(iii) Jeśli $A \sim B$ *oraz* $B \sim C$, *to* $A \sim C$.

[6] Ponieważ, jak się okaże w tym rozdziale, klasa wszystkich zbiorów nie jest zbiorem to $\sim$, z formalnego punktu widzenia, nie jest relacją.

Dowód: Pierwszy punkt wynika z tego, że $I_A : A \to A$ jest bijekcją. Drugi wynika z tego, że jeśli $f : A \to B$ jest bijekcją to $f^{-1} : B \to A$ jest też bijekcją (zob. Twierdzenie 4.4). Wreszcie trzeci punkt wynika z tego, że złożenie bijekcji jest bijekcją. ■

Zakładamy, że każdemu zbiorowi A możemy przyporządkować taki obiekt $|A|$, że dla dowolnych zbiorów A, B obiekty im przyporządkowane są równe wtedy i tylko wtedy, gdy te zbiory są równoliczne, tzn.

$$A \sim B \quad \text{wtw, gdy} \quad |A| = |B|. \tag{17}$$

Obiekt $|A|$ nazywamy *mocą* zbioru A. Zatem o mocy danego zbioru można myśleć jak o klasie wszystkich zbiorów równolicznych z tym zbiorem. W teorii mnogości tak można zdefiniować przyporządkowanie każdemu zbiorowi jego mocy, że moce są też zbiorami.[7] Moce zbiorów są też nazywane *liczbami kardynalnymi*.

Powiemy, że zbiór A jest *skończony*, gdy istnieje $n \in N$ takie, że $A \sim n$. W tym przypadku mówimy, że A ma n elementów. Przyjmujemy, że moc zbioru n elementowego jest n. Zbiór, który nie jest skończony nazwiemy zbiorem *nieskończonym*.

Poniższe twierdzenie mówi, że przyporządkowanie zbiorom skończonym jako mocy liczby elementów tych zbiorów jest poprawne, tzn. (17) jest spełnione. Moc zbioru liczb naturalnych oznaczamy symbolem $\aleph_0$ (alef zero).

Twierdzenie 6.3

(i) Dla każdego $n \in N$, nie istnieje funkcja różnowartościowa z $n \cup \{n\}$ w n.

(ii) Dla $m, n \in N$, jeśli $m \sim n$, to $m = n$.

(iii) Żadna liczba naturalna nie jest równoliczna z N, a zatem N jest nieskończony.

Dowód: Zaczniemy od dowodu (i). Dowód jest przez indukcję. Dla $n = 0$ teza oczywiście zachodzi, bo nie istnieje funkcja ze zbioru niepustego w $\emptyset$. Załóżmy, że teza zachodzi dla n i niech

$$f : n \cup \{n\} \cup \{n'\} \to n \cup \{n\}$$

będzie funkcją różnowartościową. Jeśli f nie przyjmuje wartości n, lub jeśli $f(n') = n$, to obcinając f do zbioru $n \cup \{n\}$ (czyli biorąc funkcję $f \cap (n' \times n')$) dostaniemy funkcję różnowartościową z $n \cup \{n\}$ w n, co daje sprzeczność z założeniem indukcyjnym. Jeśli natomiast $f(i) = n$, dla pewnego $i \leq n$, to niech j będzie wartością f na elemencie n'.

[7] Klasa wszystkich zbiorów równolicznych danemu zbiorowi A nie jest zbiorem, o ile $A \neq \emptyset$.

Ponieważ f jest różnowartościowa, to $j < n$. Wówczas funkcja $g : n \cup \{n\} \to n$ zdefiniowana wzorem

$$g(x) = \begin{cases} f(x), & \text{jeśli } x \neq i \\ j, & \text{jeśli } x = i \end{cases}$$

jest funkcją różnowartościową (łatwy dowód pozostawiamy czytelnikowi). Otrzymana sprzeczność dowodzi, że f nie może być różnowartościowa. To kończy dowód (i).

Dla dowodu (ii) pokażemy indukcyjnie dla $m, n \in N$, że

$$\text{jeśli istnieje różnowartościowa funkcja z } m \text{ w } n, \text{ to } m \subseteq n. \tag{18}$$

Indukcje prowadzimy ze względu na m. Dla $m = 0$ teza jest oczywista. Załóżmy więc, że (18) zachodzi i niech $f : m' \to n$ będzie funkcją różnowartościową. Ponieważ $m \subseteq m'$, to istnieje funkcja różnowartościowa z m w n, a zatem, na mocy założenia indukcyjnego, $m \subseteq n$. Przypadek $m = n$ na mocy poprzedniego punktu jest niemożliwy. Zatem $m \neq n$ i korzystając z Twierdzenia 3.3 (iv) dostajemy $m \in n$. Zatem $m' = m \cup \{m\} \subseteq n$, co kończy dowód (18). Zauważmy, że (ii) wynika natychmiast z (18).

Ostatnia część twierdzenia wynika bezpośrednio z pierwszej, bowiem jeśli $f : N \to n$ jest funkcją różnowartościową, to jej obcięcie do $n \cup \{n\}$ dawałoby funkcję różnowartościową z $n \cup \{n\}$ w n, co przeczy (i). ■

6.1 Zbiory przeliczalne

Zbiór A nazwiemy *przeliczalnym* gdy A jest skończony lub równoliczny ze zbiorem liczb naturalnych. Poniższe twierdzenie charakteryzuje zbiory przeliczalne jako te, które można ustawić w ciąg.

Twierdzenie 6.4 *Zbiór A jest przeliczalny wtedy i tylko wtedy, gdy $A = \emptyset$ lub istnieje funkcja z N na A.*

Dowód: Implikacja z lewej w prawo jest oczywista. Udowodnimy implikację odwrotną. Ponieważ każdy skończony zbiór jest przeliczalny, to przyjmijmy, że istnieje funkcja f z N na A oraz, że A jest nieskończony. Zdefiniujemy nową funkcję $g : N \to A$, która będzie poprawioną wersją funkcji f. Funkcję g definiujemy przez indukcję (zob. Twierdzenie 4.11). Niech $g(0) = f(0)$. Dalej, niech $g(n') = f(k)$, gdzie k jest najmniejszą liczbą o tej własności, że

$$f(k) \notin \{g(0), \ldots, g(n)\}$$

Liczba k o powyższych własnościach istnieje bo A jest nieskończony. Natomiast istnienie najmniejszej liczby o powyższej własności wynika z Zasady Minimum (zob. Twierdzenie 3.2).

Polecamy czytelnikowi jako ćwiczenie określenie funkcji h z Twierdzenia 4.11 dla powyższej indukcyjnej definicji.

Pokażemy, że g jest bijekcją. Najpierw pokażemy, że

$$\text{dla każdego } k \text{ istnieje } n \text{ takie, że } f(k) = g(n). \tag{19}$$

Udowodnimy to przez indukcję względem k. Dla $k = 0$ wynika to z definicji g w 0. Weźmy $k > 0$. Jeśli dla wszystkich $m \leq k$, $f(m) = f(k)$, to $f(k) = f(0) = g(0)$. W przeciwnym przypadku, niech $m < k$ będzie największą liczbą taką, że $f(m) \neq f(k)$. Istnienie takiej liczby wynika z Twierdzenia 3.4. Z założenia indukcyjnego istnieje n takie, że $f(m) = g(n)$. Z definicji g otrzymujemy, że $g(n') = f(m') = f(k)$. Zatem n' jest szukaną liczbą. To kończy dowód (19). Niech $a \in A$ będzie dowolnym elementem. Ponieważ f jest na A to istnieje k takie, że $f(k) = a$. Zatem, na mocy (19), istnieje n takie, że $g(n) = a$. Oznacza to, że g jest na A.

Dla dowodu różnowartościowości g zauważmy, że

$$\text{dla każdego } n,\ g(n) \notin \{g(i) \mid i < n\}. \tag{20}$$

Dla $n = 0$ (20) oczywiście zachodzi. Natomiast dla $n > 0$ wynika on natychmiast z definicji g.

Zatem g jest różnowartościowa i na A, co oznacza, że $N \sim A$, czyli A jest zbiorem przeliczalnym. To kończy dowód twierdzenia. ■

Następujące twierdzenie wymienia operacje na zbiorach, które zachowują klasę zbiorów przeliczalnych.

Twierdzenie 6.5

(i) Podzbiór zbioru przeliczalnego jest przeliczalny.

(ii) Jeśli $f : A \to B$ jest dowolną funkcją oraz $X \subseteq A$ jest zbiorem przeliczalnym, to obraz $\vec{f}(X)$ jest też zbiorem przeliczalnym.

(iii) Jeśli A, B są przeliczalne, to $A \times B$ jest też przeliczalny.

(iv) Jeśli $\{A_i \mid i \in I\}$ jest przeliczalną rodziną zbiorów przeliczalnych (tzn. I jest przeliczalny oraz każde A_i jest zbiorem przeliczalnym), to $\bigcup_{i \in I} A_i$ jest też zbiorem przeliczalnym.

Dowód: Niech A będzie niepustym zbiorem przeliczalnym oraz niech $B \subseteq A$ będzie niepustym podzbiorem. Na mocy Twierdzenia 6.4 istnieje funkcja f z N na A. Niech $b_0 \in B$. Definiujemy funkcję $g : A \to B$ następująco

$$g(b) = \begin{cases} b & \text{jeśli } b \in B, \\ b_0 & \text{jeśli } b \notin B. \end{cases}$$

Oczywiście g jest na B a zatem gf jest funkcją z N na B więc na mocy Twierdzenia 6.4, B jest zbiorem przeliczalnym. To dowodzi (i).

Dla dowodu drugiego punktu niech $f : A \to B$ będzie dowolną funkcją i niech $X \subseteq A$ będzie zbiorem przeliczalnym. Jeśli $X = \emptyset$, to $\vec{f}(X) = \emptyset$ jest zbiorem przeliczalnym. Jeśli $X \neq \emptyset$, to z Twierdzenia 6.4 wynika, że istnieje funkcja $g : N \to X$ na X. Niech $f' : X \to \vec{f}(X)$ będzie ograniczeniem f do X, tzn. niech $f' = f \cap (X \times B)$. Oczywiście f' jest na $\vec{f}(X)$ i złożenie $(f'g) : N \to \vec{f}(X)$ jest też funkcją na $\vec{f}(X)$. Korzystając ponownie z Twierdzenia 6.4 wnioskujemy, że $\vec{f}(X)$ jest zbiorem przeliczalnym.

Udowodnimy teraz (iii). Jeśli A lub B jest zbiorem pustym, to $A \times B$ jest też zbiorem pustym, a więc przeliczalnym. Załóżmy więc, że $A \neq \emptyset \neq B$ i niech $f : N \to A$ oraz $g : N \to B$ będą funkcjami, odpowiednio na A oraz na B . Definiujemy funkcję $h : N \times N \to A \times B$ wzorem $h(m,n) = \langle f(m), g(n) \rangle$. Oczywiście h jest funkcją na $A \times B$. Zatem $A \times B$ jest zbiorem przeliczalnym jako obraz zbioru przeliczalnego (zob. (ii) oraz Przykład 6.1 (i)).

Dla dowodu (iv) weźmy przeliczalną rodzinę $\{A_i \mid i \in I\}$ zbiorów przeliczalnych. Bez zmniejszenia ogólności możemy przyjąć, że zbiór indeksów I oraz wszystkie zbiory A_i są niepuste. Niech $f : N \to I$ będzie na I oraz dla każdego $i \in I$ niech $g_i : N \to A_i$ będzie na A_i. Definiujemy funkcję $h : N \times N \to \bigcup_{i \in I} A_i$ wzorem $h(m,n) = g_{f(m)}(n)$. Funkcja h jest na $\bigcup_{i \in I} A_i$ bowiem jeśli $a \in \bigcup_{i \in I} A_i$ to istnieje $i \in I$ takie,że $a \in A_i$. Istnieją wówczas $m, n \in N$ takie, że $f(m) = i$ (bo f jest na I) oraz $g_i(n) = a$ (bo g_i jest na A_i). Zatem

$$h(m,n) = g_{f(m)}(n) = g_i(n) = a,$$

co pokazuje, że h jest na $\bigcup_{i \in I} A_i$. Zatem $\bigcup_{i \in I} A_i$ jest zbiorem przeliczalnym, jako obraz zbioru przeliczalnego (zob. (ii)). To kończy dowód twierdzenia. ■

Przykład 6.6

(i) Zbiór Z liczb całkowitych można przedstawić jako sumę zbioru liczb naturalnych oraz zbioru liczb całkowitych ujemnych. Ponieważ ten drugi zbiór jest przeliczalny, to całość też.

(ii) Zbiór Q liczb wymiernych można przedstawić jako podzbiór produktu $Z \times N$, a zatem jest przeliczalny.

(iii) Jeśli A jest zbiorem przeliczalnym, to dla każdego $n \in N$, zbiór A^n wszystkich funkcji z n w A jest zbiorem przeliczalnym. Zatem zbiór $A^* = \bigcup\{A^n \mid n \in N\}$ wszystkich słów skończonych nad A jest zbiorem przeliczalnym.

6.2 Zbiory nieprzeliczalne

Twierdzenie 6.7 (Cantor)
Dla żadnego zbioru A, nie istnieje funkcja z A na zbiór potęgowy $P(A)$.

Dowód: Załóżmy, że $f : A \to P(A)$ jest funkcją na $P(A)$. Niech

$$A_0 = \{a \in A \mid a \notin f(a)\}.$$

Ponieważ f jest na $P(A)$, to istnieje $a_0 \in A$ taki, że $f(a_0) = A_0$. Tak więc

$$a_0 \in A_0 \text{ wtw, gdy } a_0 \in f(a_0).$$

Innymi słowy,

$$a_0 \in A_0 \text{ wtw, gdy } a_0 \notin A_0.$$

Otrzymana w ten sposób sprzeczność dowodzi, że f nie może być na $P(A)$, co dowodzi twierdzenie. ■

Wniosek 6.8

(i) Zbiór potęgowy $P(A)$ nie jest równoliczny z żadnym podzbiorem zbioru A.

(ii) Zbiór wszystkich podzbiorów zbioru liczb naturalnych oraz zbiór wszystkich nieskończonych ciągów o wyrazach 0,1 są zbiorami nieprzeliczalnymi (zob. Przykład 6.1 (v)).

(iii) Nie istnieje zbiór wszystkich zbiorów.

Dowód: Udowodnimy tylko ostatnią część wniosku. Pozostałe części wynikają natychmist z Twierdzenia 6.7. Gdyby A był zbiorem wszystkich zbiorów, to każdy podzbiór A, będąc zbiorem, należałby do A. Zatem $P(A) \subseteq A$. Wówczas $P(A)$ byłby równoliczny z pewnym podzbiorem A, co daje sprzeczność z pierwszą częścią tego wniosku. ■

Moc zbioru $P(N)$ wszystkich podzbiorów zbioru liczb naturalnych nazywamy *continuum* i oznaczamy przez $\mathfrak{c}$.

6.3 Porównywanie liczb kardynalnych

Powiemy, że moc zbioru A jest *mniejsza lub równa* mocy zbioru B, oznaczamy to przez $|A| \leq |B|$, gdy istnieje funkcja różnowartościowa z A w B. Zauważmy, że powyższa definicja jest poprawna, tzn. nie zależy od wyboru reprezentantów A i B.

Lemat 6.9 *Jeśli $A \sim A'$ oraz $B \sim B'$, to istnieje funkcja różnowartościowa z A w B wtedy i tylko wtedy, gdy istnieje funkcja różnowartościowa z A' w B'.*

Dowód: Niech $\varphi : A \to A'$ oraz $\psi : B \to B'$ będą bijekcjami. Wówczas, jeśli $f : A \to B$ jest funkcją różnowartościową, to $\psi f \varphi^{-1} : A' \to B'$ jest też funkcją różnowartościową. Podobnie, jeśli $g : A' \to B'$ jest funkcją różnowartościową, to $\psi^{-1} g \varphi : A \to B$ jest też funkcją różnowartościową. ∎

Powiemy, że moc zbioru A jest *mniejsza* od mocy B (oznaczamy to przez $|A| < |B|$), gdy $|A| \leq |B|$ oraz $|B| \not\leq |A|$.

Twierdzenie 6.10 (Lemat Banacha)
Dla dowolnych funkcji $f : A \to B$ oraz $g : B \to A$, istnieją zbiory $A_1, A_2 \subseteq A$ oraz $B_1, B_2 \subseteq B$, takie, że

(i) $A_1 \cup A_2 = A,\ A_1 \cap A_2 = \emptyset$,

(ii) $B_1 \cup B_2 = B,\ B_1 \cap B_2 = \emptyset$,

(iii) $\vec{f}(A_1) = B_1$,

(iv) $\vec{g}(B_2) = A_2$.

Lemat Banacha będzie udowodniony w dalszej części notatek (zob. Przykład 7.25) — jego dowód będzie wykorzystywał metodę punktu stałego. Lemat Banacha będzie użyty w dowodzie następnego twierdzenia zwanego twierdzeniem Cantora-Bernsteina. Najpierw udowodnimy jeszcze pewien lemat.

Lemat 6.11 *Jeśli $A \sim A'$, $B \sim B'$ oraz $A \cap B = \emptyset$ i $A' \cap B' = \emptyset$, to $A \cup B \sim A' \cup B'$.*

Dowód: Jeśli $f : A \to A'$ oraz $g : B \to B'$ są bijekcjami, to $f \cup g$ jest bijekcją ustalającą równoliczność $A \cup B \sim A' \cup B'$. Fakt, że $f \cup g$ jest funkcją wynika z tego, że $A \cap B = \emptyset$. Natomiast to, że jest ona funkcją różnowartościową wynika z $A' \cap B' = \emptyset$. ∎

Czytelnik z łatwością znajdzie przykład świadczący o tym, że założenia o pustości przecięcia A i B oraz A' i B' są istotne dla Lematu 6.11.

Twierdzenie 6.12 *Dla dowolnych zbiorów A, B, C,*

(i) $|A| \leq |A|$,

(ii) Jeśli $|A| \leq |B|$ *oraz* $|B| \leq |C|$, *to* $|A| \leq |C|$,

(iii) **(Twierdzenie Cantora-Bernsteina)** *Jeśli* $|A| \leq |B|$ *oraz* $|B| \leq |A|$, *to* $|A| = |B|$.

Dowód: Pierwsze dwie części są zupełnie oczywiste. Udowodnimy tylko trzecią część. Niech $f : A \to B$ oraz $g : B \to A$ będą funkcjami różnowartościowymi. Zastosujmy Lemat Banacha otrzymując rozbicia $A_1, A_2 \subseteq A$ oraz $B_1, B_2 \subseteq B$ takie, że

$$A_1 \cup A_2 = A, \ A_1 \cap A_2 = \emptyset \tag{21}$$

$$B_1 \cup B_2 = B, \ B_1 \cap B_2 = \emptyset \tag{22}$$

$$\vec{f}(A_1) = B_1 \tag{23}$$

$$\vec{g}(B_2) = A_2 \tag{24}$$

Z (23) wynika, że $A_1 \sim B_1$, natomiast z (24) wynika $A_2 \sim B_2$. Zatem z (21), (22) oraz z Lematu 6.11 wynika, że $A \sim B$, co kończy dowód twierdzenia. ■

Twierdzenie Cantora-Bernsteina jest bardzo pożyteczne przy wyznaczaniu mocy zbiorów. Zilustrujemy to na jednym przykładzie.

Twierdzenie 6.13 *Zbiór liczb rzeczywistych jest równoliczny ze zbiorem* $\{0,1\}^N$, *a zatem jest zbiorem mocy continuum.*

Dowód: Najpierw pokażemy, że $|\{0,1\}^N| \leq |R|$. Niech $\varphi : \{0,1\}^N \to R$ będzie funkcją zdefiniowaną następująco dla $f : N \to \{0,1\}$,

$$\varphi(f) = \begin{cases} \sum_{n=0}^{\infty} \frac{f(n)}{2^n} & \text{gdy } \vec{f}^{-1}(\{0\}) \text{ jest nieskończony,} \\ -\sum_{n=0}^{\infty} \frac{f(n)}{2^n} & \text{gdy } \vec{f}^{-1}(\{0\}) \text{ jest skończony.} \end{cases}$$

Pokażemy, φ jest różnowartościowa. Po pierwsze zauważmy, że jeśli $\vec{f}^{-1}(\{0\})$ jest nieskończony, to $\varphi(f) \geq 0$, natomiast gdy jest skończony, to $\varphi(f) < 0$. Przypuśćmy, że f oraz g są dwoma różnymi nieskończonymi ciągami zawierającymi nieskończenie wiele zer. Niech k będzie najmniejszą liczbą taką, że $f(k) \neq g(k)$. Bez zmniejszenia ogólności możemy przyjąć, że $f(k) = 0$ oraz $g(k) = 1$. Jeśli $\varphi(f) = \varphi(g)$, to odejmując pierwsze $k-1$ wyrazów w odpowiadających szeregach dostajemy

$$\sum_{n=k+1}^{\infty} \frac{f(n)}{2^n} = \frac{1}{2^k} + \sum_{n=k+1}^{\infty} \frac{g(n)}{2^n}. \tag{25}$$

Zatem szereg po lewej stronie ma sumę mniejszą (bo f zawiera nieskończenie wiele zer) od $\sum_{n=k+1}^{\infty} \frac{1}{2^n} = \frac{1}{2^k}$. Natomiast szereg po prawej stronie ma sumę co najmniej $\frac{1}{2^k}$. Zatem równość (25) jest niemożliwa, co dowodzi $\varphi(f) \neq \varphi(g)$. W przypadku, gdy f i g zawierają tylko skończenie wiele zer to postępujemy podobnie. Wówczas szereg po lewej stronie równości (25) zbiega do sumy nie większej niż $\frac{1}{2^k}$, natomiast szereg po prawej stronie zbiega do sumy większej (bo g zawiera tylko skończenie wiele zer) od $\frac{1}{2^k}$. Zatem róność (25) jest w tym przypadku też niemożliwa. Tym samym udowodniliśmy różnowartościowość przekształcenia φ oraz

$$|\{0,1\}^N| \leq |R|.$$

Dla dowodu nierówności przeciwnej określamy przekształcenie $\psi : (0,1) \to \{0,1\}^N$, które przyporządkowuje każdej liczbie rzeczywistej $0 < r < 1$ jej rozwinięcie binarne, tzn. ciąg $f : N \to \{0,1\}$ taki, że

$$r = \sum_{n=0}^{\infty} \frac{f(n)}{2^n}.$$

Ponadto umawiamy się, że jeśli dana liczba ma dwa rozwinięcia binarne: o skończonej i o nieskończonej liczbie zer, to wybieramy to które ma nieskończenie wiele zer. ψ jest oczywiście różnowartościowa, a zatem

$$|(0,1)| \leq |\{0,1\}^N|.$$

Ponieważ, z Przykładu 6.1 (iii) oraz (iv) wiemy, że $(0,1) \sim R$, to korzystając z twierdzenia Cantora-Bernsteina dostajemy tezę naszego twierdzenia. ■

6.4 Operacje na liczbach kardynalnych

Niech $A \cap B = \emptyset$. *Sumę* mocy, $|A| + |B|$ określa się jako moc zbioru $A \cup B$. Należy stwierdzić poprawność powyższej operacji, tzn. pokazać, że nie zależy ona od wyboru reprezentantów. Wynika to natychmiast z Lematu 6.11.

Iloczyn mocy $|A||B|$ definiuje się jako moc produktu $A \times B$. Następujący lemat dowodzi poprawności powyższej operacji.

Lemat 6.14 *Jeśli $A \sim A'$ oraz $B \sim B'$, to $A \times B \sim A' \times B'$.*

Dowód: Jeśli $f : A \to A'$ oraz $g : B \to B'$ są bijekcjami, to funkcja $h : A \times B \to A' \times B'$ zdefiniowana wzorem

$$h(a,b) = \langle f(a), g(b) \rangle$$

jest bijekcją. Łatwy dowód pozostawimy czytelnikowi. ■

Potęgę mocy $|A|^{|B|}$ definiuje się jako moc zbioru funkcji A^B. Poprawność wynika z następującego lematu.

Lemat 6.15 *Jeśli $A \sim A'$ oraz $B \sim B'$, to $A^B \sim A'^{B'}$.*

Dowód: Jeśli $f : A \to A'$ oraz $g : B \to B'$ są bijekcjami, to niech $\varphi : A^B \to A'^{B'}$ będzie funkcją zdefiniowaną następująco: dla dowolnej funkcji $h : A \to B$,

$$\varphi(h) = ghf^{-1}.$$

Ponieważ funkcją odwrotną do φ jest $\psi : A'^{B'} \to A^B$ zdefiniowana dla $h' : A' \to B'$,

$$\psi(h') = g^{-1}h'f,$$

to na mocy Twierdzenia 4.4, funkcja φ jest bijekcją. ■

Przykład 6.1 (i) pokazuje, że $\aleph_0\aleph_0 = \aleph_0$ i ogólnie, że dla każdego $n > 0$, zachodzi $\aleph_0^n = \aleph_0$. Natomiast Przykład 6.1 (v) pokazuje, że $2^{\aleph_0} = \mathfrak{c}$.

Powyższe trzy operacje na liczbach kardynalnych, zastosowane do liczb naturalnych (jako mocy zbiorów skończonych) pokrywają się ze zwykłymi operacjami arytmetycznymi dodawania, mnożenia i potęgowania.

Przykładem prawa dla liczb naturalnych, które przenosi się na dowolne liczby kardynalne jest następujące twierdzenie.

Twierdzenie 6.16 *Dla dowolnej liczby kardynalnej $|A|$ zachodzi*

$$|A| < 2^{|A|}.$$

Dowód: Oczywiście funkcja $\varphi : A \to P(A)$ zdefiniowana dla $a \in A$,

$$\varphi(a) = \{a\}$$

jest różnowartościowa. Zatem

$$|A| \leq 2^{|A|}.$$

Z twierdzenia Cantora (Twierdzenie 6.7)wynika natychmiast, że $|A| \neq |P(A)|$. Zatem z twierdzenia Cantora-Bernsteina (Twierdzenie 6.12 (iii)) oraz powyższej nierówności wynika, że $|P(A)| \not\leq |A|$. Dowodzi to tezy naszego twierdzenia. ■

Innym przykładem prawa dla liczb kardynalnych, które jest uogólnieniem znanego prawa dla arytmetyki liczb naturalnych jest następujące twierdzenie.

Twierdzenie 6.17 *Dla dowolnych zbiorów A, B, C,*

$$(|A|^{|B|})^{|C|} = |A|^{|B||C|}.$$

Dowód: Pokażemy, że $(A^B)^C \sim A^{B\times C}$. Niech $\varphi : (A^B)^C \to A^{B\times C}$ będzie funkcją zdefiniowaną następująco: dla $f : C \to A^B$ oraz $b \in B$ i $c \in C$,

$$\varphi(f)(b, c) = (f(c))(b).$$

Zauważmy, że w powyższym wzorze $\varphi(f)$ jest funkcją z $B \times C$ w A, natomiast $f(c)$ jest funkcją z B w A.

Następnie, niech $\psi : A^{B\times C} \to (A^B)^C$ będzie funkcją, która każdej funkcji $g : B \times C \to A$ przyporządkowuje funkcję $\psi(g) : C \to A^B$ określoną następująco. Dla $c \in C$, funkcja $(\psi(g))(c) : B \to A$ jest zdefiniowana równaniem

$$((\psi(g))(c))(b) = g(b, c).$$

Pokażemy, że ψ jest funkcją odwrotną do φ. Niech $f : C \to A^B$ będzie dowolną funkcją. Wówczas dla dowolnych $b \in B$ oraz $c \in C$ mamy

$$((\psi(\varphi(f)))(c))(b) = \varphi(f)(b, c) = (f(c))(b).$$

Zatem, ponieważ powyższe równości zachodzą dla dowolnego $b \in B$, to

$$(\psi(\varphi(f)))(c) = f(c),$$

co wobec dowolności $c \in C$ oznacza, że

$$\psi(\varphi(f)) = f.$$

Na zakończenie dowodu weźmy dowolną funkcję $g : B \times C \to A$ oraz dowolne $b \in B$ i $c \in C$. Wówczas

$$(\varphi(\psi(g))(b, c) = ((\psi(g))(c))(b) = g(b, c),$$

co wobec dowolności $b \in B$ oraz $c \in C$ daje

$$(\varphi(\psi(g)) = g.$$

Zatem ψ jest funkcją odwrotną do φ, co na mocy Twierdzenia 4.4, oznacza, że φ jest bijekcją ustalającą żądaną równoliczność. ∎

Korzystając z twierdzenia 6.17 możemy pokazać, że

$$\mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0\aleph_0} = 2^{\aleph_0} = \mathfrak{c}.$$

Zadania

6.1. Jaka jest moc zbioru wszystkich funkcji ciągłych z R w R?

6.2. Niech $f : R \to R$ będzie dowolną funkcją monotoniczną, tzn. spełniającą warunek: $r_1 \leq r_2$ implikuje $f(r_1) \leq f(r_2)$. Jaka może być największa moc zbioru wszystkich punktów nieciągłości f?

6.3. Jaka jest moc wszystkich skończonych podzbiorów zbioru N?

6.4. Jaka jest moc zbioru wszystkich funkcji z N w N?

6.5. Jaka może być maksymalna moc rodziny podzbiorów N parami rozłącznych?

6.6. Niech $r \subseteq N^N \times N^N$ będzie relacją zdefiniowaną następująco: $\langle f, g\rangle \in r$ wtw, gdy $f(n) - g(n)$ jest liczbą parzystą. Jaka jest moc klasy abstrakcji zawierającej identyczność I_N? Jaka jest moc zbioru wszystkich klas abstrakcji r?

6.7. Jaka jest moc zbioru wszystkich funkcji monotonicznych $f : N \to N$, tzn. spełniających warunek: $n_1 \leq n_2$ implikuje $f(n_1) \leq f(n_2)$? Jaka jest moc zbioru wszystkich funkcji antymonotonicznych $f : N \to N$, tzn. spełniających warunek: $n_1 \leq n_2$ implikuje $f(n_2) \leq f(n_1)$?

6.8. Jaka jest moc zbioru wszystkich ciągów liczb wymiernych, które są zbieżne do zera?

6.9. Jak dużej mocy może być zbiór liter **T** na płaszczyźnie R^2 takich, że żadne dwie litery nie przecinają się?

6.10. Jakiej największej mocy może być rodzina zbiorów $\mathcal{K} \subseteq \mathcal{P}(\mathcal{N})$ taka, że dla dowolnych $A, B \in \mathcal{K}$, zachodzi $A \subseteq B$ lub $B \subseteq A$?

6.11. Jakiej mocy jest zbiór wszystkich relacji równoważności w N?

6.12. Czy istnieje relacja równoważności $r \subseteq R \times R$, której każda klasa abstrakcji jest mocy $\aleph_0$ oraz

a.) Zbiór R/r jest mocy $\aleph_0$?

b.) Zbiór R/r jest mocy c?

6.13. Które z poniższych zdań jest prawdziwe a które fałszywe?

a.) Jeśli $f : A \to B$ jest różnowartościowa oraz nie jest na B, to $|A| < |B|$.

b.) Jeśli $|A| < |B|$ i $C \neq \emptyset$, to $|A \times C| < |B \times C|$.

6.14. Które z następujących zbiorów są równoliczne?

$$Z,\ R^N,\ Q^N,\ R \times R,\ \{0,1\}^*,\ \{0,1\}^N,\ P(Q),\ P(R).$$

6.15. Dowieść, że jeśli X jest zbiorem nieprzeliczalnym oraz A jest zbiorem przeliczalnym, to $X \cup A \sim X$. Wywnioskować stąd, że moc zbioru liczb niewymiernych jest $\mathfrak{c}$.

7 Częściowe porządki

Częściowym porządkiem w zbiorze A nazywamy parę $\langle A, \leq \rangle$, gdzie $\leq \subseteq A \times A$ jest relacją dwuargumentową spełniającą następujące warunki.

- (*Zwrotność*) Dla każdego $a \in A$, zachodzi $a \leq a$.
- (*Antysymetria*) Dla dowolnych $a, b \in A$, jeśli $a \leq b$ oraz $b \leq a$, to $a = b$.
- (*Przechodniość*) Dla dowolnych $a, b, c \in A$, jeśli $a \leq b$ oraz $b \leq c$, to $a \leq c$.

Jeśli ponadto porządek $\leq$ spełnia warunek spójności:

- (*Spójność*) Dla dowolnych $a, b \in A$, zachodzi $a \leq b$ lub $b \leq a$.

to nazywamy go *porządkiem liniowym* lub *łańcuchem.*

Jeśli $\langle A, \leq \rangle$ jest zbiorem częściowo uporządkowanym, to napis $a < b$ będzie oznaczał zdanie "$a \leq b$ oraz $a \neq b$".

Przykład 7.1 Zbiór potęgowy $\langle P(A), \subseteq \rangle$ jest zbiorem częściowo uporządkowanym relacją inkluzji. Ten zbiór jest łańcuchem wtw, gdy A ma co najwyżej jeden element.

Przykład 7.2 Zbiór liczb naturalnych N ze zwykłą relacją porządku jest liniowo uporządkowany (zob. Twierdzenie 3.3 (v)) Przypomnijmy, że N był wprowadzony jako najmniejszy zbiór induktywny, a więc jest rodziną zbiorów uporządkowaną relacja zawierania.

Powyższe dwa przykłady są szczególnym przypadkiem następującej sytuacji.

Fakt 7.3 *Każda rodzina zbiorów z relacją zawierania jest częściowym porządkiem.*

Dowód: Wynika natychmiast z własności relacji zawierania. ∎

Przykład 7.4 Zbiór liczb naturalnych dodatnich jest częściowo uporządkowany przez relację podzielności. Łatwy dowód pozostawiamy czytelnikowi.

7.1 Słowa

Podamy teraz kilka przykładów częściowych porządków związanych ze słowami.

Przykład 7.5 (*Porządek prefiksowy.*) Niech A będzie dowolnym zbiorem. W zbiorze A^*, wszystkich skończonych słów skończonych nad A, mamy określoną operację składania (zob. Przykład 4.1 (iii)). Określimy relację porządku prefiksowego. Mówimy, że słowo w jest *prefiksem* słowa u, oznaczamy to przez $w \leq u$, gdy istnieje $w' \in A^*$ taki, że

$$u = ww'.$$

Fakt 7.6 *Relacja $\leq$ porządku prefiksowego zdefiniowana wyżej jest częściowym porządkiem w zbiorze wszystkich słów A^*.*

Dowód: Oczywiście każde słowo jest swoim własnym prefiksem, a zatem $\leq$ jest relacją zwrotną. Jeśli $u = ww'$ oraz $w = uu'$ to dostajemy

$$u = (uu')w'.$$

Ponieważ operacja składania słów jest łączna,[8] tzn. $w(uv) = (wu)v$,to powyższa równość daje $u = u(u'w')$. A zatem $u'w' = \varepsilon$, czyli $u' = w' = \varepsilon$ i $u = w$. Tak więc $\leq$ jest antysymetryczna. Przechodniość $\leq$ wynika bezpośrednio z łączności operacji składania. ■

Przykład 7.7 (*Porządek leksykograficzny.*) Przypuśćmy, że mamy zbiór A częściowo uporządkowany przez relację $\leq$. Relacja ta indukuje na A^* relację $\preceq$ zwaną *porządkiem leksykograficznym* nad $\langle A, \leq\rangle$ zdefiniowaną następująco. Jeśli $w, u \in A^*$, to $w \preceq u$ gdy w jest prefiksem u lub gdy istnieje $i < min(|w|, |u|)$ takie, że $w(i) < u(i)$ oraz dla każdego $j < i$, zachodzi $w(j) = u(j)$.

Fakt 7.8 *Porządek leksykograficzny nad $\langle A, \leq\rangle$ jest częściowym porządkiem. Jest on liniowym porządkiem, o ile $\langle A, \leq\rangle$ jest liniowym porządkiem.*

Dowód: Zwrotność relacji $\preceq$ wynika bezpośrednio ze zwrotności porządku prefiksowego. Dla dowodu antysymetrii załóżmy, że $w \preceq u$ oraz $u \preceq w$. Jeśli u jest prefiksem w oraz w jest prefiksem u, to $w = u$. Jeśli natomiast istnieje $i < min(|w|, |u|)$ takie, że $w(i) < u(i)$ oraz dla każdego $j < i$, zachodzi $w(j) = u(j)$, to u nie może być prefiksem w a zatem musi istnieć $k < min(|w|, |u|)$ takie, że $u(k) < w(k)$ oraz dla każdego $j < k$, $w(j) = u(j)$. Zatem ani $i \leq k$ nie jest możliwe ani $k \leq i$ nie jest możliwe. Otrzymana sprzeczność dowodzi, że

[8] Dowód łączności operacji sładania słów pozostawimy czytelnikowi.

jedyny możliwy przypadek to gdy w jest prefiksem u oraz u jest prefiksem w. Zatem $\preceq$ jest antysymetryczna.

Udowodnimy przechodniość $\preceq$. Niech $w \preceq u$ oraz $u \preceq v$. Mamy do rozważenia następujące możliwości:

$$w \text{ jest prefiksem } u; \tag{26}$$

$$\text{istnieje } i_1 < min(|w|,|u|) \text{ takie, że } w(i_1) < u(i_1) \text{ oraz dla każdego } j < i_1,\ w(j) = u(j); \tag{27}$$

$$u \text{ jest prefiksem } v; \tag{28}$$

$$\text{istnieje } i_2 < min(|w|,|u|) \text{ takie, że } w(i_2) < u(i_2) \text{ oraz dla każdego } j < i_2,\ w(j) = u(j). \tag{29}$$

Jeśli zachodzi (26) oraz (28) to oczywiście w jest prefiksem v i $w \preceq v$. Jeśli zachodzi (26) oraz (29), to jeśli $|w| \leq i_2$, to w jest prefiksem v. Jeśli natomiast $i_2 < |w|$, to ponieważ w jest prefiksem u, to $w(i_2) = u(i_2) \leq v(i_2)$ i na wszystkich wcześniejszych pozycjach w oraz v się pokrywają. Tak więc $w \preceq v$. Jeśli zachodzi (27) oraz (28), to $i_1 < |v|$ i rozumujemy podobnie jak w poprzednim przypadku. Załóżmy wreszcie, że zachodzi (27) oraz (29). Jeśli $i_1 \leq i_2$, to $w(i_1) \leq u(i_1) \leq v(i_1)$, $w(i_1) \neq u(i_1)$, a zatem $w(i_1) \neq v(i_1)$. Ponadto dla $j < i_1$, $w(j) = u(j) = v(j)$. Zatem $w \preceq v$. Jeśli natomiast $i_2 < i_1$ to podobnie pokazujemy, że i_2 jest pierwszą pozycją, na której się różnią w oraz v i $w(i_2) \leq v(i_2)$. Tak więc ponownie $w \preceq v$, co kończy dowód przechodniości $\preceq$.

Jeśli porządek $\leq$ na A jest liniowy, to dla dowolnych słów w, u, z których żadne nie jest prefiksem drugiego, jeśli $i < min(|w|,|u|)$ jest najmniejszą liczbą taką, że $w(i) \neq u(i)$, to $w \preceq u$, o ile $w(i) \leq u(i)$; oraz $u \preceq w$, w przeciwnym przypadku. Zatem $\preceq$ jest też liniowym porządkiem. ■

Jeśli, na przykład, $\preceq$ oznacza porządek leksykograficzny nad $\langle\{0,1\},\leq\rangle$, gdzie $0 \leq 1$, to następujący ciąg tworzy łańcuch wstępujący

$$\varepsilon \preceq 0 \preceq 00 \preceq \ldots \preceq 0^k \preceq 0^{k+1} \preceq \ldots$$

natomiast ciąg

$$\ldots \preceq 0^{k+1}1 \preceq 0^k1 \preceq \ldots \preceq 1$$

tworzy łańcuch zstępujący. Ponadto dla dowolnych $k, n \in N$,

$$0^k \preceq 0^n1.$$

Tak więc, każdy element pierwszego łańcucha jest mniejszy w tym porządku od każdego elementu drugiego łańcucha.

7.2 Drzewa

Niech A będzie dowolnym zbiorem. *Drzewem* nad A nazwiemy każdy niepusty podzbiór $t \subseteq A^*$ zamknięty na prefiksy, tzn. dla $w \in t$, jeśli $u \leq w$, to $u \in t$.

Z powyższej definicji wynika, że każde drzewo zawiera słowo puste ε. Elementy drzewa t nazywamy *wierzchołkami*. Słowo puste $\varepsilon \in t$ jest nazywane *korzeniem* drzewa t. Jeśli $w \in t$ oraz $wa \in t$ dla pewnego $a \in A$, to wa jest nazywane a-tym *następnikem* (lub dzieckiem) wierzchołka w. Wierzchołek nie mający następników nazywamy *liściem*.

Jeśli A jest zbiorem nieskończonym, to w drzewie nad A mogą być wierzchołki o nieskończenie wielu następnikach. *Rzędem* wierzchołka w w drzewie t nazywamy moc zbioru następników tego wierzchołka, tzn. $|\{a \in A \mid wa \in t\}|$.

Zbiór wierzchołków $\pi \subseteq t$ w drzewie t nazwiemy *ścieżką*, gdy jest on liniowo uporządkowany relacją porządku prefiksowego $\leq$ oraz spełnia następujący warunek: dla dowolnych $w, u \in \pi$ oraz $v \in t$, jeśli $w \leq v \leq u$, to $v \in \pi$. *Długością* ścieżki π nazywamy moc zbioru π.

Przykładami drzew są:

- $\{\varepsilon\}$, drzewo o jednym wierzchołku.
- $\{a^n \mid n \in N\}$, gdzie $a \in A$ jest dowolną ustaloną literą.
- $\{w \in A^* \mid |w| \leq n\}$, pełne drzewo nad A wysokości n.
- A^*, pełne drzewo nad A.

Jako przykład ważnego twierdzenia używającego powyższych pojęć przytoczymy:

Twierdzenie 7.9 (Lemat Königa)
Niech $t \subseteq A^*$ będzie drzewem, w którym każdy wierzchołek jest skończonego rzędu. Jeśli t zawiera ścieżki skończone dowolnej długości, to t zawiera ścieżkę nieskończoną.

Dowód: Niech t będzie drzewem spełniającym założenia twierdzenia. Zdefiniujemy indukcyjnie funkcję różnowartościową $f : N \to t$, spełniającą następujący warunek: dla każdego $n \in N$, wierzchołek $f(n')$ jest następnikiem $f(n)$ w drzewie t oraz t zawiera ścieżki skończone dowolnej długości zaczynające się od $f(n)$. Niech $f(0) = \varepsilon$. Korzeń spełnia oczywiście powyższy warunek na mocy założeń twierdzenia. Przypuśćmy, że $f(n)$ jest określone i weźmy wszystkie następniki wierzchołka $f(n)$. Gdyby ścieżki zaczynające się od każdego z nich były ograniczonej długości, to wobec tego, że $f(n)$ ma tylko skończoną liczbę następników, istniałoby ograniczenie górne na długość ścieżek zaczynających się od $f(n)$, wbrew założeniu indukcyjnemu. Zatem istnieje następnik wierzchołka $f(n)$, od którego zaczynają się ścieżki dowolnej skończonej długości. Jako $f(n')$ wybieramy jeden z tych następników.

Oczywiście, jak wynika to natychmiast z definicji f, zbiór $\vec{f}(N)$ jest nieskończoną ścieżką w t. ∎

Niech t będzie drzewem nad A i niech $w \in t$. Niech

$$t|_w = \{u \in A^* \mid wu \in t\}.$$

Fakt 7.10 *Dla każdego drzewa $t \subseteq A^*$ oraz wierzchołka $w \in t$, zbiór $t|_w$ jest drzewem nad A.*

Dowód: Oczywiście $\varepsilon \in t|_w$. Ponadto jeśli v jest prefiksem słowa u, to wv jest prefiksem słowa wu. Zatem $t|_w$ jest zamknięty na prefiksy. ■

Mówimy, że drzewo r jest *poddrzewem* drzewa t, oznaczamy to przez $r \sqsubseteq t$, jeśli istnieje wierzchołek $w \in t$ taki, że $r = t|_w$. W tym przypadku mówimy o poddrzewie zaczepionym w wierzchołku w.

Przykład 7.11 (*Drzewa k-argumentowe*) Niech $k > 0$. Drzewo $t \subseteq \{0, \ldots, k-1\}^*$ nazwiemy drzewem k-argumentowym, gdy każdy wierzchołek w t, który nie jest liściem ma rząd k.

Zbiór wszystkich drzew k-argumentowych oznaczamy przez T_k. Zbiór ten, jako rodzina zbiorów, jest naturalnie częściowo uporządkowany przez relecję zawierania. Jeśli $t \subseteq r$, gdzie $t, r \in T_k$, to mówimy, że drzewo r *rozszerza* drzewo t. Przez FT_k oznaczamy zbiór wszystkich drzew skończonych k-argumentowych.

Przykładami drzew k-argumentowych są:

- $\{\varepsilon\}$.
- $p_n = \{w \in \{0, \ldots, k-1\}^* \mid |w| \leq n\}$ jest *pełnym drzewem* k-argumentowym wysokości n.
- $\{0, \ldots, k-1\}^*$ jest pełnym drzewem k-argumentowym nieskończonym.
- $t_1 = \{0^n \mid n \in N\} \cup \{0^n 1 \mid n \in N\} \cup \{0^{2n+1}10 \mid n \in N\} \cup \{0^{2n+1}11 \mid n \in N\}$ jest drzewem 2-argumentowym (binarnym).
- $t_2 = \{0^n \mid n \in N\} \cup \{0^n 1 \mid n \in N\} \cup \{0^{2n}10 \mid n \in N\} \cup \{0^{2n}11 \mid n \in N\}$ jest też drzewem binarnym.

Pożyteczne może być narysowanie drzew t_1 i t_2.

Przykład 7.12 (*Drzewa $k^{\leq}$-argumentowe*) Drzewo $t \subseteq \{0, \ldots, k-1\}^*$ nazwiemy *drzewem $k^{\leq}$-argumentowym* gdy spełnia ono następujący warunek:

$$\text{dla każdego } w \in t \text{ oraz } i < k, \text{ jeśli } wi \in t, \text{ to } wj \in t, \text{ dla każdego } j \leq i.$$

Zbiór wszystkich drzew $k^{\leq}$-argumentowych oznaczamy przez $T_{k\leq}$. Symbolem $FT_{k\leq}$ oznaczamy zbiór wszystkich skończonych drzew $k^{\leq}$-argumentowych. Oczywiście $T_k \subseteq T_{k\leq}$ oraz $T_{k\leq}$ jest naturalnie uporządkowany przez $\subseteq$.

Każde drzewo k-argumentowe jest drzewem $k^{\leq}$-argumentowym. Różnica polega na tym, że drzewa $k^{\leq}$-argumentowe mogą mieć wierzchołki rzędów pośrednich pomiędzy 0 i k. Z kolei nie każde drzewo nad $\{0,\ldots,k-1\}^*$ musi być drzewem $k^{\leq}$-argumentowym. Przykładowo, $\{\varepsilon,1\}$ nie jest drzewem $2^{\leq}$-argumentowym, ale $\{\varepsilon,0\}$ jest. Oczywiście poddrzewo drzewa $k^{\leq}$-argumentowego jest drzewem $k^{\leq}$-argumentowym.

Fakt 7.13 *Relacja $\sqsubseteq$ ograniczona do zbioru $FT_{k\leq}$ drzew skończonych jest relacją częściowego porządku.*

Dowód: Ponieważ $t = t|_\varepsilon$, to $\sqsubseteq$ jest zwrotna. Jeśli $r = t|_w$ oraz $t = s|_v$, to $r = (s|_v)|_w$. Ponieważ

$$(s|_v)|_w = s|_{vw}$$

to $r \sqsubseteq s$, co dowodzi przechodniości.

Dla pokazania antysymetrii przyjmijmy, że

$$r = t|_w \quad \text{oraz} \quad t = r|_v.$$

Zatem

$$r = r|_{wv}. \tag{30}$$

Ponieważ r jest skończonym drzewem, to niech $u' \in r$ będzie wierzchołkiem takim, że $|u'|$ jest największą liczbą w zbiorze $\{|u| \mid u \in r\}$. Zatem z (30) wynika, że $wvu' \in r$, więc $wv = \varepsilon$. Tak więc $w = v = \varepsilon$ i dostajemy $r = t$, co dowodzi antysymetrii $\sqsubseteq$. ∎

Uwaga: Relacja $\sqsubseteq$ nie jest antysymetryczna w zbiorze $T_{k\leq}$, zauważmy, że dla drzew t_1 i t_2 z Przykładu 7.11 mamy $t_1 \sqsubseteq t_2$ oraz $t_2 \sqsubseteq t_1$, ale $t_1 \neq t_2$.

7.3 Drzewa etykietowane

Ważną klasą drzew pojawiającą się często w zastosowaniach są drzewa etykietowane. Niech $\Sigma = \{\Sigma_n\}_{n\in N}$ będzie indeksowaną rodziną zbiorów. Elementy Σ_n nazywamy *etykietami rzędu* n. Załóżmy, że Σ_0 zawiera wyróżniony symbol $\perp \in \Sigma_0$.

Niech $t \in T_{k\leq}$. *Drzewem etykietowanym* nad Σ o nośniku t nazwiemy dowolną funkcję $\sigma : t \to \bigcup_{n\in N} \Sigma_n$ taką, że dla każdego $n \in N$ oraz $w \in t$, jeśli w jest rzędu n, to $\sigma(w) \in \Sigma_n$. Nośnik drzewa etykietowanego σ będziemy oznaczać przez $||\sigma||$. Niech $T_{k\leq}(\Sigma)$ oznacza zbiór wszystkich drzew etykietowanych nad Σ o nośnikach z $T_{k\leq}$. Analogicznie możemy zdefiniować $T_k(\Sigma)$.

W zbiorze $T_{k\leq}(\Sigma)$ zdefiniujemy relację $\leq$ następująco. Dla $\sigma, \tau \in T_{k\leq}(\Sigma)$, $\sigma \leq \tau$ wtw, gdy

- $||\sigma|| \subseteq ||\tau||$, oraz
- dla każdego $w \in ||\sigma||$, jeśli $\sigma(w) \neq \perp$, to $\sigma(w) = \tau(w)$.

Fakt 7.14 *Relacja $\leq$ zdefiniowana powyżej jest częściowym porządkiem w zbiorze $T_{k\leq}(\Sigma)$.*

Dowód: Relacja ta jest oczywiście zwrotna i przechodnia. Załóżmy, że $\sigma \leq \tau$ oraz $\tau \leq \sigma$. Wówczas mamy $||\sigma|| = ||\tau||$ oraz dla $w \in ||\sigma||$, jeśli $\sigma(w) \neq \perp$ lub $\tau(w) \neq \perp$, to $\sigma(w) = \tau(w)$. Zatem $\sigma(w) = \tau(w)$ zachodzi przy każdym $w \in ||\sigma||$, czyli $\sigma = \tau$. ■

Poniżej zilustrujemy na dwóch przykładach użyteczność pojęcia drzewa etykietowanego.

Przykład 7.15 (*Wyrażenia arytmetyczne*) Niech rodzina zbiorów etykiet Σ będzie zdefiniowana następująco. $\Sigma_0 = \{\perp, 1\}$, $\Sigma_1 = \emptyset$, $\Sigma_2 = \{+, \times, /\}$, $\Sigma_n = \emptyset$ dla $n > 2$. Drzewa etykietowane nad Σ nazwiemy w tym przypadku wyrażeniami arytmetycznymi.

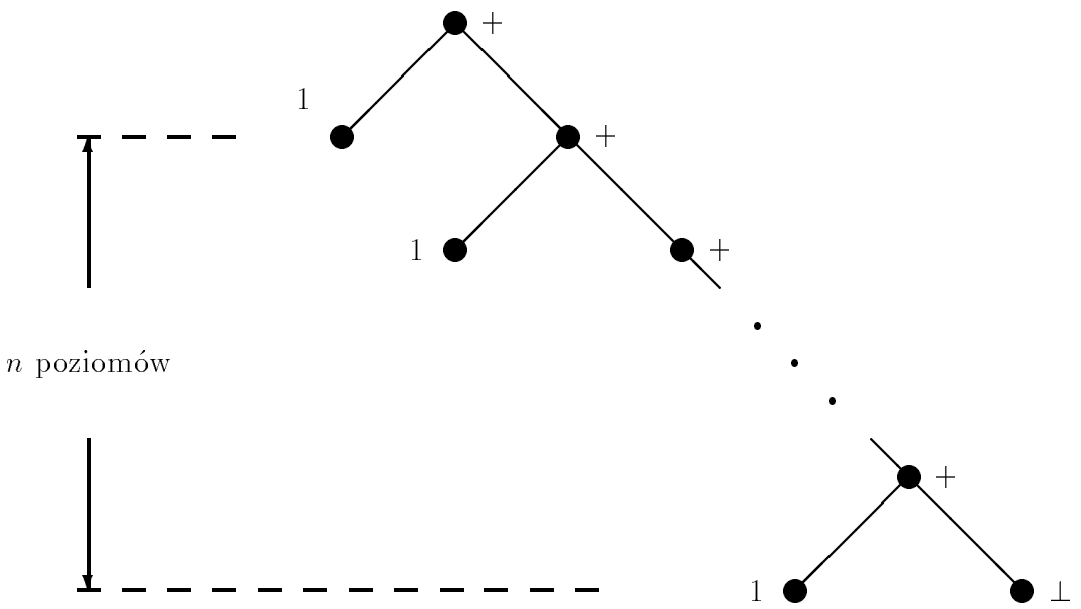
Na przykład, liczbę naturalną n możemy przedstawić formalnie jako następujące wyrażenie arytmetyczne $\tilde{n}$ o nośniku

$$||\tilde{n}|| = \{1^i \mid i \leq n\} \cup \{1^i 0 \mid i < n\},$$

oraz o następującym rozkładzie etykiet

$$\tilde{n}(w) = \begin{cases} 1 & \text{jeśli } w = 1^i 0,\ i < n, \\ \perp & \text{jeśli } w = 1^n, \\ + & \text{jeśli } w = 1^i,\ i < n. \end{cases}$$

Drzewo to jest przedstawione na rysunku 1.

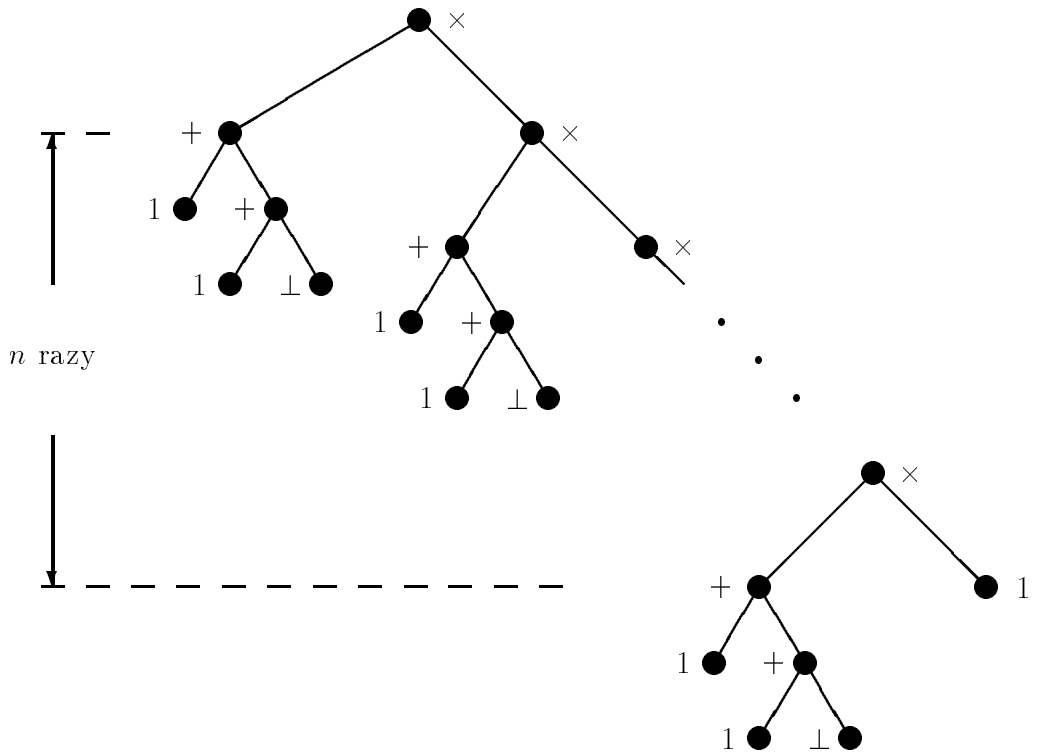


Rysunek 1: Drzewo etykietowane $\tilde{n}$.

Powyższe wyrażenie ma wartość n jeśli 1 traktować jak liczbę 'jeden', $\perp$ traktować jak liczbę 'zero' oraz + traktować jak operację dodawania liczb naturalnych. Chcielibyśmy podkreślić, że bez powyższej interpretacji $1, \perp$ oraz + są jedynie formalnymi symbolami używanymi do etykietowania wierzchołków w drzewach. Specjalny symbol $\perp$ w przypadku drzew etykietowanych pełni szczególną rolę – oznacza on te liście w drzewie, z, których możemy rozbudowywać drzewo do drzewa większego w sensie porządku $\leq$. Tak więc powyższa reprezentacja liczb naturalnych jako drzew etykietowanych ma dodatkowo tę cechę, że $\tilde{n} \leq \tilde{m}$ w sensie porządku na drzewach etykietowanych, wtw, gdy $m \leq n$ w sensie porządku na liczbach naturalnych.

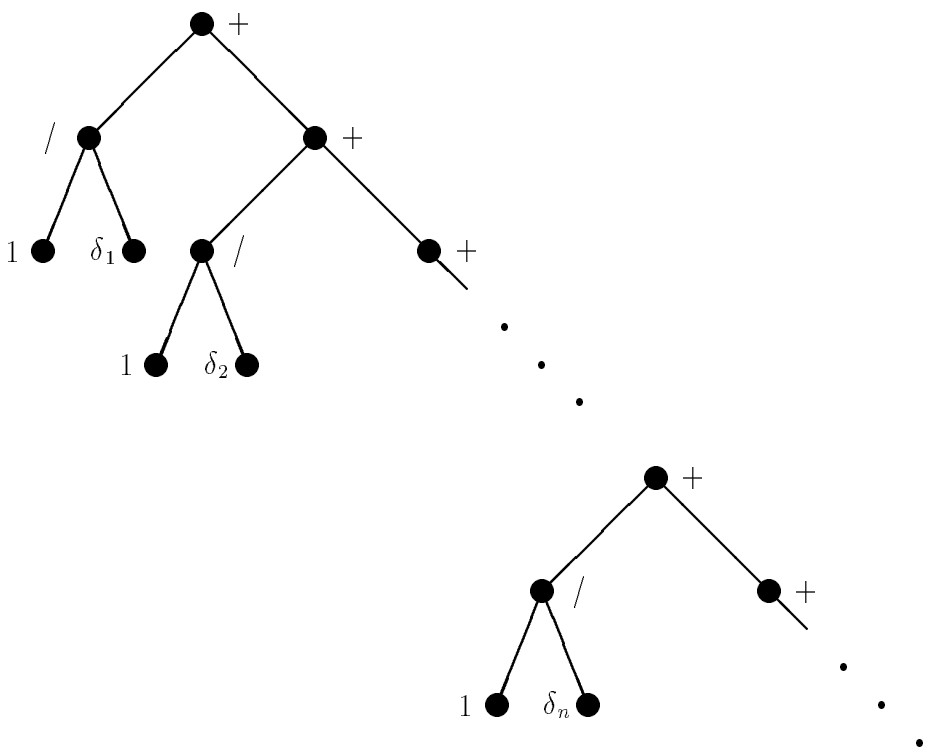
Używając symboli $\times$ i / jak operacji mnożenia i dzielenia możemy liczby naturalne przedstawiać na różne sposoby. Przykładowo, liczbę 2^n możemy przedstawić używając podobnego wyrażenia jak $\tilde{n}$, z tym że + w $\tilde{n}$ zastępujemy przez $\times$, 1 zastępujemy przez drzewo $\tilde{2}$ oraz $\perp$ zastępujemy przez 1. Zauważmy, że taka reprezentacja liczby 2^n używa liniowej w sto-

sunku do n liczby wierzchołków w odróżnieniu od wykładniczej w drzewie $\tilde{2^n}$. Na rysunku 2 przedstawiamy drzewo etykietowane δ_n, które reprezentuje liczbę 2^n przy pomocy wyżej wspomnianego wyrażenia.



Rysunek 2: Drzewo etykietowane δ_n.

Szereg nieskończony $\Sigma_{i=1}^{\infty} 1/2^i$ możemy przedstawić jako nieskończone drzewo etykietowane σ. Drzewo to jest graficznie przedstawione na rysunku 3.



Rysunek 3: Drzewo etykietowane σ.

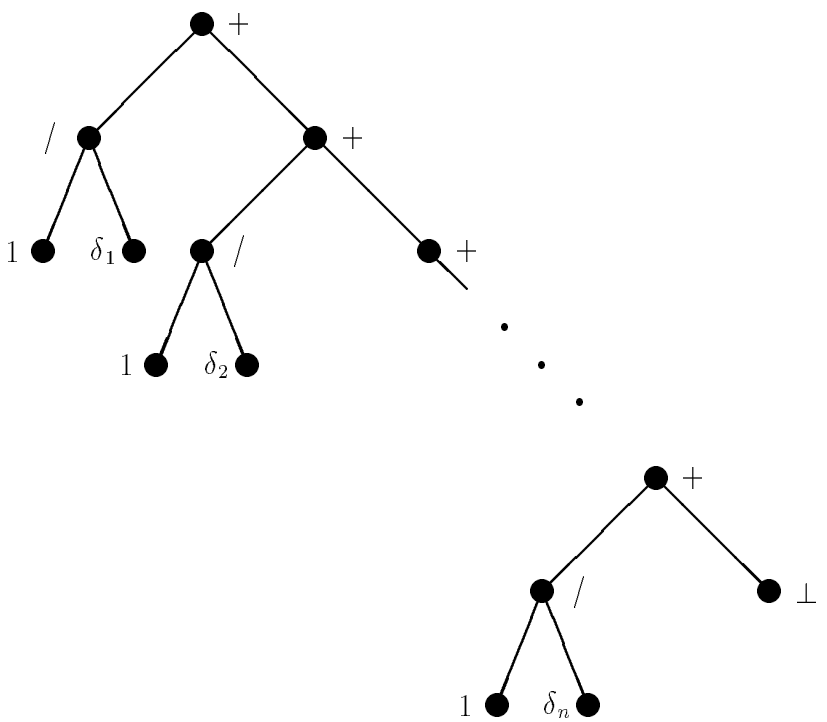
W drzewie etykietowanym z rysunku 3 i rysunku 4 symbole $\delta_1, \delta_2, \ldots, \delta_n$ nie są etykietami. Oznaczają one miejsca, na które należy wstawić drzewa etykietowane zdefiniowane na rysunku 2.

Sumę częściową $\Sigma_{i=1}^{n} 1/2^i$ tego szeregu wówczas reprezentujemy przy pomocy następującego skończonego drzewa etykietowanego σ_n (zob. Rysunek 4).

Mamy wówczas następujący wstępujący łańcuch wyrażeń

$$\sigma_1 \leq \sigma_2 \leq \ldots \sigma_n \leq \ldots \leq \sigma.$$

Powyższe aproksymowanie wyrażenia σ skończonymi wyrażeniami σ_n ma charakter czysto symboliczny, tzn. nie mają nic wspólnego ze zbieżnością szeregów liczb rzeczywistych.



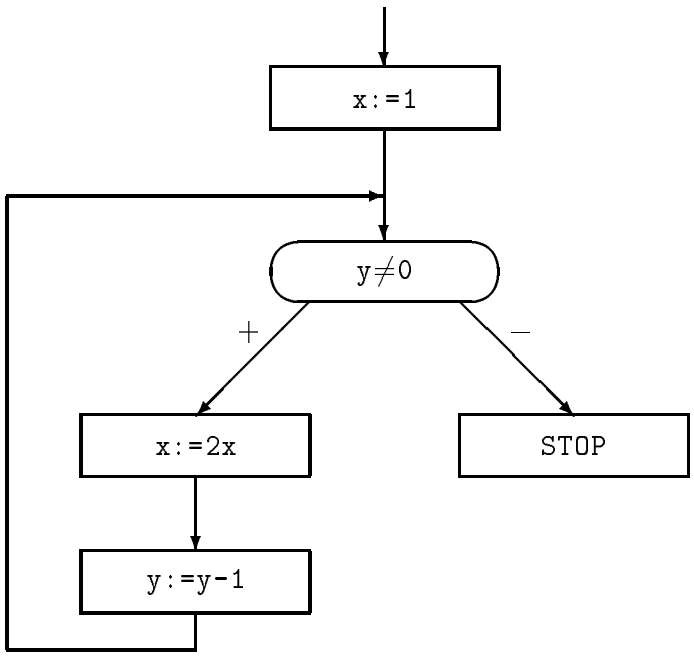
Rysunek 4: Drzewo etykietowane σ_n, n-ta aproksymacja drzewa σ.

Przykład 7.16 (*Drzewa formalnych obliczeń*) Weźmy następujące zbiory etykiet: $\Sigma_0 = \{'\texttt{STOP}',$
$\perp\}$, $\Sigma_1 = \{'\texttt{x} := 2\texttt{x}',\ '\texttt{y} := \texttt{y} - 1',\ '\texttt{x} := 1'\}$, $\Sigma_2 = \{'\texttt{y} \neq 0'\}$, $\Sigma_n = \emptyset$, dla $n > 2$. Etykiety, chociaż kojarzą się z instrukcjami języka programowania, są tutaj jedynie formalnymi napisami – dla zaznaczenia tego napisy te umieściliśmy w cudzysłowie.

Rozważmy następujący program P w Pascalu.

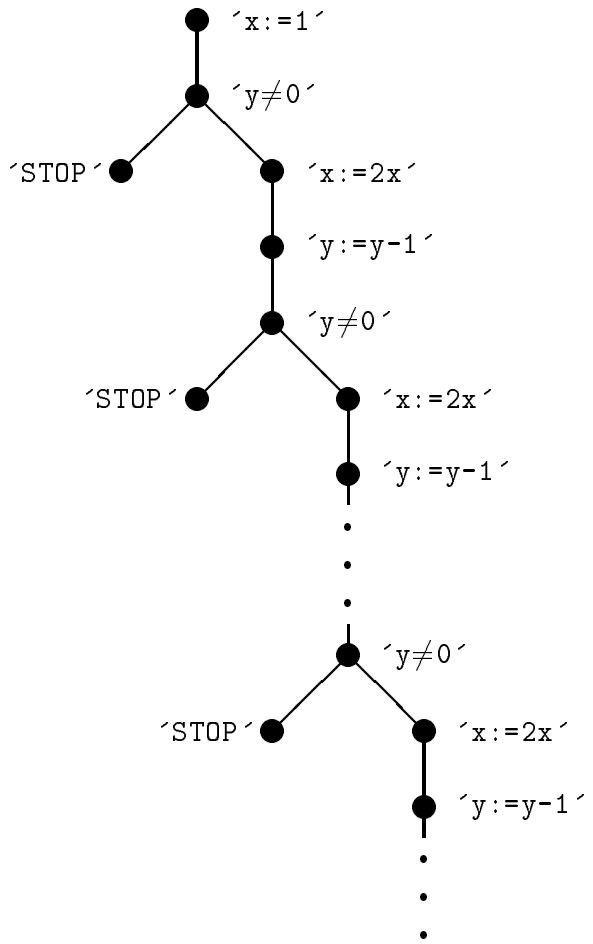
```
x := 1;
while   y ≠ 0 do
        begin x := 2x;  y := y − 1 end
```

Program ten możemy przedstawić w postaci schematu blokowego (zob. Rysunek 5) dla pokazania możliwości przepływu sterowania w programie w czasie obliczenia.



Rysunek 5: Schemat blokowy programu P.

Powyższy schemat rozwijamy do nieskończonego drzewa. W drzewie tym w naturalny sposób etykietujemy wierzchołki symbolami z powyższego zbioru etykiet. Tak otrzymane drzewo etykietowane $\pi \in T_{2\leq}(\Sigma)$ nazywa się *drzewem formalnych obliczeń* programu P, a ścieżki w tym drzewie nazywa się *ścieżkami formalnych obliczeń* programu P. Przedstawiamy go na rysunku 6.



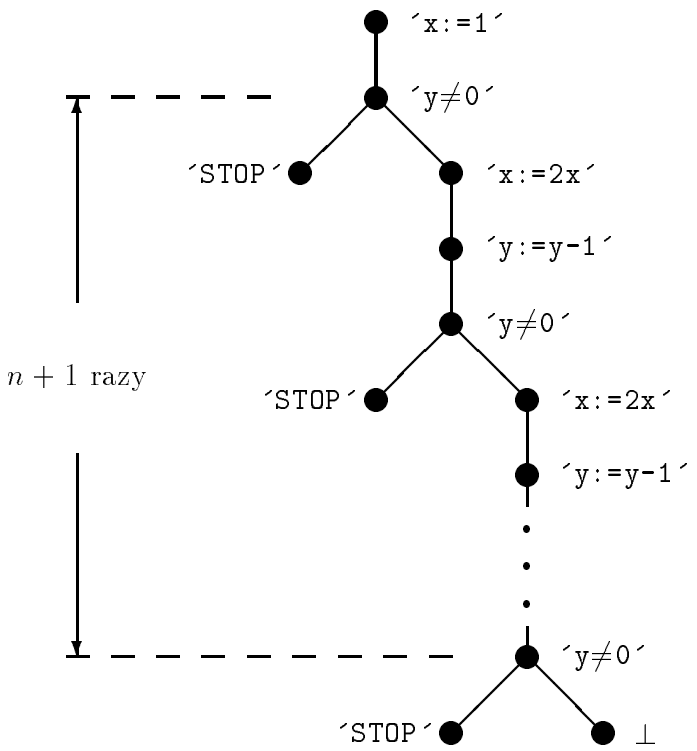
Rysunek 6: Drzewo etykietowane π formalnych obliczeń programu P.

Dla $n \in N$ niech drzewo π_n, przedstawione na rysunku 7, oznacza skończoną aproksymację drzewa π. Drzewo to reprezentuje formalne obliczenia programu P powstające w wyniku co najwyżej n przejść w P przez pętlę **while**. Osiągnięcie przez obliczenie symbolu $\perp$ w π_n intuicyjnie oznacza zapętlenie się obliczenia. Zgodnie z definicją porządku na drzewach etykietowanych mamy następujący łańcuch.

$$\pi_0 \leq \pi_1 \leq \ldots \pi_n \leq \ldots \leq \pi.$$

Dla programu P definiuje się funkcję obliczaną przez ten program. Funkcję tę nazywa się *znaczeniem* lub *semantyką* programu P. W przypadku drzew formalnych obliczeń nierówność

$\pi' \leq \pi$ implikuje, że funkcja częściowa obliczana przez program odpowiadający drzewu π' jest zawarta w funkcji częściowej obliczanej przez program odpowiadający π.



Rysunek 7: Drzewo etykietowane π_n.

Przykład 7.17 Na zakończenie części związanej z drzewami etykietowanymi wprowadzimy jeszcze jedną relację częściowego porządku, która będzie wykorzystana później.

Niech

$$FT(\Sigma) = \bigcup_{k \in N} FT_{k\leq}(\Sigma)$$

będzie zbiorem wszystkich skończonych $k^{\leq}$-argumentowych drzew etykietowanych nad Σ przy k przebiegającym wszystkie liczby naturalne. Elementy $FT(\Sigma)$ bywają nazywane *termami* nad Σ. Pojęcie poddrzewa, które zdefiniowaliśmy dla drzew nieetykietowanych, przenosi się na ważne pojęcie podtermu zdefiniowane następująco. Niech $\sigma, \tau \in FT(\Sigma)$. Term σ jest *podtermem* termu τ (oznaczamy to przez $\sigma \sqsubseteq \tau$), jeśli istnieje wierzchołek $w \in ||\tau||$ taki, że

- $||\sigma|| = (||\tau||)|_w$, oraz
- dla $u \in ||\sigma||$, $\sigma(u) = \tau(wu)$.

Definicja zbioru $FT(\Sigma)$ oraz relacja podtermu oczywiście stosują się do przypadku, gdy Σ_0 nie zawiera $\perp$. Tym niemniej musimy założyć, że $\Sigma_0 \neq \emptyset$, gdyż w przeciwnym przypadku mielibyśmy $FT(\Sigma) = \emptyset$.

Fakt 7.18 *Relacja $\sqsubseteq$ zdefiniowana powyżej jest częściowym porządkiem w $FT(\Sigma)$.*

Dowód: Wynika natychmiast z Faktu 7.13. Łatwy dowód pozostawiamy czytelnikowi. ■

7.4 Kresy zbiorów, kraty zupełne

Niech $\langle P, \leq_P \rangle$ oraz $\langle Q, \leq_Q \rangle$ będą zbiorami częściowo uporządkowanymi. Funkcję $f : P \to Q$ nazwiemy *monotoniczną* gdy dla $x, y \in P$

$$\text{jeśli } x \leq_P y, \text{ to } f(x) \leq_Q f(y).$$

Funkcja f jest *izomorfizmem* gdy f oraz f^{-1} są monotonicznymi bijekcjami. Izomorficzne zbiory częściowo uporządkowane oznaczamy $\langle P, \leq_P \rangle \simeq \langle Q, \leq_Q \rangle$.

Jako przykład izomorficznych częściowych porządków zanotujmy następujący fakt.

Fakt 7.19 *Mamy następujące izomorfizmy*

$$\langle N, \leq \rangle \ \simeq \ \langle \{0\}^*, \leq \rangle \ \simeq \langle FT_1, \subseteq \rangle$$

Dowód: Funkcja $f_1 : N \to \{0\}^*$, zdefiniowana wzorem $f_1(n) = 0^n$, dla $n \in N$ ustala izomorfizm $\langle N, \leq \rangle \ \simeq \ \langle \{0\}^*, \leq \rangle$. Natomiast funkcja $f_2 : \{0\}^* \to FT_1$ zdefiniowana wzorem $f_2(0^n) = \{0^i \mid i \leq n\}$ ustala izomorfizm $\langle \{0\}^*, \leq \rangle \ \simeq \langle FT_1, \subseteq \rangle$. ■

Niech $\langle P, \leq \rangle$ będzie częściowym porządkiem. Element $p \in P$ nazwiemy *największym* w $\langle P, \leq \rangle$ jeśli dla każdego $x \in P$ zachodzi $x \leq p$. Element $p \in P$ nazwiemy *maksymalnym* gdy dla każdego $x \in P$, jeśli $p \leq x$, to $p = x$, tzn. gdy żaden element nie jest ściśle większy od p.

Zauważmy, że jeśli $\langle P, \leq \rangle$ jest częściowym porządkiem, to $\langle P, \leq^{-1} \rangle$ jest też częściowym porządkiem. Porządek ten nazywamy *porządkiem dualnym* do $\langle P, \leq \rangle$. Jeśli mamy pewne pojęcie zdefiniowane dla częściowych porządków, to pojęcie do niego dualne otrzymuje się przez zamianę w tej definicji symbolu $\leq$ symbolem $\leq^{-1}$. Przykładowo, pojęciem dualnym do własności "być elementem maksymalnym" jest pojęcie "być elementem minimalnym" otrzymane przez dualizację powyższej definicji. Otrzymujemy następującą definicję: $p \in P$ jest elementem *minimalnym*, gdy dla każdego $x \in P$, jeśli $x \leq p$, to $p = x$. Tak więc p jest minimalny wtw, gdy p jest maksymalny w porządku dualnym. Dualnym pojęciem do definicji elementu największego jest pojęcie elementu *najmniejszego*.

Przykład 7.20 Elementem największym w $\langle P(A), \subseteq \rangle$ jest A, a najmniejszym jest $\emptyset$. Elementem najmniejszym w $\langle A^*, \leq \rangle$ jest ε, a elementu największego nie ma. Elementem najmniejszym w $\langle T_2, \subseteq \rangle$ jest $\emptyset$, a największym $\{0,1\}^*$. Elementem najmniejszym w $\langle T_{k\leq}(\Sigma), \leq \rangle$ jest drzewo jednowierzchołkowe z eteykietą $\perp$ (które też będzie oznaczane przez $\perp$), a elementu największego nie ma.

Fakt 7.21 *Element największy jest maksymalny. Każdy porządek częściowy ma co najwyżej jeden element największy.*

Dowód: Niech $p \in P$ będzie elementem największym w $\langle P, \leq \rangle$. Jeśli $p \leq x$, to ponieważ $x \leq p$, to z antysymetrii porządku otrzymujemy $p = x$.

Jeśli p_1 oraz p_2 są elementami największymi w $\langle P, \leq \rangle$, to mamay $p_1 \leq p_2$ oraz $p_2 \leq p_1$. Zatem $p_1 = p_2$. ∎

Zachodzi też twierdzenie dualne do powyższego twierdzenia.

Niech $\langle P, \leq \rangle$ będzie częściowym porządkiem i niech $X \subseteq P$ będzie dowolnym podzbiorem. Element $a \in P$ nazwiemy *ograniczeniem górnym* zbioru X, gdy dla każdego $x \in X$ zachodzi $x \leq a$. Najmniejsze ograniczenie górne zbioru X (o ile istnieje) nazywamy *kresem górnym* zbioru X. Zatem $a \in P$ jest kresem górnym zbioru X, gdy

- a jest ograniczeniem górnym X, oraz
- dla każdego $b \in P$, jeśli b jest ograniczeniem górnym X, to $a \leq b$.

Kres górny zbioru X, o ile istnieje, oznaczamy $\bigsqcup X$. Dualnymi pojęciami są: *ograniczenie dolne* i *kres dolny*. Kres dolny zbioru X (o ile istnieje) oznaczamy $\bigsqcap X$.

Zastanówmy się kiedy zbiór pusty $\emptyset$ ma kres górny (dolny) w porządku $\langle P, \leq \rangle$. Zauważmy, że każdy element zbioru P jest zarówno ograniczeniem górnym jak i dolnym $\emptyset$. Zatem, $\bigsqcup \emptyset$ (odpowiednio, $\bigsqcap \emptyset$) istnieje w $\langle P, \leq \rangle$ wtw, gdy P ma element najmniejszy (odpowiednio największy). Element najmniejszy w $\langle P, \leq \rangle$ oznaczamy $\perp$ a element największy oznaczamy $\top$. Kres zbioru może zależeć od tego w jakim zbiorze częściowo uporządkowanym

jest brany. Jeśli zachodzi konieczność zaznaczenia w jakim porządku brany jest kres (element najmniejszy, itp.) to możemy zaznaczać to używając indeksu, na przykład $\bigsqcup^P X$.

Porządek $\langle P, \leq \rangle$ nazwiemy *kratą zupełną*, gdy każdy podzbiór zbioru P ma kres górny i kres dolny.

Twierdzenie 7.22 *Niech $\langle P, \leq \rangle$ będzie częściowym porządkiem. Następujące warunki są równoważne.*

(i) $\langle P, \leq \rangle$ jest kratą zupełną.

(ii) Każdy podzbiór P ma kres górny w $\langle P, \leq \rangle$.

(iii) Każdy podzbiór P ma kres dolny w $\langle P, \leq \rangle$.

Dowód: Implikacje (i) $\Rightarrow$ (ii) oraz (i) $\Rightarrow$ (iii) oczywiście zachodzą. Udowodnimy implikację (ii) $\Rightarrow$ (i). Załóżmy, że każdy podzbiór zbioru P ma kres górny. Niech $X \subseteq P$ i niech Y będzie zbiorem wszystkich ograniczeń dolnych zbioru X w $\langle P, \leq \rangle$. Niech

$$p_0 = \bigsqcup Y.$$

Niech $x \in X$. Ponieważ dla każdego $y \in Y$, mamy $y \leq x$ to x jest ograniczeniem górnym zbioru Y. Zatem $p_0 \leq x$, co wobec dowolności wyboru x dowodzi, że p_0 jest ograniczeniem dolnym zbioru X. Jeśli y jest ograniczeniem dolnym zbioru X, to $y \in Y$, a zatem $y \leq p_0$. Czyli p_0 jest największym ograniczeniem zbioru X, więc

$$p_0 = \bigsqcap X.$$

Dowód implikacji (iii) $\Rightarrow$ (i) jest analogiczny do powyższego. Pozostawimy go czytelnikowi. ∎

Rozważmy kilka przykładów.

Przykład 7.23

(i) $\langle P(A), \subseteq \rangle$ jest kratą zupełną dla każdego zbioru A. Kresem górnym rodziny zbiorów $\mathcal{A} \subseteq P(A)$ jest suma $\bigcup \mathcal{A}$, a kresem dolnym jest przecięcie $\bigcap \mathcal{A}$, o ile $\mathcal{A} \neq \emptyset$, oraz A jeśli $\mathcal{A} = \emptyset$. Sprawdzenie powyższych własności pozostawiamy czytelnikowi.

(ii) $\langle N, \leq \rangle$ nie jest kratą zupełną bo N nie ma kresu górnego (bo nie ma ograniczenia górnego). Każdy niepusty podzbiór N ma kres dolny (bo ma element najmniejszy).

(iii) W porządku prefiksowym $\langle \{0,1\}^*, \leq \rangle$ zbiór $\{0,1\}$ nie ma kresu górnego ale ma kres dolny: $\bigsqcap \{0,1\} = \varepsilon$. Wynika to stąd, że $\{\varepsilon\}$ jest jedynym prefiksem słów 0 oraz 1.

(iv) W porządku leksykograficznym $\langle\{0,1\}^*, \preceq\rangle$ (przy uporządkowaniu liter: $0 \leq 1$) mamy

$$\bigsqcup\{0w \in \{0,1\}^* \mid w \in \{0,1\}^*\} = 1$$

Istotnie, dla każdego $w \in \{0,1\}^*$, mamy $0w \preceq 1$. Ponadto jeśli dla każdego $w \in \{0,1\}^*$ słowo $0w$ jest leksykograficznie wcześniejsze od pewnego ustalonego słowa u to u musi się zaczynać od litery 1 (gdyby $u = 0u'$ dla pewnego słowa u', to mielibyśmy $w \preceq u'$ dla dowolnych $w \in \{0,1\}^*$, a zatem u' byłoby największym elementem w $\langle\{0,1\}^*, \preceq\rangle$, co daje sprzeczność). Zatem 1, jako prefiks słowa u, jest leksykograficznie wcześniejszy od u.

Natomiast zbiór $X = \{0^n \in \{0,1\}^* \mid n \in N\}$ nie ma kresu górnego w tym porządku pomimo tego, że ma wiele ograniczeń górnych. Jeśli w jest ograniczeniem górnym zbioru X, to w musi zawierać 1. Zatem istnieje słowo w' oraz $n \in N$ takie, że $w = 0^n 1 w'$. Wówczas $0^{n+1}1w'$ jest ograniczeniem górnym X mniejszym leksykograficznie od w. Pokazaliśmy więc, że X nie ma najmniejszego ograniczenia górnego.

(v) Kresem dolnym zbioru $\{1/3^n \mid n \in N\}$ w zbiorze liczb rzeczywistych R, uporządkowanym zwykłą relacją $\leq$, jest 0. Każdy niepusty zbiór ograniczony w R z góry (z dołu) ma kres górny (dolny) w R. Natomiast $\emptyset$ nie ma ani kresu górnego ani dolnego w R.

(vi) $\bigsqcup\{\sigma_n \mid n \geq 1\} = \sigma$, w porządku z Przykładu 7.15 dla wyrażeń arytmetycznych. Wyrażenie σ_n formalnie reprezentuje skończony szereg $\Sigma_{i=1}^{n} 1/2^i$ (zob. Rysunek 4 w Przykładzie 7.15). Natomiast wyrażenie σ formalnie reprezentuje nieskończony szereg $\Sigma_{n=1}^{\infty} 1/2^i$ (zob. Rysunek 3 w Przykładzie 7.15). Pozostawimy czytelnikowi pokazanie, że σ jest kresem górnym wyrażeń σ_n.

(vii) $\bigsqcup\{\pi_n \in T_{2\leq}(\Sigma) \mid n \in N\} = \pi$, w porządku z Przykładu 7.16 dla drzew formalnych obliczeń. Drzewo π oraz drzewa π_n są przedstawione na Rysunkach 6 oraz 7 Przykładu 7.16. Pozostawimy czytelnikowi jako ćwiczenie pokazanie, że π jest kresem górnym drzew π_n.

(viii) Niech $\langle EQ(A), \subseteq\rangle$ będzie zbiorem wszystkich relacji równoważności w A, uporządkowanym relacją zawierania. Ponieważ, jak łatwo jest pokazać, przecięcie dowolnej niepustej rodziny relacji równoważności jest relacją równoważności oraz $EQ(A)$ ma element największy: $A \times A$, to każdy podzbiór w $EQ(A)$ ma kres dolny, a zatem, zgodnie z Twierdzeniem 7.22, $\langle EQ(A), \subseteq\rangle$ jest kratą zupełną. W kracie tej kres górny rodziny relacji równoważności nie zawsze pokrywa się z sumą teoriomnogościową tej rodziny.[9]

[9] Suma relacji równoważności nie musi być relacją równoważności.

7.5 Twierdzenia o punkcie stałym

Twierdzenie 7.24 (Knaster-Tarski)
Niech $\langle P, \leq \rangle$ będzie kratą zupełną i niech $f : P \to P$ będzie funkcją monotoniczną. Wtedy f ma najmniejszy punkt stały, tzn. istnieje $a_0 \in P$, taki że

- $f(a_0) = a_0$,
- *dla każdego $b \in P$, jeśli $f(b) = b$, to $a_0 \leq b$.*

Dowód: Niech $X = \{x \in P \mid f(x) \leq x\}$ i niech

$$a_0 = \bigsqcap X.$$

Jeśli $x \in X$ to $a_0 \leq x$ i z monotoniczności f oraz z definicji zbioru X otrzymujemy

$$f(a_0) \leq f(x) \leq x.$$

Zatem $f(a_0)$ jest ograniczeniem dolnym zbioru X. Poniważ a_0 jest największym ograniczeniem dolnym X to

$$f(a_0) \leq a_0. \tag{31}$$

Powyższa nierówność oraz monotoniczność f dają

$$f(f(a_0)) \leq f(a_0),$$

zatem $f(a_0) \in X$. Tak więc, ponieważ a_0 jest dolnym ograniczeniem X to $a_0 \leq f(a_0)$. Ta nierówność w połączeniu z (31) daje

$$a_0 = f(a_0).$$

Aby pokazać, że a_0 jest najmniejszym punktem stałym f załóżmy, że $f(b) = b$. Zatem $b \in X$ oraz $a_0 \leq b$. To kończy dowód twierdzenia. ■

Przykład 7.25 Podamy trzy przykłady ilustrujące zastosowanie twierdzenia Tarskiego.

(i) Załóżmy, że A jest alfabetem zawierającym 0 i 1. Niech $f : P(A^*) \to P(A^*)$ będzie funkcją zdefiniowaną następująco:

$$f(X) = \{\varepsilon\} \cup \{0w \mid w \in X\} \cup \{1w \mid w \in X\}.$$

Wtedy f jest funkcją monotoniczną oraz zbiór $\{0,1\}^*$ jest najmniejszym punktem stałym f.[10]

[10] W tym przypadku można dodatkowo pokazać, że ten zbiór jest jedynym punktem stałym f.

(ii) Niech A będzie dowolnym zbiorem i niech $R \subseteq A \times A$ będzie dowolną relacją w zbiorze A. Rozważmy następującą funkcję $\varphi : P(A \times A) \to P(A \times A)$,

$$\varphi(X) = R \cup I_A \cup (XX) \cup X^{-1}.$$

Pokażemy, że dla dowolnej relacji $X \subseteq A \times A$,

$$\varphi(X) \subseteq X \quad \text{wtw, gdy} \quad X \text{ jest relacją równoważności zawierającą } R. \tag{32}$$

Powyższa równoważność wynika natychmiast z następujących trzech równoważności, których dowód pozostawimy czytelnikowi.

$$I_A \subseteq X \quad \text{wtw, gdy} \quad X \text{ jest relacją zwrotną.}$$

$$XX \subseteq X \quad \text{wtw, gdy} \quad X \text{ jest relacją przechodnią.}$$

$$X^{-1} \subseteq X \quad \text{wtw, gdy} \quad X \text{ jest relacją symetryczną.}$$

Zatem najmniejszy punkt stały przekształcenia φ jest najmniejszą relacją równoważności zawierającą daną relację R.

(iii) **Dowód Lematu Banacha**
Dla dowodu Lematu Banacha (zob. Twierdzenie 6.10) weźmy dowolne funkcje $f : A \to B$ oraz $g : B \to A$ i zdefiniujmy $\varphi : P(A) \to P(A)$ wzorem,

$$\varphi(X) = A - \vec{g}(B - \vec{f}(X)).$$

Ponieważ operacja dopełnienia jest antymonotoniczna, tzn. odwraca porządek zawierania oraz operacja obrazu jest monotoniczna, to funkcja φ jest monotoniczna. Niech A_1 będzie najmniejszym punktem stałym φ. Pozostałe zbiory są już wyznaczone jednoznacznie przez A_1, a mianowicie $A_2 = A - A_1$, $B_1 = \vec{f}(A_1)$, oraz $B_2 = B - B_1$. Pozostaje do pokazania, że

$$A_2 = \vec{g}(B_2). \tag{33}$$

Ponieważ

$$\vec{g}(B_2) = \vec{g}(B - B_1) = \vec{g}(B - \vec{f}(A_1)),$$

to

$$A - \vec{g}(B_2) = A - \vec{g}(B - \vec{f}(A_1)) = \varphi(A_1) = A_1.$$

Zatem

$$\vec{g}(B_2) = A - A_1 = A_2,$$

co dowodzi (33). ■

Jak zobaczymy w dalszej części wykładu zdarzają się sytuacje gdy założenie, że dziedzina funkcji ma być kratą zupełną jest zbyt silne. W tym celu wprowadzimy następujące definicje. Podzbiór X zbioru uporządkowanego $\langle A, \leq \rangle$ nazwiemy *skierowanym*, gdy $X \neq \emptyset$ oraz każde dwa elementy w X mają ograniczenie górne w X, tzn. dla dowolnych $a, b \in X$, istnieje $c \in X$, taki że $a \leq c$ oraz $b \leq c$. Pojęcie zbioru skierowanego jest bardzo ważnym uogólniniem pojęcia łańcucha. Zbiór uporządkowany $\langle A, \leq \rangle$ nazwiemy *zupełnym porządkiem*, gdy A ma element najmniejszy oraz każdy zbiór skierowany ma kres górny. Niech $\langle A, \leq \rangle$ oraz $\langle B, \leq \rangle$ będą zupełnymi porządkami. Funkcję $f : A \to B$ nazwiemy *ciągłą*, gdy zachowuje ona kresy górne zbiorów skierowanych, tzn. gdy dla dowolnego zbioru skierowanego X w $\langle A, \leq \rangle$, $\vec{f}(X)$ ma kres górny oraz

$$f(\bigsqcup X) = \bigsqcup \vec{f}(X).$$

Fakt 7.26

(i) Każda funkcja ciągła jest monotoniczna.

(ii) Złożenie funkcji ciągłych jest funkcją ciągłą.

Dowód: Dla dowodu (i) niech $f : A \to B$ będzie funkcją ciągłą pomiedzy zupełnymi porządkami. Jeśli $a_1 \leq_A a_2$ to zbiór $\{a_1, a_2\}$ jest skierowany. Zatem

$$f(a_2) = f(\bigsqcup\{a_1, a_2\}) = \bigsqcup\{f(a_1), f(a_2)\}.$$

Oznacza to, że

$$f(a_1) \leq_B f(a_2).$$

A zatem f jest monotoniczna.

Dla dowodu (ii) zauważmy, że obraz zbioru skierowanego przy przekształceniu ciągłym jest zbiorem skierowanym. Wynika to z monotoniczności funkcji ciągłych. ∎

Podamy teraz dwa ważne przykłady zupełnych porządków nie będących kratami zupełnymi. Sprawdzenie, że porządki te są zupełne pozostawimy czytelnikowi.

Przykład 7.27

(i) Dla każdego k, porządek $\langle T_{k\leq}(\Sigma), \leq \rangle$ (zob. Przykład 7.15) jest zupełny.

(ii) Dla dowolnych zbiorów A, B, zbiór $PF(A, B)$ wszystkich funkcji częściowych z A w B uporządkowanych relacją zawierania jest zupełnym porządkiem. Kresem górnym zbioru skierowanego funkcji częściowych jest suma teoriomnogościowa.

Twierdzenie 7.28 *Niech $\langle A, \leq \rangle$ będzie zupełnym porządkiem oraz niech $f : A \to A$ będzie funkcją ciągłą. Wtedy f ma najmniejszy punkt stały a_o oraz*

$$a_0 = \bigsqcup\{f^n(\bot) \mid n \in N\}.$$

Dowód: Najpierw zauważmy, że $\{f^n(\bot) \mid n \in N\}$ jest łańcuchem, a zatem zbiorem skierowanym. Wynika to natychmiast z następującej własności. Dla każdego $n \in N$,

$$f^n(\bot) \leq f^{n+1}(\bot). \tag{34}$$

Dowód (34) przeprowadzamy przez indukcję względem n. Dla $n = 0$ wynika to natychmiast z tego, że $\bot$ jest najmniejszym elementem. Krok indukcyjny wynika z monotoniczności f.

Tak więc $a_0 = \bigsqcup\{f^n(\bot) \mid n \in N\}$ istnieje. Mamy:

$$\begin{aligned} f(a_0) &= f(\bigsqcup\{f^n(\bot) \mid n \in N\}) \\ &= \bigsqcup\{f^{n+1}(\bot) \mid n \in N\} \\ &= \bigsqcup(\{f^{n+1}(\bot) \mid n \in N\} \cup \{\bot\}) \\ &= \bigsqcup\{f^n(\bot) \mid n \in N\} \\ &= a_0. \end{aligned}$$

W powyższym ciągu równości druga równość wynika stąd, że f jest funkcją ciągłą, natomiast trzecia równość wynika stąd, że dodanie elementu najmniejszego $\bot$ do dowolnego zbioru nie zmienia kresu górnego.

Tak więc a_0 jest punktem stałym. Pozostaje do wykazania, że jest to najmniejszy punkt stały. Niech $f(b) = b$ będzie dowolnym punktem stałym. Przez oczywistą indukcję ze względu na n pokazujemy, że dla $n \in N$,

$$f^n(\bot) \leq b. \tag{35}$$

Dowód (35) pozostawimy czytelnikowi. Zatem b jest ograniczeniem górnym zbioru $\{f^n(\bot) \mid n \in N\}$, czyli $a_0 \leq b$. To kończy dowód twierdzenia. ■

Podamy dwa przykłady na zastosowanie powyższego twierdzenia.

Przykład 7.29

(i) Niech Σ będzie rodziną etykiet z przykładu 7.16. Niech $\varphi : T_{2\leq}(\Sigma) \to T_{2\leq}(\Sigma)$ będzie funkcją zdefiniowaną następująco. Dla $\sigma \in T_{2\leq}(\Sigma)$,

$$||\varphi(\sigma)|| = \{\varepsilon, 0, 1, 10\} \cup \{100w \mid w \in ||\sigma||\}.$$

Dla $w \in ||\varphi(\sigma)||$ definiujemy

$$\varphi(\sigma)(w) = \begin{cases} \text{'y} \neq \text{0'}, & \text{gdy } w = \varepsilon, \\ \text{'STOP'}, & \text{gdy } w = 0, \\ \text{'x} := 2\text{x'}, & \text{gdy } w = 1, \\ \text{'y} := \text{y} - 1\text{'}, & \text{gdy } w = 10, \\ \sigma(u), & \text{gdy } w = 100u,\ u \in ||\sigma||. \end{cases}$$

Funkcja φ jest naturalnym złożeniem pewnych prostych funkcji (jakich?). Można pokazać, że każda z tych funkcji jest ciągła, a zatem φ, na mocy Lematu 7.26, jest funkcją ciągłą. Pozostawimy to jako ćwiczenie dla czytelnika.

Zauważmy, że n-krotna iteracja $\varphi^n(\perp)$ przedstawia drzewo formalnych obliczeń reprezentujących co najwyżej n wykonań pętli w programie (zob. Rysunek 7 w Przykładzie 7.16)

while $\text{y} \neq 0$ **do** $\text{x} := 2\text{x};\ \text{y} := \text{y} - 1$ **od**

Natomiast najmniejszy punkt stały φ, jako kres górny ciągu iteracji, przedstawia drzewo formalnych obliczeń całego powyższego programu (zob. Rysunek 6 w Przykładzie 7.16).

(ii) Przypomnijmy, że $PF(A, B)$ oznacza zupełny porządek funkcji częściowych z Przykładu 7.27 (ii). Niech $\varphi : PF(N \times N, N) \to PF(N \times N, N)$ będzie funkcją zdefiniowaną następująco dla $f \in PF(N \times N, N)$, oraz $m, n \in N$

$$\varphi(f)(m,n) = \begin{cases} m, & \text{jeśli } n = 0, \\ f(m,k)', & \text{jeśli } n = k' \text{ oraz } \langle m,k\rangle \in Dom(f), \\ \text{nieokreślone}, & \text{w przeciwnym przypadku.} \end{cases}$$

Pozostawimy czytelnikowi jako ćwiczenie wykazanie, że φ jest funkcją ciągłą. Zauważmy, że jeśli f jest punktem stałym φ, to $Dom(f) = N \times N$, tzn. f jest funkcją totalną. Wynika to z następującego faktu, którego dowód indukcyjny pozostawimy czytelnikowi.

Jeśli f jest punktem stałym φ, to dla każdego $n \in N$ zachodzi następująca własność

$$\text{dla każdego } m \in N, \quad \text{zachodzi } \langle m,n\rangle \in Dom(f). \tag{36}$$

Tak więc powyższa definicja φ oraz (36) implikują, że każdy punkt stały f przekształcenia φ musi spełniać następujące warunki

$$\begin{aligned} f(m,0) &= m, \\ f(m,n') &= f(m,n)'. \end{aligned}$$

Czytelnik z łatwością rozpozna indukcyjną definicję dodawania (zob. Przykład 4.7). Tak więc najmniejszym (i jedynym) punktem stałym φ jest funkcja dodawania. Iteracja $\varphi^n(\perp)$ przedstawia operację częściowego dodawania $m+k$ dla $k < n$ oraz $m \in N$. Suma teoriomnogościowa tych operacji daje oczywiście pełną operację dodawania.

(iii) **Dowód twierdzenia o definiowaniu funkcji przez indukcję**
Stosując rozumowanie podobne do powyższego przykładu udowodnimy teraz Twierdzenie 4.8. Niech A i B będą dowolnymi zbiorami. Niech $g : A \to B$ oraz niech $h : B \times A \times N \to B$ będą dowolnymi funkcjami. Pokażemy że istnieje dokładnie jedna funkcja $f : A \times N \to B$ spełniająca następujące warunki dla dowolnego $a \in A$,

$$f(a,0) = g(a),$$
$$f(a,n') = h(f(a,n),a,n).$$

Jednoznaczność dowodzi się pokazując przez bardzo prostą indukcję, że jeśli f_1 i f_2 spełniają powyższą definicję to dla każdego $a \in A$,

$$\text{dla każdego } n \in N,\ f_1(a,n) = f_2(a,n).$$

Dla dowodu istnienia użyjemy, podobnie jak w poprzednim przykładzie, Twierdzenia 7.28. Niech $\varphi : PF(A \times N, B) \to PF(A \times N, B)$ będzie funkcją zdefiniowaną następująco

$$\varphi(f)(a,n) = \begin{cases} g(a), & \text{jeśli } n = 0, \\ h(f(a,k),a,k), & \text{jeśli } n = k',\ \langle a,k\rangle \in Dom(f), \\ \text{nieokreślone}, & \text{w przeciwnym przypadku.} \end{cases}$$

Funkcja φ jest ciągła jako złożenie pewnych naturalnych funkcji ciągłych (jakich?). Dowód ciągłości pozostawimy czytelnikowi jako ćwiczenie. Podobnie jak w poprzednim przykładzie zauważamy, że punkty stałe φ są funkcjami totalnymi oraz, że wszystkie punkty stałe φ spełniają powyższą definicję indukcyjną. To kończy dowód istnienia f. ■

7.6 Lemat Kuratowskiego-Zorna

Poniższe twierdzenie, znane jako lemat Kuratowskiego-Zorna, odgrywa ważną rolę w dowodach istnienia pewnych obiektów. Dowody wykorzystujące tę metodę są *niekonstruktywne* bowiem dowód istnienia obiektu nie podaje konstrukcji tego obiektu. Dowód tego twierdzenia zostanie podany w następnym rozdziale.

Twierdzenie 7.30 (Lemat Kuratowskiego-Zorna)
Jeśli $\langle A, \leq\rangle$ jest niepustym zbiorem częściowo uporządkowanym, w którym każdy łańcuch ma ograniczenie górne, to A ma element maksymalny.

Przykład 7.31 Dla zilustrowania sposobu zastosowania tego twierdzenia pokażemy, że każdy częściowy porządek można rozszerzyć do porządku liniowego, tzn. jeśli $\langle A, r_0\rangle$ jest zbiorem częściowo uporządkowanym, to istnieje liniowy porządek r_* na A, taki że $r_0 \subseteq r_*$.

Niech $\mathcal{R}$ oznacza zbiór wszystkich częściowych porządków r na A, takich że $r_0 \subseteq r$. Niech $\mathcal{L}$ będzie łańcuchem w $\mathcal{R}$ (ze względu na relację zawierania $\subseteq$). Jeśli $\mathcal{L} = \emptyset$, to r_0 jest ograniczeniem górnym $\mathcal{L}$. Załóżmy więc, że $\mathcal{L} \neq \emptyset$. Ma miejsce następujący fakt (jego dowód pozostawimy czytelnikowi).

Fakt 7.32 *Suma teoriomnogościowa łańcucha częściowych porządków w A jest częściowym porządkiem w A.*

Z faktu 7.32 natychmiast wynika, że $\bigcup \mathcal{L}$ jest ograniczeniem górnym[11] w $\mathcal{R}$ łańcucha $\mathcal{L}$. Zatem, na mocy lematu Kuratowskiego-Zorna, $\mathcal{R}$ ma element maksymalny r_*. Liniowość porządku r_* wynika natychmiast z następującego faktu, który też pozostawiamy czytelnikowi do udowodnienia.

Fakt 7.33 *Częściowy porządek r na A jest maksymalnym elementem w zbiorze wszystkich częściowych porządków na A (ze względu na relację zawierania), wtw, gdy r jest liniowym porządkiem.*

Zadania

7.1. Dowieść, że dla dowolnego drzewa $s \in FT_{k\leq}$, oraz słów v, w takich, że $vw \in s$, zachodzi $(s|_v)|_w = s|_{vw}$.

7.2. Dowieść, że relacja "być podtermem" jest relacją częściowego porządku w zbiorze wszystkich termów $FT(\Sigma)$.

7.3. Dowieść, że w zbiorze częściowo uporządkowanym $\langle P(A), \subseteq\rangle$ kres górny dowolnej rodziny zbiorów pokrywa się z sumą teoriomnogościową oraz kres dolny dowolnej niepustej rodziny zbiorów pokrywa się z przecięciem teoriomnogościowym.

7.4. Dowieść, że $\bigsqcup\{\sigma_n \mid n \geq 1\} = \sigma$, w porządku z Przykładu 7.15 dla wyrażeń arytmetycznych.

7.5. Dowieść, że $\bigsqcup\{\pi_n \in T_{2\leq}(\Sigma) \mid n \in N\} = \pi$, w porządku z Przykładu 7.16 dla drzew formalnych obliczeń.

7.6. Dowieść, że funkcja f z Przykładu 7.25 (i) ma dokładnie jeden punkt stały.

[11] Ponieważ $\mathcal{L} \neq \emptyset$, to $r_0 \subseteq \bigcup \mathcal{L}$.

7.7. Dowieść, że dla dowolnych zbiorów A, B, zbiór $PF(A,B)$ wszystkich funkcji częściowych z A w B, uporządkowany relacją zawierania jest zupełnym porządkiem.

7.8. Niech $\langle A, \leq_A \rangle$ oraz $\langle B, \leq_B \rangle$ będą zupełnymi porządkami. W produkcie $A \times B$ definiujemy relację $\leq$ w następujący sposób: $\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle$ wtw, gdy $a_1 \leq_A a_2$ oraz $b_1 \leq_B b_2$. Dowieść, że $\langle A \times B, \leq \rangle$ jest zupełnym porządkiem.

7.9. Niech $\langle A, \leq_A \rangle$ oraz $\langle B, \leq_B \rangle$ będą zupełnymi porządkami. Niech $[A,B]$ oznacza zbiór wszystkich funkcji ciągłych z A w B. Niech $\leq$ bedzie relacją w $[A,B]$ zdefiniowaną następująco: $f \leq g$ wtw, gdy dla każdego $a \in A$ zachodzi $f(a) \leq_B g(a)$. Dowieść, że $\langle [A,B], \leq \rangle$ jest zupełnym porządkiem.

7.10. Dowieść, że każda funkcja stała pomiędzy zupełnymi porządkami jest ciągła.

7.11. Niech $f \in \Sigma_n$, zdefiniujemy $\varphi_f : T_{k\leq}(\Sigma)^n \to T_{k\leq}(\Sigma)$ następująco dla $\sigma_0, \ldots, \sigma_{n-1} \in T_{k\leq}(\Sigma)$,

$$||\varphi_f(\sigma_0, \ldots, \sigma_{n-1})|| = \{\varepsilon\} \cup \bigcup_{i<n} \{iw \mid w \in ||\sigma_i||\},$$

oraz

$$\varphi_f(\sigma_0, \ldots, \sigma_{n-1})(w) = \begin{cases} f, & \text{gdy } w = \varepsilon, \\ \sigma_i(u), & \text{gdy } i < n \text{ oraz } w = iu. \end{cases}$$

Dowieść, że φ_f jest funkcją ciągłą.

7.12. Niech $\langle A, \leq_A \rangle$ oraz $\langle B, \leq_B \rangle$ będą zupełnymi porządkami. Niech $\varphi : [A,B] \times A \to B$ będzie funkcją zdefiniowaną dla $f \in [A,B]$ oraz $a \in A$ następująco,

$$\varphi(f,a) = f(a)$$

Dowieść, że φ jest funkcją ciągłą.

7.13. Dowieść, że dla dowolnych zbiorów A, B, C, funkcja $\varphi : PF(A,B) \times PF(B,C) \to PF(A,C)$ zdefiniowana wzorem $\varphi(f,g) = gf$ jest funkcją ciągłą.

7.14. Dowieść, że dla dowolnych zbiorów A, B, C, funkcja $\varphi : PF(A,B) \times PF(A,C) \to PF(A, B \times C)$ zdefiniowana wzorem

$$\varphi(f,g)(a) = \begin{cases} \langle f(a), g(a) \rangle, & \text{gdy } a \in Dom(f) \cap Dom(g), \\ \text{nieokreślone}, & \text{w przeciwnym przypadku}, \end{cases}$$

jest funkcją ciągłą.

7.15. Niech $A_1 \cap A_2 = \emptyset$. Dowieść, że funkcja $\varphi : PF(A_1,B) \times PF(A_2,B) \to PF(A_1 \cup A_2, B)$ zdefiniowana wzorem $\varphi(f,g) = f \cup g$ jest funkcją ciągłą.

7.16. Niech $C \subseteq A$. Dowieść, że funkcja $\varphi : PF(A,B) \to PF(C,B)$, zdefiniowana wzorem $\varphi(f) = f \cap (C \times B)$ jest funkcją ciągłą.

7.17. Dowieść, że następująca operacja definiowania warunkowego jest funkcją ciągłą. Niech $A_1, A_2 \subseteq A$, $A_1 \cap A_2 = \emptyset$. Niech $\varphi : PF(A,B) \times PF(A,B) \to PF(A,B)$ będzie zdefiniowana następującym wzorem dla $f, g \in PF(A,B)$ oraz $a \in A$,

$$\varphi(f,g)(a) = \begin{cases} f(a), & \text{gdy } a \in A_1 \cap Dom(f), \\ g(a), & \text{gdy } a \in A_2 \cap Dom(g), \\ \text{nieokreślone}, & \text{w przeciwnym przypadku.} \end{cases}$$

Dowieść, że φ jest funkcją ciągłą.

7.18. Udowodnić Fakt 7.32 oraz Fakt 7.33.

8 Dobre ufundowanie

Zbiór częściowo uporządkowany $\langle A, \leq \rangle$ nazwiemy *dobrze ufundowanym*, gdy nie istnieje w A nieskończony zstępujący ciąg elementów, tzn. gdy nie istnieje różnowartościowa funkcja $f : N \to A$ taka, że dla wszystkich $n \in N$, zachodzi $f(n+1) \leq f(n)$. Dobrze ufundowany liniowy porządek nazywamy *dobrym porządkiem.*

Przypomnijmy, że jeśli $\leq$ jest częściowym porządkiem, to dla zaznaczenia, że element a jest ściśle mniejszy od b (tzn. $a \neq b$ oraz $a \leq b$) będziemy pisać $a < b$.

Następujące twierdzenie podaje pożyteczną charakteryzację porządków dobrze ufundowanych.

Twierdzenie 8.1 *Częściowy porządek $\langle A, \leq \rangle$ jest dobrze ufundowany, wtw, gdy każdy niepusty podzbiór zbioru A ma element minimalny.*

Dowód: Niech $\langle A, \leq_A \rangle$ będzie zbiorem dobrze ufundowanym i załóżmy, że $X \subseteq A$ jest niepustym podzbiorem nie mającym elementu minimalnego. Zdefiniujemy ciąg $f : N \to X$ następująco. Niech $f(0) \in X$ będzie dowolnym elementem. Załóżmy, że f została zdefiniowana dla liczb $k \leq n$ oraz, że dla wszystkich $k < n$ mamy $f(k') <_A f(k)$. Wówczas $f(n')$ wybieramy jako dowolny element zbioru X taki, że $f(n') <_A f(n)$. Istnienie takiego elementu $f(n')$ wynika stąd, że $f(n)$ nie jest elementem minimalnym w X. Tak więc zdefiniowaliśmy nieskończony zstępujący ciąg elementów zbioru A. Otrzymana sprzeczność dowodzi, że każdy niepusty podzbiór zbioru A ma element minimalny.

Na odwrót, jeśli $f : N \to A$ jest nieskończonym zstępującym ciągiem elementów A to oczywiście obraz $\vec{f}(N)$ jest niepustym podzbiorem A nie mającym elementu minimalnego. ∎

Bezpośrednią konsekwencją powyższego twierdzenia oraz zasady minimum (zob. Twierdzenie 3.5) jest następujący wynik.

Twierdzenie 8.2 *Zbiór liczb naturalnych ze zwykłym porządkiem jest dobrym porządkiem.*

Przykład 8.3

1. Dla dowolnego zbioru A, zbiór wszystkich słów nad A uporządkowany porządkiem prefiksowym jest dobrze ufundowany. Istotnie, gdyby $w_0 > w_1 > \ldots$ był zstępującym ciągiem słów, to biorąc pod uwagę ich długości dostalibyśmy zstępujący ciąg liczb naturalnych $|w_0| > |w_1| > \ldots$, co jest niemożliwe na mocy Twierdzenia 8.2.

2. Zbiór $\langle \{0,1\}^*, \preceq \rangle$ z porządkiem leksykograficznym indukowanym przez porządek $0 \leq 1$ (zob. Przykład 7.8) nie jest dobrze ufundowany bowiem ciąg

$$\ldots \preceq 0^{k+1}1 \preceq 0^k 1 \preceq \ldots \preceq 1$$

tworzy nieskończony łańcuch zstępujący.

3. Jeśli $\mathcal{F}$ jest dowolną rodziną zbiorów skończonych, to $\langle \mathcal{F}, \subseteq \rangle$ jest dobrze ufundowanym porządkiem. Wynika to stąd, że dla zbiorów skończonych A, B, jeśli A jest właściwym podzbiorem B, to $|A| < |B|$. Zatem nieskończony zstępujący ciąg zbiorów w $\mathcal{F}$ prowadziłby do nieskończonego zstępującego ciągu liczb naturalnych. Tak więc, zbiór FT_k skończonych drzew k-argumentowych z relacją zawierania jest dobrze ufundowany dla każdego k.

4. $\langle FT_k, \sqsubseteq \rangle$ (zob. Fakt 7.13) jest dobrze ufundowany. Stosuje się tutaj rozumowanie analogiczne do przedstawionego w poprzednim punkcie.

5. Dla każdego zbioru etykiet Σ, zbiór $FT(\Sigma)$ termów nad Σ (zob. Przykład 7.17) uporządkowany relacją $\sqsubseteq$ ("być podtermem") jest dobrze ufundowany. Powód jest ten sam co w poprzednich dwóch punktach.

6. Oczywiście każdy skończony porządek jest dobrze ufundowany.

7. Zbiór $\langle T_1, \subseteq \rangle$ drzew 1-argumentowych jest dobrze uporządkowany. Wynika to stąd, że jedynym drzewem nieskończonym w T_1 jest $\{0\}^*$. Jest to element największy w T_1. Tak więc $\langle T_1, \subseteq \rangle$ można otrzymać ze zbioru dobrze uporządkowanego $\langle FT_1, \subseteq \rangle$ przez dodanie elementu największego. Operacja dodawania elementu największego oczywiście nie psuje własności dobrego ufundowania.

8. Zbiór $\langle T_2, \subseteq \rangle$ natomiast nie jest dobrze ufundowany. Weźmy następujący ciąg drzew 2-argumentowych

$$t_n = \{0^n w \mid w \in \{0,1\}^*\} \cup \{0^i \mid i < n\} \cup \{0^i 1 \mid i < n\}$$

Dla dowolnej liczby n, zbiór t_{n+1} jest właściwym podzbiorem t_n (zauważmy, że $0^n 11 \in t_n - t_{n+1}$). Powyższy ciąg jest nieskończonym ciągiem zstępującym. Przykład ten bez trudu można przenieść na dowolne $\langle T_k, \subseteq \rangle$ dla $k \geq 2$.

8.1 Indukcja noetherowska

W zbiorach dobrze ufundowanych obowiązuje zasada indukcji. Jest to naturalne uogólnienie zwykłej zasady indukcji dla liczb naturalnych.

Twierdzenie 8.4 (Zasada indukcji noetherowskiej)
Niech $\langle A, \leq_A \rangle$ będzie porządkiem dobrze ufundowanym i niech $P \subseteq A$ będzie zbiorem spełniającym następujący warunek,

dla każdego $x \in A$, z faktu że wszystkie elementy $y <_A x$ należą do P wynika, że $x \in P$

Wówczas $P = A$.

Dowód: Jeśli $A - P \neq \emptyset$, to niech $x_0 \in A - P$ będzie elementem minimalnym. Zatem jeśli $y <_A x_0$, to $y \in P$. Z założeń twierdzenia wynika, że $x_0 \in P$. Otrzymana sprzeczność dowodzi, że $A - P = \emptyset$, czyli $A = P$. ■

Niech $\langle A, \leq \rangle$ będzie porządkiem dobrze ufundowanym. Wprowadzimy następujące oznaczenie. Dla dowolnego $a \in A$, definiujemy

$$\mathcal{O}(a) = \{x \in A \mid x < a\}.$$

Każdy zbiór postaci $\mathcal{O}(a)$ będziemy nazywać *odcinkiem początkowym* w zbiorze $\langle A, \leq \rangle$. Powyższa notacja zbiorów $\mathcal{O}(a)$ nie uwzględnia zależności od częściowego porządku $\langle A, \leq \rangle$. Zwykle nie będzie to prowadziło do niejednoznaczności. W wątpliwych przypadkach będziemy używali indeksu dla podkreślenia zależności.

Na zbiorach dobrze ufundowanych można indukcyjnie definiować funkcje, podobnie jak w przypadku zbioru liczb naturalnych.

Twierdzenie 8.5 (O definiowaniu funkcji przez indukcję noetherowską)
Niech $\langle A, \leq \rangle$ będzie zbiorem dobrze ufundowanym. Dla dowolnych zbiorów B oraz C i dowolnej funkcji $h : PF(A \times C, B) \times A \times C \to B$ istnieje dokładnie jedna funkcja $f : A \times C \to B$ spełniająca poniższy warunek dla dowolnych $x \in A$ oraz $c \in C$:

$$f(x, c) = h(f \cap (\mathcal{O}(x) \times C \times B), x, c). \tag{37}$$

Dowód: Pokażemy najpierw, że dla każdego $x \in A$ istnieje funkcja $f_x : (\mathcal{O}(x) \cup \{x\}) \times C \to B$ taka, że dla dowolnych $y \leq x$ oraz $c \in C$,

$$f_x(y, c) = h(f_x \cap (\mathcal{O}(y) \times C \times B), x, c). \tag{38}$$

Powyższą własność udowodnimy przez indukcję noetherowską ze względu na x. Niech $y < x$ i niech $f_y : (\mathcal{O}(y) \cup \{y\}) \times C \to B$ będzie funkcją spełniającą powyższy warunek. Weźmy dowolne $y_1, y_2 < x$. Twierdzimy, że dla dowolnego $z \in A$ takiego, że $z \leq y_1$, $z \leq y_2$ oraz dla dowolnego $c \in C$ mamy

$$f_{y_1}(y, c) = f_{y_2}(y, c).$$

Wynika to natychmiast z założenia indukcyjnego i z wzoru (38).

Zatem $g = \bigcup\{f_y \mid y < x\}$ jest funkcją o dziedzinie $\mathcal{O}(x) \times C$. Tak więc możemy zdefiniować funkcję f_x następująco

$$f_x(y, c) = g \cup \{\langle x, h(g, y, c)\rangle\},$$

gdzie $y \leq x$ oraz $c \in C$. Pozostawiamy czytelnikowi sprawdzenie,że f_x spełnia (38). To kończy dowód (38).

Z udowodnionej powyżej własności natychmiast wynika, że dla dowolnych $x_1, x_2 \in A$, mamy

$$f_{x_1}(y, c) = f_{x_2}(y, c),$$

gdzie $y \leq x_1$, $y \leq x_2$ oraz $c \in C$.

Zatem $f = \bigcup\{f_x \mid x \in A\}$ jest funkcją o dziedzinie $A \times C$. Mamy

$$f(x, c) = f_x(x, c) = h(f_x \cap (\mathcal{O}(x) \times C \times B), x, c) = h(f \cap (\mathcal{O}(x) \times C \times B), x, c).$$

Powyższa równość kończy dowód twierdzenia. ∎

Zbiór C w powyższym twierdzeniu pełni rolę zbioru parametrów. Zauważmy, że definicja indukcyjna funkcji w (37) polega na określaniu funkcji na elemencie x w zależności od już zdefiniowanej części funkcji dla argumentów mniejszych od x. W szczególności jeśli x jest elementem minimalnym w A, to (37) redukuje się do wzoru:

$$f(x, c) = h(\emptyset, x, c)$$

Przykład 8.6 Zilustrujemy zastosowanie twierdzenia 8.5 na przykładzie definicji funkcji konkatenacji słów $f : X^* \times X^* \to X^*$. Załóżmy, że dla każdego $a \in X$ mamy daną funkcję $g_a : X^* \to X^*$, która każdemu słowu $w \in X^*$ przyporządkowuje słowo aw. Funkcję g_a można nazwać a-tym następnikiem.

Intuicyjnie, następująca rodzina równań definiuje f,

$$f(\varepsilon, w) = w \tag{39}$$

$$f(au, w) = g_a(f(u, w)), \quad \text{dla } a \in X \tag{40}$$

Można tę definicję sformalizować stosując twierdzenie 8.5. Niech $A = B = C = X^*$ oraz niech $h : PF(X^* \times X^*, X^*) \times X^* \times X^* \to X^*$ będzie funkcją zdefiniowaną następująco

$$h(f, u, w) = \begin{cases} g_a(f(u', w)) & \text{jeśli } u = au' \text{ oraz } (u', w) \in Dom(f) \\ w & \text{w przeciwnym przypadku} \end{cases}$$

Porządek $\leq_s$ na zbiorze A definiujemy następująco. Dla $u, w \in A$, mamy $w \leq_s u$ wtedy i tylko wtedy, gdy w jest przyrostkiem u, tzn., gdy istnieje $w' \in A$ takie, że $u = w'w$. Porządek $\langle A, \leq_s \rangle$ jest dobrze ufundowany, gdyż jest on izomorficzny z porządkiem prefiksowym na A (izomorfizm ustala fukcja, która każdemu słowu w przyporządkowuje słowo w^R, powstające z w przez odwrócenie kolejności liter w w).

Łatwo jest zauważyć, że równania (39), (40) definiujące f są równoważne równaniu (37) z twierdzenia 8.5 przy h zdefiniowanym powyżej.

Więcej przykładów definicji funkcji przez indukcję noetherowską poznamy w następnych działach poświęconych logice.

8.2 Dobre porządki

Przypomnijmy, że dobry porządek to liniowy prządek dobrze ufundowany.

Fakt 8.7 *Niech $\langle A, \leq\rangle$ będzie zbiorem dobrze uporządkowanym. Dla dowolnych $a, b \in A$, jeśli $a \neq b$, to odcinki początkowe $\mathcal{O}(a)$ i $\mathcal{O}(b)$ nie są izomorficzne.*

Dowód: Załóżmy, że $b < a$ oraz, że $f : \mathcal{O}(a) \to \mathcal{O}(b)$ jest izomorfizmem. Niech $a \in A$ będzie najmniejszym elementem, dla którego istnieje $c < a$ taki, że $\mathcal{O}(a)$ i $\mathcal{O}(c)$ są izomorficzne. Ponieważ $\mathcal{O}(b)$ jest właściwym podzbiorem zbioru $\mathcal{O}(a)$, to zbiór $\mathcal{O}(b) - \vec{f}(\mathcal{O}(b))$ jest niepusty. Niech c będzie najmniejszym elementem w tym zbiorze. Oczywiście $\vec{f}(\mathcal{O}(b)) \subseteq \mathcal{O}(c)$. Z wyboru elementu c wynika, że dla dowolnego $x < c$, ponieważ $x \in \mathcal{O}(b)$, to $x \in \vec{f}(\mathcal{O}(b))$. Zatem

$$\vec{f}(\mathcal{O}(b)) = \mathcal{O}(c),$$

czyli odcinki początkowe $\mathcal{O}(b)$ i $\mathcal{O}(c)$ są izomorficzne. Ponieważ $c < b < a$, to otrzymujemy sprzeczność z wyborem elementu a. ∎

Z powyższego faktu natychmiest otrzymujemy następujący wniosek.

Wniosek 8.8 *Żaden zbiór dobrze uporządkowany nie jest izomorficzny ze swoim odcinkiem początkowym.*

Przedstawimy teraz konstrukcję, do której będziemy się odwoływać w kilku natępnych lematach oraz w części poświęconej liczbom porządkowym. Niech $\langle A, \leq_A\rangle$ oraz $\langle B, \leq_B\rangle$ będą zbiorami dobrze uporządkowanymi. Niech $*$ będzie elementem nie należącym do zbioru B. Niech $B' = B \cup \{*\}$. Porządek na B' jest rozszerzeniem porządku $\leq_B$ przez dołączenie $*$ jako elemntu największego. Zdefiniujemy $g : A \to B'$ przez indukcję noetherowską. Dla $a \in A$, niech $g(a)$ będzie najmniejszym elementem w zbiorze $B - \{g(x) \mid x <_A a\}$, o ile ten zbiór jest niepusty. Jeśli $B - \{g(x) \mid x <_A a\} = \emptyset$, to definiujemy $g(a) = *$. Funcję g nazwiemy *przekształceniem kanonicznym* indukowanym przez $\langle A, \leq_A\rangle$ i $\langle B, \leq_B\rangle$.

Lemat 8.9 *Niech $\langle A, \leq_A\rangle$ i $\langle B, \leq_B\rangle$ będą zbiorami dobrze uporządkowanymi i niech $g : A \to B'$ będzie przekształceniem kanonicznym indukowanym przez te zbiory.*

(i) Dla każdego $a \in A$, jeśli $g(a) \neq *$, to $\vec{g}(\mathcal{O}(a)) = \mathcal{O}(g(a))$.

(ii) Jeśli $a \in A$ jest najmniejszym elementem takim, że $g(a) = *$, to $\vec{g}(\mathcal{O}(a)) = B$.

Dowód: Udowodnimy (i) przez indukcję noetherowską ze względu na a. Zauważmy, że ponieważ $g(a) \neq *$, to nie ma znaczenia czy odcinek początkowy wyznaczony przez $g(a)$ jest brany względem zbioru B czy B'. Z założenia o funkcji g wynika, że

$$g(a) \notin \{g(x) \mid x <_A a\}. \tag{41}$$

Weźmy dowolny $c \in \mathcal{O}(a)$. Gdyby $g(a) <_{B'} g(c)$, to mielibyśmy

$$g(a) \in \mathcal{O}(g(c)) = \vec{g}(\mathcal{O}(c)) \subseteq \{g(x) \mid x <_A a\},$$

co przeczy (41). Z tych samych powodów mamy $g(c) \neq g(a)$. Zatem

$$\vec{g}(\mathcal{O}(a)) \subseteq \mathcal{O}(g(a)).$$

Na odwrót, weźmy $b <_B g(a)$ dla pewnego $b \in B$. Ponieważ $g(a)$ jest najmniejszym elementem spełniającym (41), to istnieje $c <_A a$ taki, że $b = g(c)$. Zatem $b \in \vec{g}(\mathcal{O}(a))$, co kończy dowód (i).

Dla dowodu (ii) zauważmy, że ponieważ $g(a) = *$, to $B \subseteq \{g(x) \mid x <_A a\} = \vec{g}(\mathcal{O}(a))$. Z drugiej strony, z założeń w punkcie (ii) wynika, że dla każdego $c <_A a$, mamy $g(c) \in B$. Zatem $\vec{g}(\mathcal{O}(a)) \subseteq B$. To kończy dowód lematu. ∎

Z powyższego lematu otrzymujemy natychmiast następujący wniosek, którego dowód pozostawiamy czytelnikowi.

Wniosek 8.10 *Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą zbiorami dobrze uporządkowanymi i niech $g : A \to B'$ będzie przekształceniem kanonicznym indukowanym przez te zbiory.*

(i) g jest monotoniczna.

(ii) Jeśli $* \notin \vec{g}(A)$, to g jest różnowartościowa.

(iii) Jeśli $* \in \vec{g}(A)$ oraz $a \in A$ jest najmniejszym elementem takim, że $g(a) = *$, to $\langle B, \leq_B \rangle$ jest izomorficzny z odcinkiem początkowym $\mathcal{O}(a)$.

Następny fakt pokazuje, że przekształcenie kanoniczne jest najmniejszym spośród wszystkich funkcji monotonicznych pomiędzy dwoma ustalonymi dobrymi porządkami.

Lemat 8.11 *Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą zbiorami dobrze uporządkowanymi i niech $g : A \to B'$ będzie przekształceniem kanonicznym indukowanym przez te zbiory. Dla dowolnej funkcji monotonicznej i różnowartościowej $f : A \to B$ i dla dowolnego $a \in A$ mamy*

$$g(a) \leq_B f(a).$$

W szczególności wynika stąd, że jeśli istnieje monotoniczna i różnowartościowa funkcja z $\langle A, \leq_A \rangle$ w $\langle B, \leq_B \rangle$ to $* \notin \vec{g}(A)$ oraz $g : A \to B$ jest rożnowartościowa.

Dowód: Najpierw udwodnimy powyższą nierówność przez indukcję noetherowską ze względu na a, przy dodatkowym założeniu, że $g(a) \neq *$. Weźmy dowolny a taki, że $g(a) \neq *$ i przypuśćmy, że $f(a) <_B g(a)$. Ponieważ $g(a) \notin \{g(x) \mid x <_A a\}$, to z definicji funkcji g wynika, że istnieje $x <_A a$ taki,że $f(a) = g(x)$. Z założenia indukcyjnego mamy $g(x) \leq_B f(x)$. Zatem $f(a) \leq_B f(x)$, co przeczy założeniu o monotoniczności i różnowartościowości f. Otrzymana sprzeczność dowodzi nierówności $f(a) \leq_B g(a)$.

Przypuśćmy teraz, że $g(a) = *$ i niech $a \in A$ będzie najmniejszym elementem o tej własności. Z Faktu 8.9 (ii) wynika, że $B = \{g(x) \mid x <_A a\}$. Zatem istnieje $x <_A a$ taki,że $f(a) = g(x)$. Z powyższej części dowodu wiemy, że $g(x) \leq_B f(x)$. Zatem $f(a) \leq_B f(x)$ i podobnie jak wyżej, otrzymujemy sprzeczość. Zatem musi być $g(a) \neq *$.

Druga część Lematu 8.11 wynika z pierwszej oraz z Wniosku 8.10 (ii). ■

Lemat 8.12 *Niech $\langle A, \leq_A\rangle$ i $\langle B, \leq_B\rangle$ będą zbiorami dobrze uporządkowanymi i niech $g : A \to B'$ oraz $h : B \to A'$ będą przekształceniami kanonicznymi indukowanymi przez te zbiory. Wtedy dla każdego $a \in A$ takiego, że $g(a) \neq *$, zachodzi $hg(a) = a$.*

Dowód: Dowodzimy lemat przez indukcję noetherowską ze względu na $a \in A$, spełniające warunek $g(a) \neq *$. Weźmy dowolne takie a i rozważmy zbiór $X = \{h(y) \mid y <_B g(a)\}$. Pokażemy, że

$$X = \mathcal{O}(a). \tag{42}$$

Niech $x = h(y)$ dla pewnego $y <_B g(a)$. Z definicji funkcji g wynika, że istnieje $z <_A a$ taki, że $y = g(z)$. Zatem, stosując założenie indukcyjne otrzymujemy

$$h(y) = hg(z) = z.$$

Wynika stąd, że $x <_A a$.

Na odwrót, weźmy $x <_A a$, wtedy na mocy Lematu 8.9 mamy $g(x) <_B g(a)$ oraz z założenia indukcyjnego $x = hg(x)$. Zatem $x \in X$. To kończy dowód (42).

Tak więc $A - X \neq \emptyset$ i $hg(a)$ jest najmniejszym elementem w tym zbiorze. Jest to oczywiście element a, na mocy (42). ■

8.3 Liczby porządkowe

Przypomnijmy, że liczby kardynalne są obiektami przyporządkowanymi zbiorom w ten sposób, że dwa zbiory mają przyporządkowany ten sam obiekt wtedy i tylko wtedy, gdy zbiory te są równoliczne. Zatem liczby kardynalne reprezentują w pewnym sensie klasy zbiorów

równolicznych. Analogiczną rolę w stosunku do dobrych porządków spełniają liczby porządkowe — reprezentują one klasy dobrych porządków izomorficznych. Tak więc, *liczbami porządkowymi* są obiekty przyporządkowane każdemu dobremu porządkowi w ten sposób, że dwóm porządkom jest przyporządkowany ten sam obiekt wtedy i tylko wtedy, gdy te porządki są izomorficzne. Jeśli α jest liczbą porządkową odpowiadającą dobremu porządkowi $\langle A, \leq\rangle$, to mówimy też, że $\langle A, \leq\rangle$ jest *uporządkowany w typ* α. Będziemy to oznaczać $\overline{\langle A, \leq_A\rangle} = \alpha$.

Liczbą porządkową odpowiadającą dobremu porządkowi $\langle n, \leq\rangle$ jest liczba n. Natomiast porządkowi $\langle N, \leq\rangle$ odpowiada liczba porządkowa oznaczana ω (omega).

Liczby porządkowe można dodawać. Jeśli α jest liczbą porządkową związaną z dobrym porządkiem $\langle A, \leq_A\rangle$ a liczba β jest związana z $\langle B, \leq_B\rangle$, to liczba $\alpha+\beta$ jest z definicji związana z porządkiem, który jest takim rozszerzeniem porządków $\leq_A$ oraz $\leq_B$, że wszystkie elementy A są mniejsze od wszystkich elementów B (zakładamy, bez zmniejszenia ogólności, że A i B są rozłączne). Pozostawimy czytelnikowi dowód, że tak określony porządek jest dobrym porządkiem. Zauważmy, że $1+\omega = \omega$ oraz, że $\omega+1 \neq \omega$, bowiem $\omega+1$ reprezentuje porządek z elementem największym, a ω reprezentuje porządek bez elementu największego, a ponadto izomorfizm przeprowadza element największy na element największy. Zatem dodawanie liczb porządkowych nie jest operacją przemienną. Dla skończonych liczb porządkowych pokrywa się ono ze zwykłym dodawaniem liczb naturalnych.

Przykładowo, liczba $\omega+1$ jest przyporządkowana dobremu porządkowi drzew 1-argumentowych $\langle T_1, \subseteq\rangle$.

Liczby porządkowe można porównywać. Jeśli $\overline{\langle A, \leq_A\rangle} = \alpha$ oraz $\overline{\langle B, \leq_B\rangle} = \beta$, to mówimy, że α jest mniejsza lub równa β (piszemy $\alpha \leq \beta$), wtw, gdy istnieje monotoniczna i różnowartościowa funkcja $f : A \to B$. Definiujemy $\alpha < \beta$, gdy $\alpha \leq \beta$ oraz $\langle A, \leq_A\rangle$ i $\langle B, \leq_B\rangle$ nie są izomorficzne.

Poniżej zajmiemy się pewnymi podstawowymi własnościami tak zdefiniowanego związku.[12]

Fakt 8.13 *Dla dowolnych zbiorów dobrze uporządkowanych* $\langle A, \leq_A\rangle$ *oraz* $\langle B, \leq_B\rangle$, *mamy* $\overline{\langle A, \leq_A\rangle} < \overline{\langle B, \leq_B\rangle}$ *wtedy i tylko wtedy, gdy* $\langle A, \leq_A\rangle$ *jest izomorficzny z pewnym odcinkiem początkowym w* $\langle B, \leq_B\rangle$.

Dowód: ($\Rightarrow$) Niech $g : A \to B'$ będzie przekształceniem kanonicznym indukowanym przez $\langle A, \leq_A\rangle$ i $\langle B, \leq_B\rangle$. Z Wniosku 8.10 wynika, że g jest różnowartościowa oraz $g : A \to B$. Z założenia wynika, że g nie może być na B. Niech $b \in B - \vec{g}(A)$ będzie najmniejszym elementem. Pokażemy, że

$$\vec{g}(A) = \mathcal{O}(b) \tag{43}$$

Niech $a \in A$ będzie dowolnym elementem. Gdyby $b <_B g(a)$ to z Lematu 8.9 istniałoby $x <_A a$ takie, że $b = g(x)$, wbrew wyborowi b. Zatem $g(a) <_B b$, czyli $g(a) \in \mathcal{O}(b)$. Na odwrót, jeśli $c <_B b$, to z wyboru b wynika,że $c \in \vec{g}(A)$. To dowodzi (43).

[12] Ściśle mówiąc porównywanie liczb porządkowych nie jest relacją bo nie istnieje zbiór wszystkich liczb porządkowych.

Z (43) wynika, że $\langle A, \leq_A \rangle$ jest izomorficzny z $\mathcal{O}(b)$.

Implikacja ($\Leftarrow$) jest oczywista — gdyby $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ były izomorficzne, to $\langle B, \leq_B \rangle$ byłby izomorficzny ze swoim odcinkiem początkowym, co jest niemożliwe na mocy Wniosku 8.8. ∎

Twierdzenie 8.14 (Cantor)
Dla dowolnych zbiorów dobrze uporządkowanych $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$, jeśli $\overline{\langle A, \leq_A \rangle} \leq \overline{\langle B, \leq_B \rangle}$ oraz $\overline{\langle B, \leq_B \rangle} \leq \overline{\langle A, \leq_A \rangle}$, to $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ są izomorficzne.

Dowód: Weźmy kanoniczne przekształcenia $g : A \to B'$ oraz $h : B \to A'$, indukowane przez $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$. Z Lematu 8.11 wynika, że $* \notin \vec{g}(A)$ oraz $* \notin \vec{h}(B)$. Zatem, na mocy Lematu 8.12, funkcje $g : A \to B$ i $h : B \to A$ są izomorfizmami. ∎

Twierdzenie 8.15 (O trichotomii)
Dla dowolnych liczb porządkowych α, β zachodzi dokładnie jedna z następujących możliwości:

(i) $\alpha < \beta$;

(ii) $\beta < \alpha$;

(iii) $\alpha = \beta$.

Dowód: Oczywiście żadne dwa z powyższych warunków nie mogą zajść jednocześnie. Dla dowodu, że zawsze musi zajść któryś z tych warunków weźmy dowolne zbiory dobrze uprządkowane $\langle A, \leq_A \rangle$ oraz $\langle B, \leq_B \rangle$ takie, że $\overline{\langle A, \leq_A \rangle} = \alpha$ oraz $\overline{\langle B, \leq_B \rangle} = \beta$. Rozważmy przekształcenia kanoniczne $g : A \to B'$ oraz $h : B \to A'$, indukowane przez te zbiory.

Na mocy Wniosku 8.10, jeśli $* \notin \vec{g}(A)$ to $\alpha \leq \beta$, a zatem zachodzi (i) lub (iii). Podobnie, jeśli $* \notin \vec{h}(B)$, to $\beta \leq \alpha$ i zachodzi (ii) lub (iii). Jeśli $* \in \vec{g}(A)$, to na mocy Wniosku 8.10 zachodzi (ii). Wreszcie, jeśli $* \in \vec{h}(B)$, to zachodzi (i). ∎

Twierdzenie 8.16 *Każdy zbiór liczb porządkowych jest dobrze uporządkowany przez $\leq$.*

Dowód: Weźmy dowolny zbiór Z liczb porządkowych. Z Twierdzeń 8.14 oraz 8.15 wynika, że Z jest liniowo uporządkowany.

Przypuśćmy, że mamy nieskończony zstępujący łańcuch w Z

$$\alpha_1 > \alpha_1 > \ldots$$

Niech $\overline{\langle A_i, \leq_{A_i}\rangle} = \alpha_i$ dla $i \geq 0$. Pokażemy, że dla każdego $i > 0$, istnieje $a_i \in A_0$ taki, że odcinek początkowy $\mathcal{O}(a_i)$ jest izomorficzny z A_i oraz $a_{i+1} <_{A_0} a_i$.

Powyższą własność dowodzimy przez indukcję ze względu na i. Ponieważ $\alpha_1 < \alpha_0$, to na mocy Faktu 8.13, istnieje $a_1 \in A_0$ taki, że $\langle A_1, \leq_{A_1}\rangle$ jest izomorficzny z $\mathcal{O}(a_1)$.

Weźmy dowolne $i > 1$. Stosując podobne rozumowanie znajdujemy $c \in A_{i-1}$ taki, że $\langle A_i, \leq_{A_i}\rangle$ jest izomorficzny z $\mathcal{O}(c)$. Z założenia indukcyjnego $\langle A_{i-1}, \leq_{A_{i-1}}\rangle$ jest izomorficzny z $\mathcal{O}(a_{i-1}) \subseteq A_0$. Niech $a_i \in \mathcal{O}(a_{i-1})$ będzie elementem, na który przechodzi c przy tym izomorfizmie. Ponieważ przy izomorfizmie odcinek początkowy jest przekształcany na odcinek początkowy, to odcinki $\mathcal{O}(c)$ i $\mathcal{O}(a_i)$ są izomorficzne. Zatem $\langle A_i, \leq_{A_i}\rangle$ jest izomorficzny z $\mathcal{O}(a_i)$.

Tak więc zdefiniowaliśmy nieskończony zstępujący ciąg w $\langle A_0, \leq_{A_0}\rangle$. Otrzymana sprzeczność dowodzi, że Z jest dobrze uporządkowany. ■

8.4 Twierdzenie Zermelo i dowód lematu Kuratowskiego-Zorna

Na zakończenie informacji o dobrym ufundowaniu przytoczymy twierdzenie mające charakter równie niekonstruktywny jak lemat Kuratowskiego-Zorna.

Twierdzenie 8.17 (Zermelo)
Każdy zbiór można dobrze uporządkować, tzn. dla każdego zbioru A istnieje relacja dobrego porządku na A.

Dowód: Niech $\mathcal{R}$ będzie zbiorem wszystkich par $\langle X, r\rangle$ takich, że $X \subseteq A$ oraz r jest dobrym porządkiem w X. Niech Z będzie zbiorem wszystkich liczb porządkowych α takich, że istnieje $\langle X, r\rangle \in \mathcal{R}$, uporządkowany w typ α. Na mocy Twierdzenia 8.16 zbiór Z jest dobrze uporządkowany relacją $\leq$.

Zdefiniujemy funkcję $f : Z \to A$ przez indukcję noetherowską. Niech $a_0 \in A$ będzie dowolnym ustalonym elementem.[13] Dla $\alpha \in Z$, jako $f(\alpha)$ wybieramy dowolny element ze zbioru $A - \{f(\beta) \mid \beta < \alpha\}$, o ile zbiór ten jest niepusty. Jeśli $\{f(\beta) \mid \beta < \alpha\} = A$, to kładziemy $f(\alpha) = a_0$.

Pokażemy, że

$$\vec{f}(Z) = A. \tag{44}$$

Przypuśćmy, że $X = \vec{f}(Z) \neq A$. Wówczas, jak łatwo wynika z definicji f, funkcja f jest różnowartościowa, a zatem w zbiorze X można określić dobry porządek r, indukowany przez porządek w Z. Porządek ten jest oczywiście izomorficzny z $\langle Z, \leq\rangle$. Niech $\gamma = \overline{\langle Z, \leq\rangle}$. Ponieważ $\langle X, r\rangle \in \mathcal{R}$, to $\gamma \in Z$ i, co za tym idzie, $\mathcal{O}(\gamma) \subseteq Z$. Zatem Z byłby izomorficzny ze swoim odcinkiem początkowym. Otrzymana sprzeczność dowodzi (44).

[13] Bez zmniejszenia ogólności możemy przyjąć, że $A \neq \emptyset$.

Jeśli istnieje $\alpha \in Z$ taka, że $\{f(\beta) \mid \beta < \alpha\} = A$, to niech α będzie najmniejsza o tej własności. Wówczas f, ograniczona do $\mathcal{O}(\alpha)$, jest różnowartościowa i ponieważ $\vec{f}(\mathcal{O}(\alpha)) = A$, to indukuje ona dobry porządek na A. Jeśli dla każdego $\alpha \in Z$ mamy $\{f(\beta) \mid \beta < \alpha\} \neq A$, to f jest różnowartościowa i z (44) wynika, że również w tym przypadku, f indukuje dobry porządek na A. ■

Jako bezpośredni wniosek z Twierdzenia 8.15 oraz Twierdzenia 8.17 otrzymujemy następujący wniosek.

Wniosek 8.18 *Dla dowolnych zbiorów A, B zachodzi $|A| \leq |B|$ lub $|B| \leq |A|$.*

Dowód: Zbiory A i B można dobrze uporządkować. Niech α i β będą typami porządkowymi tych zbiorów. Na mocy Twierdzenia 8.15 mamy, że $\alpha \leq \beta$ lub $\beta \leq \alpha$. W pierwszym przypadku zachodzi $|A| \leq |B|$, a w drugim $|B| \leq |A|$. ■

Skorzystamy teraz z twierdzenia Zermelo do udowodnienia Lematu Kuratowskiego-Zorna (por. Twierdzenie 7.30).

Dowód lematu Kuratowskiego-Zorna:

Niech $\langle A, \leq_A \rangle$ będzie częściowym porządkiem, w którym każdy łańcuch ma ograniczenie górne. Pokażemy, że A zawiera element maksymalny.

Niech Z będzie dowolnym zbiorem o mocy większej niż A i niech $\preceq$ będzie dobrym porządkiem w Z — taki porządek istnieje na mocy twierdzenia Zermelo. Zdefiniujemy funkcję monotoniczną $f : Z \to A$ przez indukcję noetherowską.

Niech $z \in Z$ i rozważmy zbiór $X = \{f(u) \mid u \prec z\}$. Z założenia indukcyjnego wynika, że X jest łańcuchem, a zatem ma ograniczenie górne. Jeśli X ma jakieś ograniczenie górne a należące do zbioru $A - X$, to definiujemy $f(z) = a$, gdzie a jest dowolnie wybranym elementem o tej własności. W przeciwnym przypadku X zawiera swoje własne ograniczenie górne a, które musi być zarazem elementem największym w X. Wówczas kładziemy $f(z) = a$.

Ponieważ $|Z| > |A|$, to funkcja f nie może być różnowartościowa. Zatem istnieje $z_0 \in Z$ taki, że dla wszystkich z, jeśli $z_0 \prec z$, to $f(z_0) = f(z)$. Z definicji funkcji f wynika, że $f(z_0)$ jest elementem maksymalnym w $\langle A, \leq_A \rangle$. To kończy dowód lematu Kuratowskiego-Zorna. ■

Zarówno lemat Kuratowskiego-Zorna jak i twierdzenie Zermelo wymagają dla dowodu nowego aksjomatu. Aksjomat ten, zwany *pewnikiem wyboru* orzeka, że dla każdej niepustej rodziny zbiorów niepustych istnieje funkcja wyboru, tzn. funkcja, która każdemu zbiorowi

tej rodziny przyporządkowuje pewien element tego zbioru. Można pokazać, że pewnik wyboru, twierdzenie Zermelo oraz lemat Kuratowskiego-Zorna są sobie równoważne na gruncie pozostałych aksjomatów teorii mnogości.

Zauważmy, że obydwa twierdzenia mają niekonstruktywny dowód, tzn. dowodzi się w nich istnienie obiektu (dobrego prządku w przypadku twierdzenia Zermelo oraz elementu maksymalnego w przypadku lematu Kuratowskiego-Zorna), którego konstrukcji dowód nie podaje.

Zadania

8.1. Dowieść, że jeśli $f : A \to B$ jest monotoniczną bijekcją pomiędzy dobrymi porządkami $\langle A, \leq_A \rangle$ oraz $\langle B, \leq_B \rangle$, to funkcja odwrotna f^{-1} jest też monotoniczna. Czy założenie, że mamy do czynienia z dobrymi porządkami jest istotne?

8.2. Niech $\langle A, \leq_A \rangle$ będzie zupełnym porządkiem i niech $f : A \to A$ będzie funkcją monotoniczną. Dowieść, że f ma najmniejszy punkt stały. (*Wskazówka:* wziąć dostatecznie dużą liczbe porządkową α i zdefiniować łańcuch iteracji $\{f^\beta(\bot) \mid \beta < \alpha\}$, funkcji f na elemencie najmniejszym $\bot$.)

8.3. Dowieść, że jeśli $\langle A, \leq_A \rangle$ oraz $\langle B, \leq_B \rangle$ są dobrze ufundowane oraz $A \cap B = \emptyset$, to porządek $\langle A \cup B, \leq \rangle$ zdefiniowany poniżej jest też dobrze ufundowany:

$$x \leq y \text{ wtw, gdy } \begin{cases} x \leq_A y, & \text{lub} \\ x \leq_B y, & \text{lub} \\ x \in A \text{ oraz } y \in B \end{cases}$$

8.4. Dowieść, że jeśli $\langle A, \leq_A \rangle$ oraz $\langle B, \leq_B \rangle$ są dobrze ufundowane, to porządek $\langle A \times B, \leq \rangle$ zdefiniowany poniżej jest też dobrze ufundowany:

$$\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle \text{ wtw, gdy } \begin{cases} b_1 <_B b_2, & \text{lub} \\ b_1 = b_2 \text{ oraz } a_1 \leq_A a_2 \end{cases}$$

8.5. Podzbiór X zbioru częściowo uporządkowanego $\langle A, \leq_A \rangle$ nazwiemy *antyłańcuchem*, gdy żadne dwa elementy zbioru X nie są porównywalne w sensie relacji $\leq_A$.

Dowieść, że jeśli $\langle A, \leq_A \rangle$ oraz $\langle B, \leq_B \rangle$ nie zawierają nieskończonych antyłańcuchów to $\langle A \times B, \leq \rangle$ też nie zawiera nieskończonych antyłańcuchów, gdzie porządek w produkcie $A \times B$ jest zdefiniowany w poprzednim zadaniu.

8.6. Niech $\langle A, \leq_A \rangle$ będzie częściowym porządkiem dobrze ufundowanym. Niech $P_{fin}(A)$ oznacza zbiór wszystkich skończonych podzbiorów zbioru A. Definiujemy następującą relację $\prec$ w zbiorze $P_{fin}(A)$. Dla skończonych zbiorów $X, Y \subseteq A$, zachodzi $X \prec Y$ wtw, gdy istnieje $a \in Y$ oraz zbiór $Z \subseteq A$ taki, że

- dla każdego $z \in Z$, zachodzi $z <_A a$ oraz
- $X = (Y - \{a\}) \cup Z$.

Dowieść, że następująca relacja $\sqsubseteq$ w $P_{fin}(A)$ jest dobrze ufundowanym częściowym porządkiem: $X \sqsubseteq Y$ zachodzi wtw, gdy $X = Y$ lub istnieje $n > 0$ oraz ciąg $X_0, \ldots X_{n-1}$ skończonych podzbiorów zbioru A taki, że $X = X_0$, $Y = X_{n-1}$ oraz dla każdego $i < n$, zachodzi $X_i \prec X_{i+1}$.

Czy teza zadania zachodzi jeśli w definicji relacji $\prec$ zastąpimy $<_A$ przez $\leq_A$? Relację $\prec$ oraz $\sqsubseteq$ można analogicznie zdefiniować w całym zbiorze $P(A)$. Czy relacja $\sqsubseteq$ jest wówczas częściowym porządkiem dobrze ufundowanym?

8.7. Dowieść, że jeśli $\langle A, \leq_A \rangle$ nie zawiera nieskończonych antyłańcuchów, to $\langle P_{fin}(A), \sqsubseteq \rangle$ też nie zawiera nieskończonych antyłańcuchów, gdzie $\sqsubseteq$ jest relacją zdefiniowaną w poprzednim zadaniu.

Część II

Wstęp do logiki

9 Elementy algebry uniwersalnej

Sygnaturą Σ nazwiemy rodzinę $\{\Sigma_n \mid n \in N\}$ zbiorów parami rozłącznych. Elementy zbioru Σ_n nazywamy symbolami operacji n-argumentowych.

Algebrą $\mathfrak{A}$ nad sygnaturą Σ (lub po prostu Σ-algebrą) nazywamy niepusty zbiór A wraz z interpretacją która każdemu symbolowi f operacji n-argumentowej przyporządkowuje funkcję n-argumentową $f^{\mathfrak{A}} : A^n \to A$. Zbiór A nazywamy *nośnikiem* algebry $\mathfrak{A}$.

Przykład 9.1 (Przykłady algebr)

(i) Niech $\Sigma_0 = \{\varepsilon\}$, $\Sigma_2 = \{\cdot\}$, oraz $\Sigma_n = \emptyset$ dla $n = 1$ lub $n > 2$. Przykładem Σ-algebry jest $\langle \{0,1\}^*, \cdot, \varepsilon\rangle$, tzn interpretacją symbolu $\cdot$ jest binarna operacja konkatenacji słów oraz interpretacją symbolu stałej ε jest słowo puste. Zauważmy, że używamy tu tej samej nazwy na oznaczenie dwóch różnych rzeczy: formalnego symbolu operacji oraz interpretacji tego symbolu czyli funkcji. Zwykle dla uproszczenia notacji będziemy korzystać z tego rodzaju wielokrotnego użycia tej samej nazwy dla oznaczania różnych obiektów – znaczenie tej nazwy będzie zawsze wynikało z kontekstu, w którym się jej używa. Inne przykłady Σ-algebr: $\langle N, \times, 0\rangle$, $\langle R, \times, 1\rangle$ z naturalną interpretacją symboli operacji.

(ii) Niech $\Sigma_0 = \{0,1\}$, $\Sigma_1 = \{-\}$, $\Sigma_2 = \{\cdot, +\}$ oraz $\Sigma_n = \emptyset$ dla $n > 2$. Przykłady Σ-algebr:

$$\langle P(N), \cap, \cup, -, \emptyset, N\rangle,$$

$$\langle N, \times, +, 0, 1\rangle.$$

W pierwszym przykładzie Σ-algebry interpretacją symbolu $\cdot$ jest operacja przecięcia zbiorów $\cap$, interpretacją $-$ jest dopełnienie, interpretacją symbolu stałej 1 jest zbiór $N \in P(N)$, itd. W powyższym zapisie nieformalnie odwołujemy się do porządku, w którym są wymienione elementy sygnatury oraz odpowiadające im interpretacje w algebrze. Zwykle z kontekstu będzie jasno wynikało o jaki porządek chodzi. Przykładowo, powyższa algebra jest oczywiście inną algebrą od

$$\langle P(N), \cup, \cap, -, \emptyset, N\rangle,$$

gdzie interpretacją $\cdot$ jest suma teoriomnogościowa $\cup$ a interpretacją $+$ jest operacja przecięcia.

9.1 Algebra termów

Niech Σ będzie sygnaturą taką, że $\Sigma_0 \neq \emptyset$. Przypomnijmy, że dla $k \in N$, symbolem $FT_{k\leq}(\Sigma)$ oznaczamy zbiór wszystkich skończonych drzew etykietowanych nad Σ, w których wszystkie

wierzchołki są rzędu co najwyżej k. Niech

$$FT(\Sigma) = \bigcup_{k \in N} FT_{k\leq}(\Sigma).$$

Elementy zbioru $FT(\Sigma)$ nazywamy Σ-*termami bez zmiennych*. Na zbiorze $FT(\Sigma)$ określimy strukturę Σ-algebry. Niech $n \geq 0$ i niech $f \in \Sigma_n$. Wówczas dla $\sigma_1, \ldots, \sigma_n \in FT(\Sigma)$, definiujemy $f^{FT(\Sigma)}(\sigma_1, \ldots, \sigma_n)$ jako następujące drzewo etykietowane:

$$||f^{FT(\Sigma)}(\sigma_1, \ldots, \sigma_n)|| = \{\varepsilon\} \cup \bigcup_{i=1}^{n} \{iw \mid w \in ||\sigma_i||\}$$

oraz

$$(f^{FT(\Sigma)}(\sigma_1, \ldots, \sigma_n))(u) = \begin{cases} f & \text{jeśli } u = \varepsilon, \\ \sigma_i(w) & \text{jeśli } u = iw. \end{cases}$$

Termy możemy też wprowadzić używając liniowej notacji. $FT(\Sigma)$ jest najmniejszym zbiorem słów nad alfabetem $\bigcup_{n \in N} \Sigma_n \cup \{(,), ,\}$ spełniającym następujące warunki

- Jeśli $f \in \Sigma_0$, to słowo jednoliterowe f należy do $FT(\Sigma)$.
- Jeśli $f \in \Sigma_n$, $n > 0$, oraz $\sigma_1, \ldots, \sigma_n \in FT(\Sigma)$, to słowo $f(\sigma_1, \ldots, \sigma_n)$ należy do $FT(\Sigma)$.

Niech Z będzie dowolnym zbiorem rozłącznym z każdym Σ_n. Niech $\Sigma(Z)$ będzie sygnaturą zdefiniowaną następująco

$$\Sigma(Z)_n = \begin{cases} \Sigma_0 \cup Z & \text{jeśli } n = 0, \\ \Sigma_n & \text{jeśli } n \neq 0. \end{cases}$$

Niech $FT(\Sigma, Z)$ oznacza zbiór $\Sigma(Z)$-termów ze strukturą Σ-algebry, tzn. symbole z Z nie są interpretowane w tej algebrze. Te symbole nazywamy *zmiennymi*, a elementy algebry $FT(\Sigma, Z)$ nazywamy Σ-*termami o zmiennych* z Z. Zgodnie z powyższymi założeniami konstrukcja $FT(\Sigma, Z)$ ma sens pod warunkiem, że $\Sigma_0 \cup Z \neq \emptyset$.

Niech X oznacza dowolny nieskończony przeliczalny zbiór zmiennych. Zbiór ten będzie ustalony w dalszej części wykładu. Jedynym założeniem jakie musimy przyjąć jest aby X było rozłączne z symbolami sygnatury.

Dla dowolnego termu $\sigma \in FT(\Sigma, X)$ zdefiniujemy zbiór $FV(\sigma)$, zmiennych występujących w σ. Użyjemy w tym celu indukcji noetherowskiej.

- Jeśli $f \in \Sigma_0$, to $FV(f) = \emptyset$.
- Jeśli $x \in X$, to $FV(x) = \{x\}$.
- Jeśli $f \in \Sigma_n$, dla pewnego $n > 0$, oraz $\sigma_1, \ldots, \sigma_n \in FT(\Sigma, X)$, to $FV(f(\sigma_1, \ldots, \sigma_n)) = FV(\sigma_1) \cup \ldots \cup FV(\sigma_n)$.

9.2 Homomorfizmy

Niech $\mathfrak{A}$ oraz $\mathfrak{B}$ będą Σ-algebrami nad tą samą sygnaturą Σ. Funkcję $h : A \to B$ nazwiemy *homomorfizmem* algebry $\mathfrak{A}$ w $\mathfrak{B}$ gdy zachowuje ona wszystkie operacje algebry $\mathfrak{A}$, tzn. gdy dla każdego $n \in N$ oraz $f \in \Sigma_n$ i dla dowolnych $a_1, \ldots, a_n \in A$,

$$h(f^{\mathfrak{A}}(a_1, \ldots, a_n)) = f^{\mathfrak{B}}(h(a_1), \ldots, h(a_n)).$$

Zauważmy, że dla $n = 0$ powyższa równość oznacza zachowywanie stałych, tzn. przeprowadzanie przez h interpretacji stałej f w $\mathfrak{A}$ w interpretację tej samej stałej w $\mathfrak{B}$. Różnowartościowy homomorfizm nazwiemy *monomorfizmem*. Jeśli h jest na B to h nazwiemy *epimorfizmem*, a jeśli h jest bijekcją, to nazwiemy go *izomorfizmem*.

Podamy kilka przykładów homomorfizmów. Funkcja przyporządkowująca każdemu słowu $w \in \{0,1\}^*$ jego długość $|w|$ jest epimorfizmem z algebry $\langle \{0,1\}^*, \cdot, \varepsilon \rangle$ na algebrę $\langle N, +, 0 \rangle$. Funkcja logarytmu jest izomorfizmem z algebry $\langle \{r \in R \mid r > 0\}, \cdot, 1 \rangle$ na algebrę $\langle R, +, 0 \rangle$. Natomiast funkcja, która przyporządkowuje każdej liczbie rzeczywistej r jej część całkowitą $\lfloor r \rfloor \in Z$ nie jest homomorfizmem z $\langle R, + \rangle$ w algebrę $\langle Z, + \rangle$ gdyż nie zachowuje operacji dodawania. Bowiem $\lfloor 0.5 + 0.5 \rfloor = 1$, ale $\lfloor 0.5 \rfloor + \lfloor 0.5 \rfloor = 0 + 0 = 0$. W przykładach tego paragrafu używamy standardowych oznaczeń na operacje wymienionych wyżej algebr, tzn $+$ oznacza operację dodawania (w N, R, Z), $\cdot$ oznacza konkatenację w $\{0,1\}^*$ oraz mnożenie w zbiorze liczb rzeczywistych.

Ważnym przykładem homomorfizmu, do którego będziemy się często odwoływać w dalszej części tych notatek jest *wartościowanie termu* w algebrze. Niech Σ będzie dowolną sygnaturą i niech $\mathfrak{A}$ będzie dowolną Σ-algebrą. *Wartościowaniem* w $\mathfrak{A}$ nazwiemy dowolną funkcję $v : X \to A$. Mając wartościowanie v zdefiniujemy dla każdego termu $\sigma \in FT(\Sigma, X)$ wartość $\sigma^{\mathfrak{A}}[v] \in A$ tego termu w algebrze $\mathfrak{A}$ przy wartościowaniu v. Definicja jest przeprowadzona przez indukcję ze względu na budowę termu σ.

$$\sigma^{\mathfrak{A}}[v] = \begin{cases} v(x) & \text{jeśli } \sigma = x \in X, \\ f^{\mathfrak{A}}(\sigma_1^{\mathfrak{A}}[v], \ldots, \sigma_n^{\mathfrak{A}}[v]) & \text{jeśli } \sigma = f(\sigma_1, \ldots, \sigma_n), \text{ gdzie } f \in \Sigma_n \text{ oraz} \\ & \sigma_1, \ldots, \sigma_n \in FT(\Sigma, X). \end{cases}$$

Z powyższej definicji natychmiast wynika następujący fakt.

Fakt 9.2 *Dla każdej Σ-algebry $\mathfrak{A}$ oraz dowolnego wartościowania $v : X \to A$, funkcja $(-)^{\mathfrak{A}}[v] : FT(\Sigma, X) \to A$ jest homomorfizmem Σ-algebr.*

Dowód: Weźmy dowolną Σ-algebrę $\mathfrak{A}$ i dowolne wartościowanie v. Niech $h : FT(\Sigma, X) \to A$ oznacza funkcję, która każdemu $\sigma \in FT(\Sigma, X)$ przyporządkowuje $\sigma^{\mathfrak{A}}[v] \in A$. Niech $n \in N$, niech $f \in \Sigma_n$ oraz niech $\sigma_1, \ldots, \sigma_n \in FT(\Sigma, X)$. Wówczas

$$\begin{aligned} h((f^{FT(\Sigma,X)}(\sigma_1,\ldots,\sigma_n)) &= h(f(\sigma_1,\ldots,\sigma_n)) \\ &= (f(\sigma_1,\ldots,\sigma_n))^{\mathfrak{A}}[v] \\ &= f^{\mathfrak{A}}(\sigma_1^{\mathfrak{A}}[v],\ldots,\sigma_n^{\mathfrak{A}}[v]) \\ &= f^{\mathfrak{A}}(h(\sigma_1),\ldots,h(\sigma_n)). \end{aligned}$$

■

Poniższy fakt pokazuje związek pomiędzy wartością danego termu a wartością termu o zmienionych zmiennych.

Fakt 9.3 *Niech $\sigma \in FT(\Sigma,X)$ i niech Y będzie zbiorem równolicznym z $FV(\sigma)$. Niech $\xi : Y \to FV(\sigma)$ będzie bijekcją i niech $\hat{\xi} : X \to X$ będzie dowolną funkcją rozszerzającą ξ.*
Istnieje wówczas term $\sigma' \in FT(\Sigma,X)$ taki, że

(i) $FV(\sigma') = Y$;

(ii) Dla każdej algebry $\mathfrak{A}$ i dla każdego wartościowania $v : X \to A$, zachodzi

$$\sigma^{\mathfrak{A}}[v] = \sigma'^{\mathfrak{A}}[v\hat{\xi}.]$$

Dowód: Dowód przeprowadzimy przez indukcję ze względu na σ. Jeśli σ jest zmienną x, to dla pewnej zmiennej y mamy $Y = \{y\}$ oraz $\xi(y) = x$. Niech term σ' będzie zmienną y. Łatwo sprawdzić zachodzenie warunków (i) oraz (ii).

Załóżmy teraz, że $\sigma = f(\sigma_1,\ldots,\sigma_n)$ dla pewnego $f \in \Sigma_n$ oraz $\sigma_1,\ldots,\sigma_n \in FT(\Sigma,X)$. Niech $\xi : Y \to FV(\sigma)$ będzie bijekcją i niech $\hat{\xi} : X \to X$ będzie dowolnym jej rozszerzeniem. Dla $i = 1,\ldots,n$ niech $Y_i = \vec{\xi}^{-1}(FV(\sigma_i))$ i niech $\xi_i : Y_i \to FV(\sigma_i)$ będzie obcięciem ξ do zbioru Y_i. Na mocy założenia indukcyjnego znajdujemy termy $\sigma'_1,\ldots,\sigma'_n$ o żądanych własnościach. Niech $\sigma' = f(\sigma'_1,\ldots,\sigma'_n)$. Oczywiście

$$FV(\sigma') = \bigcup_{i=1}^{n} FV(\sigma'_i) = \bigcup_{i=1}^{n} Y_i = Y.$$

Ponadto dla dowolnej algebry $\mathfrak{A}$ i wartościowania $v : X \to A$ mamy

$$\begin{aligned} \sigma^{\mathfrak{A}}[v] &= f^{\mathfrak{A}}(\sigma_1^{\mathfrak{A}}[v],\ldots,\sigma_n^{\mathfrak{A}}[v]) \\ &= f^{\mathfrak{A}}(\sigma_1'^{\mathfrak{A}}[v\hat{\xi}],\ldots,\sigma_n'^{\mathfrak{A}}[v\hat{\xi}]) \\ &= \sigma'^{\mathfrak{A}}[v\hat{\xi}.] \end{aligned}$$

Druga równość w powyższym ciągu równości zachodzi na mocy założenia indukcyjnego oraz faktu, że $\hat{\xi}$ rozszerza każde ξ_i dla $i = 1, \ldots, n$. To kończy dowód faktu. ∎

Następny fakt pokazuje, że wartość każdego termu zależy tylko od zmiennych w nim występujących.

Fakt 9.4 *Dla dowolnego termu σ, dowolnej algebry $\mathfrak{A}$ i dowolnych wartościowań $v, v' : x \to A$, jeśli dla $x \in FV(\sigma)$ zachodzi $v(x) = v'(x)$, to*

$$\sigma^{\mathfrak{A}}[v] = \sigma^{\mathfrak{A}}[v'].$$

Dowód: Dowód przeprowadzimy przez indukcję ze względu na σ. Jeśli σ jest zmienną to teza oczywiście zachodzi. Niech σ będzie postaci $f(\sigma_1, \ldots, \sigma_n)$, gdzie $n \geq 0$, $f \in \Sigma_n$ oraz $\sigma_1, \ldots, \sigma_n \in FT(\Sigma, X)$. Weźmy dowolną algebrę $\mathfrak{A}$ i wartościowania $v, v' : X \to A$ takie, że

$$v(x) = v'(x), \text{ dla } x \in FV(\sigma). \tag{45}$$

Wówczas mamy

$$\begin{aligned} \sigma^{\mathfrak{A}}[v] &= f^{\mathfrak{A}}(\sigma_1^{\mathfrak{A}}[v], \ldots, \sigma_n^{\mathfrak{A}}[v] \\ &= f^{\mathfrak{A}}(\sigma_1^{\mathfrak{A}}[v'], \ldots, \sigma_n^{\mathfrak{A}}[v'] \\ &= \sigma^{\mathfrak{A}}[v]. \end{aligned}$$

Druga równość w powyższym ciągu równości wynika z (45) oraz z założenia indukcyjnego (ponieważ $FV(\sigma_i) \subseteq FV(\sigma)$). To kończy dowód faktu. ∎

Fakt 9.5 *Dla dowolnych Σ-algebr $\mathfrak{A}$ oraz $\mathfrak{B}$, dowolnego homomorfizmu $h : A \to B$, dowolnego termu $\sigma \in FT(\Sigma, X)$ oraz dla dowolnego wartościowania $v : X \to A$, zachodzi*

$$h(\sigma^{\mathfrak{A}}[v]) = \sigma^{\mathfrak{B}}[hv].$$

Dowód: Dowód przeprowadzimy przez indukcję ze względu na term σ. Jeśli σ jest zmienną to oczywiście równość zachodzi. Załóżmy, że σ jest postaci $f(\sigma_1, \ldots, \sigma_n)$. Wówczas

$$\begin{aligned} h(\sigma^{\mathfrak{A}}[v]) &= h(f^{\mathfrak{A}}(\sigma_1^{\mathfrak{A}}[v], \ldots, \sigma_n^{\mathfrak{A}}[v])) \\ &= f^{\mathfrak{B}}(h(\sigma_1^{\mathfrak{A}}[v]), \ldots, h(\sigma_n^{\mathfrak{A}}[v])) \\ &= f^{\mathfrak{B}}(\sigma_1^{\mathfrak{B}}[hv], \ldots, \sigma_n^{\mathfrak{B}}[hv]) \\ &= \sigma^{\mathfrak{B}}[hv]. \end{aligned}$$

∎

9.3 Podalgebry

Niech $\mathfrak{A}$ będzie dowolną Σ-algebrą. Każdy niepusty podzbiór $B \subseteq A$ zamknięty na operacje algebry $\mathfrak{A}$ nazwiemy podalgebrą $\mathfrak{A}$. Każda podalgebra w naturalny sposób indukuje strukturę Σ-algebry poprzez wzięcie obcięć operacji $\mathfrak{A}$ do podzbioru stanowiącego podalgebrę.

Przykładowo, niech $\mathfrak{A} = \langle P(N),\ \cup,\ \cap,\ \emptyset\rangle$ będzie algebrą. Wówczas zbiór $P_{fin}(N)$ wszystkich skończonych podzbiorów N jest podalgebrą $\mathfrak{A}$. Wyznacza ona algebrę $\langle P(N)_{fin},\ \cup,\ \cap,\ \emptyset\rangle$. Natomiast zbiór wszystkich nieskończonych podzbiorów N nie jest podalgebrą $\mathfrak{A}$ bo nie zawiera $\emptyset$ (nie jest też zamknięty na przeciecia).

Fakt 9.6 *Niech $I \neq \emptyset$. Jeśli $\{A_i \mid i \in I\}$ jest rodziną podalgebr algebry $\mathfrak{A}$ o niepustym przecięciu, to $\bigcap_{i\in I} A_i$ jest podalgebrą $\mathfrak{A}$.*

Dowód: Niech $n \in N$ i weźmy dowolną $f \in \Sigma_n$. Niech $a_1, \ldots, a_n \bigcap_{i\in I} A_i$. Wówczas dla każdego $i \in I$ mamy $a_1 \ldots, a_n \in A_i$ i ponieważ A_i jest podalgebrą $\mathfrak{A}$ to $f^{\mathfrak{A}}(a_1, \ldots, a_n) \in A_i$. Wobec dowolności $i \in I$ otrzymujemy, że $f^{\mathfrak{A}}(a_1, \ldots, a_n) \in \bigcap_{i\in I} A_i$. Dowodzi to, że $\bigcap_{i\in I} A_i$ jest podalgebrą $\mathfrak{A}$. ■

Powyższy fakt pozwala przeprowadzić następującą konstrukcję podalgebry generowanej przez podzbiór. Niech $\mathfrak{A}$ będzie dowolną Σ-algebrą i niech $H \subseteq A$ będzie dowolnym podzbiorem takim, że $\Sigma_0 \cup H \neq \emptyset$. *Podalgebrą generowaną* przez H nazwiemy przecięcie rodziny $\mathcal{K}$ wszystkich podalgebr algebry $\mathfrak{A}$, które zawierają H. Rodzina ta jest niepusta bo $A \in \mathcal{K}$ oraz przeciecie tej rodziny jest niepuste bo zawiera zbiór $\{f^{\mathfrak{A}} \mid f \in \Sigma_0\} \cup H$. Podalgebrę generowaną przez H oznaczamy przez $[H]$. Mówimy, że $\mathfrak{A}$ jest generowana przez H, gdy $\mathfrak{A} = [H]$.

Następujące twierdzenie jest użyteczne przy wyznaczaniu postaci elementów, które muszą należeć do podalgebry generowanej przez podzbiór.

Twierdzenie 9.7 *Niech $\mathfrak{A}$ będzie dowolną Σ-algebrą $\mathfrak{A}$ i niech $H \subseteq A$ będzie podzbiorem takim, że $\Sigma_0 \cup H \neq \emptyset$. Wówczas dla każdego $a \in A$, $a \in [H]$ wtedy i tylko wtedy, gdy istnieje term $\sigma \in FT(\Sigma, X)$ oraz wartościowanie $v : X \to H$ takie, że*

$$a = \sigma^{\mathfrak{A}}[v].$$

Dowód: Niech

$$B = \{a \in A \mid \text{istnieje } \sigma \in FT(\Sigma, X) \text{ oraz istnieje wartościowanie } v : X \to H \text{ takie, że } a = \sigma^{\mathfrak{A}}[v]\}.$$

Aby pokazać, że $[H] \subseteq B$ wystarczy dowieść:

$$H \subseteq B, \tag{46}$$

$$B \text{ jest podalgebrą } \mathfrak{A}. \tag{47}$$

Dla dowodu (46) zauważmy, że dla dowolnego $a \in H$ mamy $a = x^{\mathfrak{A}}[v]$, gdzie $x \in X$ jest dowolną ustaloną zmienną oraz $v : X \to H$ jest funkcją stale równą a.

Dla dowodu (47) weźmy dowolną $f \in \Sigma_n$ oraz $a_1, \ldots, a_n \in B$. Pokażemy, że $f^{\mathfrak{A}}(a_1, \ldots, a_n) \in B$. Dla każdego $1 \leq i \leq n$ istnieje $\sigma_i \in FT(\Sigma, X)$ oraz $v_i : X \to H$ takie, że

$$a_i = \sigma_i^{\mathfrak{A}}[v_i].$$

Dla $i = 1, \ldots, n$ niech Y_i będzie równoliczny z $FV(\sigma_i)$ tak, że zbiory $Y_1, \ldots, Y_n$ są parami rozłączne. Niech $\xi_i : Y_i \to FV(\sigma_i)$ będzie bijekcją i niech $\hat{\xi} : X \to X$ będzie dowolną funkcją rozszerzającą funkcję $\bigcup_{i=1}^{n} \xi_i$. Niech $\sigma'_i, \ldots, \sigma'_n$ będą termami takimi, że

$$FV(\sigma'_i) = Y_i$$

oraz dla dowolnego $v : X \to A$,

$$\sigma_i^{\mathfrak{A}}[v] = \sigma_i'^{\mathfrak{A}}[v\hat{\xi}].$$

Istnienie tych termów wynika z Faktu 9.3.

Niech $\sigma = f(\sigma'_1, \ldots, \sigma'_n)$ i niech $v : X \to H$ będzie funkcją zdefiniowaną następująco

$$v(z) = \begin{cases} v_i\xi_i(z) & \text{jeśli } z \in Y_i, \\ a_0 & \text{jeśli } z \notin \bigcup_{i=1}^{n} Y_i, \end{cases}$$

gdzie $a_0 \in A$ jest dowolnym ustalonym elementem. Wówczas mamy

$$\begin{aligned} \sigma^{\mathfrak{A}}[v] &= f^{\mathfrak{A}}(\sigma_1'^{\mathfrak{A}}[v], \ldots, \sigma_n'^{\mathfrak{A}}[v]) \\ &= f^{\mathfrak{A}}(\sigma_1'^{\mathfrak{A}}[v_1\xi_1], \ldots, \sigma_n'^{\mathfrak{A}}[v_n\xi_n]) \\ &= f^{\mathfrak{A}}(\sigma_1^{\mathfrak{A}}[v_1], \ldots, \sigma_n^{\mathfrak{A}}[v_n]) \\ &= f^{\mathfrak{A}}(a_1, \ldots, a_n). \end{aligned}$$

Druga równość w powyższym ciągu wynika stąd, że dla $z \in Y_i$ mamy $v(z) = v_i\xi_i(z) = v_i\hat{\xi}(z)$. Zatem v oraz $v_i\hat{\xi}(z)$ pokrywają się na $Y_i = FV(\sigma_i)$ i z Faktu 9.4 otrzymujemy, że

$$\sigma_i'^{\mathfrak{A}}[v] = \sigma_i'^{\mathfrak{A}}[v\hat{\xi}].$$

Tym samym udowodniliśmy, że $f^{\mathfrak{A}}(a_1, \ldots, a_n) \in B$, zatem B jest podalgebrą $\mathfrak{A}$.

Dla dowodu zawierania $B \subseteq [H]$ udowodnimy przez indukcję ze względu na σ następującą własność: dla każdego $\sigma \in FT(\Sigma, X)$ i dla każdego $v : X \to H$,

$$\sigma^{\mathfrak{A}}[v] \text{ należy do każdej podalgebry zawierającej } H. \tag{48}$$

Jeśli $\sigma = x$ to oczywiście $\sigma^{\mathfrak{A}}[v] = v(x) \in H$, a zatem $\sigma^{\mathfrak{A}}[v]$ należy do każdej podalgebry zawierającej H. Niech σ będzie postaci $f(\sigma_1, \ldots, \sigma_n)$, gdzie $f \in \Sigma_n$ jest symbolem operacji

n-argumentowej dla pewnego $n \geq 0$ oraz $\sigma_1, \ldots, \sigma_n \in FT(\Sigma, X)$. Weźmy dowolne $v : X \to H$ i dowolną podalgebrę C algebry $\mathfrak{A}$, zawierającą H. Wówczas z założenia indukcyjnego każde $\sigma_i^{\mathfrak{A}}[v]$ należy do C. Zatem $f^{\mathfrak{A}}(\sigma_1^{\mathfrak{A}}[v], \ldots, \sigma_n^{\mathfrak{A}}[v]) \in C$, czyli $\sigma^{\mathfrak{A}}[v] \in C$, co kończy dowód (48). Tym samym Twierdzenie 9.7 jest udowodnione. ∎

Przykładowo, podalgebrą generowaną przez $\emptyset$ w $\langle \{0,1\}^*, \cdot, \varepsilon \rangle$ jest $\{\varepsilon\}$. Podalgebrą generowaną przez $\{0\}$ w powyższej algebrze jest $\{0\}^*$, natomiast podalgebrą generowaną przez $\{0,1\}$ jest cała algebra $\{0,1\}^*$. Dla każdego zbioru Z takiego, że $\Sigma_0 \cup Z \neq \emptyset$, Σ-algebra $FT(\Sigma, Z)$ jest generowana przez zbiór Z.

9.4 Kongruencje

Niech $\mathfrak{A}$ będzie Σ-algebrą. Relację równoważności $r \subseteq A \times A$ nazwiemy *kongruencją* jeśli spełnia one następujący warunek zgodności dla operacji algebry. Dla dowolnego $n \in N$, $f \in \Sigma_n$ oraz $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$, jeśli $(a_1, b_1) \in r, \ \ldots, \ (a_n, b_n) \in r$, to

$$(f^{\mathfrak{A}}(a_1, \ldots, a_n), f^{\mathfrak{A}}(b_1, \ldots, b_n)) \in r.$$

Powyższa definicja pozwala w naturalny sposób wprowadzić strukturę Σ-algebry na zbiorze ilorazowym A/r, Algebrę tę nazywamy *algebrą ilorazową*. Dla $f \in \Sigma_n$ oraz $a_1, \ldots, a_n \in A$ operację $f^{A/r}$ definiujemy następująco,

$$f^{A/r}([a_1]_r, \ldots, [a_n]_r) = [f^{\mathfrak{A}}(a_1, \ldots, a_n)]_r.$$

Poprawność powyższej definicji wynika natychmiast z definicji kongruencji (jest to dokładnie tyle ile potrzeba aby powyższa definicja była poprawna). Z powyższej definicji wynika natychmiast następująca własność.

Fakt 9.8 *Jeśli r jest kongruencją w $\mathfrak{A}$ to przekształcenie kanoniczne $[-]_r : A \to A/r$ jest epimorfizmem algebr.*

Poniższe twierdzenie zbiera łączy pewne pojęcia dotąd wprowadzone. łatwy dowód tego twierdzenia pozostawimy czytelnikowi.

Twierdzenie 9.9 (O izomorfizmie)
Niech $\mathfrak{A}, \mathfrak{B}$ będą Σ-algerbrami i niech $h : \mathfrak{A} \to \mathfrak{B}$ będzie dowolnym homomorfizmem. Wówczas h daje się przedstawić jako złożenie następujących trzech funkcji:

$$\mathfrak{A} \overset{[-]_r}{\to} \mathfrak{A}/r \overset{\tilde{h}}{\to} \vec{h}(\mathfrak{A}) \overset{\iota_{\vec{h}(\mathfrak{A}),\mathfrak{B}}}{\to} \mathfrak{B},$$

gdzie

- $r = ker(h)$ *oraz* $[-]_r$ *jest kanonicznym epimorfizmem;*
- $\tilde{h}$ *jest izomorfizmem zdefiniowanym dla* $[a]_r \in A/r$*, przez warunek* $\tilde{h}([a]_r) = h(a)$*;*
- $\iota_{\tilde{h}(\mathfrak{A}),\mathfrak{B}}$ *jest identycznościowym włożeniem, które jest monomorfizmem.*

W szczególności $\mathfrak{A}/r$ *jest izomorficzna z podalgebrą algebry* $\mathfrak{B}$*.*

Na zakończenie podamy kilka przykładów kongruencji.

Przykład 9.10 (Przykłady kongruencji)

(i) Niech $\mathfrak{A} = \langle \{0,1\}^*,\ \cdot,\ \varepsilon \rangle$. Wówczas relacja r_1 taka, że $(w_1, w_2) \in r_1$ wtw, gdy liczba zer w w_1 i w w_2 są takie same jest kongruencją w $\mathfrak{A}$. Algebra ilorazowa $\mathfrak{A}/r_1$ jest izomorficzna z $\mathcal{N} = \langle N,\ +,\ 0 \rangle$. Podobnie jest dla relacji r_2 w $\mathfrak{A}$, gdzie $(w_1, w_2) \in r_2$ wtw, gdy $|w_1| = |w_2|$. Algebra ilorazowa $\mathfrak{A}/r_2$ jest też izomorficzna z $\mathcal{N}$, choć $r_1 \neq r_2$.

(ii) Relacja przystawania modulo n jest kongruencją w algebrze $\langle Z,\ \cdot,\ +,\ 0,\ 1 \rangle$. Algebra ilorazowa jest izomorficzna z algebrą o nośniku $\{0, 1, \ldots, n-1\}$, w którym operacje dodawania i mnożenia są wykonywane modulo n.

(iii) Niech $\mathfrak{A}$ będzie dowolną Σ-algebrą i niech $v : X \to A$ będzie dowolnym ustalonym wartościowaniem. Wówczas relacja $r \subseteq FT(\Sigma, X) \times FT(\Sigma, X)$ zdefiniowana $(\sigma_1, \sigma_2) \in r$ wtw, gdy $\sigma_1^{\mathfrak{A}}[v] = \sigma_2^{\mathfrak{A}}[v]$ jest kongruencją w $FT(\Sigma, X)$.

9.5 Uogólnione produkty algebr

Niech $\{A_i \mid i \in I\}$ będzie dowolną rodziną zbiorów. *Uogólnionym produktem* tej rodziny jest zbiór wszystkich funkcji $\xi : I \to \bigcup_{i \in I} A_i$ takich, że dla $i \in I$, zachodzi $\xi(i) \in A_i$. Uogólniony produkt rodziny $\{A_i \mid i \in I\}$ będziemy oznaczać przez $\prod_{i \in I} A_i$.

Niech $\{\mathfrak{A}_i \mid i \in I\}$ będzie rodziną Σ-algebr. Na uogólnionym produkcie $\prod_{i \in I} A_i$ określimy strukturę Σ-algebry definiując wszystkie operacje "po współrzędnych". Dla $n \in N$, $f \in \Sigma_n$ oraz $\xi_1, \ldots \xi_n \in \prod_{i \in I} A_i$ definiujemy dla dowolnego $j \in I$,

$$f^{\prod_{i \in I} \mathfrak{A}_i}(\xi_1, \ldots, \xi_n)(j) = f^{\mathfrak{A}_j}(\xi_1(j), \ldots, \xi_n(j)).$$

Dla zilustrowania powyższej konstrukcji zauważmy, że jeśli mamy rodzinę algebr

$$\mathfrak{A}_n = \langle \{0,1\},\ min,\ max,\ 0,\ 1 \rangle$$

dla $n \in N$, to uogólniony produkt $\prod_{n \in N} \mathfrak{A}_n$ jest algebrą izomorficzną z $\langle P(N),\ \cap,\ \cup,\ \emptyset,\ N \rangle$.

9.6 Klasy równościowo definiowalne

Wyrażenie $\sigma = \tau$, gdzie $\sigma, \tau \in FT(\Sigma, X)$ nazywamy *równością*. Mówimy, że równość $\sigma = \tau$ jest *prawdziwa* w Σ-algebrze $\mathfrak{A}$, gdy dla każdego wartościowania $v : X \to A$,

$$\sigma^{\mathfrak{A}}[v] = \tau^{\mathfrak{A}}[v].$$

Prawdziwość równości $\sigma = \tau$ w $\mathfrak{A}$ oznaczamy przez

$$\mathfrak{A} \models \sigma = \tau.$$

Zauważmy, że dotychczas używaliśmy znaku $=$ jako symbolu oznaczającego (matematyczną) równość obiektów. Symbol $=$ użyty w wyrażeniach, które nazywamy równościami jest symbolem formalnym. Nie będziemy wprowadzać specjalnych oznaczeń dla rozróżnienia tych symboli. Ich znaczenie będzie zawsze wynikało z kontekstu, w którym będą użyte.

Przykład 9.11

(i) Niech $\mathfrak{A} = \langle \{0,1\}^*,\ \cdot,\ \varepsilon \rangle$. Przykładem równości prawdziwej w $\mathfrak{A}$ jest

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

Równość ta wyraża własność łączności operacji konkatenacji w algebrze słów. Natomiast równość

$$x \cdot y = y \cdot x$$

nie jest prawdziwa w $\mathfrak{A}$ bo operacja konkatenacji słów nad $\{0,1\}$ nie jest przemienna.

(ii) Przykładami równości prawdziwych w $\langle Z,\ \cdot,\ +,\ 0,\ 1 \rangle$ są

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

oraz

$$x \cdot y = y \cdot x.$$

(iii) W algebrze $\langle P(N),\ \cap,\ \cup,\ \emptyset,\ N \rangle$ prawdziwe są następujące przykłady równości

$$x \cap \emptyset = \emptyset$$

$$x \cap (x \cup y) = x$$

Klasę $\mathcal{K}$ Σ-algebr nazwiemy *klasą równościowo definiowalną* gdy istnieje zbiór Δ równości nad sygnaturą Σ taki, że dla dowolnej Σ-algebry $\mathfrak{A}$,

$$\mathfrak{A} \in \mathcal{K},\ \text{wtw, gdy wszystkie równości z } \Delta \text{ są prawdziwe w } \mathfrak{A}.$$

Klasy równościowo definiowalne bywają też nazywane *rozmaitościami*.

Przykład 9.12 (Przykłady rozmaitości)

(i) Klasa wszystkich Σ-algebr jest rozmaitością. Zbiorem definiujących równości jest w tym przypadku zbiór pusty.

(ii) Powyższa rozmaitość jest największą rozmaitością dla zadanej sygnatury. Najmniejszą rozmaitością dla sygnatury Σ jest rozmaitość algebr jednoelementowych. Jest ona zadana równością

$$x = y$$

Jest to tzw. *rozmaitość trywialna*.

(iii) (*Półgrupy*) Sygnaturą dla półgrup jest $\Sigma_2 = \{\cdot\}$ oraz $\Sigma_n = \emptyset$ dla $n \neq 2$. Definiującą równością jest łączność:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

(iv) (*Półgrupy przemienne*) Sygnatura ta sama co dla półgrup. Definiujące równości to równość wyrażająca łączność oraz przemienność operacji $\cdot$

$$x \cdot y = y \cdot x$$

(v) (*Monoidy*) Rozszerzamy powyższą sygnaturę przez dodanie symbolu stałej $\varepsilon \in \Sigma_0$. Definiujące równości to łączność operacji $\cdot$ oraz dwie równości dla dodanej stałej:

$$x \cdot \varepsilon = x$$

$$\varepsilon \cdot x = x$$

(vi) (*Kraty*) Sygnatura składa się z dwóch symboli operacji dwuargumentowych $\vee, \wedge$. Równości definiujące to łączność i przemienność każdej z tych operacji oraz następujące równości:

$$x \vee x = x$$

$$x \wedge x = x$$

$$x \wedge (x \vee y) = x$$

$$x \vee (x \wedge y) = x$$

Można pokazać, że w każdej algebrze $\mathfrak{A}$ spełniającej równości krat można zdefiniować częściowy porządek w ten sposób, że $\vee^{\mathfrak{A}}$ jest operacją kresu górnego dwóch elementów a $\wedge^{\mathfrak{A}}$ jest operacją kresu dolnego w tym porządku.

(vii) (*Kraty rozdzielne*) Sygnatura ta sama co dla krat. Równości definiujące to wszystkie równości definiujące dla krat oraz następujące dwie równości rozdzielności:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

(viii) (*Algebry Boole'a*) Sygnatura krat powiększona o dwa symbole stałych $0, 1$ oraz symbol operacji jednoargumentowej $-$. Równości definiujące to wszystkie równości dla krat rozdzielnych oraz następujące równości dla dodanych symboli:

$$x \wedge 0 = 0$$

$$x \wedge 1 = x$$

$$x \vee 0 = x$$

$$x \vee 1 = 1$$

$$x \vee (-x) = 1$$

$$x \wedge (-x) = 0$$

Następujące twierdzenie podaje pełną algebraiczną chrakteryzację klas równościowo definiowalnych. Dowód tego twierdzenia podamy w następnym dziale.

Twierdzenie 9.13 (Birkhoff)
Niech $\mathcal{K}$ będzie niepustą klasą Σ-algebr. Klasa $\mathcal{K}$ jest równościowo definiowalna wtedy i tylko wtedy, gdy $\mathcal{K}$ jest zamknięta na podalgebry, obrazy homomorficzne i produkty uogólnione, tzn, gdy każda z powyższych trzech operacji wykonana na algebrach z klasy $\mathcal{K}$ daje algebrę z klasy $\mathcal{K}$.

Korzystając z powyższego twierdzenia łatwo jest pokazać, że na przykład, klasa ciał nie jest równościowo definiowalna.

9.7 Algebry wolne

W tej części zajmiemy się rozszerzeniami do homomorfizmu funkcji zadanych na zbiorze generatorów. Podejście to zostanie użyte w dowodzie twierdzenia Brikhoffa (por. Twierdzenie 9.13).

Zacznijmy od następującego twierdzenia, które mówi, że funkcję zdefiniowaną na zbiorze generatorów danej algebry można rozszerzyć do homomorfizmu na co najwyżej jeden sposób.

Twierdzenie 9.14 *Niech $\mathfrak{A}$ będzie Σ-algebrą i niech $H \subseteq A$ będzie zbiorem generatorów algebry $\mathfrak{A}$. Jeśli $h_1, h_2 : \mathfrak{A} \to \mathfrak{B}$ są homomorfizmami algebr takimi, że $h_1(a) = h_2(a)$, dla $a \in H$, to $h_1 = h_2$.*

Dowód: Niech $\sigma \in FT(\Sigma, X)$ oraz niech $v : X \to H$ będzie dowolnym wartościowaniem. Wówczas $h_1 v = h_2 v$ oraz

$$\begin{aligned} h_1(\sigma^{\mathfrak{A}}[v]) &= \sigma^{\mathfrak{B}}[h_1 v] \\ &= \sigma^{\mathfrak{B}}[h_2 v] \\ &= h_2(\sigma^{\mathfrak{A}}[v]) \end{aligned}$$

Pierwsza i trzecia równość wynikają z Faktu 9.5.Na mocy Twierdzenia 9.7 wnioskujemy, że h_1 ih_2 są równe na wszystkich elementach podalgebry generowanej przez H, czyli na $\mathfrak{A}$. ■

Oczywiście nie każdą funkcję da się rozszerzyć ze zbioru generatorów do homomorfizmu. Natępujące twierdzenie podaje warunek konieczny i wystarczający.

Twierdzenie 9.15 *Niech $\mathfrak{A}$ i $\mathfrak{B}$ będą Σ-algebrami i niech G będzie zbiorem generatorów algebry $\mathfrak{A}$. Dla dowolnej funkcji $g : G \to B$ następujące warunki są równoważne*

(i) g rozszerza się do homomorfizmu $\bar{g} : \mathfrak{A} \to \mathfrak{B}$;

(ii) Dla dowolnych termów $\sigma, \tau \in FT(\Sigma, X)$ oraz dla dowolnego wartościowania $v : X \to G$, zachodzi

$$\sigma^{\mathfrak{A}}[v] = \tau^{\mathfrak{A}}[v] \quad \Longrightarrow \quad \sigma^{\mathfrak{B}}[gv] = \tau^{\mathfrak{B}}[gv].$$

Dowód: Implikacja (i) $\Longrightarrow$ (ii) jest wynika natychmiast w Faktu 9.5. Dla dowodu implikacji (ii) $\Longrightarrow$ (i) definiujemy funkcję $\bar{g} : \mathfrak{A} \to \mathfrak{B}$ następująco. Dla $a \in A$ bierzemy $\sigma \in FT(\Sigma, X)$ oraz vartościowanie $v : X \to G$ takie, że $\sigma^{\mathfrak{A}}[v] = a$ (por. Twierdzenie 9.7). Wówczas definiujemy $\bar{g}(a) = \sigma^{\mathfrak{B}}[gv]$. Warunek (ii) dowodzi poprawności tej definicji. Łatwe sprawdzenie, że $\bar{g} : \mathfrak{A} \to \mathfrak{B}$ jest homomorfizmem pozostawiamy czytelnikowi. ■

Uwagi te stanowią motywację dla następującej definicji. Niech $\mathcal{K}$ będzie klasą Σ-algebr. Niech $\mathfrak{W}$ będzie Σ-algebrą i niech G będzie zbiorem generatorów algebry $\mathfrak{W}$. Powiemy, że algebra $\mathfrak{W}$ jest *wolna* w klasie $\mathcal{K}$ na zbiorze *wolnych generatorów* G jeśli $\mathfrak{W} \in \mathcal{K}$ oraz dla dowolnej algebry $\mathfrak{B} \in \mathcal{K}$ dowolna funkcja $f : G \to B$ rozszerza się do homomorfizmu algebry $\mathfrak{W}$ w $\mathfrak{B}$. W powyższej definicji ważne są wszystkie trzy parametry: klasa $\mathcal{K}$, algebra $\mathfrak{W} \in \mathcal{K}$ oraz zbiór generatorów G algebry $\mathfrak{W}$.

Podstawową własnością algebry wolnej w danej klasie jest to, że jakikolwiek związek pomiędzy wolnymi generatorami tej algebry uogólnia się na równość prawdziwą we wszystkich algebrach tej klasy. Jest to treścią następującego twierdzenia.

Twierdzenie 9.16 *Niech $\mathfrak{W}$ będzie algebrą wolną w klasie $\mathcal{K}$ na zbiorze wolnych generatorów G. Niech $v : X \to G$ będzie wartościowaniem takim, że dla pewnych termów $\sigma, \tau \in FT(\Sigma, X)$ zachodzi $\sigma^{\mathfrak{W}}[v] = \tau^{\mathfrak{W}}[v]$ oraz v, ograniczone do zbioru $FV(\sigma) \cup FV(\tau)$, jest funkcją różnowartościową. Wówczas*

$$\mathcal{K} \models \sigma = \tau,$$

tzn. równość $\sigma = \tau$ zachodzi we wszystkich algebrach klasy $\mathcal{K}$.

Dowód: Niech $\mathfrak{A} \in \mathcal{K}$ i weźmy dowolne wartościowanie $u : X \to A$. Zdefiniujmy funkcję $g : G \to A$ następująco dla $w \in G$:

$$g(w) = \begin{cases} u(x), & \text{gdy } v(x) = w \text{ oraz } x \in FV(\sigma) \cup FV(\tau) \\ a_0, & \text{w przeciwnym przypadku,} \end{cases}$$

gdzie $a_0 \in A$ jest dowolnym ustalonym elementem. Ponieważ funkcja v jest różnowartościowa na zbiorze $FV(\sigma) \cup FV(\tau)$, to powyższa definicja jest poprawna. Zauważmy, że dla $x \in FV(\sigma) \cup FV(\tau)$ zachodzi $gv(x) = u(x)$. Niech $\bar{g} : \mathfrak{W} \to \mathfrak{A}$ będzie rozszerzeniem g do homomorfizmu. Wówczas

$$\begin{aligned} \sigma^{\mathfrak{A}}[u] &= \sigma^{\mathfrak{A}}[gv] \\ &= \bar{g}(\sigma^{\mathfrak{W}}[v]) \\ &= \bar{g}(\tau^{\mathfrak{W}}[v]) \\ &= \tau^{\mathfrak{A}}[gv] \\ &= \tau^{\mathfrak{A}}[u]. \end{aligned}$$

Druga i czwarta równość w powyższym ciągu zachodzi na mocy Faktu 9.2. Wobec dowolności u dostajemy $\mathfrak{A} \models \sigma = \tau$. ∎

Z powyższego twierdzenia natychmiast dostajemy następujący wniosek.

Wniosek 9.17 *Jeśli $\mathfrak{W}$ jest algebrą wolną w klasie $\mathcal{K}$, to dla dowolnych termów $\sigma, \tau \in FT(\Sigma, X)$ mamy,*

$$\mathfrak{W} \models \sigma = \tau \iff \mathcal{K} \models \sigma = \tau.$$

Następujące dwa twierdzenia podają przykłady algebr wolnych.

Twierdzenie 9.18 *Dla każdego zbioru G rozłącznego z sygnaturą Σ i takiego, że $\Sigma_0 \cup G \neq \emptyset$, algebra termów $FT(\Sigma, G)$ o zmiennych ze zbioru G jest wolna w klasie wszystkich Σ-algebr oraz G jest zbiorem wolnych generatorów. Algebrę tę nazywa się często algebrą absolutnie wolną.*

Dowód: Niech $\mathfrak{B}$ będzie dowolną Σ-algebrą i niech $v : G \to B$ będzie dowolną funkcją. Wówczas $(-)^{\mathfrak{B}}[v]$, na mocy Faktu 9.2, jest homomorfizmem rozszerzającym v. ■

Twierdzenie 9.19 *Dla każdego zbioru G, algebra $\langle G^*, \cdot, \varepsilon\rangle$ jest wolna w klasie wszystkich monoidów oraz G jest zbiorem wolnych generatorów.*

Dowód: Niech $\mathfrak{A} = \langle A, \cdot, 1\rangle$ będzie dowolnym monoidem i niech $f : G \to A$ będzie dowolną funkcją. Rozszerzenie $\hat{f} : G^* \to A$ funkcji f definiujemy przez indukcję noetherowską (zob. Twierdzenie 8.5).

$$\hat{f}(\varepsilon) = 1,$$
$$\hat{f}(aw) = f(a) \cdot \hat{f}(w),$$

dla $a \in G$, $w \in G^*$.

Zauważmy, że ponieważ dla $a \in G$ mamy $\hat{f}(a) = \hat{f}(a \cdot \varepsilon) = f(a) \cdot \hat{f}(\varepsilon) = f(a) \cdot 1 = f(a)$, to istotnie $\hat{f}$ jest rozszerzeniem f.

Pokażemy, że $\hat{f}$ jest homomorfizmem monoidów. Musimy jedynie pokazać, że $\hat{f}$ zachowuje operację mnożenia. Pokażemy, że dla dowolnych $u, w \in G^*$ zachodzi

$$\hat{f}(uw) = \hat{f}(u) \cdot \hat{f}(w).$$

Powyższą równość dowodzimy przez indukcję ze względu na u (tzn. dobrze ufundowanym porządkiem dla tego dowodu jest $\langle G^*, \leq\rangle$, gdzie $\leq$ jest porządkiem prefiksowym). Dla $u = \varepsilon$ mamy

$$\hat{f}(\varepsilon w) = \hat{f}(w) = 1 \cdot \hat{f}(w) = \hat{f}(\varepsilon) \cdot \hat{f}(w).$$

Niech $u \neq \varepsilon$. Zatem u ma postać $u = au'$, dla pewnego $a \in G$ oraz $u' \in G^*$. Mamy wówczas

$$\begin{aligned}
\hat{f}((au')w) &= \hat{f}(a(u'w)) \\
&= f(a) \cdot \hat{f}(u'w) \\
&= f(a) \cdot (\hat{f}(u') \cdot \hat{f}(w)) \\
&= (f(a) \cdot \hat{f}(u')) \cdot \hat{f}(w) \\
&= \hat{f}(au') \cdot \hat{f}(w) \\
&= \hat{f}(u) \cdot \hat{f}(w).
\end{aligned}$$

Druga i piąta równość w powyższym ciągu wynika z łączności operacji mnożenia w G^* oraz w $\mathfrak{A}$. Czwarta równość wynika z założenia indukcyjnego (bo $u' < u$). Zatem $\hat{f}$ jest istotnie homomorfizmem monoidów, co kończy dowód twierdzenia. ■

Nie w każdej klasie algebr są algebry wolne dla tej klasy. Poniższe twierdzenie podaje warunek wystarczający dla istnienia algebr wolnych. Wywnioskujemy z niego twierdzenie Birkhoffa.

Twierdzenie 9.20 *Niech $\mathcal{K}$ będzie klasą Σ-algebr zamkniętą na izomorfizmy, podalgebry i produkty uogólnione. Jeśli $\mathcal{K}$ zawiera algebrę o co najmniej dwóch elementach, to dla każdego zbioru G istnieje algebra wolna w klasie $\mathcal{K}$ na zbiorze wolnych generatorów G.*

Dowód: Podamy szkic dowodu. Ustalmy klasę $\mathcal{K}$ oraz zbiór G. Niech C będzie zbiorem wszystkich kongruencji $r \subseteq FT(\Sigma, G) \times FT(\Sigma, G)$ takich, że $FT(\Sigma, G)/r \in \mathcal{K}$. Niech $\mathfrak{B} = \prod_{r \in C} FT(\Sigma, G)/r$ i niech $\mathfrak{W}$ będzie podalgebrą algebry $\mathfrak{B}$ generowaną przez zbiór $\tilde{G} = \{\xi_g \mid g \in G\}$, gdzie funkcja $\xi : C \to \bigcup_{r \in C} FT(\Sigma, G)/r$ jest zdefiniowana następująco dla $r \in C$, $\xi_g(r) = [g]_r$.

Z faktu, że $\mathcal{K}$ zawiera algebrę o co najmniej dwóch elementach wynika, że funkcja $\theta : G \to \tilde{G}$ taka, że $\theta(g) = \xi_g$ jest bijekcją. Ponieważ $\mathcal{K}$ jest zamknięta na podalgebry i uogólnione produkty, to $\mathfrak{W} \in \mathcal{K}$. Pokażemy, że $\mathfrak{W}$ jest wolna w $\mathcal{K}$, na zbiorze wolnych generatorów $\tilde{G}$. Biorąc izomorficzną kopię $\mathfrak{W}$, generowaną przez G, dostaniemy żądaną algebrę wolną.

Niech $\mathfrak{A} \in \mathcal{K}$ i niech $g : \tilde{G} \to A$ będzie dowolną funkcją. Weźmy termy $\sigma, \tau \in FT(\Sigma, X)$ oraz wartościowanie $v : X \to \tilde{G}$ takie, że $\sigma^{\mathfrak{W}}[v] = \tau^{\mathfrak{W}}[v]$. Musimy pokazać, że $\sigma^{\mathfrak{A}}[gv] = \tau^{\mathfrak{A}}[gv]$. Rozważmy funkcję $g\theta : G \to A$ oraz jej rozszerzenie $\bar{g\theta} : FT(\Sigma, G) \to \mathfrak{A}$ do homomorfizmu. Niech $r = ker(\bar{g\theta})$. Z twierdzenia o izomorfizmie (por. Twierdzenie 9.9) wynika, że $FT(\Sigma, G)/r$ jest izomorficzna z pewną podalgebrą algebry $\mathfrak{A}$, więc $FT(\Sigma, G)/r \in \mathcal{K}$ oraz $r \in C$.

Niech $\pi_r : \mathfrak{W} \to FT(\Sigma, G)/r$ będzie funkcją zdefiniowaną następująco $\pi_r(\xi) = \xi(r)$. Z faktu, że operacje w produkcie są wykonywane po współrzędnych wynika, że dla każdego termu $\rho \in FT(\Sigma, X)$ mamy

$$\pi_r(\rho^{\mathfrak{W}}[v]) = [\sigma^{FT(\Sigma,G)}[\theta^{-1}v]]_r,$$

a co za tym idzie

$$(\sigma^{FT(\Sigma,G)}[\theta^{-1}v], \tau^{FT(\Sigma,G)}[\theta^{-1}v]) \in r.$$

Zatem

$$\begin{aligned} \sigma^{\mathfrak{A}}[gv] &= \bar{g\theta}(\sigma^{FT(\Sigma,G)}[\theta^{-1}v]) \\ &= \bar{g\theta}(\tau^{FT(\Sigma,G)}[\theta^{-1}v]) \\ &= \tau^{\mathfrak{A}}[gv]. \end{aligned}$$

Pierwsza i trzecia równość w powyższym ciągu wynika z Faktu 9.5. Zatem, korzystając z Twierdzenia 9.15 wnioskujemy, że g rozszerza się do homomorfizmu. To kończy dowód Twierdzenia 9.20. ∎

Na zakończenie udowodnimy twierdzenie Birkhoffa.

Dowód Twierdzenia Birkhoffa

Sprawdzenie faktu, że każda klasa równościowo definiowalna jest zamknięta na obrazy homomorficzne, podalgebry, i uogólnione produkty pozostawimy czytelnikowi. Tutaj udowodnimy implikację odwrotną.

Niech $\mathcal{K}$ będzie klasą Σ-algebr zamkniętą na obrazy homomorficzne, podalgebry, i uogólnione produkty. Bez zmniejszenia ogólności możemy założyć, że $\mathcal{K}$ zawiera algebrę o co najmniej dwóch elementach (bo klasa wszystkich algebr jednoelementowych jest definiowalna przez równość $x = y$). Niech Δ będzie zbiorem wszystkich równości prawdziwych we wszystkich algebrach z $\mathcal{K}$. Pokażemy, że Δ definiuje $\mathcal{K}$. Niech $\mathfrak{A}$ będzie dowolną Σ-algebrą, w której wszystkie równości z Δ są prawdziwe. Niech $\mathfrak{W} \in \mathcal{K}$ będzie algebrą wolną w klasie $\mathcal{K}$, na zbiorze wolnych generatorów A. Pokażemy, że funkcja identycznościowa $I_A : A \to A$ rozszerza się do homomorfizmu $\bar{I}_A : \mathfrak{W} \to \mathfrak{A}$. To zakończy dowód, bowiem $\mathfrak{A}$ musi należeć do $\mathcal{K}$, jako obraz homomorficzny algebry $\mathfrak{W} \in \mathcal{K}$.

W tym celu skorzystamy z Twierdzenia 9.15. Weźmy dowolne dwa termy $\sigma, \tau \in FT(\Sigma, X)$ oraz wartościowanie $v : X \to A$ i załóżmy, że $\sigma^{\mathfrak{W}}[v] = \tau^{\mathfrak{W}}[v]$. Pokażemy, że $\sigma^{\mathfrak{A}}[gv] = \tau^{\mathfrak{A}}[gv]$. Jeśli v nie jest różnowartościowe na $FV(\sigma) \cup FV(\tau)$ to 'poprawiamy' termy następująco. Jeśli $v(x) = v(y)$ dla pewnych zmiennych $x, y \in FV(\sigma) \cup FV(\tau)$, to podstawiamy w obu termach y na wszystkie wystąpienia x, eliminując w ten sposób zmienną x. Po skończonej liczbie kroków otrzymujemy dwa termy σ_* oraz τ_* takie, że v jest różnowartościowa na $FV(\sigma_*) \cup FV(\tau_*)$. Ponadto, jak łatwo jest pokazać, mamy $\sigma^{\mathfrak{W}}[v] = \sigma_*^{\mathfrak{W}}[v]$ oraz $\tau^{\mathfrak{W}}[v] = \tau_*^{\mathfrak{W}}[v]$. Zatem, na mocy Twierdzenia 9.16 wnioskujemy, że $\mathcal{K} \models \sigma_* = \tau_*$, a zatem $\mathfrak{A} \models \sigma_* = \tau_*$. Tak więc mamy $\sigma_*^{\mathfrak{A}}[gv] = \tau_*^{\mathfrak{A}}[gv]$. Ponieważ $\sigma^{\mathfrak{A}}[gv] = \sigma_*^{\mathfrak{A}}[gv]$ oraz $\tau^{\mathfrak{A}}[gv] = \tau_*^{\mathfrak{A}}[gv]$, to ostatecznie otrzymujemy $\sigma^{\mathfrak{A}}[gv] = \tau^{\mathfrak{A}}[gv]$, co kończy dowód.

Zadania

9.1. Wyznaczyć wszystkie homomorfizmy z algebry $\langle \{0\}^*, \cdot, \varepsilon \rangle$ w algebrę $\langle \{0,1\}^*, \cdot, \varepsilon \rangle$, gdzie $\cdot$ oznacza w obu algebrach operację konkatenacji, a ε oznacza słowo puste.

9.2. Dowieść, że dla każdej sygnatury Σ i dwóch różnych zmiennych x, y, algebry termów $FT(\Sigma, \{x\})$ oraz $FT(\Sigma, \{x, y\})$ nie są izomorficzne.

9.3. Wyznaczyć wszystkie możliwe zbiory generatorów dla następujących algebr.

a. $\langle A^*, \cdot, \varepsilon \rangle$, gdzie $\cdot$ oznacza operację konkatenacji, a ε oznacza słowo puste.

b. $\langle A^*, \cdot, \rangle$, gdzie $\cdot$ oznacza operację konkatenacji.

c. $FT(\Sigma, X)$

d. $\langle N, \cdot, 0, 1 \rangle$, gdzie $\cdot$ oznacza operacje mnożenia.

e. $\langle N,\ + \rangle$, gdzie $+$ oznacza operację dodawania.

9.4. Dowieść, że dla każdej algebry $\mathfrak{A}$, suma łańcucha podalgebr algebry $\mathfrak{A}$ jest podalgebrą algebry $\mathfrak{A}$. Czy suma dowolnych dwóch podalgebr musi być podalgebrą?

9.5. Niech Σ będzie sygnaturą taką, że $\Sigma_0 \neq \emptyset$. Dowieść, że dla dowolnej Σ-algebry $\mathfrak{A}$ zbiór wszystkich podalgebr algebry $\mathfrak{A}$, uporządkowany relacją zawierania, tworzy kratę zupełną. Podać przykład świadczący o tym, że założenie $\Sigma_0 \neq \emptyset$ jest istotne. (*Wskazówka:* rozważyć algebrę $\langle N, s\rangle$, gdzie $s : N \to N$ jest operacją następnika.)

9.6. Dowieść, że zbiór wszystkich kongruencji danej algebry, uporządkowany relacją zawierania, tworzy kratę zupełną.

9.7. Podać przykład nieskończonej algebry, która ma tylko dwie kongruencje. (*Wskazówka:* rozważyć algebrę $\langle N, \cdot, f\rangle$, gdzie $\cdot$ jest operacją mnożenia, a $f : N \times N \to N$ jest funckją charakterystyczną relacji pozrądku $\leq \subseteq N \times N$.)

9.8. Dowieść, że uogólniony produkt $\prod_{n\in N} \mathfrak{A}_n$ jest algebrą izomorficzną z $\langle P(N),\ \cap,\ \cup,\ \emptyset,\ N\rangle$, gdzie $\mathfrak{A}_n = \langle \{0,1\},\ min,\ max,\ 0,\ 1\rangle$, dla wszystkich $n \in N$.

9.9. Niech $\mathfrak{A}$ będzie algebrą, w której prawdziwe są wszystkie równości dla krat (zob. Przykład 9.12 (vi)). W zbiorze A definiujemy relację $\leq$ następująco, dla dowolnych $a, b \in A$, $a \leq b$ wtw, gdy $a = a \wedge^{\mathfrak{A}} b$. Dowieść, że $\leq$ jest częściowym porządkiem w A oraz, że dla dowolnych $a, b \in A$, wynik $a \vee^{\mathfrak{A}} b$ jest kresem górnym oraz $a \wedge^{\mathfrak{A}} b$ jest kresem dolnym zbioru $\{a, b\}$ w $\langle A,\ \leq\rangle$.

9.10. Dowieść, że każda rozmaitość jest zamknięta ze względu na podalgebry, obrazy homomorficzne i produkty uogólnione.

9.11. Niech $H \neq \emptyset$. Dowieść, że algebra $\langle H^*,\ \cdot,\ \varepsilon\rangle$ nie jest wolna w klasie wszystkich algebr tej sygnatury, na żadnym zbiorze wolnych generatorów. Dowieść, że $\langle H^*,\ \cdot,\ \varepsilon\rangle$ nie jest wolna w klasie wszystkich monoidów, na zbiorze wolnych generatorów $H \cup \{\varepsilon\}$.

9.12. Podać przykład algebry, która nie jest wolna w żadnej klasie algebr tej samej sygnatury, na żadnym zbiorze wolnych generatorów. (*Wskazówka:* rozważyć algebrę $\langle N, +\rangle$, gdzie $+$ jest operacją dodawania.)

10 Unifikacja

Rozpatrzymy szczególny przypadek wartościowań, gdy algebra z której brane są wartości jest algebrą termów $FT(\Sigma, X)$. Każde takie wartościowanie $v : X \to FT(\Sigma, X)$ jest nazywane *podstawieniem*. Podstawienie v, tak jak każde wartościowanie, rozszerza się do homomorfizmu

$$(-)^{FT(\Sigma,X)}[v] : FT(\Sigma, X) \to FT(\Sigma, X).$$

Dla każdego termu $\sigma \in FT(\Sigma, X)$, $\sigma^{FT(\Sigma,X)}[v]$ jest wynikiem wykonania podstawienia v na termie σ. Wykonanie podstawienia v na termie σ intuicyjnie polega na zastąpieniu w termie σ każdego wystąpienia zmiennej x termem $v(x)$, dla dowolnej zmiennej $x \in X$. Dla uproszczenia notacji przyjmiemy oznaczenie $v(\sigma)$ na wynik zastosowania podstawienia v na termie σ. Tak więc z definicji mamy

$$v(\sigma) = \sigma^{FT(\Sigma,X)}[v],$$

oraz funkcję $v : X \to FT(\Sigma, X)$ możemy jednocześnie traktować jak rozszerzenie v do homomorfizmu $v : FT(\Sigma, X) \to FT(\Sigma, X)$. Oznaczenie to nie powinno prowadzić do niejednoznaczności, gdyż $X \subseteq FT(\Sigma, X)$ oraz funkcja $v : FT(\Sigma, X) \to FT(\Sigma, X)$ obcięta do X pokrywa się z oryginalnym podstawieniem $v : X \to FT(\Sigma, X)$.

Dla termów $\sigma, \tau \in FT(\Sigma, X)$ oraz zmiennej x, symbolem $\sigma(\tau/x)$ oznaczamy term otrzymany z σ przez podstawienie τ na wszystkie wystąpienia x w σ. Zatem zgodnie z naszymi oznaczeniami $\sigma(\tau/x) = v(\sigma)$, gdzie $v : X \to FT(\Sigma, X)$ jest podstawieniem zdefiniowanym następująco:

$$v(y) = \begin{cases} \tau & \text{jeśli } y = x, \\ y & \text{jeśli } y \neq x. \end{cases}$$

Twierdzenie 10.1 (O podstawieniu)
Dla dowolnej zmiennej $x \in X$ oraz termu $\tau \in FT(\Sigma, X)$, jeśli $v : X \to FT(\Sigma, X)$ jest podstawieniem takim, że $v(x) = v(\tau)$, to dla każdego termu $\sigma \in FT(\Sigma, X)$,

$$v(\sigma(\tau/x)) = v(\sigma).$$

Dowód: Indukcja strukturalna ze względu na σ. Jeśli σ jest zmienną x to równość oczywiście zachodzi na mocy założeń twierdzenia. Jeśli σ jest zmienną różną od x, to równość też oczywiście zachodzi.

Jeśli σ jest postaci $f(\sigma_1, \ldots, \sigma_m)$, dla pewnego symbolu $f \in \Sigma_m$ $(m \geq 0)$, to

$$v(\sigma(\tau/x)) = f(v(\sigma_1(\tau/x)), \ldots, v(\sigma_m(\tau/x))) = f(v(\sigma_1), \ldots, v(\sigma_m)) = v(\sigma).$$

Pierwsza i ostatnia równość w powyższym ciągu równości wynika stąd, że v jest homomorfizmem, natomiast środkowa równość wynika z założenia indukcyjnego. ∎

Powiemy, że podstawienie v jest *bardziej ogólne* niż podstawienie u (będziemy to oznaczać przez $v \leq u$), gdy istnieje podstawienie v' takie, że

$$v'(v(x)) = u(x) \tag{49}$$

zachodzi dla dowolnych $x \in X$. Łatwo jest podać przykład świadczący o tym, że relacja $\leq$ nie jest antysymetryczna.

Niech $S \subseteq FT(\Sigma, X) \times FT(\Sigma, X)$ będzie zbiorem par termów. Powiemy, że podstawienie v *unifikuje* zbiór S, gdy dla każdej pary $\langle \sigma, \tau \rangle \in S$,

$$v(\sigma) = v(\tau).$$

Powiemy, że zbiór S jest *unifikowalny*, gdy istnieje podstawienie, które go unifikuje. Każde takie podstawienie będziemy nazywać *unifikatorem* zbioru S. Powiemy, że para termów $\langle \sigma, \tau \rangle$ jest unifikowalna, gdy zbiór $\{\langle \sigma, \tau \rangle\}$ jest unifikowalny.

Fakt 10.2 *Dla dowolnego zbioru S i podstawienia v, jeśli v unifikuje S oraz $v \leq u$, to u też unifikuje S.*

Dowód: Jeśli $v \leq u$ oraz v' jest podstawieniem spełniającym (49) to dla każdego termu $\sigma \in FT(\Sigma, X)$,

$$v'(v(\sigma)) = u(\sigma).$$

Oczywisty dowód powyższej równości (indukcja strukturalna po σ) pozostawimy czytelnikowi. Z powyższej równości wynika natychmiast, że jeśli v było unifikatorem S to u jest też unifikatorem S. ∎

Przykład 10.3 Załóżmy, że w sygnaturze mamy stałą c oraz dwa symbole dwuargumentowe f, oraz g.

(i) Para $\langle c, f(x,x) \rangle$ nie jest unifikowalna bo przy każdym podstawieniu v, zachodzi $v(c) = c$ oraz $v(f(x,x)) = f(v(x), v(x))$ i oczywiście termy c i $f(\sigma, \sigma)$ nie są równe przy każdym wyborze termu σ. Z podobnych powodów para $\langle f(x,y), g(x,y) \rangle$ nie jest unifikowalna.

(ii) Para $\langle x, f(x,c) \rangle$ też nie jest unifikowalna, ale powody teraz są inne. Gdyby v unifikowało tę parę to mielibyśmy

$$v(x) = f(v(x), c).$$

Zatem term $v(x)$ zawierałby samego siebie jako swój właściwy podterm. To jednak nie jest możliwe dla skończonych termów, gdyż jeśli k jest długością najdłuższej drogi w $v(x)$, to najdłuższa droga w $f(v(x), c)$ ma długość $k + 1$.

(iii) Rozważmy parę, w której lewym argumentem jest term

$$f(x_1, f(x_2, f(\ldots, f(x_n, x_{n+1})\ldots))),$$

a prawym argumentem jest term otrzymany z poprzedniego przez zastąpienie każdej zmiennej x_i termem $f(x_{i-1}, x_{i-1})$, dla $i = 1, \ldots, n+1$. Sprawdzanie czy dana para termów jest unifikowalna polega na rozwiązywaniu stosownego równania w algebrze termów. W naszym przykładzie poszukujemy rozwiązań na zmienne $x_0, \ldots, x_{n+1}$. Podstawowa własność algebry termów, z której tutaj korzystamy to prawo "skracania". W naszym przykładzie dostajemy natychmiast $n+1$ równań

$$x_1 = f(x_0, x_0),\ \ldots\ ,\ x_{n+1} = f(x_n, x_n).$$

Wykonując odpowiednie podstawienia dostajemy rozwiązanie, które dla $i = 1, \ldots, n+1$, każdej zmiennej x_i przyporządkowuje term będący pełnym drzewem binarnym wysokości i zbudowanym z symbolu f oraz z liści etykietowanych zmienną x_0. Powyższe rozwiązanie wyznacza podstawienie, które jest unifikatorem pary z naszego przykładu. Zauważmy, że znaleziony unifikator jest w pewnym intuicyjnym sensie minimalny, tzn nie ma mniejszego podstawienia unifikującego tę parę. Własność ta zostanie sformalizowana później. Zauważmy też, że rozmiar termu przyporządkowanego zmiennej x_{n+1} jest wykładniczy od rozmiaru oryginalnej pary, którą unifikowaliśmy.

10.1 Algorytm unifikacji

Przedstawimy algorytm, który dla danej pary termów $\langle \sigma_1, \sigma_2 \rangle$ sprawdza czy są one unifikowalne i jeśli są, to znajduje unifikator tej pary. Działanie algorytmu będzie polegało na próbie zunifikowania wszystkich par znajdujących się na stosie S. Początkowo stos będzie zawierał jedynie parę $\langle \sigma_1, \sigma_2 \rangle$. Algorytm kończy pracę z chwilą odkrycia sprzeczności przy próbie unifikacji stosu lub z chwilą gdy stos staje się pusty (a zatem oczywiście unifikowalny). Dodatkowo, algorytm będzie przechowywał informację o konstruowanym podstawieniu w skończonym zbiorze P par postaci: $\langle$zmienna, term$\rangle$. Początkowo P jest pusty.

Tak długo jak stos jest niepusty, algorytm powtarza następujący makro krok.

Makro krok

M-1. Zdejmujemy z wierzchołka stosu parę $\langle \tau_1, \tau_2 \rangle$. Jeśli $\tau_1 = \tau_2$ to na tym kończymy makro krok. Jeśli termy te nie są równe, to przechodzimy do następnego kroku.

M-2. Jeśli τ_1 jest zmienną, powiedzmy x, to sprawdzamy czy x występuje w τ_2. Jeśli tak, to algorytm przerywa pracę z komunikatem ``nie ma unifikacji''. Jeśli x nie występuje w τ_2, to podstawiamy τ_2 na wszystkie wystąpienia x w stosie S i w zbiorze P oraz dodajemy do P parę $\langle x, \tau_2 \rangle$. Na tym kończymy makro krok.

Jeśli τ_1 nie jest zmienną, to przechodzimy do następnego kroku.

M-3. Jśli τ_2 jest zmienną, to wykonujemy wszystkie czynności poprzedniego kroku na parze $\langle \tau_2, \tau_1 \rangle$.

Jeśli τ_2 nie jest zmienną to przechodzimy do następnego kroku.

M-4. W tej sytuacji τ_1 musi mieć postać $f(\rho_1, \ldots, \rho_n)$ oraz τ_2 musi mieć postać $g(\rho'_1, \ldots, \rho'_m)$ dla pewnego $f \in \Sigma_n$ oraz $g \in \Sigma_m$ (przypadek $n = 0$ lub $m = 0$ również dopuszczamy). Jeśli f i g są różnymi symbolami, to algorytm kończy pracę z komunikatem ``nie ma unifikacji´´. Jeśli natomiast $f = g$, to $m = n$ i algorytm wpisuje na stos pary: $\langle \rho_1, \rho'_1 \rangle$, ..., $\langle \rho_n, \rho'_n \rangle$. Na tym kończymy makro krok.

W następnych dwóch paragrafach udowodnimy *poprawność* powyższego algorytmu, tzn pokażemy, że algorytm zatrzymuje się przy każdych danych wejściowych (jest to własność *terminacji algorytmu*) oraz, że zawsze jeśli algorytm daje wynik, to wynik ten jest poprawny (jest to własność nazywana *częściową poprawnością*).

W dalszej części tego rozdziału będziemy używać następujących oznaczeń. Dla liczby $n \geq 0$ przypuśćmy, że algorytm wykonuje co najmniej n makro kroków. Wówczas przez S_n będziemy oznaczać zawartość stosu po wykonaniu n makro kroków. Podobne oznaczenie stosujemy do P_n. Tak więc $S_0 = \langle \sigma_1, \sigma_2 \rangle$ oraz $P_0 = \emptyset$. Powiemy, że para $\langle x, \tau \rangle$ *pojawia się* w n-tym kroku algorytmu jeśli n-te wykonanie makro kroku kończy się w punkcie (M-2) lub (M-3) podstawieniem τ na x.

Jeśli $P \subseteq X \times FT(\Sigma, X)$ jest funkcją częściową, to przez $\tilde{P}$ będziemy oznaczać podstawienie $\tilde{P} : X \to FT(\Sigma, X)$ naturalnie rozszerzającę P,

$$\tilde{P}(x) = \begin{cases} P(x) & \text{jeśli } x \in dom(P), \\ x & \text{jeśli } x \notin dom(P). \end{cases}$$

10.2 Terminacja algorytmu

Dla skończonego zbioru S par termów niech $\sharp S$ oznacza parę liczb $\langle m, n \rangle \in N^2$, gdzie m jest sumą długości wszystkich termów z S oraz n jest liczbą różnych zmiennych występujących w S.

Przypomnijmy, że zbiór N^2 z relacją porządku $\leq_p$ zdefiniowaną poniżej jest dobrze ufundowany (zob. Zadanie 8.3).

$$\langle m_1, n_1) \rangle \leq_p \langle m_2, n_2 \rangle \quad \text{wtw, gdy} \quad n_1 < n_2 \text{ lub } (n_1 = n_2 \text{ oraz } m_1 \leq m_2).$$

Będziemy pisać $\langle m_1, n_1 \rangle <_p \langle m_2, n_2 \rangle$ dla oznaczenia: $\langle m_1, n_1 \rangle \leq_p \langle m_2, n_2 \rangle$ oraz $\langle m_1, n_1 \rangle \neq \langle m_2, n_2 \rangle$.

Lemat 10.4 *Jeśli algorytm wykonuje co najmniej $n+1$ kroków, to*

$$\sharp S_{n+1} <_p \sharp S_n.$$

Dowód: Indukcja ze względu na n. Przejście od stosu S_n do S_{n+1} następuje albo przez wykonanie podstawienia (część (M-2) lub (M-3) algorytmu) – wówczas suma długości termów na stosie może wzrosnąć, ale zmniejsza się o jeden liczba zmiennych (zmienna, na którą podstawiamy zostaje wyeliminowna); albo przez zastąpienie wierzchołka stosu, który jest postaci

$$\langle f(\rho_1, \ldots, \rho_m), f(\rho'_1, \ldots, \rho'_m)\rangle$$

ciągiem elementów

$$\langle \rho_1, \rho'_1\rangle \cdots \langle \rho_m, \rho'_m\rangle.$$

W tym przypadku liczba zmiennych występujących na stosie nie zmienia się ale suma długości termów jest mniejsza o 2. To kończy dowód. ∎

Zatem ponieważ zbiór $\langle N^2, \leq_p\rangle$ jest dobrze ufundowany, to na mocy Lematu 10.4, algorytm musi się zatrzymać przy każdych danych wejściowych. Tym samym otrzymujemy następującą własność.

Twierdzenie 10.5 (Terminacja)
Dla każdych danych wejściowych $\langle \sigma_1, \sigma_2\rangle$ algorytm zatrzymuje sie z pewnym wynikiem.

10.3 Częściowa poprawność algorytmu

W tym paragrafie udowodnimy następujące twierdzenie

Twierdzenie 10.6 (Częściowa poprawność)
Dla dowolnej pary termów $\langle \sigma_1, \sigma_2\rangle$ stanowiącej wejście dla algorytmu:

(i) jeśli algorytm zatrzymuje się z komunikatem ``nie ma unifikacji'', to para $\langle \sigma_1, \sigma_2\rangle$ nie jest unifikowalna;

(ii) jeśli algorytm zatrzymuje się z pustym stosem i z wynikiem P, to $P \subseteq X \times FT(\Sigma, X)$ jest funkcją częściową oraz $\tilde{P}$ jest unifikatorem pary $\langle \sigma_1, \sigma_2\rangle$.

Lemat 10.7 *Jeśli podstawienie v unifikuje $\langle \sigma_1, \sigma_2\rangle$, to dla każdego n, jeśli algorytm dla danych wejściowych $\langle \sigma_1, \sigma_2\rangle$ wykonuje co najmniej n kroków, to v unifikuje S_n.*

Dowód: Indukcja ze względu na n. Dla $n = 0$ teza wynika z założeń lematu. Załóżmy, że v unifikuje S_n oraz, że algorytm wykonuje co najmniej $n + 1$ kroków. Rozważmy następujące dwa możliwe przypadki.

Przypadek (I) W $(n + 1)$-szym kroku algorytmu pojawia sie para $\langle x, \tau \rangle$. Jeśli krok ten kończy się w punkcie (M-2), to

$$S_n = \langle x, \tau \rangle \langle \xi_1, \xi_1' \rangle \cdots \langle \xi_m, \xi_m' \rangle$$

oraz

$$S_{n+1} = \langle \xi_1(\tau/x), \xi_1'(\tau/x) \rangle \cdots \langle \xi_m(\tau/x), \xi_m'(\tau/x) \rangle.$$

Jeśli natomiast krok ten się kończy w punkcie (M-3), to pierwszym elementem stosu S_n jest para (τ, x), pozostałe elementy są jak wyżej.

Z założenia indukcyjnego wiemy, że v unifikuje S_n, zatem

$$v(x) = v(\tau). \tag{50}$$

Zatem, na mocy Twierdzenia 10.1 oraz założenia indukcyjnego, dla każdego $1 \leq i \leq m$,

$$v(\xi_i(\tau/x)) = v(\xi_i) = v(\xi_i') = v(\xi_i'(\tau/x)).$$

Powyższe równości oraz (50) dowodzą, że v unifikuje S_{n+1}.

Przypadek (II) W $(n + 1)$-szym kroku działanie algorytmu kończy się w punkcie (M-4). Wówczas S_n nie może się zaczynać od pary postaci $\langle f(\rho_1, \ldots, \rho_k), g(\rho_1', \ldots, \rho_m') \rangle$, gdzie f i g są różne. Zatem:

$$S_n = \langle f(\rho_1, \ldots, \rho_k), f(\rho_1', \ldots, \rho_k') \rangle \langle \xi_1, \xi_1' \rangle \cdots \langle \xi_m, \xi_m' \rangle$$

oraz

$$S_{n+1} = \langle \rho_1, \rho_1' \rangle \cdots \langle \rho_k, \rho_k' \rangle \langle \xi_1, \xi_1' \rangle \cdots \langle \xi_m, \xi_m' \rangle.$$

Ponieważ każde podstawienie unifikujące S_n unifikuje też S_{n+1}, to korzystając z założenia indukcyjnego otrzymujemy tezę. ∎

Zauważmy, że z Lematu 10.7 wynika natychmiast pierwsza część Twierdzenia 10.6 bowiem w chwili zatrzymania algorytmu z komunikatem ``nie ma unifikacji´´stos S nie jest unifikowalny.

Lemat 10.8 *Dla każdego n, jeśli algorytm wykonuje co najmniej n kroków to $P_n \subseteq X \times FT(\Sigma, X)$ jest funkcją częściową oraz żadna ze zmiennych z $dom(P_n)$ nie występuje w żadnym z termów z S_n.*

Dowód: Dowodzimy przez indukcję ze względu na n. Dla $n = 0$ teza oczywiście zachodzi. Załóżmy, że P_n spełnia tezę oraz, że algorytm wykonuje co najmniej $n + 1$ kroków i $P_n \neq P_{n+1}$. Zatem w $n + 1$-szym kroku musiała się pojawić para $\langle x, \tau \rangle$. Ponieważ zmienna x występowała na stosie S, to z założenia indukcyjnego wynika, że $x \notin dom(P_n)$ zatem dodanie pary $\langle x, \tau \rangle$ nie psuje własności funkcji częściowej. Ponieważ podstawialiśmy τ na x w S_n oraz x nie występowało w τ, to w S_{n+1} zmienna x nie występuje. Zatem ponownie korzystając z założenia indukcyjnego wnioskujemy, że żadna ze zmiennych z $dom(P_{n+1})$ nie występuje w termach z S_{n+1}. To kończy dowód. ∎

Lemat 10.9 *Załóżmy, że w n-tym kroku algorytmu pojawia się para $\langle x, \tau \rangle$. Wówczas dla każdego $m \geq n$, jeśli algorytm wykonuje co najmniej m kroków, to*

$$\tilde{P}_m(x) = \tilde{P}_m(\tau).$$

Dowód: Indukcja ze względu na m spełniające: $m \geq n$ oraz takie, że algorytm wykonuje co najmniej m kroków. Jeśli $m = n$ to $\tilde{P}_n(x) = \tau$ oraz zauważmy, że ponieważ żadna ze zmiennych występujących w τ nie należy do $dom(P_n)$ (wynika to z Lematu 10.8 oraz z faktu, że x nie występuje w τ), to $\tilde{P}_n(\tau) = \tau$, co daje tezę.

Załóżmy, że teza lematu zachodzi dla m, że algorytm wykonuje co najmniej $m+1$ kroków oraz, że $P_m \neq P_{m+1}$. Oznacza to, że w $m+1$-szym kroku algorytmu pojawia się pewna para, powiedzmy $\langle y, \rho \rangle$. Zauważmy, że z opisu algorytmu wynika natychmiast, że

$$\tilde{P}_{m+1} = v\,\tilde{P}_m, \tag{51}$$

gdzie v jest postawieniem termu ρ na zmienną y, czyli

$$v(z) = \begin{cases} \rho & \text{jeśli } z = y, \\ z & \text{jeśli } z \neq y. \end{cases}$$

Korzystając z (51) oraz z założenia indukcyjnego natychmiast dostajemy tezę lematu dla $m + 1$. To kończy dowód. ∎

Lemat 10.10 *Załóżmy, że algorytm po wykonaniu M kroków zatrzymał się z wynikiem P i pustym stosem. Wówczas dla każdego $n \leq M$, podstawienie $\tilde{P}$ unifikuje S_n.*

Dowód: Indukcja ze względu na n w zbiorze $\{0, \ldots, M\}$ uporządkowanym przez $\leq^{-1}$. Dla $n = M$ teza oczywiście zachodzi bo $S_M = \emptyset$. Załóżmy, że $\tilde{P}$ unifikuje S_{n+1} dla pewnego $n + 1 \leq M$. Rozważmy następujące dwa możliwe przypadki.

Przypadek (I) W $n+1$-szym kroku algorytmu pojawia sie para $\langle x, \tau\rangle$. Jeśli krok ten kończy się w punkcie (M-2), to

$$S_n = \langle x, \tau\rangle\langle \xi_1, \xi_1'\rangle \cdots \langle \xi_m, \xi_m'\rangle$$

oraz

$$S_{n+1} = \langle \xi_1(\tau/x), \xi_1'(\tau/x)\rangle \cdots \langle \xi_m(\tau/x), \xi_m'(\tau/x)\rangle.$$

Jeśli natomiast krok ten się kończy w punkcie (M-3), to pierwszym elementem stosu S_n jest para $\langle \tau, x\rangle$, pozostałe elementy są jak wyżej.

Na mocy Lematu 10.9 mamy

$$\tilde{P}(x) = \tilde{P}(\tau). \tag{52}$$

Zatem, na mocy Twierdzenia 10.1 oraz założenia indukcyjnego, dla każdego $1 \leq i \leq m$,

$$\tilde{P}(\xi_i) = \tilde{P}(\xi_i(\tau/x)) = \tilde{P}(\xi_i'(\tau/x)) = \tilde{P}(\xi_i').$$

Powyższe równości oraz (52) dowodzą, że $\tilde{P}$ unifikuje S_n.

Przypadek (II) W $n+1$-szym kroku działanie algorytmu kończy się w punkcie (M-4). Wówczas

$$S_n = \langle f(\rho_1, \ldots, \rho_k), f(\rho_1', \ldots, \rho_k')\rangle\langle \xi_1, \xi_1'\rangle \cdots \langle \xi_m, \xi_m'\rangle$$

oraz

$$S_{n+1} = \langle \rho_1, \rho_1'\rangle \cdots \langle \rho_k, \rho_k'\rangle\langle \xi_1, \xi_1'\rangle \cdots \langle \xi_m, \xi_m'\rangle.$$

Ponieważ każde podstawienie unifikujące S_{n+1} unifikuje też S_n, to korzystając z założenia indukcyjnego otrzymujemy tezę. ■

Zauważmy, że z Lematu 10.8 oraz z Lematu 10.10 wynika natychmiast druga część Twierdzenia 10.6, co kończy dowód poprawności algorytmu.

10.4 Najbardziej ogólny unifikator

Zacznijmy od następującego lematu.

Lemat 10.11 *Jeśli v jest dowolnym unifikatorem pary $\langle \sigma_1, \sigma_2\rangle$ oraz algorytm wykonuje co najmniej n kroków dla danych wejściowych $\langle \sigma_1, \sigma_2\rangle$, to*

$$v = v\tilde{P}_n.$$

Dowód: Dowodzimy przez indukcję ze względu na n, gdzie n jest nie większe od liczby kroków algorytmu dla powyższej pary. Dla $n = 0$ teza jest oczywista, gdyż $P_0 = \emptyset$. Załóżmy tezę dla n i załóżmy, że algorytm wykonuje co najmniej $n+1$ kroków. Ponadto załóżmy,

że $P_n \neq P_{n+1}$. Oznacza to, że w $n+1$ kroku pojawia się pewna para, powiedzmy $\langle x, \tau \rangle$. Wówczas P_n ma postać

$$P_n = \{\langle y_1, \xi_1 \rangle, \ldots, \langle y_k, \xi_k \rangle\}$$

oraz P_{n+1} ma postać

$$P_{n+1} = \{\langle x, \tau \rangle, \langle y_1, \xi_1(\tau/x) \rangle, \ldots, \langle y_k, \xi_k(\tau/x) \rangle\}.$$

Ponieważ para $\langle x, \tau \rangle$ występuje na stosie S_n, to na mocy Lematu 10.7

$$v(x) = v(\tau). \tag{53}$$

Zatem, korzystając z założenia indukcyjnego, (53) oraz z Twierdzenia 10.1, dostajemy

$$v(y_i) = v(\xi_i) = v(\xi_i(\tau/x)) = v(\tilde{P}_{n+1}(y_i)).$$

Ponadto (53) daje

$$v(x) = v(\tilde{P}_{n+1}(x)).$$

Zatem pokazaliśmy, że dla wszystkich zmiennych $z \in X$,

$$v(z) = v(\tilde{P}_{n+1}(z)).$$

Powyższa równość przenosi się na równość dla dowolnego termu σ (oczywisty dowód indukcyjny ze względu na budowę termu σ pozostawiamy czytelnikowi)

$$v(\sigma) = v(\tilde{P}_{n+1}(\sigma)),$$

co kończy dowód lematu. ■

Poniższe twierdzenie pokazuje, że podstawienie znajdowane przez nasz algorytm jest najbardziej ogólnym unifikatorem dla pary wejściowej $\langle \sigma_1, \sigma_2 \rangle$, o ile para ta jest unifikowalna.

Twierdzenie 10.12 *Jeśli para $\langle \sigma_1, \sigma_2 \rangle$ jest unifikowalna i v jest jej dowolnym unifikatorem oraz P jest wynikiem, z którym algorytm zatrzymuje się dla powyższej pary na wejściu, to*

$$\tilde{P} \leq v.$$

Dowód: Z Lematu 10.11 otrzymujemy, że

$$v = v\tilde{P}$$

Zatem $\tilde{P} \leq v$. ■

Zadania

10.1. Niech x, y będą dwoma różnymi zmiennymi oraz niech $\tau, \rho \in FT(\Sigma, X)$ będą dowolnymi termami takimi, że $\tau \neq x$ oraz $\rho \neq y$. Dla dowolnego termu $\sigma \in FT(\Sigma, X)$ zdefiniujmy podstawienie $\sigma(\tau/x,\ \rho/y)$ jako $v(\sigma)$, gdzie $v : X \to FT(\Sigma, X)$ jest podstawieniem zdefiniowanym następująco

$$v(z) = \begin{cases} \tau, & \text{jeśli } z = x, \\ \rho, & \text{jeśli } z = y, \\ z, & \text{jeśli } z \neq x,\ z \neq y. \end{cases}$$

Wyznaczyć wszystkie czwórki $\langle \tau, x, \rho, y \rangle$ takie, że dla każdego $\sigma \in FT(\Sigma, X)$ zachodzi:

a. $\sigma(\tau/x,\ \rho/y) = \sigma(\tau/x)(\rho/y)$.

b. $\sigma(\tau/x)(\rho/y) = \sigma(\rho/y)(\tau/x)$.

10.2. Udowodnić, że jeśli algorytm unifikacji (zob. paragraf 10.1) uruchomimy na nieskończonym stosie S zawierającym pary termów, oraz algorytm się zatrzyma, to S nie jest unifikowalny. Udowodnić ponadto, że jeśli w termach z S występuje tylko skończenie wiele różnych zmiennych oraz algorytm się nie zatrzyma, to S jest unifikowalny. Czy założenie o skończonej liczbie różnych zmiennych w S jest istotne?

10.3. Niech S będzie zbiorem par termów z $FT(\Sigma, X)$ (S może być nieskończony), zawierającym skończenie wiele różnych zmiennych. Dowieść, że S jest unifikowalny wtw, gdy każdy skończony podzbiór S jest unifikowalny. Podać przykład, że założenie skończoności zbioru zmiennych występujących w S jest istotne.

10.4. Dowieść, że dla podstawień v, u, zachodzi $v \leq u$ oraz $u \leq v$ wtw, gdy istnieją podzbiory $X_1, X_2 \subseteq X$ oraz bijekcja $f : X_1 \to X_2$ taka, że $fv = u$.

10.5. Oszacować od góry liczbę kroków algorytmu unifikacji (zob. dział 10.1) w zależności od sumy długości termów na wejściu tego algorytmu.

10.6. Załóżmy, że zbiór S par termów jest unifikowalny. Niech v_* będzie najbardziej ogólnym unifikatorem dla S. Dla podstawienia u niech uS oznacza zbiór $uS = \{\langle u(\tau), u(\rho)\rangle \mid \langle \tau, \rho\rangle \in S\}$. Dowieść, że dla dowolnego podstawienia u, zbiór uS jest unifikowalny wtw, gdy istnieje podstawienie v takie, że $v_* \leq v$ oraz $u \leq v$.

11 Rachunek zdań

W tej części omówimy pewne elementy rachunku zdań. Zaczniemy od składni, następnie podamy semantykę formuł, później omówimy trzy postawowe style systemów dowodzenia: system hilbertowski, naturalnej dedukcji oraz system gentzenowski. Ostanie dwie części będą zawierały wprowadzenie do logiki intuicjonistycznej oraz elementy teorii modeli.

11.1 Składnia

Niech P będzie nieskończonym przeliczalnym zbiorem. Elementy zbioru P będziemy nazywać *zmiennymi zdaniowymi*. Zmienne będziemy oznaczać $p, q, \ldots$, ewentualnie z indeksami. *Formuły rachunku zdań* są termami ze zbioru $FT(\Sigma, P)$, gdzie sygnatura Σ zawiera symbol stałej $\bot$ (*fałsz*) oraz trzy symbole operacji dwuargumentowych: $\vee$ (*alternatywa*), $\wedge$ (*koniunkcja*) oraz $\to$ (*implikacja*). Elementy sygnatury Σ nazywamy *spójnikami zdaniowymi*. Formuły rachunku zdań będziemy oznaczać $\alpha, \beta, \gamma, \ldots$. Operacje będziemy zapisywać w postaci infiksowej, tzn zamiast na przykład $\vee(\alpha, \beta)$ będziemy pisać $(\alpha \vee \beta)$.

W dalszej części notatek będziemy używać następującego skrótu: dla dowolnej formuły α, napis $\neg\alpha$ będzie oznaczał formułę $\alpha \to \bot$. Formuła $\neg\alpha$ nazywa się *negacją* formuły α.

11.2 Semantyka

W poprzedniej częśći opisaliśmy składnię formuł, tzn opisaliśmy jak wyglądają poprawnie zbudowane napisy zwane formułami. Obecnie opiszemy znaczenie tych napisów czyli podamy semantykę formuł. Niech $\mathfrak{B}$ będzie Σ-algebrą zdefiniowaną następująco. Nośnikiem $\mathfrak{B}$ jest zbiór $\{0, 1\}$, interpretacją stałej $\bot$ jest 0, interpretacją $\vee$ jest operacja maksimum, interpretacją $\wedge$ jest operacja mimnimum oraz interpretacją $\to$ jest funkcja charakterystyczna porządku w $\{0, 1\}$, w którym $0 \leq 1$.

Dana jest formuła α oraz wartościowanie $v : P \to \{0, 1\}$, mówimy, że α jest *spełniona* przez wartościowanie v i oznaczamy przez $\models \alpha[v]$, gdy $\alpha^{\mathfrak{B}}[v] = 1$. Zgodnie z powyższą definicją struktury $\mathfrak{B}$ mamy następujące własności dla dowolnego wartościowania v.

$$\text{nie zachodzi } \models \bot[v]$$

$$\models (\alpha \vee \beta)[v] \quad \text{wtw, gdy} \quad \models \alpha[v] \text{ lub } \models \beta[v]$$

$$\models (\alpha \wedge \beta)[v] \quad \text{wtw, gdy} \quad \models \alpha[v] \text{ oraz } \models \beta[v]$$

$$\models (\alpha \to \beta)[v] \quad \text{wtw, gdy} \quad \text{jeśli } \models \alpha[v] \text{ to } \models \beta[v]$$

Zauważmy, że zgodnie z naszą definicją negacji szczególnym przypadkiem powyższej własności implikacji i fałszu jest następująca równoważność.

$$\models (\neg\alpha)[v] \quad \text{wtw, gdy nie zachodzi} \quad \models \alpha[v].$$

Formułę α nazwiemy *tautologią*, gdy jest ona spełniona przez wszystkie wartościowania, tzn gdy dla każdego wartościowania v zachodzi $\models \alpha[v]$. Formuły rachunku zdań przedstawiają schematy zdań, w których atomowe zdania (zmienne zdaniowe) stanowią miejsca na wstawianie konkretnych zdań. Wartość logiczna całego takiego schematu zależy jedynie od wartości logicznych wstawianych zdań. Tautologie są to takie schematy, które dają zawsze zdanie prawdziwe bez względu na prawdziwość zdań atomowych.

Przykład 11.1 Formuły

$$(p \to p)$$
$$(p \to (q \to p))$$
$$(p \to (q \to r)) \to ((p \to q) \to (p \to r))$$
$$(\neg p \to \neg q) \to ((\neg p \to q) \to q)$$

są tautologiami. Pozostawimy czytelnikowi sprawdzenie tego faktu.

Ogólnie, jeśli dana formuła α ma n zmiennych zdaniowych to aby sprawdzić czy jest ona tautologią wystarczy sprawdzić jej wartość logiczną dla wszystkich możliwych wartościowań przyporządkowujących wartości jedynie zmiennym występującym w tej formule. Takich wartościowań jest 2^n. Tak więc, sprawdzenie według tego algorytmu czy dana formuła jest tautologią zajmie wykładniczą liczbę kroków w zależności od liczby zmiennych (o zatem od rozmiaru) formuły. Nie jest znany żaden algorytm działający w liczbie kroków wielomianowo zależącej od rozmiaru formuły, pozwalający sprawdzić czy dana formuła jest tautologią. Pytanie czy taki algorytm istnieje stanowi jeden z głośnych otwartych problemów teoretycznej informatyki.

Powiemy, że dwie formuły α i β są *równoważne* (przyjmujemy oznaczenie $\models \alpha \leftrightarrow \beta$), gdy przyjmują one te same wartości logiczne dla wszystkich wartościowań. Zatem

$$\models \alpha \leftrightarrow \beta \text{ wtw, gdy } \models (\alpha \to \beta) \wedge (\beta \to \alpha).$$

Innymi słowy formuły α i β są równoważne, gdy równość[14] $\alpha = \beta$ jest prawdziwa w algebrze $\mathcal{B}$, tzn. gdy

$$\mathcal{B} \models \alpha = \beta$$

Spójniki zdaniowe, które podaliśmy wyżej nie stanowią minimalnego zbioru spójników, tzn. niektóre z nich można zdefiniować przy pomocy pozostałych. Przykładowo koniunkcję i alternatywę można zdefiniować opierając się na implikacji i negacji

$$\models (\alpha \wedge \beta) \leftrightarrow \neg(\alpha \to \neg\beta)$$

[14]Tutaj formuły traktujemy jak termy nad odpowiednią sygnaturą.

oraz

$$\models (\alpha \vee \beta) \leftrightarrow (\neg\alpha \rightarrow \beta).$$

Oznacza to, że moglibyśmy oprzeć definicję formuł na tylko dwóch symbolach $\rightarrow$ oraz $\bot$ i pozostałe dwa zdefiniować przy pomocy powyższych równoważności.

11.3 Systemy dowodzenia

Systemy dowodzenia służą formalnemu wyprowadzaniu wyrażeń postaci $\Delta \vdash \alpha$, gdzie Δ jest zbiorem formuł (dopuszczamy zbiory nieskończone) oraz α jest formułą. Napisy te będziemy nazywać *sekwentami*. Sekwent $\emptyset \vdash \alpha$ będziemy oznaczać $\vdash \alpha$. Możliwość wyprowadzenia sekwentu $\Delta \vdash \alpha$ w danym systemie czytamy jako "α jest dowodliwa ze zbioru hipotez Δ". Każdy system dowodzenia zawiera dwa składniki:

- początkowy zbiór sekwentów, których nie musimy dowodzić – sekwenty te są nazywane *aksjomatami*;
- zbiór reguł przekształcania sekwentów w sekwenty – te reguły są nazywane *regułami dowodzenia*.

Reguły dowodzenia opisują warunki, przy pomocy których można otrzymać nowy sekwent (nazywany *konkluzją*) z otrzymanych już sekwentów (nazywanych *przesłankami*). *Dowodem* sekwentu $\Delta \vdash \alpha$ nazywamy skończone drzewo etykietowane sekwentami tak, że etykietą korzenia jest $\Delta \vdash \alpha$, etykietami liści są aksjomaty oraz etykiety wierzchołków wewnętrznych są otrzymane z etykiet ich potomków zgodnie z regułami systemu, tzn. etykieta danego wierzchołka wewnętrznego jest wynikiem zastosowania jednej z reguł systemu do etykiet potomków tego wierzchołka.

W dalszej części opiszemy trzy systemy dowodzenia: sytem typu hilbertowskiego, sytem naturalnej dedukcji oraz gentzenowski rachunek sekwentów. Ostatnie dwa systemy znajdują zastosowanie w pewnych działach sztucznej inteligencji oraz systemach automatycznego dowodzenia twierdzeń.

11.3.1 System hilbertowski

Poniższy system dowodzenia dotyczy formuł zbudowanych przy użyciu jedynie spójnika $\rightarrow$, stałej $\bot$ oraz zmiennych zdaniowych. Przypomnijmy, że dla dowolnej formuły α, napis $\neg\alpha$ jest skrótem zapisu $\alpha \rightarrow \bot$. Symbol Δ w poniższym systemie oznacza dowolny zbiór formuł, a symbole α, β, γ oznaczają dowolne formuły.

Aksjomaty
(A0) $\Delta, \alpha \vdash \alpha$;
(A1) $\Delta \vdash \alpha \rightarrow (\beta \rightarrow \alpha)$;

(A2) $\Delta \vdash (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$;
(A3) $\Delta \vdash \neg\neg\alpha \to \alpha$

Reguła dowodzenia

$$(MP) \qquad \frac{\Delta \vdash \alpha;\ \Delta \vdash \alpha \to \beta}{\Delta \vdash \beta}$$

Powyższa reguła jest nazywana *regułą odrywania* lub też regułą modus ponens.

Fakt, że sekwent $\Delta \vdash \alpha$ daje się wyprowadzić w powyższym systemie będziemy zaznaczać przez $\Delta \vdash_H \alpha$, a sam system będziemy oznaczać przez $\vdash_H$.

Przykład 11.2 Pokażemy wyprowadzenie sekwentu $\vdash p \to p$ w powyższym systemie. Symbol ξ oznacza formułę $p \to ((p \to p) \to p) \to (((p \to (p \to p)) \to (p \to p))$ i jest wystąpieniem aksjomatu (A2).

$$\dfrac{\dfrac{\vdash \xi \qquad \vdash p \to ((p \to p) \to p)}{\vdash (p \to (p \to p)) \to (p \to p)} \qquad \vdash p \to (p \to p)}{\vdash p \to p}$$

Zauważmy, że w powyższym przykładzie możemy wszędzie zastąpić zmienną p przez dowolną formułę α dostając dowód sekwentu $\vdash \alpha \to \alpha$.

Następujące twierdzenie jest bardzo użyteczne przy wyprowadzaniu sekwentów w omawianym systemie.

Twierdzenie 11.3 (O dedukcji)
Dla dowolnego zbioru Δ formuł oraz dowolnych formuł α, β, jeśli $\Delta, \alpha \vdash_H \beta$, to $\Delta \vdash_H \alpha \to \beta$.

Dowód: Dowód jest indukcyjny ze względu na liczbę kroków w wyprowadzeniu sekwentu $\Delta, \alpha \vdash \beta$. Jeśli $\Delta, \alpha \vdash \beta$ jest aksjomatem to albo $\alpha = \beta$ i stosując wyprowadzenie z Przykładu 11.2 otrzymujemy $\Delta \vdash \alpha \to \alpha$, lub $\Delta \vdash \beta$ jest jednym z aksjomatów (Ai) dla i=0,1,2,3. Wówczas otrzymujemy $\Delta \vdash \alpha \to \beta$, stosując regułę odrywania do aksjomatu $\Delta \vdash \beta \to (\alpha \to \beta)$ oraz do $\Delta \vdash \beta$.

Załóżmy teraz, że ostatnim krokiem w wyprowadzeniu sekwentu $\Delta, \alpha \vdash \beta$ jest zastosowanie reguły (MP) do sekwentów $\Delta, \alpha \vdash \gamma \to \beta$ oraz $\Delta, \alpha \vdash \gamma$, dla pewnej formuły γ. Z założenia indukcyjnego istnieją wyprowadzenia $\Delta \vdash \alpha \to (\gamma \to \beta)$ oraz $\Delta \vdash \alpha \to \gamma$. Oznaczmy przez ξ formułę $(\alpha \to (\gamma \to \beta)) \to ((\alpha \to \gamma) \to (\alpha \to \beta))$, jest ona wystąpieniem aksjomatu (A2). Wyprowadzenie sekwentu wygląda wówczas następująco.

$$\dfrac{\dfrac{\Delta \vdash \xi \qquad \Delta \vdash \alpha \to (\gamma \to \beta)}{\Delta \vdash (\alpha \to \gamma) \to (\alpha \to \beta)} \qquad \Delta \vdash \alpha \to \gamma}{\Delta \vdash \alpha \to \beta}$$

To kończy dowód twierdzenia o dedukcji. ■

Powiemy, że formuła α jest *semantyczną konsekwencją* formuł ze zbioru Δ (oznaczamy to przez $\Delta \models \alpha$), jeśli każde wartościowanie spełniające wszystkie formuły z Δ spełnia też α.

Twierdzenie 11.4 (O adekwatności)
Jeśli $\Delta \vdash_H \alpha$, to $\Delta \models \alpha$. W szczególności, jeśli $\vdash_H \alpha$, to α jest tautologią.

Dowód: Dowód jest indukcyjny ze względu na liczbę kroków w wyprowadzeniu sekwentu $\Delta \vdash \alpha$. Jeśli $\Delta \vdash \alpha$ jest jednym z aksjomatów to oczywiście każde wartościowanie spełniające Δ spełnia też α.

Załóżmy teraz, że $\Delta \vdash \alpha$ jest otrzymany przez zastsownaie (MP) do sekwentów $\Delta \vdash \beta \to \alpha$ oraz $\Delta \vdash \beta$. Z założenia indukcyjnego mamy

$$\Delta \models \beta \to \alpha \text{ oraz } \Delta \models \beta. \tag{54}$$

Niech v będzie dowolnym wartościowaniem spełniającym wszystkie formuły z Δ. Zatem, na mocy (54), wartościowanie v spełnia $\beta \to \alpha$ oraz spełnia β. Wynika stąd, że v spełnia α. Tym samym udowodniliśmy, że $\Delta \models \alpha$. To kończy dowód. ■

Zajmiemy się teraz udowodnieniem implikacji odwrotnej do drugiej części Twierdzenia 11.4. Pokażemy, że każda tautologia jest twierdzeniem systemu $\vdash_H$.

Lemat 11.5 *Dla dowolnych formuł α, β zbudowanych przy użyciu $\to$ oraz $\bot$, następujące sekwenty są wyprowadzalne w systemie $\vdash_H$.*

(i) $\vdash \alpha \to (\neg\beta \to \neg(\alpha \to \beta))$;

(ii) $\vdash \bot \to \alpha$;

(iii) $\vdash (\alpha \to \beta) \to ((\neg\alpha \to \beta) \to \beta)$;

Dowód: Dla dowodu (i) zauważmy, że mamy następujące wyprowadzenie

$$\dfrac{\Delta \vdash \beta \to \bot \qquad \dfrac{\Delta \vdash \alpha \to \beta \qquad \Delta \vdash \alpha}{\Delta \vdash \beta}}{\Delta \vdash \bot}$$

Stosując do sekwentu $\Delta \vdash \bot$ trzy razy twierdzenie o dedukcji dostajemy

$$\vdash \alpha \to ((\beta \to \bot) \to ((\alpha \to \beta) \to \bot)).$$

Czyli

$$\vdash \alpha \to (\neg\beta \to \neg(\alpha \to \beta)).$$

Teraz udowodnimy (ii). Poniżej podajemy drzewo dowodu. Podwójną linią zaznaczamy zastosowanie twierdzenia o dedukcji.

$$\dfrac{\dfrac{\perp \vdash \neg\neg\alpha \to \alpha \qquad \dfrac{\perp,\ \neg\alpha \vdash \perp}{\perp \vdash \neg\neg\alpha}}{\perp \vdash \alpha}}{\vdash \perp \to \alpha}$$

Na koniec przedstawimy dowód (iii). Niech $\Delta = \{\alpha \to \beta, \neg\alpha \to \beta\}$. Oczywiście wystarczy pokazać wyprowadzenie sekwentu $\Delta \vdash \beta$. Stosując dwa razy twierdzenie o dedukcji do tego sekwentu otrzymamy tezę. Poniżej przedstawiamy drzewo dowodu sekwentu $\Delta \vdash \beta$.

$$\dfrac{\Delta \vdash \neg\neg\beta \to \beta \qquad \dfrac{\dfrac{\Delta, \neg\beta \vdash \neg\beta \qquad \dfrac{\dfrac{\Delta, \neg\beta \vdash \neg\alpha \to \beta \qquad \dfrac{\dfrac{\dfrac{\Delta, \alpha, \neg\beta \vdash \neg\beta \qquad \dfrac{\Delta, \alpha, \neg\beta \vdash \alpha \to \beta \qquad \Delta, \alpha, \neg\beta \vdash \alpha}{\Delta, \alpha, \neg\beta \vdash \beta}}{\Delta, \alpha, \neg\beta \vdash \perp}}{\Delta, \neg\beta \vdash \neg\alpha}}{\Delta, \neg\beta \vdash \beta}}{\Delta, \neg\beta \vdash \perp}}{\Delta \vdash \neg\neg\beta}}{\Delta \vdash \beta}$$

■

Lemat 11.6 (Kalmar)
Niech α będzie formułą zbudowaną przy użyciu $\to$ oraz $\perp$, o zmiennych zawartych w zbiorze $\{q_1, \ldots q_n\}$ i niech $v : P \to \{0,1\}$ będzie dowolnym wartościowaniem. Dla $i = 1, \ldots, n$ definiujemy formuły:

$$q_i' = \begin{cases} q_i & \text{jeśli } v(q_i) = 1, \\ \neg q_i & \text{jeśli } v(q_i) = 0. \end{cases}$$

Niech α' będzie formułą identyczną z α, jeśli $\models \alpha[v]$. Natomiast jeśli $\not\models \alpha[v]$, to jako α' bierzemy $\neg\alpha$. Wówczas

$$\{q_1', \ldots, q_n'\} \vdash_H \alpha'.$$

Dowód: Dowód jest prowadzony przez indukcję ze względu na budowę formuły α. Jeśli α jest zmienną q_i to $\alpha' = q_i'$. Zatem sekwent $\{q_1', \ldots, q_n'\} \vdash \alpha'$ jest aksjomatem.

Jeśli α jest stałą $\bot$, to $\alpha' = \neg\bot$ i oczywiście dla dowolnego wyboru $q_1', \ldots, q_n'$ zachodzi

$$\{q_1', \ldots, q_n'\} \vdash_H \neg\bot.$$

Załóżmy teraz,że α jest postaci $\beta \to \gamma$ i rozważmy następujące przypadki.
(A) $\not\models \beta[v]$.
Wówczas $\alpha' = \alpha$ oraz $\beta' = \neg\beta$. Z założenia indukcyjnego mamy $\{q_1', \ldots, q_n'\} \vdash_H \neg\beta$. Zatem $\{q_1', \ldots, q_n'\}, \beta \vdash_H \bot$. Z Lematu 11.5(ii) mamy $\{q_1', \ldots, q_n'\}, \beta \vdash_H \bot \to \gamma$. Zatem, stosując (MP) dostajemy $\{q_1', \ldots, q_n'\}, \beta \vdash_H \gamma$ i z twierdzenia o dedukcji

$$\{q_1', \ldots, q_n'\} \vdash_H \beta \to \gamma.$$

(B) $\models \gamma[v]$.
Wówczas $\alpha' = \alpha$, oraz $\gamma' = \gamma$. Z założenia indukcyjnego mamy $\{q_1', \ldots, q_n'\} \vdash_H \gamma$. Zatem $\{q_1', \ldots, q_n'\}, \beta \vdash_H \gamma$ i z twierdzenia o dedukcji dostajemy

$$\{q_1', \ldots, q_n'\} \vdash_H \beta \to \gamma.$$

(C) $\models \beta[v]$ oraz $\not\models \gamma[v]$.
Wówczas $\alpha' = \neg\alpha$. $\beta' = \beta$ oraz $\gamma' = \neg\gamma$. Z założenia indukcyjnego mamy

$$\{q_1', \ldots, q_n'\} \vdash_H \beta \text{ oraz } \{q_1', \ldots, q_n'\} \vdash_H \neg\gamma.$$

Z Lematu 11.5(i) mamy

$$\{q_1', \ldots, q_n'\} \vdash_H \beta \to (\neg\gamma \to \neg(\beta \to \gamma)).$$

Stosując do powyższego sekwentu dwukrotnie (MP) dostajemy

$$\{q_1', \ldots, q_n'\} \vdash_H \neg(\beta \to \gamma).$$

To kończy dowód lematu. ■

Lemat 11.7 *Dla dowolnego zbioru formuł Δ i dla dowolnych formuł α i β, jeśli $\Delta, \alpha \vdash_H \beta$ oraz $\Delta, \neg\alpha \vdash_H \beta$, to $\Delta \vdash_H \beta$.*

Dowód: Jeśli $\Delta, \alpha \vdash_H \beta$ to na mocy twierdzenia o dedukcji mamy $\Delta \vdash_H \alpha \to \beta$. Podobnie dostajemy $\Delta \vdash_H \neg\alpha \to \beta$. Stosując Lemat 11.5(iii), oraz dwukrotnie regułę odrywania dostajemy $\Delta \vdash_H \beta$. ■

Lemat Kalmara odgrywa kluczową rolę w dowodzie poniższego twierdzenia o pełności.

Twierdzenie 11.8 (O pełności dla $\vdash_H$)
Jeśli α jest tautologią zbudowaną przy użyciu $\rightarrow$ oraz $\bot$, to $\vdash_H \alpha$.

Dowód: Załóżmy, że α jest tautologią. Niech $\{q_1, \ldots, q_n\}$ będą wszystkimi zmiennymi występującymi w α. Dla dowolnej liczby $0 \leq m \leq n$ nazwiemy *m-zbiorem* każdy zbiór formuł $\{q'_1, \ldots, q'_m\}$, gdzie q'_i jest albo q_i lub $\neg q_i$. Zauważmy, że 0-zbiór jest pusty.

Udowodnimy następującą własność:

$$\text{dla każdego } 0 \leq m \leq n, \text{ jeśli } \Delta \text{ jest } m\text{-zbiorem, to } \Delta \vdash_H \alpha. \tag{55}$$

Zauważmy, że biorąc $m = 0$ w (55) dostajemy tezę twierdzenia. Dowód (55) przeprowadzimy przez indukcję ze względu na m w zbiorze $\{0, \ldots, n\}$ uporządkownym relacją $\leq^{-1}$. Dla $m = n$ (55) wynika z Lematu 11.6 oraz z faktu, że α jest tautologią. Załóżmy, że (55) zachodzi dla $m + 1 \leq n$ i niech Δ będzie dowolnym m-zbiorem. Z założenia indukcyjnego dostajemy

$$\Delta, q_{m+1} \vdash_H \alpha$$

oraz

$$\Delta, \neg q_{m+1} \vdash_H \alpha.$$

Zatem na mocy Lematu 11.7 dostajemy

$$\Delta \vdash_H \alpha.$$

To kończy dowód (55) i tym samym twierdzenia o pełności. ■

Powyższy system można łatwo rozszerzyć do systemu dla formuł opartych o pozostałe spójniki logiczne. Wystarczy w tym celu dodać jako aksjomaty sekwenty wyrażające równoważności definiujące te spójniki.
(A4) $\Delta \vdash (\alpha \wedge \beta) \rightarrow \neg(\alpha \rightarrow \neg\beta)$
(A5) $\Delta \vdash \neg(\alpha \rightarrow \neg\beta) \rightarrow (\alpha \wedge \beta)$
(A6) $\Delta \vdash (\alpha \vee \beta) \rightarrow (\neg\alpha \rightarrow \beta)$
(A7) $\Delta \vdash (\neg\alpha \rightarrow \beta) \rightarrow (\alpha \vee \beta)$

Tak otrzymany system oznaczymy przez $\vdash_{H^+}$.

Twierdzenie 11.9 (O adekwatności dla $\vdash_{H^+}$)
Dla dowolnego zbioru Δ formuł i dla dowolnej formuły α (formuły z Δ i α zawierają $\vee, \wedge, \rightarrow, \bot$), jeśli $\Delta \vdash_{H^+} \alpha$ to $\Delta \models \alpha$.

Dowód: Wystarczy sprawdzić, że aksjomaty (A4)–(A7) są prawdziwe. Konkluzja wynika z twierdzenia o adekwatności dla $\vdash_H$ (por. Twierdzenia 11.4). ■

Pokażemy, że twierdzenie o pełności można rozszerzyć do $\vdash_{H^+}$. Najpierw udowodnimy następujący lemat.

Lemat 11.10 *Dla dowolnej formuły α istnieje formuła $\tilde{\alpha}$ zbudowana przy użyciu jedynie $\rightarrow$ oraz $\bot$, taka że $\vdash_{H^+} \alpha \rightarrow \tilde{\alpha}$ oraz $\vdash_{H^+} \tilde{\alpha} \rightarrow \alpha$.*

Dowód: Dana formuła α, zastąpmy każdą podformułę w α postaci $\beta \wedge \gamma$ formułą $\neg(\beta \rightarrow \neg\gamma)$ oraz każdą podformułę w α postaci $\beta \vee \gamma$ formułą $\neg\beta \rightarrow \gamma$. Aksjomaty (A4)–(A7) mówią, że zastąpione formuły są równoważne. Tak więc łatwo dostajemy $\vdash_{H^+} \alpha \rightarrow \tilde{\alpha}$ oraz $\vdash_{H^+} \tilde{\alpha} \rightarrow \alpha$. Szczegóły dowodu pozostawimy czytelnikowi. ■

Korzystając z powyższego lematu natychmiast dostajemy twierdzenie o pełności dla $\vdash_{H^+}$.

Twierdzenie 11.11 (O pełności dla $\vdash_{H^+}$)
Jeśli α jest tautologią, to $\vdash_{H^+} \alpha$.

Dowód: Jeśli α jest tautologią to ponieważ $\vdash_{H^+} \alpha \rightarrow \tilde{\alpha}$, to z twierdzenia o adekwatności wnioskujemy, że $\models \alpha \rightarrow \tilde{\alpha}$. Zatem $\tilde{\alpha}$ jest tautologią. Z twierdzenia o pełności dla systemu $\vdash_H$ dostajemy $\vdash_H \tilde{\alpha}$. Zatem $\vdash_{H^+} \tilde{\alpha}$ i ponieważ $\vdash_{H^+} \tilde{\alpha} \rightarrow \alpha$ (por. Lemat 11.10) to stosując (MP) dostajemy $\vdash_{H^+} \tilde{\alpha}$ ■

Prawdziwe jest silniejsze twierdzenie od powyższego twierdzenia. Udowodnimy go w następnej części (poświęconej elementom teorii modeli).

11.3.2 System naturalnej dedukcji

System naturalnej dedukcji służy do wyprowadzania sekwentów postaci $\Delta \vdash \alpha$. Jego charakterystyczną cechą jest położenie głównego nacisku na reguły dowodzenia, przy bardzo prostym aksjomacie. Reguły dowodzenia (za wyjątkiem reguły (PS) "przez sprzeczność") są podzielone na grupy, po jednej dla każdego spójnika. W ramach jednej takiej grupy mamy dwa rodzaje reguł: *reguły wprowadzenia* tego spójnika, mówiące o tym w jakiej sytuacji można wprowadzić ten spójnik na prawo od znaku $\vdash$; oraz *reguły eliminacji* mówiące o tym w jakiej sytuacji można ten spójnik wyeliminować, tzn. jakie wnioski można wyciągać z sekwentów, w których najbardziej zewnętrznym spójnikiem formuły stojącej na prawo od znaku $\vdash$ jest ten spójnik. Regułę dowodzenia "przez sprzeczność" można traktować jako silną regułę eliminacji $\bot$. Pamiętajmy, że $\neg\alpha$ oznacza formułę $\alpha \rightarrow \bot$.

Aksjomat
(A0) $\Delta, \alpha \vdash \alpha$

Reguły dowodzenia

$$(\to\text{-intro})\ \frac{\Delta, \alpha \vdash \beta}{\Delta \vdash \alpha \to \beta} \qquad (\to\text{-elim})\ \frac{\Delta \vdash \alpha \to \beta;\ \Delta \vdash \alpha}{\Delta \vdash \beta}$$

$$(\wedge\text{-intro})\ \frac{\Delta \vdash \alpha;\ \Delta \vdash \beta}{\Delta \vdash \alpha \wedge \beta} \qquad (\wedge\text{-elim})\ \frac{\Delta \vdash \alpha \wedge \beta}{\Delta \vdash \alpha} \qquad (\wedge\text{-elim})\ \frac{\Delta \vdash \alpha \wedge \beta}{\Delta \vdash \beta}$$

$$(\vee\text{-intro})\ \frac{\Delta \vdash \alpha}{\Delta \vdash \alpha \vee \beta} \qquad (\vee\text{-intro})\ \frac{\Delta \vdash \beta}{\Delta \vdash \alpha \vee \beta} \qquad (\vee\text{-elim})\ \frac{\Delta \vdash \alpha \vee \beta;\ \Delta, \alpha \vdash \gamma;\ \Delta, \beta \vdash \gamma}{\Delta \vdash \gamma}$$

$$(\text{PS})\ \frac{\Delta, \neg\alpha \vdash \bot}{\Delta \vdash \alpha}$$

Zauważmy, że szczególnym przypadkiem reguły ($\to$-intro) jest następująca reguła, można ją traktować jak regułę wprowadzenia negacji.

$$\frac{\Delta, \alpha \vdash \bot}{\Delta \vdash \neg\alpha}$$

Zauważmy też, że szczególnym przypadkiem reguły ($\to$-elim) jest następująca reguła, można ją traktować jak regułę eliminacji negacji.

$$\frac{\Delta \vdash \neg\alpha;\ \Delta \vdash \alpha}{\Delta \vdash \bot}$$

Podobnie jak w poprzedniej części, dowodem sekwentu $\Delta \vdash \alpha$ w systemie naturalnej dedukcji nazwiemy drzewo etykietowane sekwentami tak, że korzeń ma etykietę $\Delta \vdash \alpha$, liście są etykietowane aksjomatami oraz każdy wewnętrzny wierzchołek jest etykietowny sekwentem, który się otrzymuje z etykiet potomków tego wierzchołka przy zastosowaniu jednej z reguł. Fakt, że istnieje dowód w systemie naturalnej dedukcji sekwentu $\Delta \vdash \alpha$ będziemy zaznaczać przez $\Delta \vdash_{ND} \alpha$.

Poniżej podajemy kilka przykładów dowodów w systemie naturalnej dedukcji.

Przykład 11.12

- Pokażemy $\vdash_{ND} p \to p$.

$$\frac{p \vdash p}{\vdash p \to p}\ (\to\text{-intro})$$

- Pokażemy $\vdash_{ND} p \to (q \to p)$.

$$\dfrac{\dfrac{p, q \vdash p}{p \vdash q \to p}\,(\to\text{-intro})}{\vdash p \to (q \to p)}\,(\to\text{-intro})$$

- Pokażemy $\vdash_{ND} \neg\neg p \to p$.

$$\dfrac{\dfrac{\dfrac{\neg\neg p, \neg p \vdash \neg\neg p \qquad \neg\neg p, \neg p \vdash \neg p}{\neg\neg p, \neg p \vdash \bot}\,(\to\text{-}elim)}{\neg\neg p \vdash p}\,(\text{SP})}{\vdash \neg\neg p \to p}\,(\to\text{-intro})$$

Twierdzenie 11.13 *Dla dowolnego sekwentu $\Delta \vdash \alpha$ mamy następującą równoważność:*

$$\Delta \vdash_{ND} \alpha \quad \textit{wtw, gdy} \quad \Delta \vdash_{H^+} \alpha.$$

Dowód: Aby pokazać, że każdy dowód w $\vdash_{ND}$ daje się przerobić na dowód w $\vdash_{H^+}$ wystarczy pokazać, że każda z reguł systemu ND jest wyprowadzalna w H^+. Zauważmy, że wyprowadzalność reguły(→-intro) jest konsekwencją twierdzenia o dedukcji, natomiast reguła (→-elim) jest regułą (MP). Przykładowo pokażemy wyprowadzenie (∨-elim) oraz (PS) w H^+, pozostawiając wyprowadzenie pozostałych reguł czytelnikowi.

Załóżmy, że mamy w H^+ dowody następujących sekwentów: $\Delta \vdash \alpha \vee \beta$, $\Delta, \alpha \vdash \gamma$ oraz $\Delta, \beta \vdash \gamma$. Wówczas, stosując aksjomat (A6) i regułę (MP) mamy

$$\Delta \vdash \neg\alpha \to \beta.$$

Zatem $\Delta, \neg\alpha \vdash_{H^+} \beta$ i ponieważ $\Delta \vdash_{H^+} \beta \to \gamma$ to również i $\Delta, \neg\alpha \vdash_{H^+} \beta \to \gamma$. Zatem

$$\Delta, \neg\alpha \vdash \gamma.$$

Z Lematu 11.10 otrzymujemy więc $\Delta \vdash_{H^+} \gamma$.

Dla wyprowadzenia (PS) załóżmy, że $\Delta, \neg\alpha \vdash_{H^+} \bot$. Z twierdzenia o dedukcji dostajemy $\Delta \vdash_{H^+} \neg\neg\alpha$. Tak więc z (A3) i (MP) dostajemy $\Delta \vdash_{H^+} \alpha$.

Dla pokazania implikacji odwrotnej wystarczy pokazać, że wszystkie aksjomaty systemu H^+ są twierdzeniami w ND. Wyprowadzenia (A1) i (A3) w ND zostały podane powyżej (przed sformułowaniem twierdzenia). Przykładowo pokażemy wyprowadzenia (A2) i (A5). Zaczniemy od wyprowadzenia (A2). Niech $\Delta = \{\alpha \to (\beta \to \gamma),\ \alpha \to \beta,\ \alpha\}$.

$$\dfrac{\dfrac{\Delta \vdash \alpha \to (\beta \to \gamma) \quad \Delta \vdash \alpha}{\Delta \vdash \beta \to \gamma}\,(\to\text{-elim}) \qquad \dfrac{\Delta \vdash \alpha \to \beta \quad \Delta \vdash \alpha}{\Delta \vdash \beta}\,(\to\text{-elim})}{\Delta \vdash \gamma}\,(\to\text{-elim})$$

Stosując trzy razy ($\rightarrow$ -intro) do sekwentu $\Delta \vdash \gamma$ dostajemy wyprowadzenie aksjomatu (A2).

Następnie pokażemy dowód (A5) w ND. Zaczniemy od wyprowadzenia sekwentu $\neg(\alpha \rightarrow \neg\beta) \vdash \alpha$. Niech $\Delta = \{\neg(\alpha \rightarrow \neg\beta), \neg\alpha\}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta, \alpha, \beta \vdash \neg\alpha \quad \Delta, \alpha, \beta \vdash \alpha}{\Delta, \alpha, \beta \vdash \bot}(\rightarrow\text{-elim})}{\Delta, \alpha \vdash \neg\beta}(\rightarrow\text{-intro})}{\Delta \vdash \alpha \rightarrow \neg\beta}(\rightarrow\text{-intro}) \qquad \Delta \vdash \neg(\alpha \rightarrow \neg\beta)}{\Delta \vdash \bot}(\rightarrow\text{-elim})}{\neg(\alpha \rightarrow \neg\beta) \vdash \alpha}(PS)$$

Następnie wyprowadzimy sekwent $\neg(\alpha \rightarrow \neg\beta) \vdash \beta$. Niech $\Delta = \{\neg(\alpha \rightarrow \neg\beta), \neg\beta\}$

$$\dfrac{\dfrac{\dfrac{\Delta, \alpha \vdash \neg\beta}{\Delta \vdash \alpha \rightarrow \neg\beta}(\rightarrow\text{-intro}) \qquad \Delta \vdash \neg(\alpha \rightarrow \neg\beta)}{\Delta \vdash \bot}(\rightarrow\text{-elim})}{\neg(\alpha \rightarrow \neg\beta) \vdash \beta}(PS)$$

Mając wyprowadzone sekwenty $\neg(\alpha \rightarrow \neg\beta) \vdash \alpha$ oraz $\neg(\alpha \rightarrow \neg\beta) \vdash \beta$ możemy zakończyć dowód (A5).

$$\dfrac{\dfrac{\neg(\alpha \rightarrow \neg\beta) \vdash \alpha \quad \neg(\alpha \rightarrow \neg\beta) \vdash \beta}{\neg(\alpha \rightarrow \neg\beta) \vdash \alpha \wedge \beta}(\wedge\text{-intro})}{\vdash \neg(\alpha \rightarrow \neg\beta) \rightarrow (\alpha \wedge \beta)}(\rightarrow\text{-intro})$$

■

11.3.3 Gentzenowski rachunek sekwentów

Dla przedstawienia systemu gentzenowskiego rozszerzymy nieco pojęcie sekwentu. Przez sekwent będziemy rozumieć napis $\Delta \vdash \Gamma$, gdzie Δ oraz Γ są skończonymi zbiorami formuł. Intuicyjnie, wyprowadzalność sekwentu $\Delta \vdash \Gamma$ w systemie gentzenowskim będzie oznaczać, że "alternatywa formuł z Γ jest twierdzeniem wynikającym z hipotez Δ. Gdy Γ jest zbiorem jednoelementowym dostajemy sekwenty (i stosujące się do nich pojęcia) w starym znaczeniu.

Rozważamy formuły, podobnie jak w poprzedniej części, oparte na spójnikach $\rightarrow, \vee, \wedge$ oraz na stałej zdaniowej $\bot$. Negację $\neg$ traktujemy jako spójnik zdefiniowany przez $\rightarrow$ i $\bot$.

Charakterystyczną cechą systemu gentzenowskiego są reguły polegające na przedstawieniu sytuacji kiedy możemy dany spójnik wprowadzić na lewo od znaku $\vdash$ oraz kiedy możemy wprowadzić na prawo. Dla każdego spójnika mamy odpowiadającą parę reguł. Dla symbolu fałszu $\bot$ mamy tylko regułę wprowadzania na lewo.

Aksjomaty
(A0) $\Delta, \alpha \vdash \Gamma, \alpha$
(A$\bot$) $\Delta, \bot \vdash \Gamma$

Reguły dowodzenia

$$(\rightarrow\text{-lewa})\ \frac{\Delta \vdash \Gamma, \alpha; \quad \beta, \Delta \vdash \Gamma}{\Delta, \alpha \rightarrow \beta \vdash \Gamma} \qquad (\rightarrow\text{-prawa})\ \frac{\Delta, \alpha \vdash \Gamma, \beta}{\Delta \vdash \Gamma, \alpha \rightarrow \beta}$$

$$(\wedge\text{-lewa})\ \frac{\Delta, \alpha, \beta \vdash \Gamma}{\Delta, \alpha \wedge \beta \vdash \Gamma} \qquad (\wedge\text{-prawa})\ \frac{\Delta \vdash \Gamma, \alpha; \quad \Delta \vdash \Gamma, \beta}{\Delta \vdash \Gamma, \alpha \wedge \beta}$$

$$(\vee\text{-lewa})\ \frac{\Delta, \alpha \vdash \Gamma; \quad \Delta, \beta \vdash \Gamma}{\Delta, \alpha \vee \beta \vdash \Gamma} \qquad (\vee\text{-prawa})\ \frac{\Delta \vdash \Gamma, \alpha, \beta}{\Delta \vdash \Gamma, \alpha \vee \beta}$$

Aksjomat (A$\bot$) można traktować jako regułę (bez przesłanek) wprowadzenia $\bot$ z lewej strony znaku $\vdash$.

Dowodem sekwentu $\Delta \vdash \Gamma$, tak jak poprzednio, nazywamy drzewo etykietowane sekwentami tak, że korzeń jest etykietowany przez $\Delta \vdash \Gamma$, liście są etykietowane aksjomatami oraz wierzchołki wewnętrzne są etykietowane sekwentami otrzymanymi poprawnie przez zastosowanie pewnej z reguł dowodzenia. Istnienie dowodu sekwentu $\Delta \vdash \Gamma$ w gentzenowskim rachunku sekwentów będziemy oznaczać przez $\Delta \vdash_G \Gamma$.

Zauważmy, że jeśli mamy sekwent $\Delta \vdash \Gamma, \alpha$ to stosując aksjomat (A$\bot$), a następnie ($\rightarrow$-lewa) dostajemy sekwent $\Delta, \neg\alpha \vdash \Gamma$. Zatem natępująca reguła jest wyprowadzalna w systemie $\vdash_G$,

$$(\neg\text{-lewa})\ \frac{\Delta \vdash \Gamma, \alpha}{\Delta, \neg\alpha \vdash \Gamma}$$

Ponadto zauważmy, że jeśli mamy dowód sekwentu $\Delta \vdash \Gamma$, to dla każdej formuły α możemy ją dodać do prawej strony każdego sekwentu w tym dowodzie i otrzymamy dowód sekwentu $\Delta \vdash \Gamma, \alpha$. W szczególności jeśli mamy udowodniony sekwent $\Delta, \alpha \vdash \Gamma$, to możemy też udowodnić sekwent $\Delta, \alpha \vdash \Gamma, \bot$. Stosując do niego regułę ($\rightarrow$-prawa) otrzymujemy sekwent $\Delta \vdash \Gamma, \neg\alpha$. Tym samym pokazaliśmy, że następująca reguła jest wyprowadzalna w systemie $\vdash_G$,

$$(\neg\text{-prawa})\ \frac{\Delta, \alpha \vdash \Gamma}{\Delta \vdash \Gamma, \neg\alpha}$$

Twierdzenie 11.14 *Dla każdej formuły α, mamy następującą równoważność*

$$\vdash_G \alpha \quad \textit{wtw, gdy} \quad \alpha \textit{ jest tautologią.}$$

Powyższe twierdzenie pozostawimy bez dowodu. Łatwo jest pokazać, że każde twierdzenie systemu gentzenowskiego jest tautologią. Dla dowodu implikacji odwrotnej rozszerza się system $\vdash_G$ przez dodanie nowej reguły zwanej *cięciem*.

$$\text{(cięcie)} \ \frac{\Delta, \alpha \vdash \Gamma; \quad \Delta \vdash \alpha, \Gamma}{\Delta \vdash \Gamma}$$

Niech $\vdash_{GC}$ oznacza system gentzenowski z cięciem. Łatwo jest pokazać, że reguła odrywania jest wyprowadzalna w $\vdash_{GC}$. Zatem, korzystając z twierdzenia o pełności dla systemu hilbertowskiego, łatwo pokazujemy, że każda tautologia jest twierdzeniem systemu $\vdash_{GC}$. Główna trudność w dowodzie twierdzenia o pełności dla systemu $\vdash_G$ polega na udowodnieniu następującego twierdzenia *o eliminacji cięcia*. Twierdzenie to podajemy bez dowodu.

Twierdzenie 11.15 (O eliminacji cięcia)
Dla każdego sekwentu $\Delta \vdash \Gamma$, jeśli $\Delta \vdash_{GC} \Gamma$, to $\Delta \vdash_G \Gamma$.

Systemy gentzenowskie znajdują zastosowanie w automatycznym dowodzeniu twierdzeń gdyż jest w nich łatwo szukać dowodów formuł. Pokażemy to na przykładzie.

Przykład 11.16

1. Poszukamy dowodu sekwentu $\vdash \neg\neg\alpha \to \alpha$ w $\vdash_G$. Ponieważ najbardziej zewnętrznym spójnikiem w rozważanej formule jest $\to$, to ostatnią regułą w poszukiwanym dowodzie musiała być reguła ($\to$-prawa). Zatem wystarczy znaleźć dowód sekwentu $\neg\neg\alpha \vdash \alpha$. Najbardziej zewnętrznym spójnikiem formuły po lewej stronie jest $\neg$, a zatem na mocy reguły ($\neg$-lewa) wystarczy udowodnić sekwent $\vdash \alpha, \neg\alpha$. Podobnie, na mocy reguły ($\neg$-prawa) wystarczy udowdnić sekwent $\alpha \vdash \alpha$. Ponieważ ten sekwent jest aksjomatem, to odwracając wszystkie kroki w powyższym rozumowaniu otrzymujemy dowód sekwentu $\vdash \neg\neg\alpha \to \alpha$ w systemie $\vdash_G$.

2. Jeśli zastosujemy powyższą procedurę do formuły, która nie jest tautologią, to dostaniemy wskazówkę na znalezienie kontrprzykładu. Dla zilustrowania tej tezy weźmy bardzo prosty sekwent $\vdash p \to q$. Postępując podobnie jak porzednio dochodzimy do sekwentu $p \vdash q$, który nie jest aksjomatem, i którego nie możemy już dalej rozłożyć. Wartościowanie falsyfikujące sekwent $\Delta \vdash \Gamma$ to takie, które spełnia wszystkie formuły z Δ oraz falsyfikuje wszystkie formuły z Γ. W naszym przypadku wystarczy wziąć wartościowanie spełniające p i falsyfikujące q.

11.4 Elementy teorii modeli

Powiemy, że zbiór formuł Δ jest *spełnialny* gdy istnieje wartościowanie $v : P \to \{0,1\}$ spełniające wszystkie formuły ze zbioru Δ.

Twierdzenie 11.17 (O zwartości)
Zbiór formuł Δ jest spełnialny wtw, gdy każdy skończony podzbiór zbioru Δ jest spełnialny.

Dowód: Powiemy, że zbiór Δ jest *skończenie spełnialny*, gdy każdy skończony podzbiór zbioru Δ jest spełnialny.

Szkic dowodu twierdzenia o zwartości wygląda następująco. Bez zmniejszenia ogólności możemy przyjąć, że wszystkie rozważane formuły są zbudowane przy użyciu jedynie spójników $\to$ oraz $\bot$. Używając lematu Kuratowskiego-Zorna pokazujemy najpierw, że istnieje maksymalny skończenie spełnialny zbiór formuł Γ zawierający Δ. Oczywiście mamy

$$\bot \notin \Gamma. \tag{56}$$

Następnie, korzystając z maksymalności Γ dowodzimy następującą pomocniczą własność. Dla dowolnych formuł α, β,

$$(\alpha \to \beta) \in \Gamma \quad \text{wtw, gdy} \quad \alpha \notin \Gamma, \text{ lub } \beta \in \Gamma. \tag{57}$$

Teraz możemy zdefiniować wartościowanie $v : P \to \{0,1\}$ tak, że dla dowolnej zmiennej $p \in P$, $v(p) = 1$ wtw, gdy $p \in \Gamma$. Z następującej własności wynika, że v spełnia wszystkie formuły ze zbioru Γ, a zatem Δ jest zbiorem spełnialnym.

Dla dowolnej formuły α,

$$\models \alpha[v] \quad \text{wtw, gdy} \quad \alpha \in \Gamma. \tag{58}$$

Dowód (58) przeprowadzamy przez indukcję ze względu na budowę formuły α. Własności (56) używamy dla przypadku gdy α jest $\bot$, a (57) dla przypadku, gdy zewnętrznym spójnikiem α jest $\to$. ■

Jako wniosek z twierdzenia o zwartości otrzymujemy następujące wzmocnienie twierdzenia o pełności (por. Twierdzenie 11.11).

Twierdzenie 11.18 (Silne twierdzenie o pełności)
Dla dowolnego zbioru formuł Δ oraz formuły α, jeśli α jest semantyczną konsekwencją zbioru Δ, to $\Delta \vdash_{H^+} \alpha$.

Dowód: Jeśli $\Delta \models \alpha$ to zbiór $\Delta \cup \{\neg\alpha\}$ nie jest spełnialny. Zatem na mocy twierdzenia o zwartości istnieje skończony podzbiór $\Delta_0 \subseteq \Delta$ taki, że $\Delta_0 \cup \{\neg\alpha\}$ nie jest spełnialny. Zatem $\Delta_0 \models \alpha$. Tak więc jeśli $\Delta_0 = \{\beta_1, \ldots, \beta_n\}$ to oczywiście formuła $\beta_1 \to (\beta_2 \to \cdots (\beta_n \to \alpha) \cdots)$ jest tautologią. Z twierdzenia o pełności wnioskujemy, że $\vdash_H \beta_1 \to (\beta_2 \to \cdots (\beta_n \to \alpha) \cdots)$. Stosując n razy (MP) do powyższego sekwentu dostajemy

$$\Delta_0 \vdash_H \alpha.$$

Czyli $\Delta \vdash_H \alpha$, co kończy dowód twierdzenia. ∎

Przykład 11.19 Pokażemy jak można stosować twierdzenie o zwartości. Pokażemy, że jeśli nieskończonej mapy (o przeliczalnej liczbie krajów) nie da się pokolorować przy pomocy k kolorów, to istnieje skończony fragment tej mapy, którego też nie da się pokolorować przy pomocy k kolorów. Niech I będzie zbiorem krajów tej mapy. Rozważmy zmienne zdaniowe $p_{(i,j)}$, gdzie $i \in I$ oraz $j < k$. Wartościowania będą odpowiadać kolorowaniom mapy. Intencją jest to aby wartościowanie przypisywało zmiennej $p_{(i,j)}$ wartość 1 wtw, gdy kraj i ma na mapie kolor j. Poniższe formuły przedstawiają podstawowe warunki dotyczące kolorowania.

Każdy kraj ma jakiś kolor: dla każdego $i \in I$ mamy,

$$p_{(i,0)} \vee p_{(i,1)} \vee \ldots \vee p_{(i,k-1)}.$$

Każdy kraj ma co najwyżej jeden kolor: dla każdego $i \in I$, oraz $j \neq j'$, $(j < k,\ j' < k)$ mamy,

$$\neg(p_{(i,j)} \wedge p_{(i,j')}).$$

Każde dwa sąsiadujące kraje mają różne kolory: dla $i, i' \in I$ takich, że i oraz i' sąsiadują oraz dla każdego $j < k$ mamy,

$$\neg(p_{(i,j)} \wedge p_{(i',j)}).$$

Niech Δ będzie zbiorem wszystkich formuł wyżej przedstawionych. Jest oczywiste, że Δ jest spełnialny wtw, gdy mapę da się pokolorować k kolorami. Zatem jeśli mapy nie da się pokolorować k kolorami to Δ nie jest spełnialny i z twierdzenia o zwartości wynika, że istnieje skończony podzbiór Δ_0, który nie jest spełnialny. Wówczas fragmentu mapy zawierającego kraje wymienione w indeksach zmiennych występujących w formułach z Δ_0 nie da się pokolorować przy pomocy k kolorów.

11.5 Informacja o logice intuicjonistycznej

Logikę intuicjonistyczną można przedstawić jako fragment logiki klasycznej wprowadzonej powyżej. Intuicjonizm odrzuca pewne reguły wnioskowania logiki klasycznej jako takie, które

powodują, że na przykład dowody istnienia pewnych obiektów nie podają żadnego sposobu na skonstruowanie tych obiektów. Regułą kwestionowaną przez intuicjonistów jest przykładowo *reguła wyłączonego środka*, która mówi, że dla każdego zdania α spełnione jest α lub $\neg\alpha$. Klasycznym dowodem, podawanym przez intuicjoinistów jako przykład niekonstruktywnego rozumowania, które wykorzystuje wyżej wspomnianą regułę jest dowód następującego twierdzenia.

Twierdzenie 11.20 *Istnieją liczby niewymierne $a, b \in R$, takie że a^b jest liczbą wymierną.*

Dowód: Jeśli $\sqrt{2}^{\sqrt{2}}$ jest liczbą wymierną, to bierzemy $a = b = \sqrt{2}$. Jeśli natomiast $\sqrt{2}^{\sqrt{2}}$ jest liczbą niewymierną, to bierzemy $a = \sqrt{2}^{\sqrt{2}}$ oraz $b = \sqrt{2}$. Wówczas

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2.$$

To kończy dowód twierdzenia. ■

Zauważmy, że powyższy dowód nie podaje przykładu takiej pary liczb i z tego powodu jest odrzucany przez intuicjonistów. Dowody w logice intuicjonistycznej mają tę cechę, że często z dowodu danej formuły można wyprowadzić algorytm, który w pewnym sensie zawiera w sobie konstruktywne elementy dowodu tej formuły. Z tego względu logika intuicjonistyczna cieszy się rosnącym zainteresowaniem informatyki, zwłaszcza działami związanymi z syntezą i poprawnością programów.

Łatwo jest zauważyć, że w systemie naturalnej dedukcji, który był przedstawiony wcześniej, reguła rozumowania "przez sprzeczność" (reguła (PS)) reprezentuje wyżej wspomniane prawo wyłączonego środka. Logikę intuicjonistyczną przedstawimy przy pomocy systemu naturalnej dedukcji, w którym reguła (PS) jest zastąpiona słabszą regułą $\bot$-eliminacji. System ten w całości podajemy poniżej.

Aksjomat
(A0) $\Delta, \alpha \vdash \alpha$

Reguły dowodzenia

$$(\rightarrow\text{-intro})\ \frac{\Delta, \alpha \vdash \beta}{\Delta \vdash \alpha \rightarrow \beta} \qquad (\rightarrow\text{-elim})\ \frac{\Delta \vdash \alpha \rightarrow \beta;\ \Delta \vdash \alpha}{\Delta \vdash \beta}$$

$$(\wedge\text{-intro})\ \frac{\Delta \vdash \alpha;\ \Delta \vdash \beta}{\Delta \vdash \alpha \wedge \beta} \qquad (\wedge\text{-elim})\ \frac{\Delta \vdash \alpha \wedge \beta}{\Delta \vdash \alpha} \qquad (\wedge\text{-elim})\ \frac{\Delta \vdash \alpha \wedge \beta}{\Delta \vdash \beta}$$

$$(\vee\text{-intro})\ \frac{\Delta \vdash \alpha}{\Delta \vdash \alpha \vee \beta} \qquad (\vee\text{-intro})\ \frac{\Delta \vdash \beta}{\Delta \vdash \alpha \vee \beta} \qquad (\vee\text{-elim})\ \frac{\Delta \vdash \alpha \vee \beta;\ \Delta, \alpha \vdash \gamma;\ \Delta, \beta \vdash \gamma}{\Delta \vdash \gamma}$$

$$(\bot\text{-elim})\ \frac{\Delta \vdash \bot}{\Delta \vdash \alpha}$$

Wyprowadzalność sekwentu w powyższym systemie definiujemy analogicznie jak dla logiki klasycznej. Napis $\Delta \vdash_{NDI} \alpha$ oznacza, że sekwent $\Delta \vdash \alpha$ jest wyprowadzalny w powyższym systemie. Powiemy, że formuła α jest *twierdzeniem logiki intuicjonistycznej* jeśli $\vdash_{NDI} \alpha$.

Ponieważ w pierwszych dwóch punktach Przykładu 11.12 nie używaliśmy reguły (SP) to wnioskujemy, że $p \to p$ oraz $p \to (q \to p)$ są twierdzeniami logiki intuicjonistycznej, tzn $\vdash_{NDI} p \to p$ oraz $\vdash_{NDI} p \to (q \to p)$. Z drugiej strony można udowodnić, że formuła $\neg\neg p \to p$ *nie* jest twierdzeniem logiki intuicjonistycznej. Pokażemy, że formuła $p \to \neg\neg p$ daje się udowodnić w logice intuicjonistycznej. Przypomnijmy, że $\neg\alpha$ oznacza formułę $\alpha \to \bot$.

Przykład 11.21

- Pokażemy, że $\vdash_{NDI} p \to \neg\neg p$.

$$\dfrac{\dfrac{\dfrac{p, \neg p \vdash \neg p \qquad p, \neg p \vdash p}{p, \neg p \vdash \bot}\,(\to\text{-elim})}{p \vdash \neg\neg p}\,(\to\text{-intro})}{\vdash p \to \neg\neg p}\,(\to\text{-intro})$$

- Pokażemy, że $p \to (\neg p \to q)$ jest twierdzeniem logiki intuicjonistycznej.

$$\dfrac{\dfrac{\dfrac{\dfrac{p, \neg p \vdash \neg p \qquad p, \neg p \vdash p}{p, \neg p \vdash \bot}\,(\to\text{-elim})}{p, \neg p \vdash q}\,(\bot\text{-elim})}{p \vdash \neg p \to q}\,(\to\text{-intro})}{\vdash p \to (\neg p \to q)}\,(\to\text{-intro})$$

Zadania

11.1. Powiemy, że zbiór funkcji $f_1 : \{0,1\}^{n_1} \to \{0,1\}, \ldots, f_k : \{0,1\}^{n_k} \to \{0,1\}$ jest *funkcyjnie zupełny*, gdy dla każdego $m \in N$ i dla każdej funkcji $g : \{0,1\}^m \to \{0,1\}$, funkcja g może być otrzymana z funkcji $f_1, \ldots, f_k$ przez operację składania.[15]

[15] Operacji składania nie będziemy tu definiować formalnie. Chodzi o to by dla dowolnej funkcji g znaleźć wyrażenie zbudowane poprawnie z funkcji $f_1, \ldots, f_k$ oraz zmiennych $x_1, \ldots, x_m$ (ta sama funkcja bądź ta sama zmienna może być użyta wiele razy) reprezentujące g. Przykładowo, wyrażenie $f_1(x, f_2(x, x))$ reprezentuje identyczność $I : \{0,1\} \to \{0,1\}$, gdzie f_1 jest $\vee^{\mathfrak{B}}$ a f_2 jest $\wedge^{\mathfrak{B}}$.

(i) Dowieść, że zbiór $\{\rightarrow^{\mathfrak{B}}, \bot^{\mathfrak{B}}\}$ jest funkcyjnie zupełny.

(ii) Dowieść, że zbiór $\{\vee^{\mathfrak{B}}, \neg^{\mathfrak{B}}\}$ jest funkcyjnie zupełny.

(iii) Dowieść, że zbiór $\{\rightarrow^{\mathfrak{B}}, \vee^{\mathfrak{B}}\}$ nie jest funkcyjnie zupełny.

(iv) Dowieść, że zbiór $\{\vee^{\mathfrak{B}}, \wedge^{\mathfrak{B}}\}$ nie jest funkcyjnie zupełny.

(v) Znaleźć wszystkie funkcje $f : \{0,1\}^2 \rightarrow \{0,1\}$, takie że zbiór $\{f\}$ jest funkcyjnie zupełny.

11.2. Dla dowolnej formuły α niech $\hat{\alpha}$ oznacza dualizację formuły α, tzn. formułę powstającą z α przez zastąpienie każdego wystąpienia $\wedge$ symbolem $\vee$ oraz każdego wystąpienia $\vee$ symbolem $\wedge$.

(i) Dowieść,że α jest tautologią wtw, gdy $\neg\hat{\alpha}$ jest tautologią.

(ii) Dowieść, że $\alpha \leftrightarrow \beta$ jest tautologią wtw, gdy $\hat{\alpha} \leftrightarrow \hat{\beta}$ jest tautologią.

11.3. Niech $\vdash_{H_1}$ oznacza system dowodzenia $\vdash_H$, w którym aksjomat (A3) został zastąpiony przez następujący aksjomat.
(A3') $\Delta \vdash (\neg\alpha \rightarrow \neg\beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \alpha)$

Dowieść, że obydwa systemy są równoważne, tzn., że dla dowolnego sekwentu $\Delta \vdash \alpha$, zachodzi $\Delta \vdash_H \alpha$ wtw, gdy $\Delta \vdash_{H_1} \alpha$.

11.4. Niech $\vdash_{H_2}$ oznacza system dowodzenia $\vdash_H$, w którym aksjomat (A3) został zastąpiony przez następujący aksjomat.
(A3") $\Delta \vdash (\neg\alpha \rightarrow \neg\beta) \rightarrow (\beta \rightarrow \alpha)$

Dowieść, że obydwa systemy są równoważne, tzn., że dla dowolnego sekwentu $\Delta \vdash \alpha$, zachodzi $\Delta \vdash_H \alpha$ wtw, gdy $\Delta \vdash_{H_2} \alpha$.

11.5. Dowieść, że aksjomatu (A3) nie da się wyprowadzić z aksjomatów (A0-2) przy pomocy reguły odrywania.

11.6. Dowieść $\vdash_H \neg p \rightarrow (p \rightarrow q)$ używając twierdzenie o dedukcji oraz bez użycia tego twierdzenia.

11.7. Pokazać, że w systemie $\vdash_H$ wyprowadzalna jest następująca reguła.

$$\frac{\Delta \vdash \alpha \rightarrow \beta;\ \Delta \vdash \neg\beta}{\Delta \vdash \neg\alpha}$$

11.8. Każdy z poniższych sekwentów wyprowadzić w systemie $\vdash_{H^+}$, $\vdash_{ND}$, $\vdash_G$.

(i) $\vdash \bot \rightarrow p$

(ii) $\{p \to q, q \to r\} \vdash p \to r$

(iii) $\vdash (\neg p \to p) \to p$

(iv) $\{p, \neg p\} \vdash q$

(v) $\{p \to (q \to r)\} \vdash q \to (p \to r)$

(vi) $\vdash (\neg p \to \neg q) \to (q \to p)$

(vii) $\vdash \neg(p \wedge q) \to (\neg p \vee \neg q)$

11.9. Dowieść, że jeśli $\Delta \vdash_{ND} \alpha$, to dla dowolnej formuły β, zachodzi $\Delta, \beta \vdash_{ND} \alpha$.

11.10. Dowieść, że jeśli $\Delta \vdash_{ND} \bot$, to dla dowolnej formuły α, zachodzi $\Delta \vdash_{ND} \alpha$.

11.11. Dowieść, że dla każdej formuły α nie będącej tautologią istnieje maksymalny zbiór formuł Δ taki, że sekwent $\Delta \vdash \alpha$ nie daje się wyprowadzić w systemie naturalnej dedukcji.

11.12. Wyprowadzić regułę odrywania w gentzenowskim rachunku sekwentów powiększonym o regułę ciecia.

11.13. Dla każdego z sytemów $\vdash_{H^+}$, $\vdash_{ND}$, $\vdash_G$ dowieść, że jeśli sekwent $\Delta \vdash \alpha$ jest wyprowadzalny w tym systemie oraz S jest podstawieniem formuł na zmienne zdaniowe, to sekwent $\vec{S}(\Delta) \vdash S(\alpha)$ powstający w wyniku podstawienia jest też wyprowadzalny w tym systemie.

11.14. Dowieść, że silne twierdzenie o pełności (Twierdzenie 11.18) pociąga twierdzenie o zwartości.

11.15. Dany jest nieskończony zbiór chłopców, z których każdy ma skończoną liczbę narzeczonych. Ponadto dla każdego $k \in N$, dowolnych k chłopców ma co najmniej k narzeczonych. Dowieść, że każdy chłopiec może się ożenić z jedną ze swoich narzeczonych bez popełnienia bigamii.

12 Język pierwszego rzędu

12.1 Składnia

Dotychczas rozważaliśmy tylko sygnatury zawierające wyłącznie symbole operacji. W tym rozdziale rozszerzymy pojęcie sygnatury, dopuszczając również symbole relacji. Tak więc przez sygnaturę Σ będziemy teraz rozumieć rodzinę zbiorów Σ_n^F, dla $n \geq 0$ oraz rodzinę zbiorów Σ_n^R, dla $n \geq 1$. Elementy Σ_n^F będziemy nazywać *symbolami operacji n-argumentowych*, a elementy Σ_n^R będziemy nazywać *symbolami relacji n-argumentowych*. Przyjmujemy, że wszystkie te zbiory są parami rozłączne oraz, że Σ_2^R zawiera symbol $=$.

Zbiór termów nad sygnaturą Σ (oznaczamy go przez $FT(\Sigma, X)$), definiuje się tak jak poprzednio, z tym zastrzeżeniem, że oczywiście termy są budowane w oparciu jedynie o część funkcyjną Σ^F sygnatury Σ.

Zbiór *formuł pierwszego rzędu* nad sygnaturą Σ jest najmniejszym zbiorem wyrażeń spełniającym następujące warunki:

- $\bot$ jest formułą.
- Jeśli r jest symbolem relacji n-argumentowej oraz $\sigma_1, \ldots, \sigma_n$ są termami, to $r(\sigma_1, \ldots, \sigma_n)$ jest formułą. Gdy r jest symbolem równości $=$ to formułę tę zapisujemy $\sigma_1 = \sigma_2$.
- Jeśli α i β są formułami to

  $$(\alpha \wedge \beta), \ (\alpha \vee \beta), \ (\alpha \to \beta)$$

  są też formułami.
- Jeśli α jest formułą oraz $x \in X$ jest zmienną, to

  $$\forall x \alpha, \ \exists x \alpha$$

  są też formułami.

W powyższej definicji przyjmujemy, że symbole $\wedge$, $\vee$, $\to$, $\forall$, $\exists$ nie należą do sygnatury Σ, nad którą budujemy formuły. Tak jak w dziale poświęconym rachunkowi zdań będziemy używać skrótu $\neg\alpha$ dla oznaczenia formuły $\alpha \to \bot$. Symbol $\forall$ nazywa się *kwantyfikatorem uniwersalnym* a symbol $\exists$ nazywa się *kwantyfikatorem egzystencjalnym*.

Chcielibyśmy zwrócić uwagę czytelnika na użycie nazwy *term* w tym i w poprzednim rozdziale tych notatek. Formuły rachunku zdań zdefiniowaliśmy jako termy nad sygnaturą zawierającą $\wedge, \vee, \to$ jako symbole operacji dwuargumentowych oraz $\bot$ jako symbol stałej. Wybraliśmy ten sposób wprowadzenia formuł ze względu na zwięzłość zapisu. Pojęcie *term* używane w tym rozdziale oznacza poprawnie zbudowany napis nad dowolną ustaloną sygnaturą Σ. Formuły pierwszego rzędu nad sygnaturą Σ zostały zdefiniowane indukcyjnie. Obie

kategorie syntaktyczne: formuły i termy nad sygnaturą Σ tworzą rozłączne zbiory, różne dla różnych sygnatur Σ.

Zbiór $FV(\alpha)$ *zmiennych wolnych* formuły α definiujemy indukcyjnie.
$FV(\bot) = \emptyset$;
$FV(r(\sigma_1, \ldots, \sigma_n)) = FV(\sigma_1) \cup \ldots \cup FV(\sigma_n)$;
$FV(\alpha \wedge \beta) = FV(\alpha \vee \beta) = FV(\alpha \to \beta) = FV(\alpha) \cup FV(\beta)$;
$FV(\forall x\alpha) = FV(\exists x\alpha) = FV(\alpha) - \{x\}$.

W powyższej definicji dla dowolnego termu σ, symbolem $FV(\sigma)$ oznaczamy zbiór wszystkich zmiennych występujących w termie σ. Łatwą indukcyjną definicję tego zbioru pozostawimy czytelnikowi jako ćwiczenie.

Wszystkie wystąpienia zmiennej wolnej x w formule α stają się wystąpieniami *związanymi* w formule $\forall x\alpha$. Mówimy, że te wystąpienia są związane kwantyfikatorem $\forall$. Podobnie jest w przypadku formuły $\exists x\alpha$. Formuła bez zmiennych wolnych nazywa się *zdaniem*.

12.2 Semantyka

Niech Σ będzie sygnaturą. *Strukturą* $\mathfrak{A}$ nad sygnaturą Σ (lub po prostu Σ-strukturą) nazwiemy niepusty zbiór A, zwany *nośnikiem*, wraz interpretacją każdego symbolu operacji $f \in \Sigma_n^F$ $(n \geq 0)$ jako funkcji n argumentowej $f^{\mathfrak{A}} : A^n \to A$ oraz każdego symbolu relacji $r \in \Sigma_n^R$ $(n \geq 1)$ jako relacji n-argumentowej $r^{\mathfrak{A}} \subseteq A^n$. W przypadku, gdy Σ^R jest zbiorem pustym powyższa definicja pokrywa się z definicją Σ-algebry.

Wartościowaniem w Σ-strukturze $\mathcal{A}$ nazwiemy dowolną funkcję $v : X \to A$. Dla wartościowania v, zmiennej $x \in X$ oraz elementu $a \in A$ definiujemy nowe wartościowanie $v_x^a : X \to A$, będące modyfikacją wartościowania v na argumencie x, w następujący sposób,

$$(v_x^a)(y) = \begin{cases} v(y) & \text{gdy } y \neq x, \\ a & \text{gdy } y = x. \end{cases}$$

Semantykę formuł języka pierwszego rzędu definiuje się w oparciu o relację *spełniania*

$$\mathfrak{A} \models \alpha[v],$$

gdzie $\mathfrak{A}$ jest Σ strukturą, α jest formułą nad sygnaturą Σ oraz v jest wartościowaniem w $\mathfrak{A}$. Związek ten czytamy: formuła α jest spełniona w strukturze $\mathfrak{A}$ przy wartościowaniu v. Ten sposób definiowania semantyki pochodzi od Alfreda Tarskiego. Relację spełniania definiujemy przez indukcję ze względu na budowę formuły α.

- Nie zachodzi $\mathfrak{A} \models \bot[v]$;
- $\mathfrak{A} \models r(\sigma_1, \ldots, \sigma_n)[v]$ wtw, gdy $(\sigma_1^{\mathfrak{A}}[v], \ldots \sigma_n^{\mathfrak{A}}[v]) \in r^{\mathfrak{A}}$;

- $\mathfrak{A} \models (\sigma_1 = \sigma_2)[v]$ wtw, gdy $\sigma_1^{\mathfrak{A}}[v] = \sigma_2^{\mathfrak{A}}[v]$;
- $\mathfrak{A} \models (\alpha \wedge \beta)[v]$ wtw, gdy zachodzą $\mathfrak{A} \models \alpha[v]$ oraz $\mathfrak{A} \models \beta[v]$;
- $\mathfrak{A} \models (\alpha \vee \beta)[v]$ wtw, gdy zachodzi $\mathfrak{A} \models \alpha[v]$ lub $\mathfrak{A} \models \beta[v]$;
- $\mathfrak{A} \models (\alpha \to \beta)[v]$ wtw, gdy $\mathfrak{A} \models \alpha[v]$ nie zachodzi lub zachodzi $\mathfrak{A} \models \beta[v]$;
- $\mathfrak{A} \models (\forall x \alpha)[v]$ wtw, gdy dla każdego $a \in A$, $\mathfrak{A} \models \alpha[v_x^a]$;
- $\mathfrak{A} \models (\exists x \alpha)[v]$ wtw, gdy istnieje $a \in A$ takie, że $\mathfrak{A} \models \alpha[v_x^a]$.

Powiemy, że formuła α jest spełnialna w $\mathfrak{A}$, gdy istnieje wartościowanie v w strukturze $\mathfrak{A}$ takie, że zachodzi $\mathfrak{A} \models \alpha[v]$. Powiemy, że formuła α jest *spełnialna*, gdy istnieje struktura $\mathfrak{A}$, w której α jest spełnialna. Powiemy, że formuła α jest *prawdziwa* w $\mathfrak{A}$, gdy dla każdego wartościowania v w $\mathfrak{A}$ zachodzi $\mathfrak{A} \models \alpha[v]$. W tym przypadku mówimy też, że $\mathfrak{A}$ jest *modelem* dla formuły α (oznaczamy to przez $\mathfrak{A} \models \alpha$). Dla zbioru formuł Δ i Σ-struktury $\mathfrak{A}$ powiemy, że $\mathfrak{A}$ jest modelem dla Δ (oznaczamy $\mathfrak{A} \models \Delta$), gdy dla każdej formuły $\alpha \in \Delta$, zachodzi $\mathfrak{A} \models \alpha$. Powiemy, że formuła α jest *tautologią* (oznaczamy to przez $\models \alpha$), gdy jest ona prawdziwa w każdej Σ-strukturze. Można pokazać,że za wyjątkiem zdegenerowanych sygnatur (na przykład sygnatura składająca się jedynie z symbolu równości i stałych) nie istnieje algorytm na sprawdzanie czy dana formuła pierwszego rzędu jest tautologią.

Przykład 12.1

(i) Jeśli α jest tautologią rachunku zdań to każda formuła otrzymana z α przez wstawienie dowolnych formuł pierwszego rzędu na miejsce zmiennych zdaniowych (tak, że ta sama formuła jest wstawiana na miejsce tej samej zmiennej) jest tautologią języka pierwszego rzędu.

(ii) Niech α, β będą dowolnymi formułami języka pierwszego rzędu. Formuła $\forall x(\alpha \to \beta) \to (\forall x \alpha \to \forall x \beta)$ jest tautologią języka pierwszego rzędu. Aby to pokazać weźmy dowolną Σ-strukturę $\mathfrak{A}$, dowolne wartościowanie v i załóżmy, że zachodzą $\mathfrak{A} \models (\forall x(\alpha \to \beta))[v]$ oraz $\mathfrak{A} \models (\forall x \alpha)[v]$. Pokażemy, że zachodzi $\mathfrak{A} \models (\forall x \beta)[v]$. Niech $a \in A$ będzie dowolnym elementem. Ponieważ $\mathfrak{A} \models (\alpha \to \beta)[v_x^a]$ zachodzi oraz $\mathfrak{A} \models \alpha[v_x^a]$ zachodzi, to $\mathfrak{A} \models \beta[v_x^a]$ też zachodzi, co wobec dowolności a dowodzi, że $\mathfrak{A} \models (\forall x \beta)[v]$. W ten sposób pokazaliśmy, że

$$\mathfrak{A} \models (\forall x(\alpha \to \beta) \to (\forall x \alpha \to \forall x \beta))[v],$$

co wobec dowolności $\mathfrak{A}$ oraz v dowodzi, że rozważana formuła jest tautologią. Formuła ta reprezentuje prawo przesuwania kwantyfikatora ogólnego w głąb implikacji.

(iii) Pokażemy, że dla pewnych formuł α, β, formuła $(\forall x\alpha \to \forall x\beta) \to \forall x(\alpha \to \beta)$ nie jest tautologią języka pierwszego rzędu. Niech α będzie formułą $r_1(x)$ i niech β będzie formułą $r_2(x)$, gdzie r_1 oraz r_2 są symbolami relacji jednoargumentowych. Niech $A = \{0,1\}$ oraz $r_1^{\mathfrak{A}} = \{0\}$, $r_2^{\mathfrak{A}} = \{1\}$. Wówczas każda z formuł $\forall x\alpha$, $\forall x\beta$ oraz $\forall x(\alpha \to \beta)$ nie jest prawdziwa w $\mathfrak{A}$, a zatem cała rozważana formuła nie jest prawdziwa w $\mathfrak{A}$.

(iv) Ponieważ $=$ jest interpretowana w każdej strukturze jako relacja równości, to oczywiście formuła $\forall x \forall x(x = y \to y = x)$ jest tautologią języka pierwszego rzędu.

(v) Niech r będzie symbolem relacji dwuargumentowej. Formuła α_1 zdefiniowana wzorem
$\forall x\, r(x,x)$ jest prawdziwa w strukturze $\mathfrak{A} = \langle A, r^A \rangle$ wtw, gdy r^A jest relacją zwrotną. Podobnie formuła α_2 określona jako $\forall x \forall y((r(x,y) \wedge r(y,x)) \to x = y)$ wyraża antysymetrię r^A oraz formuła α_3 określona jako $\forall x \forall y \forall z((r(x,y) \wedge r(y,z)) \to r(x,z))$ wyraża przechodniość relacji r^A. Tak więc, formuła $\alpha_1 \wedge \alpha_2 \wedge \alpha_3$ jest prawdziwa w strukturze $\mathfrak{A} = \langle A, r^A \rangle$ wtw, gdy r^A jest częściowym porządkiem.

Niech β będzie formułą $\forall x(\forall y(r(x,y) \to x = y) \to \forall y r(y,x))$. Wówczas formuła $\alpha \to \beta$ wyraża własność relacji r^A: jeśli r^A jest częściowym porządkiem to każdy element maksymalny w r^A jest elementem największym. Oczywiście ta formuła nie jest tautologią. Jako przykład struktury, w której nie jest ona prawdziwa wystarczy wziąć jakikolowiek częściowy porządek, w którym ta własność nie zachodzi.

Natomiast, jeśli α_4 jest formułą $\forall x \forall y(r(x,y) \vee r(y,x))$ wyrażającą liniowść porządku, to formuła $(\alpha \wedge \alpha_4) \to \beta$ jest tautologią języka pierwszego rzędu. Wyraża ona własność, że w każdym liniowym porządku element maksymalny jest największy.

(vi) (*Dualność kwantyfikatorów*) Formułę $\exists x\alpha$ możemy wyrazić używając kwantyfikatora uniwersalnego i negacji: $\neg\forall x\neg\alpha$. Oznacza to, że formuły $\exists x\alpha \to \neg\forall x\neg\alpha$ oraz $(\neg\forall x\neg\alpha) \to \exists x\alpha$ są tautologiami języka pierwszego rzędu.

Zupełnie analogicznie można wyrazić kwatyfikator uniwersalny przy pomocy negacji i kwantyfikatora egzystencjalnego.

12.3 Podstawianie termów

Dla formuły α, termu σ i zmiennej x, napis $\alpha(\sigma/x)$ oznacza wynik podstawienia σ na wszystkie wolne wystąpienia x w α. Wykonywanie takiego podstawienia bez dodatkowych zastrzeżeń może prowadzić do kłopotów. Rozważmy formułę $\forall x\alpha$ i załóżmy, że jest ona prawdziwa w strukturze $\mathfrak{A}$. Zatem dla dowolnego termu σ powinna być też prawdziwa w $\mathfrak{A}$ formuła $\alpha(\sigma/x)$. Niestety tak być nie musi jak wynika z poniższego przykładu.

Niech α będzie formułą $\exists y(y \neq x)$. Niech term σ będzie zmienną y i niech $\mathfrak{A}$ będzie strukturą mającą co najmniej dwa elementy. Wówczas $\forall x\alpha$ jest prawdziwa w $\mathfrak{A}$, ale $\alpha(y/x)$ jest formułą $\exists y(y \neq y)$ i nie jest prawdziwa w $\mathfrak{A}$.

Źródłem problemu w powyższym przykładzie było to, że po wykonaniu podstawienia termu na miejsce zmiennej pojawiały się nowe wiązania kwantyfikatorem. Sugeruje to następującą definicję. Powiemy, że term σ jest *dopuszczalny* dla zmiennej x w formule α jeśli żadne wolne wystąpienie x w α nie jest zawarte w zasięgu kwantyfikatora $\forall y$ lub $\exists y$, gdzie y jest pewną zmienną występującą w σ.

Lemat 12.2 (O podstawieniu)
Niech $\mathfrak{A}$ będzie dowolną strukturą oraz $v : X \to A$ dowolnym wartościowaniem w $\mathfrak{A}$. Niech σ będzie dowolnym termem.

(i) Dla dowolnego termu τ i zmiennej x mamy

$$(\tau(\sigma/x))^{\mathfrak{A}}[v] = \tau^{\mathfrak{A}}[v^a_x],$$

gdzie $a = \sigma^{\mathfrak{A}}[v]$.

(ii) Dla dowolnej formuły α, jeśli term σ jest dopuszczalny dla x w formule α, to

$$\mathfrak{A} \models (\alpha(\sigma/x))[v] \quad \textit{wtedy i tylko wtedy, gdy} \quad \mathfrak{A} \models \alpha[v^a_x],$$

gdzie $a = \sigma^{\mathfrak{A}}[v]$.

Dowód: Część (i) dowodzimy prze indukcję ze względu na budowę termu τ. Jeśli τ jest zmienną x, to obie strony są równe $\sigma^{\mathfrak{A}}[v]$. Jeśli τ jest zmienną y (y jest różne od x), to obie strony są równe $v(y)$. Jeśli τ jest postaci $f(\tau_1, \ldots, \tau_n)$, to mamy następujące równości.

$$\begin{aligned}
(\tau(\sigma/x))^{\mathfrak{A}}[v] &= (f(\tau_1(\sigma/x), \ldots, \tau_n(\sigma/x)))^{\mathfrak{A}}[v] \\
&= f^{\mathfrak{A}}((\tau_1(\sigma/x))^{\mathfrak{A}}[v], \ldots, (\tau_n(\sigma/x))^{\mathfrak{A}}[v]) \\
&= f^{\mathfrak{A}}(\tau_1^{\mathfrak{A}}[v^a_x], \ldots, \tau_n^{\mathfrak{A}}[v^a_x]) \\
&= (f(\tau_1, \ldots, \tau_n))^{\mathfrak{A}}[v^a_x] = \tau^{\mathfrak{A}}[v^a_x].
\end{aligned}$$

Dowód (ii) przeprowadzamy przez indukcję ze względu na budowę formuły α. Jeśli α jest $\perp$ to teza jest oczywista. Jeśli α jest formułą atomową, to tezę natychmiast dostajemy z wyżej udowodnionej części (i). Na przykład, jeśli α jest postaci $\tau_1 = \tau_2$ to mamy:

$$\begin{aligned}
\mathfrak{A} \models (\alpha(\sigma/x))[v] &\iff (\tau_1(\sigma/x))^{\mathfrak{A}}[v] = (\tau_2(\sigma/x))^{\mathfrak{A}}[v] \\
&\iff \tau_1^{\mathfrak{A}}[v^a_x] = \tau_2^{\mathfrak{A}}[v^a_x] \\
&\iff \mathfrak{A} \models (\tau_1 = \tau_2)[v^a_x].
\end{aligned}$$

Druga z powyższych równoważności wynika z (i).

Krok indukcyjny dla przypadku, gdy α jest postaci $\beta \wedge \gamma$, lub $\beta \vee \gamma$, lub $\beta \to \gamma$ jest oczywisty i pozostawimy go czytelnikowi. Rozważymy przypadek gdy α jest postaci $\forall y\, \beta$. Wówczas zmienne x oraz y są różne oraz z dopuszczalności σ dla x w α wynika, że y nie występuje w σ. Ponadto $\alpha(\sigma/x)$ jest identyczne z $\forall y\, \beta(\sigma/x)$. Mamy nastepujące równoważności:

$$\begin{aligned} \mathfrak{A} \models (\forall y\, \beta(\sigma/x))[v] &\iff \text{dla każdego } d \in A,\ \mathfrak{A} \models (\beta(\sigma/x))[v^d_y] \\ &\iff \text{dla każdego } d \in A,\ \mathfrak{A} \models (\beta(\sigma/x))[v^{d\,a'}_{y\,x}], \end{aligned} \tag{59}$$

gdzie $a' = \sigma^{\mathfrak{A}}[v^d_y]$. Ponieważ y nie występuje w σ, to $a' = \sigma^{\mathfrak{A}}[v^d_y] = \sigma^{\mathfrak{A}}[v] = a$. Ponieważ zmienne x oraz y są różne, to $v^{d\,a}_{y\,x} = v^{a\,d}_{x\,y}$. Tak więc (59) jest równoważne zachodzeniu $\mathfrak{A} \models \beta[v^{a\,d}_{x\,y}]$, dla każdego $d \in A$. Czyli

$$\mathfrak{A} \models (\forall y\, \beta(\sigma/x))[v^a_x].$$

Przypadek, gdy α jest postaci $\exists y\, \beta$ jest bardzo podobny do powyższego i pozostawimy go czytelnikowi. ■

Natychmiastowym wnioskiem z Lematu 12.2 jest następujący przykład tautologii.

Fakt 12.3 *Dla dowolnej formuły α, zmiennej x i termu σ dopuszczalnego dla x w α, formuła*

$$\forall x \alpha \to \alpha(\sigma/x)$$

jest tautologią jezyka pierwszego rzędu.

12.4 Hilbertowski system dowodzenia

Ustalamy sygnaturę Σ. W poniższym systemie słowo *formuła* będzie oznaczać formułę w języku pierwszego rzędu nad Σ. Poniższy system dowodzenia dotyczy formuł opartych na spójnikach $\to$, $\bot$ oraz na kwantyfikatorze $\forall$. Przypomnijmy, że $\neg\alpha$ oznacza formułę $\alpha \to \bot$.

Przez *sekwent* będziemy rozumieć napis postaci $\Delta \vdash \alpha$, gdzie Δ jest zbiorem formuł a α jest formułą. Przez *generalizację* sekwentu $\Delta \vdash \alpha$ będziemy rozumieć jakikolwiek sekwent postaci $\Delta \vdash \forall x_1 \ldots \forall x_n \alpha$, gdzie $x_1, \ldots x_n$ są dowolnymi zmiennymi.

Aksjomaty
(A0) $\Delta, \alpha \vdash \alpha$;
Dowolne generalizacje następujących sekwentów:
(A1) $\Delta \vdash \alpha \to (\beta \to \alpha)$;
(A2) $\Delta \vdash (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$;
(A3) $\Delta \vdash \neg\neg\alpha \to \alpha$;

(A4) $\Delta \vdash \forall x(\alpha \to \beta) \to (\forall x\alpha \to \forall x\beta)$;
(A5) $\Delta \vdash \alpha \to \forall x\alpha$, o ile $x \notin FV(\alpha)$;
(A6) $\Delta \vdash \forall x\alpha \to \alpha(\sigma/x)$, o ile σ jest dopuszczalny dla x w α;
(A7) $\Delta \vdash x = x$;
(A8) $\Delta \vdash x_1 = y_1 \to (x_2 = y_2 \to \cdots \to (x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)) \cdots)$, dla $f \in \Sigma_n^F,\ n \geq 0$;
(A9) $\Delta \vdash x_1 = y_1 \to (x_2 = y_2 \to \cdots \to (x_n = y_n \to (r(x_1, \ldots, x_n) \to r(y_1, \ldots, y_n))) \cdots)$, dla $r \in \Sigma_n^R,\ n \geq 1$.

Reguła dowodzenia

$$(MP) \qquad \frac{\Delta \vdash \alpha;\ \Delta \vdash \alpha \to \beta}{\Delta \vdash \beta}$$

Wyprowadzanie sekwentów w powyższym systemie definiuje się dokładnie tak samo jak w przypadku rachunku zdań (por. uwagi na początku działu "Systemy dowodzenia" dla rachunku zdań). Fakt, że sekwent $\Delta \vdash \alpha$ daje się wyprowadzić w powyższym systemie będziemy oznaczać przez $\Delta \vdash_H \alpha$. Sam system, podobnie jak w przypadku rachunku zdań, będziemy oznaczać przez $\vdash_H$. Nie powinno prowadzić to do niejednoznaczności. Zwróćmy uwagę, że system $\vdash_H$ zależy od sygnatury Σ. Tak więc mamy różne systemy dla różnych sygnatur.

Powiemy, że zbiór formuł Δ jest *sprzeczny*, gdy $\Delta \vdash_H \bot$. Zbiór, który nie jest sprzeczny nazwiemy *niesprzecznym*. Zauważmy, że pojęcie 'być zbiorem sprzecznym' milcząco zakłada, że pracujemy z ustalonym systemem formalnym $\vdash_H$. Dla innego systemu formalnego mogłoby się tak zdarzyć, że klasa zbiorów sprzecznych jest inna.[16]

Przykład 12.4 Pokażemy dowód formuły $(x = y \to y = x)$.

1. $\vdash \forall x_1 \forall x_2 \forall y_1 \forall y_2 (x_1 = y_1 \to (x_2 = y_2 \to (x_1 = x_2 \to y_1 = y_2)))$ (A9)
2. $\vdash x = y \to (x = x \to (x = x \to y = x))$ na mocy (A6) oraz (MP)
3. $\vdash x = x \to (x = y \to (x = x \to y = x))$ z (2), na mocy rozumowania w rachunku zdań;
4. $\vdash x = x$ (A7)
5. $\vdash x = y \to (x = x \to y = x)$ (MP(4,3))
6. $\vdash x = x \to (x = y \to y = x)$ z (5), na mocy rozumowania w rachunku zdań;
7. $\vdash x = x$ (A7)

[16] Tak oczywiście nie może się zdarzyć dla żadnego systemu formalnego, który jest równoważny systemowi $\vdash_H$.

8. $\vdash x = y \to y = x$ (MP(7,6))

Twierdzenie 12.5 (O dedukcji)
Dla dowolnego zbioru Δ formuł oraz dowolnych formuł α, β, jeśli $\Delta, \alpha \vdash_H \beta$, to $\Delta \vdash_H \alpha \to \beta$.

Dowód: Dowód tego twierdzenia jest dokładnie taki sam jak analogicznego twierdzenia dla rachunku zadań (por. Twierdzenie 11.3). ∎

Natępujące twierdzenie mówi, że wybór nazwy na zmienną zwiazaną nie ma wpływu na 'dowodliwość' formuły. Jest to tzw. własność *α-konwersji.*

Twierdzenie 12.6 (O α-konwersji)
Jeśli $\Delta \vdash_H \forall x\ \beta$ oraz zmienna y jest dopuszczalna dla x w β oraz $y \notin FV(\forall x\ \beta)$, to $\Delta \vdash_H \forall y\ \beta(y/x)$.

Dowód: Ponieważ $y \notin FV(\forall x\ \beta)$, to na mocy (A5) mamy

$$\Delta \vdash (\forall x\ \beta) \to (\forall y \forall x\ \beta). \tag{60}$$

Z drugiej strony mamy następującą wersję aksjomatu (A6)

$$\Delta \vdash \forall y\ ((\forall x\ \beta) \to \beta(y/x)),$$

co łącznie z aksjomatem (A4) daje

$$(\forall y \forall x\ \beta) \to \forall y\ \beta(y/x). \tag{61}$$

Tak więc, zakładając $\Delta \vdash_H \forall x\ \beta$ i stosując (MP) do (60), a następnie do (61) dostajemy

$$\Delta \vdash \forall y\ \beta(y/x),$$

co kończy dowód. ∎

Podamy jeszcze jedno użyteczne twierdzenie. Mówi ono, że tzw. *reguła generalizacji* jest *dopuszczalna* w systemie $\vdash_H$. Niech

$$FV(\Delta) = \bigcup \{FV(\alpha) \mid \alpha \in \Delta\}.$$

Twierdzenie 12.7 (O generalizacji)
Jeśli zachodzi $\Delta \vdash_H \alpha$, to dla dowolnej zmiennej x, jeśli $x \notin FV(\Delta)$, to $\Delta \vdash_H \forall x\ \alpha$.

Dowód: Dowodzimy twierdzenie przez indukcję ze względu na liczbę kroków (czyli rozmiar drzewa) w dowodzie $\Delta \vdash_H \alpha$. Jeśli sekwent $\Delta \vdash \alpha$ jest aksjomatem (A1-9), to dowolna generalizacja tego sekwentu jest też aksjomatem, więc teza zachodzi. Dla generalizacji aksjomatu (A0) używamy aksjomatu (A5) i reguły (MP).

Jeśli natomiast ostatnią regułą w dowodzie było zastosowanie (MP), to dla pewnej formuły β mamy $\Delta \vdash_H \beta \to \alpha$ oraz $\Delta \vdash_H \beta$ w mniejszej liczbie kroków. Z założenia indukcyjnego otrzymujemy $\Delta \vdash_H \forall x\ (\beta \to \alpha)$ oraz $\Delta \vdash_H \forall x\ \beta$. Zatem

$$\dfrac{\dfrac{\Delta \vdash \forall x(\beta \to \alpha) \to (\forall x\beta \to \forall x\alpha) \quad \Delta \vdash \forall x\ (\beta \to \alpha)}{\Delta \vdash \forall x\beta \to \forall x\alpha} \qquad \Delta \vdash \forall x\ \beta}{\Delta \vdash \forall x\ \alpha}$$

W powyższym drzewie wykorzystaliśmy aksjomat (A4). ∎

Powiemy, że formuła α jest *konsekwencją semantyczną* zbioru formuł Δ (oznaczamy to przez $\Delta \models \alpha$), gdy dla każdej struktury $\mathfrak{A}$ i dla każdego wartościowania v w $\mathfrak{A}$, jeśli dla każdej formuły $\beta \in \Delta$ mamy $\mathfrak{A} \models \beta[v]$, to również zachodzi $\mathfrak{A} \models \alpha[v]$. Zwróćmy uwagę, że jeśli Δ jest zbiorem zdań, to powyższa definicja jest równoważna następującej własności: każdy model dla Δ jest modelem dla α. W ogólnym przypadku, gdy formuły z Δ mogą zawierać zmienne wolne, powyższe dwie definicje nie są równoważne. Na przykład, mamy $x = y \not\models f(z) = z$, ale każdy model dla $x = y$ (czyli jednoelementowy) jest modelem dla $f(z) = z$. Przyjęliśmy tutaj, że f jest symbolem operacji jednoargumentowej w sygnaturze.

Twierdzenie 12.8 (O adekwatności)
Dla dowolnego zbioru formuł Δ i formuły α, jeśli $\Delta \vdash_H \alpha$, to $\Delta \models \alpha$.

Dowód: Dowód przeprowadzamy przez indukcję ze względu na liczbę kroków w dowodzie sekwentu $\Delta \vdash \alpha$. Oczywiście mamy $\Delta, \alpha \models \alpha$. Sprawdzamy, że jeśli $\Delta \vdash \alpha$ jest dowolną generalizacją sekwentu (A1-9), to zachodzi $\Delta \models \alpha$. Oczywiście reguła (MP) zachowuje relację semantycznej konsekwencji, tzn. jeśli $\Delta \models \alpha$ i $\Delta \models \alpha \to \beta$, to $\Delta \models \beta$. ∎

Twierdzenie o adekwatności może być użyte do pokazania, że pewne sekwenty nie dają się wyprowadzić w systemie $\vdash_H$. Przykładowo, zobaczmy, że $x = y \not\vdash_H \forall x\ x = y$. Istotnie, biorąc strukturę $\mathfrak{A}$ dwuelementową oraz wartościowanie, które 'skleja' zmienne x oraz y dostajemy $x = y \not\models \forall x\ x = y$. Zatem z twierdzenia o adekwatności wnioskujemy, że $x = y \not\vdash_H \forall x\ x = y$. Jest to również przykład na to, że system $\vdash_H$ nie jest zamknięty na dowolne generalizacje, tzn. założenie $x \notin FV(\Delta)$ w twierdzeniu o generalizacji jest istotne.

Zachodzi również odwrotne twierdzenie do Twierdzenia 12.8. Jest to tzw. *silne twierdzenie o pełności* dla systemu $\vdash_H$. Udowodnimy go w dziale poświęconym teorii modeli.

System formalny dla formuł zawierających pozostałe spójniki: $\wedge$, $\vee$ i kwantyfikator egzystencjalny otrzymuje się z $\vdash_H$ przez dodanie aksjomatów charakteryzujących te symbole:
(C1) $\Delta \vdash (\alpha \wedge \beta) \rightarrow \neg(\alpha \rightarrow \neg\beta)$
(C2) $\Delta \vdash \neg(\alpha \rightarrow \neg\beta) \rightarrow (\alpha \wedge \beta)$
(D1) $\Delta \vdash (\alpha \vee \beta) \rightarrow (\neg\alpha \rightarrow \beta)$
(D2) $\Delta \vdash (\neg\alpha \rightarrow \beta) \rightarrow (\alpha \vee \beta)$
(E1) $\Delta \vdash \exists x\ \alpha \rightarrow \neg\forall x\ \neg\alpha$
(E2) $\Delta \vdash (\neg\forall x\ \neg\alpha) \rightarrow \exists x\ \alpha$

12.5 Teorie aksjomatyczne

Niech Δ będzie zbiorem zdań nad sygnaturą Σ. Formuły ze zbioru Δ możemy traktować jak aksjomaty specyficzne pewnej teorii, czyli formuły które przyjmujemy bez dowodu. *Teorią* nad zbiorem aksjomatów Δ nazwiemy zbiór $Th(\Delta)$ wszystkich formuł α takich, że $\Delta \vdash_H \alpha$. Z twierdzenia o pełności wynika, że do $Th(\Delta)$ należą dokładnie wszystkie formuły α, które są prawdziwe we wszystkich modelach zbioru Δ.

Poniżej podamy dwa przykłady takich teorii: arytmetykę Peano i teorię mnogości Zermelo-Fraenkla.

12.5.1 Arytmetyka Peano

Sygnatura Σ dla tej teorii jest zdefiniowana następująco.
$\Sigma_0^F = \{0\}$,
$\Sigma_1^F = \{S\}$,
$\Sigma_2^F = \{+,\ \times\}$,
$\Sigma_2^R = \{<,\ =\}$.

Symboli $+$, $\times$ oraz $<$ używamy stosując infiksową notację. Na przykład, napis $x + y$ oznacza term $+(x, y)$, a napis $x < y$ oznacza formułę $<(x, y)$.

Arytmetykę Peano przedstawia się w oparciu o nieskończony zbiór aksjomatów. Pierwsze osiem aksjomatów wygląda następująco.

(P-1) $\forall x\ \neg(S(x) = 0)$
(P-2) $\forall x \forall y\ (S(x) = S(y) \rightarrow x = y)$
(P-3) $\forall x\ x + 0 = 0$
(P-4) $\forall x \forall y\ x + S(y) = S(x + y)$
(P-5) $\forall x\ x \times 0 = 0$
(P-6) $\forall x \forall y\ x \times S(y) = (x \times y) + x$
(P-7) $\forall x\ \neg(x < 0)$

(P-8) $\forall x \forall y\ (x < S(y) \to (\neg(x = y) \to x < y))$

Ostatnia grupa aksjomatów jest wyznaczona przez następujący schemat przedstawiający zasadę indukcji. Aksjomat $(\text{P-9})_{\alpha,x}$ zależy od wyboru formyły α oraz zmiennej x wolno występującej w α.

$(\text{P-9})_{\alpha,x}$ $\forall y_1 \ldots \forall y_n\ (\alpha(0/x) \to (\forall x\ (\alpha \to \alpha(S(x)/x)) \to \forall x\ \alpha))$

gdzie $y_1, \ldots, y_n$ są wszystkimi zmiennymi wolnymi formuły α za wyjątkiem zmiennej x.

12.5.2 Teoria mnogości Zermelo-Fraenkla

Poniższa aksjomatyka została zaproponowana przez E. Zermelo i uzupełniona przez A.A. Fraenkla. Sygnatura Σ dla tej aksjomatyki składa się jedynie z dwóch dwuargumentowych symboli relacji: $\in$ oraz $=$.

Aksjomaty wyrażają własności, do których nieformalnie odwoływaliśmy się podczas tego wykładu.

(ZFC-1) (*Aksjomat ekstensjonalności*)
$\forall y \forall z(\forall x(x \in y \leftrightarrow x \in z) \to y = z)$

(ZFC-2) (*Aksjomat zbioru pustego*)
$\exists x \forall y(y \notin x)$

(ZFC-3) (*Aksjomat sumy*)
$\forall x \exists u \forall y(y \in u \leftrightarrow \exists z(z \in x \wedge y \in z))$

(ZFC-4) (*Aksjomat zbioru potęgowego*)
$\forall x \exists p \forall y(y \in p \leftrightarrow \forall z(z \in y \to z \in x))$

(ZFC-5) (*Aksjomat nieskończoności*)
$\exists x((\emptyset \in x) \wedge \forall y(y \in x \to \exists z(z \in x \wedge \forall u(u \in z \leftrightarrow (u \in y \vee u = y)))))$

Powyższy aksjomat wyraża istnienie zbioru induktywnego. Dla ułatwienia czytania tej formuły użyliśmy symbolu $\emptyset$ spoza języka. Symbol ten można wyeliminować pisząc zamiast $(\emptyset \in x)$ formułę $(\exists p((\forall y\ y \notin p) \wedge p \in x))$.

(ZFC-6) (*Aksjomat regularności*)
$\forall x(\exists y y \in x) \to \exists y(y \in x \wedge \forall z(z \in x \to z \notin y))$

Aksjomat regularności postuluje, że każdy niepusty zbiór x zawiera element rozłączny z x. W szczególności wynika z tego aksjomatu, że $x \notin x$.

Pozostałe dwa aksjomaty opiszemy słowami. Wyrażenie ich w języku teorii mnogości pozostawimy czytelnikowi jako ćwiczenie.

(ZFC-7) (*Aksjomat wyboru*)
Dla dowolnego niepustego zbioru x zbiorów niepustych i parami rozłącznych istnieje zbiór y mający z każdym elementem zbioru x dokładnie jeden element wspólny.

Ostatni schemat reprezentuje nieskończenie wiele aksjomatów, po jednym dla każdego wyboru formuły α oraz zmiennych x i y. Formuła α może zawierać zmienne wolne inne niż x oraz y.[17] Niech $x_1, \ldots, x_n$ będą wszystkimi zmiennymi wolnymi fromuły α różnymi od x oraz y.

$(\text{ZFC-8})_{\alpha,x,y}$ (*Aksjomat zastępowania dla formuły α i zmiennych x oraz y*)
Dla dowolnych $x_1, \ldots, x_n$ następująca własność zachodzi: jeśli dla każdego x istnieje dokładnie jeden taki y, że spełniony jest warunek α, to dla każdego zbioru z istnieje taki zbiór u zawierający te i tylko te elementy y takie, że istnieje x należący do z, spełniający warunek α.

W powyższym aksjomacie zmienne $x_1, \ldots, x_n$ pełnią rolę parametrów. Zbiór u, o którym mowa w tym aksjomacie zależy nie tylko od zbioru z, ale też od parametrów $x_1, \ldots, x_n$. Podamy trzy przykłady zastosowania tego aksjomatu.

Przykład 12.9 Weźmy jako formułę α w $(\text{ZFC-8})_{\alpha,x,y}$

$$\forall p \ (p \notin y).$$

Zatem zmienna x nie występuje w α. Z aksjomatu zbioru pustego i aksjomatu ekstensjonalności wynika, że dla każdego x istnieje dokładnie jeden y spełniający formułę α (a mianowicie zbiór pusty). Biorąc w aksjomacie zastępowania jako z dowolny zbiór niepusty otrzymujemy istnienie zbioru u, którego jedynym elementem jest zbiór pusty, czyli istnienie $u = \{\emptyset\}$.

Przykład 12.10 Weźmy teraz jako formułę α w $(\text{ZFC-8})_{\alpha,x,y}$

$$y = x_1.$$

Zmienna x nie występuje w α a zmienna x_1 jest parametrem. Niech x_1 będzie dowolnym zbiorem. Oczywiście istnieje dokładnie jeden zbiór y taki, że α zachodzi. Niech z będzie dowolnym zbiorem niepustym, np. $z = \{\emptyset\}$. Zatem istnieje zbiór u taki, że dla każdego y, zachodzi

$$y \in u \leftrightarrow \exists x (x \in z \wedge y = x_1).$$

Ponieważ z jest niepusty oraz x nie występuje w $y = x_1$, to powyższa formuła jest równoważna

$$y \in u \leftrightarrow y = x_1.$$

Zatem pokazaliśmy istnienie zbioru $\{x_1\}$ dla każdego zbioru x_1.

[17] Zauważmy, że nie zakładamy tutaj, że x oraz y muszą występować wolno w α. Zauważmy też, że jeśli y nie występuje wolno w α to $(\text{ZFC-8})_{\alpha,x,y}$ przedstawia tautologię.

Przykład 12.11 Weźmy jako α formułę

$$\forall p\ (p \in y \leftrightarrow p = x).$$

Jak wynika z Przykładu 12.10 oraz z aksjomatu ekstensjonalności, dla każdego x istnieje dokładnie jeden y dla którego prawdziwa jest α. Zatem w tym przypadku aksjomat zastępowania mówi, że dla każdego zbioru z istnieje zbiór u, który się składa z wszystkich singletonów zbioru z, czyli

$$u = \{\{x\} \mid x \in z\}.$$

12.6 Elementy teorii modeli

W tej części notatek przedstawimy kilka klasycznych wyników z teorii modeli. Podstawowym narzędziem będzie tzw. *twierdzenie o istnieniu modelu.* Pokażemy szereg zastosowań i wniosków wynikających z tego bardzo ważnego twierdzenia, między innymi *twierdzenie o zwartości* i *silne twierdzenie o pełności.* Metoda dowodu twierdzenia o istnieniu modelu poolega ona na budowaniu modelu ze stałych. Zaproponował ją L. Henkin.

Najpierw wprowadzimy następującą definicję. Niech Γ będzie zbiorem zdań pierwszego rzędu nad sygnaturą Σ oraz niech $C \subseteq \Sigma_0$ będzie pewnym zbiorem stałych. Powiemy, że Γ jest zbiorem *C-nasyconym*, gdy Γ jest zbiorem niesprzecznym oraz dla dowolnej formuły $\alpha(x)$ o jednej zmiennej wolnej (x może nie występować w α), jeśli $\Gamma \nvdash \forall x\ \alpha(x)$, to istnieje stała $c \in C$, taka że $\Gamma \vdash \neg\alpha(c/x)$.

Niech Γ będzie C-nasycony. Zauważmy, że jeśli $\Gamma \vdash \neg\forall x\ \alpha(x)$ oraz jeśli α jest postaci $\neg\beta$ (α zawiera co najwyżej jedną zmienną wolną), to wówczas $\Gamma \vdash \neg\forall x\ \alpha(x)$ jest równoważne $\Gamma \vdash \exists x\ \beta(x)$. Ponadto z warunku C-nasyconości Γ wynika istnienie stałej $c \in C$ takiej, że $\Gamma \vdash \neg\alpha(c/x)$. To ostatnie jest równoważne (na mocy prawa podwójnego przeczenia) $\Gamma \vdash \beta(c/x)$. Tak więc w tym przypadku c jest 'świadkiem' zachodzenia $\Gamma \vdash \exists x\ \beta(x)$.

Mocą sygnatury Σ nazwiemy moc zbioru $(\bigcup_{n=0}^{\infty} \Sigma_n^F) \cup (\bigcup_{n=1}^{\infty} \Sigma_n^R)$. Moc sygnatury Σ będziemy oznaczać przez $|\Sigma|$.

Lemat 12.12 (O nasyceniu)
Niech C będzie nieskończonym zbiorem, rozłącznym z sygnaturą Σ oraz takim, że $|\Sigma| \leq |C|$. Niech Δ będzie niesprzecznym zbiorem zdań nad Σ. Istnieje zbiór zdań Γ nad sygnaturą $\Sigma(C)$ taki, że $\Delta \subseteq \Gamma$ oraz Γ jest C-nasycony.

Dowód: Przedstawimy dowód dla przypadku kiedy Σ i C są zbiorami przeliczalnymi. Dowód ogólnego przypadku pozostawimy czytelnikowi do uzupełnienia. Ustawmy zbiór wszystkich formuł nad $\Sigma(C)$ o jednej zmiennej wolnej x w ciąg $\alpha_0, \alpha_1, \ldots$. Zdefiniujemy ciąg zbiorów $\{\Gamma_n \mid n \in N\}$ oraz ciąg stałych $\{c_n \mid n \in N\}$ o następujących własnościach:

- Γ_n zawiera skończenie wiele stałych z C.

- $\Delta \subseteq \Gamma_n$ jest niesprzecznym zbiorem zdań nad $\Sigma(C)$.
- Jeśli $\Gamma_n \not\vdash \forall x\ \alpha_n(x)$, to
$$\Gamma_{n+1} = \Gamma_n \cup \{\neg\alpha_n(c_n/x)\}.$$

Przyjmujemy $\Gamma_0 = \Delta$. Jeśli $\Gamma_n \vdash \forall x\ \alpha_n(x)$, to definiujemy $\Gamma_{n+1} = \Gamma_n$. Jeśli natomiast $\Gamma_n \not\vdash \forall x\ \alpha_n(x)$ to niech c_n będzie stałą nie występującą w Γ_n ani w α_n. Musimy pokazać, że $\Gamma_{n+1} = \Gamma_n \cup \{\neg\alpha_n(c_n/x)\}$ jest zbiorem niesprzecznym. Załóżmy przeciwnie, że

$$\Gamma_{n+1} \vdash \bot.$$

Zatem $\Gamma_n \vdash \neg\neg\alpha_n(c_n/x)$ i z (A3) dostajemy $\Gamma_n \vdash \alpha_n(c_n/x)$. Ponieważ c_n nie występuje w Γ_n ani w α_n to możemy w dowodzie powyższego sekwentu zamienić wszystkie wystąpienia c_n przez nową zmienną z, która się w tym dowodzie nie pojawiła. Tak więc otrzymujemy $\Gamma_n \vdash \alpha_n(z/x)$ oraz $z \notin FV(\Gamma_n)$. Na mocy twierdzenia o generalizacji (por. Twierdzenie 12.7) dostajemy $\Gamma_n \vdash \forall z\ \alpha_n(z/x)$. Stosując α-konwersję (por. Twierdzenie 12.6) dostajemy $\Gamma_n \vdash \forall x\ \alpha_n(x)$. Otrzymana sprzeczność dowodzi niesprzeczności zbioru Γ_{n+1}. To kończy konstrukcję zbiorów Γ_n oraz stałych c_n.

Niech

$$\Gamma = \bigcup_{n\in N} \Gamma_n.$$

Pokażemy, że Γ jest zbiorem C-nasyconym. Oczywiście Γ jako suma łańcucha zbiorów niesprzecznych jest również zbiorem niesprzecznym. Niech $\alpha(x)$ będzie dowolną formułą nad $\Sigma(C)$ o jednej zmiennej wolnej i załóżmy, że $\Gamma \not\vdash \forall x\ \alpha(x)$. Niech n będzie miejscem, na którym pojawia się formuła α w ciągu $\alpha_0, \alpha_1, \ldots$. Oczywiście mamy $\Gamma_n \not\vdash \forall x\ \alpha_n(x)$ i z konstrukcji zbiorów Γ_n wynika, że $\Gamma_{n+1} \vdash \neg\alpha_n(c_n/x)$. Zatem $\Gamma \vdash \neg\alpha_n(c_n/x)$, co dowodzi C-nasyconości zbioru Γ. ■

Teraz możemy przejść do twierdzenia o istnieniu modelu.

Twierdzenie 12.13 (O istnieniu modelu)
Dla dowolnej sygnatury Σ, każdy niesprzeczny zbiór zdań nad Σ ma model.

Dowód: Załóżmy, że Δ jest niesprzecznym zbiorem zdań. Niech C będzie dowolnym nieskończonym zbiorem rozłącznym z Σ i takim, że $|C| \geq |\Sigma|$. Zbudujemy model dla Δ ze stałych z C. Z lematu o nasyceniu (por. Lemat 12.12) wiemy, że istnieje zbiór zdań $\Gamma \supseteq \Delta$ nad sygnaturą $\Sigma(C)$, który jest C-nasycony. Stosując w sposób całkowicie rutynowy lemat Kuratowskiego-Zorna dowodzimy, że istnieje taki zbiór Γ maksymalny. Niech Γ będzie takim zbiorem. Dalsza część dowodu będzie przebiegała w odniesieniu do ustalonego zbioru Γ.

Najpierw zanotujmy następującą ważną własność zbioru Γ. Dla dowolnego zdania α,

$$\text{jeśli } \Gamma \not\vdash \alpha, \text{ to } \Gamma \cup \{\alpha\} \text{ jest zbiorem sprzecznym.} \tag{62}$$

Dla dowodu (62) zauważmy, że jeśli $\Gamma \cup \{\alpha\}$ jest zbiorem niesprzecznym, to jest on C-nasycony. Istotnie, jeśli $\Gamma \cup \{\alpha\} \not\vdash \forall x\ \beta(x)$, dla pewnej formuły β o jednej zmiennej wolnej, to mamy również $\Gamma \not\vdash \forall x\ \beta(x)$. Zatem dla pewnej stałej $c \in C$ zachodzi $\Gamma \vdash \neg\beta(c/x)$, więc oczywiście również $\Gamma \cup \{\alpha\} \vdash \neg\beta(c/x)$. Tak więc z maksymalności zbioru Γ wynika, że $\Gamma \cup \{\alpha\}$ musi być zbiorem sprzecznym. To dowodzi (62).

W zbiorze C definiujemy relację równoważności $\sim$:

$$c_1 \sim c_2 \quad \text{wtedy i tylko wtedy, gdy} \quad \Gamma \vdash c_1 = c = c_2.$$

Nośnikiem struktury $\mathfrak{A}_\Gamma$, która będzie modelem dla Γ (a zatem i dla Δ) jest zbiór ilorazowy $C/\sim$. Musimy określić interpretację symboli operacji i relacji z Σ. Dla przykładu załóżmy, że $f \in \Sigma_2^F$ jest symbolem operacji dwuargumentowej. Funkcję $f^{\mathfrak{A}_\Gamma} : C/\sim \to C/\sim$ definiujemy następującym warunkiem

$$f^{\mathfrak{A}_\Gamma}([c_1]_\sim, [c_2]_\sim) = [d]_\sim \quad \text{wtedy i tylko wtedy, gdy} \quad \Gamma \vdash f(c_1, c_2) = d.$$

Dla pokazania, że $f^{\mathfrak{A}_\Gamma}$ jest dobrze określoną funkcją musimy sprawdzić następujące dwie własności:

$$\text{Dla dowolnych } c_1, c_2 \in C \text{ istnieje } d \in C \text{ takie, że } \Gamma \vdash f(c_1, c_2) = d \tag{63}$$

$$\text{Jeśli } c_1 \sim c_1',\ c_2 \sim c_2' \text{ oraz } \Gamma \vdash f(c_1, c_2) = d \text{ i } \Gamma \vdash f(c_1', c_2') = d',\ \text{to } d \sim d'. \tag{64}$$

Własność (63) wynika z faktu, że Γ jest C-nasycony. Zauważmy najpierw, że $\Gamma \vdash \neg\forall x\ \neg f(c_1, c_2) = x$. Istotnie, załóżmy $\forall x\ \neg f(c_1, c_2) = x$. Wówczas a aksjomatu (A6) dostajemy $\neg f(c_1, c_2) = f(c_1, c_2)$. Z drugiej strony z aksjomatu (A7) i (A6) dostajemy $f(c_1, c_2) = f(c_1, c_2)$. Tak więc otrzymujemy $\bot$, co pokazuje $\Gamma \vdash \neg\forall x\ \neg f(c_1, c_2) = x$. Zatem z C-nasyconości Γ wynika istnienie stałej $d \in C$ takiej, że $\Gamma \vdash \neg\neg f(c_1, c_2) = d$. Korzystając teraz z (A3) dostajemy $\Gamma \vdash f(c_1, c_2) = d$.

(64) wynika natychmiast z następującej postaci aksjomatu (A8) (postać tę otrzymujemy z (A8) z pomocą aksjomatu (A6))

$$c_1 = c_1' \to (c_2 = c_2' \to f(c_1, c_2) = f(c_1', c_2')).$$

Interpretacja symboli relacji w $\mathfrak{A}_\Gamma$ wygląda podobnie. Dla przykładu zdefiniujemy relację $r^{\mathfrak{A}_\Gamma}$ dla symbolu $r \in \Sigma_2^R$.

$$([c_1]_\sim, [c_2]_\sim) \in r^{\mathfrak{A}_\Gamma} \quad \text{wtedy i tylko wtedy, gdy} \quad \Gamma \vdash r(c_1, c_2).$$

W tym przypadku również musimy dowieść poprawności definicji (tzn. niezależności od wyboru reprezentantów). Czyli musimy pokazać, że jeśli $c_1 \sim c_1'$ oraz $c_2 \sim c_2'$, to

$$\Gamma \vdash r(c_1, c_2) \quad \text{wtedy i tylko wtedy, gdy} \quad \Gamma \vdash r(c_1', c_2').$$

Wynika to natychmiast z aksjomatu (A9) i (A6).

Następująca własność jest wystarczająca dla zakończenia dowodu (zauważmy, że wynika z niej iż $\mathfrak{A}_\Gamma$ jest modelem dla Γ). Dla dowolnej formuły α takiej, że $FV(\alpha) \subseteq \{x_1, \ldots, x_n\}$ oraz dla dowolnego wartościowania v, jeśli $v(x_i) = [c_i]_\sim$, dla $i = 1, \ldots, n$, to

$$\mathfrak{A}_\Gamma \models \alpha[v] \quad \text{wtedy i tylko wtedy, gdy} \quad \Gamma \vdash \alpha(c_1/x_1, \ldots, c_n/x_n). \tag{65}$$

Powyższą własność dowodzimy przez indukcję ze względu na budowę formuły α. Dla formuł atomowych musimy dowieść następującą pomocniczą własność. Dla dowolnego termu τ i stałej $d \in C$ mamy

$$\tau^{\mathfrak{A}_\Gamma}[v] = [d]_\sim \quad \text{wtedy i tylko wtedy, gdy} \quad \Gamma \vdash \tau(c_1/x_1, \ldots, c_n/x_n) = d, \tag{66}$$

gdzie $FV(\tau) \subseteq \{x_1, \ldots, x_n\}$ oraz $v(x_i) = [c_i]_\sim$, dla $i = 1, \ldots, n$. Dowód (66) przeprowadzamy przez rytunową indukcję ze względu na budowę termu τ. Szczegóły pozostawiamy czytelnikowi.

Powracamy do dowodu (65). Jeśli α jest formułą $\tau_1 = \tau_2$, to $\tau_1^{\mathfrak{A}_\Gamma}[v] = \tau_2^{\mathfrak{A}_\Gamma}[v]$ wtedy i tylko wtedy, gdy dla pewnego $d \in C$ zachodzi $\tau_1^{\mathfrak{A}_\Gamma}[v] = [d]_\sim$ oraz $\tau_2^{\mathfrak{A}_\Gamma}[v] = [d]_\sim$. Na mocy (66) jest to równoważne temu, że dla pewnego $d \in C$ zachodzi $\Gamma \vdash \tau_1(c_1/x_1, \ldots, c_n/x_n) = d$ oraz $\Gamma \vdash \tau_2(c_1/x_1, \ldots, c_n/x_n) = d$. Ostatnia własność jest równoważna (na mocy C-nasyconości zbioru Γ) zachodzeniu $\Gamma \vdash \tau_1(c_1/x_1, \ldots, c_n/x_n) = \tau_2(c_1/x_1, \ldots, c_n/x_n)$.

Załóżmy teraz, że α jest formułą postaci $\beta \to \gamma$. Niech β^* oznacza formułę $\beta(c_1/x_1, \ldots, c_n/x_n)$ oraz niech γ^* oznacza formułę $\gamma(c_1/x_1, \ldots, c_n/x_n)$. Załóżmy, że zachodzi $\mathfrak{A}_\Gamma \models \alpha[v]$ i rozważmy dwa przypadki. Jeśli $\Gamma \vdash \beta^*$, to na mocy założenia indukcyjnego mamy $\mathfrak{A}_\Gamma \models \beta[v]$. Zatem $\mathfrak{A}_\Gamma \models \gamma[v]$ i korzystając ponownie z założenia indukcyjnego otrzymujemy $\Gamma \vdash \gamma^*$. Zatem na mocy aksjomatu (A1) i reguły (MP) otrzymujemy $\Gamma \vdash \beta^* \to \gamma^*$. Jeśli natomiast $\Gamma \nvdash \beta^*$, to jak wynika z (62) $\Gamma \cup \{\beta^*\}$ jest zbiorem sprzecznym. Zatem $\Gamma \cup \{\beta^*\} \vdash \gamma^*$ i z twierdzenia o dedukcji (por. Twierdzenie 12.5) dostajemy ponownie $\Gamma \vdash \beta^* \to \gamma^*$. Dowód implikacji odwrotnej, tzn., że $\Gamma \vdash \beta^* \to \gamma^*$ pociąga $\mathfrak{A}_\Gamma \models \alpha[v]$ pozostawiamy czytelnikowi do uzupełnienia.

Na koniec rozważmy przypadek gdy α jest postaci $\forall y\ \beta(y)$. Załóżmy, że $\mathfrak{A}_\Gamma \models \alpha[v]$. Niech β^* oznacza formułę $\beta(c_1/x_1, \ldots, c_n/x_n)$. Formuła β^* ma co najwyżej jedną zmienną wolną y. Jeśli $\Gamma \nvdash \forall y\ \beta^*$, to z C-nasyconości Γ istnieje taka stała $d \in C$, że $\Gamma \vdash \neg\beta^*(d/y)$. Zatem na mocy założenia indukcyjnego otrzymujemy $\mathfrak{A}_\Gamma \not\models \beta[v_y^{[d]_\sim}]$, co daje sprzeczność z naszym założeniem $\mathfrak{A}_\Gamma \models \alpha[v]$. Tak więc musi być $\Gamma \vdash \forall y\ \beta^*$. Na odwrót, załóżmy, że $\Gamma \vdash \forall y\ \beta^*$ i niech $d \in C$ będzie dowolną stałą. Z aksjomatu (A6) dostajemy $\Gamma \vdash \beta^*(d/y)$ i na mocy założenia indukcyjnego dostajemy $\mathfrak{A}_\Gamma \models \beta[v_y^{[d]_\sim}]$. Ponieważ d jest dowolne, to powyższe spełnianie dowodzi $\mathfrak{A}_\Gamma \models \alpha[v]$. Tym samym dowód twierdzenia jest zakończony. ■

Natychmiastowym wnioskiem z twierdzenia o istnieniu modelu jest twierdzenie o zwartości.

Twierdzenie 12.14 (O zwartości)
Dla dowolnej sygnatury Σ i dowolnego zbioru Δ zdań nad Σ, jeśli każdy skończony podzbiór zbioru Δ ma model, to cały zbiór Δ ma model.

Dowód: Jeśli każdy skończony podzbiór zbioru Δ ma model, to Δ musi być niesprzeczny. Istotnie, gdyby $\Delta \vdash_H \bot$, to dla pewnego skończonego podzbioru $\Delta_0 \subseteq \Delta$ mielibyśmy $\Delta_0 \vdash_H \bot$. Zatem z twierdzenia o adekwatności, Δ_0 nie ma modelu. Stosując twierdzenie o istnieniu modelu do niesprzecznego zbioru Δ dostajemy tezę. ■

Twierdzenie o zwartości bywa bardzo użyteczne do pokazywania, że pewne własności nie dają się wyrazić w języku pierwszego rzędu. Podamy przykład takiej własności.

Twierdzenie 12.15 *Niech Σ będzie dowolną sygnaturą zawierającą symbol dwuargumentowej relacji r. Nie istnieje zbiór Δ zdań nad Σ taki, że dla dowolnej Σ-struktury $\mathfrak{A}$, relacja $r^{\mathfrak{A}}$ jest dobrze ufundowana wtw, gdy $\mathfrak{A} \models \Delta$. Zatem własność relacji 'być dobrze ufundowaną' nie jest wyrażalna w języku pierwszego rzędu.*

Dowód: Załóżmy, że taki zbiór Δ istnieje. Niech $\{c_n \mid n \in N\}$ będzie nieskończonym zbiorem stałych nie należących do sygnatury Σ. Niech Γ będzie zdefiniowane następująco

$$\Gamma = \Delta \cup \{r(c_{n+1}, c_n) \wedge \neg c_{n+1} = c_n \mid n \in N\}.$$

Pokażemy, że każdy skończony podzbiór zbioru Γ ma model. Jeśli $\Gamma_0 \subseteq \Gamma$ jest skończony, to jako model dla Γ_0 można wziąć zbiór liczb naturalnych N, w którym r jest interpretowane jako $\leq$. Stałe interpretujemy następująco: niech c_n będzie stałą o największym indeksie n, występującą w Γ_0. Wówczas dla $i \leq n$ interpretujemy c_i jako liczbę $n - i$. Pozostałe stałe c_i, dla $i > n$ interpretujemy jako 0. Oczywiście mamy w takiej strukturze $c_0 > c_1 > \ldots > c_n$, co wystarcza do tego żeby ta struktura była modelem dla Γ_0. Z twierdzenia o zwartości wynika, że cały zbiór Γ ma model $\mathfrak{A}$. W tym modelu relacja $r^{\mathfrak{A}}$ nie jest dobrze ufundowana bo stałe $c_0^{\mathfrak{A}}, c_1^{\mathfrak{A}}, \ldots$ tworzą nieskończony zstępujący ciąg. Otrzymana sprzeczność dowodzi, że postulowany zbiór zdań Δ nie istnieje. ■

Innym wnioskiem z twierdzenia o zwartości jest następujące twierdzenie pokazujące jak mogą wyglądać moce modeli nieskończonych dla dowolnych zbiorów zdań pierwszego rzędu.

Twierdzenie 12.16 (Löwenheim, Skolem, Tarski)
Niech Δ będzie dowolnym zbiorem formuł nad sygnaturą Σ. Jeśli Δ ma nieskończony model, to Δ ma model każdej nieskończonej mocy, nie mniejszej niż $|\Sigma|$.

Dowód: Niech C będzie dowolnym nieskończonym zbiorem takim, że $|C| \geq |\Sigma|$. Rozważmy następujący zbiór zdań nad sygnaturą $\Sigma(C)$.

$$\Gamma = \Delta \cup \{\neg c = d \mid c, d \in C \text{ są różnymi stałymi}\}.$$

Oczywiście każdy model zbioru Γ ma moc co najmniej $|C|$. Pokażemy, że Γ ma model mocy $|C|$. Ponieważ każdy skończony podzbiór zbioru Γ ma model (bo Δ ma model nieskończony), to na mocy twierdzenia o zwartości Γ ma model. Co więcej, jak wynika to z dowodu twierdzenia o istnieniu modelu, Γ ma model (zbudowany z nowych stałych) o mocy nie większej niż $|C| = |\Sigma(C)|$. Zatem Γ ma model mocy $|C|$. ■

W szczególności wynika z powyższego twierdzenia, że jeśli teoria mnogości ma model, to ma model przeliczalny. Podobnie, jeśli aksjomatyka Peano ma model, to ma model dowolnej nieprzeliczalnej mocy.

Na zakończenie udowodnimy zapowiedziane wcześniej silne twierdzenie o pełności dla systemu $\vdash_H$. Jest ono prostym wnioskiem z twierdzenia o istnieniu modelu.

Twierdzenie 12.17 (Silne twierdzenie o pełności)
Dla dowolnego zbioru formuł Δ i dla dowolnej formuły α, jeśli $\Delta \models \alpha$, to $\Delta \vdash_H \alpha$. W szczególności, jeśli α jest tautologią języka pierwszego rzędu, to $\vdash_H \alpha$.

Dowód: Załóżmy, że $\Delta \not\vdash \alpha$. Niech $C = \{c_0, c_1, \ldots\}$ będzie nieskończonym przeliczalnym zbiorem stałych, rozłącznym z sygnaturą Σ. Dla dowolnej formuły β nad sygnaturą Σ niech β^* oznacza zdanie nad sygnaturą $\Sigma(C)$ otrzymane z β przez zastąpienie każdej zmiennej x_n wolno występującej w β przez stałą c_n. Niech $\Delta^* = \{\beta^* \mid \beta \in \Delta\}$.

Twierdzimy, że zbiór zdań $\Delta^* \cup \{\neg\alpha^*\}$ jest zbiorem niesprzecznym. Załóżmy przeciwnie, że

$$\Delta^* \cup \{\neg\alpha^*\} \vdash \bot.$$

Wówczas dla pewnego skończonego podzbioru $\Delta_0 \subseteq \Delta$ mamy $\Delta_0^* \cup \{\neg\alpha^*\} \vdash \bot$. Z twierdzenia o dedukcji dostajemy $\Delta_0^* \vdash \neg\neg\alpha^*$ i na mocy aksjomatu (A3) mamy $\Delta_0^* \vdash \alpha^*$ Niech $\Delta_0 = \{\beta_1, \ldots, \beta_n\}$. Tak więc, stosując n razy twierdzenie o dedukcji, dostajemy

$$\vdash \beta_1^* \to (\ldots \to (\beta_n^* \to \alpha^*)\ldots).$$

Zastępując w powyższym dowodzie stałe c_i nowymi, nigdzie w tym dowodzie nie pojawiającymi się zmiennymi z_i, następnie generalizując (por. Twierdzenie 12.7) i podstawiając na miejsce zmiennych związanych z_i (por. aksjomat (A6)) zmienne x_i dostajemy[18]

$$\vdash \beta_1 \to (\ldots \to (\beta_n \to \alpha)\ldots),$$

[18]Zauważmy, że zmienna x_i jest dopuszczalna dla z_i w stosownej formule.

czyli $\Delta_0 \vdash \alpha$, a co za tym idzie również $\Delta \vdash \alpha$, wbrew założeniu. Tak więc zbiór $\Delta^* \cup \{\neg\alpha^*\}$ jest niesprzeczny.

Z twierdzenia o istnieniu modelu wynika, że $\Delta^* \cup \{\neg\alpha^*\}$ ma model. Czyli istnieje $\Sigma(C)$-struktura $\mathfrak{A}$ taka, że $\mathfrak{A} \models \Delta^*$ oraz $\mathfrak{A} \not\models \alpha^*$. Niech $v : X \to A$ będzie wartościowaniem, które każdej zmiennej x_i przypisuje wartość $c_i^{\mathfrak{A}}$. Mamy wówczas $\mathfrak{A} \models \beta[v]$, dla każdej formuły $\beta \in \Delta$ oraz $\mathfrak{A} \not\models \alpha[v]$. Dowodzi to $\Delta \not\models \alpha$. ∎

Zadania

12.1. Dla każdego z następujących schematów formuł pierwszego rzędu stwierdzić czy przy dowolnym doborze formuł α, β, schemat ten daje tautologię. Dla tych schematów, dla których odpowiedź jest negatywna podać kontrprzykład (tzn. konkretne formuły, strukturę, wartościowanie oraz uzasadnić poprawność kontrprzykładu). Tam gdzie odpowiedź jest pozytywna pokazać wyprowadzenie w $\vdash_H$.

(i) $(\forall x\alpha \to \forall x\beta) \to \forall x(\alpha \to \beta)$

(ii) $(\exists x\alpha \to \forall x\beta) \to \forall x(\alpha \to \beta)$

(iii) $\forall x(\alpha \to \beta) \to (\exists x\alpha \to \forall x\beta)$

(iv) $\forall x(\alpha \to \beta) \to (\exists x\alpha \to \forall x\beta)$, gdzie β jest formułą, w której x nie występuje wolno.

12.2. Podać przykład formuły α oraz zmienych x, z świadczący o tym, że $\forall x\ \alpha \to \forall z\ \alpha(z/x)$ nie musi być tautologią. Co należy założyć o α, x, z any powyższa formuła była tautologią? Odpowiedź uzasadnić.

12.3. Niech r, s będą symbolami jednoargumentowych relacji. Zbadać czy następujące formuły pierwszego rzędu są tautologiami:

(i) $\exists x\ (r(x) \wedge s(x)) \to (\exists x\ r(x) \wedge \exists x\ s(x))$,

(ii) $(\exists x\ r(x) \wedge \exists x\ s(x)) \to \exists x\ (r(x) \wedge s(x))$.

12.4. Dla każdej z poniższych formuł stwierdzić czy jest ona spełnialna oraz czy jest ona tautologią.

(i) $(\forall x(f(f(x)) = f(x)) \ \wedge\ \forall x\exists y(f(y) = x)) \ \to\ \forall x(f(x) = x)$.

(ii) $\forall x(g(f(x)) = x) \ \wedge\ \exists y(f(g(y)) \neq y)$.

(iii) $(\forall x\forall y(r(x,y) \vee r(y,x)) \ \wedge\ \forall x\forall y(r(x,y) \to r(y,x))) \ \to\ \forall x\forall y\, r(x,y)$.

12.5. Niech $\vdash_{ND}$ oznacza następujący system dla formuł opartych o $\to$, $\bot$ oraz $\forall$. Aksjomaty (A0), (A7-9) systemu $\vdash_H$ oraz reguły ($\to$-intro) i ($\to$-elim) są takie same jak w systemie $\vdash_{ND}$ dla rachunku zdań. Ponadto dodajemy reguły

$$(\forall\text{-intro}) \qquad \frac{\Delta \vdash \alpha}{\Delta \vdash \forall x\ \alpha} \qquad x \notin FV(\Delta)$$

$$(\forall\text{-elim}) \qquad \frac{\Delta \vdash \forall x\ \alpha}{\Delta \vdash \alpha(\sigma/x)} \qquad (\sigma \text{ jest dopuszczalny dla } x \text{ w } \alpha)$$

Dowieść, że dla dowolnego sekwentu $\Delta \vdash \alpha$, zachodzi $\Delta \vdash_H \alpha$ wtw, gdy $\Delta \vdash_{ND} \alpha$.

12.6. Dowieść, że następująca reguła *osłabiania* jest dopuszczalna w systemach $\vdash_H$ i $\vdash_{ND}$.

$$\frac{\Delta \vdash \alpha}{\Gamma \vdash \alpha} \qquad \Delta \subseteq \Gamma.$$

12.7. Niech α będzie dowolną formułą. Dowieść, że dla każdej Σ-struktury $\mathfrak{A}$ oraz dowolnych dwóch wartościowań v, v', jeśli dla $x \in FV(\alpha)$ zachodzi $v(x) = v'(x)$, to

$$\mathfrak{A} \models \alpha[v] \quad \text{wtw, gdy} \quad \mathfrak{A} \models \alpha[v'].$$

12.8. Podać przykład świadczący o tym, że założenia lematu o podstawianiu (Lemat 12.2) są istotne.

12.9. Niech $\vdash_{H'}$ oznacza system powstały z $\vdash_H$ przez usunięcie aksjomatów (A4) i (A5) oraz dodanie reguły ($\forall$-intro). Pokazać, że systemy $\vdash_H$ oraz $\vdash_{H'}$ wyprowadzają te same sekwenty.

12.10. Powiemy, że Σ-struktury $\mathfrak{A}$ oraz $\mathfrak{B}$ są *izomorficzne* gdy istnieje bijekcja $f : A \to B$ taka, że f oraz f^{-1} zachowują odpowiadające sobie operacje i relacje w strukturach. Dowieść, że jeśli Σ-struktury $\mathfrak{A}$ oraz $\mathfrak{B}$ są izomorficzne, to dla każdej formuły α zachodzi

$$(*) \qquad \mathfrak{A} \models \alpha \quad \text{wtw, gdy} \quad \mathfrak{B} \models \alpha.$$

Czy jeśli dla dowolnej formuły α zachodzi $(*)$, to struktury $\mathfrak{A}$ i $\mathfrak{B}$ muszą być izomorficzne?

12.11. Wyrazić w języku teorii mnogości aksjomat wyboru i aksjomat zastępowania.

12.12. Dowieść w teorii mnogości Zermelo-Fraenkla, że dla dowolnego zbioru z i dowolnej formuły α mającej tylko jedną zmienna wolną x, istnieje dokładnie jeden zbiór u taki, że

$$\forall x\ (x \in u \leftrightarrow (x \in z \wedge \alpha)).$$

12.13. Dowieść w teorii mnogości Zermelo-Fraenkla, że dla dowolnych zbiorów x, y istnieje ich iloczyn kartezjański.

12.14. Dowieść, że dla dowolnej sygnatury Σ nie istnieje zbiór Δ zdań nad Σ taki, że dla dowolnej Σ-struktury $\mathfrak{A}$, nośnik A jest zbiorem skończonym wtw, gdy $\mathfrak{A} \models \Delta$. Zatem własność "stuktura jest skończona" nie jest wyrażalna w języku pierwszego rzędu.

13 Język drugiego rzędu

13.1 Składnia

Język drugiego rzędu jest rozszerzeniem języka pierwszego rzędu przez wprowadzenie zmiennych przebiegających relacje skończenie argumentowe. Dla $n \geq 1$, niech V_n będzie przeliczalnym zbiorem zmiennych, zwanych *zmiennymi relacyjnymi n-argumentowymi*. Zmienne te będziemy oznaczać literami $R, P, Q, \ldots$. Zmienne relacyjne n-argumentowe będą wartościowane w modelu relacjami n-argumentowymi. Zakładamy, że zbiory V_n są rozłączne z sygnaturą Σ, ze zbiorem X zmiennych indywiduowych oraz, że $V_n \cap V_m = \emptyset$, dla $m \neq n$. Niech

$$V_* = \bigcup_{n \geq 1} V_n.$$

Zbiór $FT(\Sigma, X)$, termów nad sygnaturą Σ definiuje się tak jak w Rozdziale 12. Zbiór *formuł drugiego rzędu* nad sygnaturą Σ definiujemy jako najmniejszy zbiór wyrażeń spełniający następujące warunki (dla pełności prezentacji powtarzamy tu wszystkie warunki dla formuł pierwszego rzędu):

- $\bot$ jest formułą drugiego rzędu.
- Jeśli r jest symbolem relacji n-argumentowej oraz $\sigma_1, \ldots, \sigma_n$ są termami, to $r(\sigma_1, \ldots, \sigma_n)$ jest formułą drugiego rzędu.
- Jeśli R jest zmienną relacyjną n-argumentową (dla pewnego $n \geq 1$) oraz $\sigma_1, \ldots, \sigma_n$ są termami, to $R(\sigma_1, \ldots, \sigma_n)$ jest formułą drugiego rzędu.
- Jeśli α i β są formułami drugiego rzędu, to

  $$(\alpha \wedge \beta), \ (\alpha \vee \beta), \ (\alpha \to \beta)$$

  są też formułami drugiego rzędu.
- Jeśli α jest formułą drugiego rzędu oraz $x \in X$ jest zmienną indywiduową, to

  $$\forall x \ \alpha, \ \exists x \ \alpha$$

  są też formułami drugiego rzędu.
- Jeśli α jest formułą drugiego rzędu oraz $R \in V_*$ jest zmienną relacyjną, to

  $$\forall R \ \alpha, \ \exists R \ \alpha$$

  są też formułami drugiego rzędu.

Przykład 13.1 Przykładem formuły drugiego rzędu jest
$\forall x\ R(x,x) \wedge \forall x \forall y\ ((R(x,y) \wedge R(y,x)) \rightarrow x = y) \wedge \forall x \forall y \forall z\ ((R(x,y) \wedge R(y,z)) \rightarrow R(x,z)) \wedge$
$\exists Q\ (\forall x \forall y\ (R(x,y) \rightarrow Q(x,y)) \wedge \forall x \exists y\ Q(x,y\ ) \wedge\ \forall x \forall y_1 \forall y_2\ ((Q(x,y_1) \wedge Q(x,y_2)) \rightarrow y_1 = y_2))$

W powyższej formule R oraz Q są zmiennymi relacyjnymi dwuargumentowymi. Zmienna R występuje wolno, a zmienna Q jest związana.

Nie będziemy precyzyjnie definiować wolnych i związanych wystąpień zmiennych drugiego rzędu. Definicje są całkowicie analogiczne do przypadku zmiennych indywiduowych. Formuła (drugiego rzędu) bez zmiennych wolnych nazywa się *zdaniem*.

13.2 Semantyka

Niech $\mathfrak{A}$ będzie Σ-strukturą. Wartościowaniem (drugiego rzędu) w $\mathfrak{A}$ nazwiemy funkcję $v : X \cup V_* \rightarrow A \cup \bigcup_{n \geq 1} P(A^n)$ taką, że dla $x \in X$ zachodzi $v(x) \in X$ oraz dla $R \in V_n$ i $n \geq 1$ zachodzi $v(R) \in P(A^n)$.

Przypomnijmy, że dla $x \in X$, $a \in A$ oraz wartościowania v, nowe wartościowanie v^a_x oznacza modyfikację starego tak, że $v^a_x(x) = a$. Dla pozostałych zmiennych v i v^a_x przyjmują takie same wartości. Podobnie dla $R \in V_n$, relacji $B \subseteq A^n$ oraz wartościowania v, nowe wartościowanie v^B_R oznacza modyfikację starego tak, że $v^B_R(R) = B$.

Semantyka formuł drugiego rzędu wyraża się relacją *spełniania* $\mathfrak{A} \models \alpha[v]$, gdzie $\mathfrak{A}$ jest Σ-strukturą, α jest formułą drugiego rzędu, a v jest wartościowaniem drugiego rzędu. Podobnie jak w przypadku formuł pierwszego rzędu relację spełniania definiujemy przez indukcję ze względu na budowę formuły α.

- Nie zachodzi $\mathfrak{A} \models \bot[v]$;
- Dla $r \in \Sigma^R_n$ oraz termów $\sigma_1, \ldots, \sigma_n$, zachodzi
$$\mathfrak{A} \models r(\sigma_1, \ldots, \sigma_n)[v] \text{ wtw, gdy } (\sigma^{\mathfrak{A}}_1[v], \ldots \sigma^{\mathfrak{A}}_n[v]) \in r^{\mathfrak{A}};$$
- Dla $R \in V_n$ oraz termów $\sigma_1, \ldots, \sigma_n$, zachodzi
$$\mathfrak{A} \models R(\sigma_1, \ldots, \sigma_n)[v] \text{ wtw, gdy } (\sigma^{\mathfrak{A}}_1[v], \ldots \sigma^{\mathfrak{A}}_n[v]) \in v(R);$$
- Zachodzi $\mathfrak{A} \models (\sigma_1 = \sigma_2)[v]$ wtw, gdy $\sigma^{\mathfrak{A}}_1[v] = \sigma^{\mathfrak{A}}_2[v]$;
- Zachodzi $\mathfrak{A} \models (\alpha \wedge \beta)[v]$ wtw, gdy zachodzą $\mathfrak{A} \models \alpha[v]$ oraz $\mathfrak{A} \models \beta[v]$;
- Zachodzi $\mathfrak{A} \models (\alpha \vee \beta)[v]$ wtw, gdy zachodzi $\mathfrak{A} \models \alpha[v]$ lub $\mathfrak{A} \models \beta[v]$;
- Zachodzi $\mathfrak{A} \models (\alpha \rightarrow \beta)[v]$ wtw, gdy nie zachodzi $\mathfrak{A} \models \alpha[v]$ lub zachodzi $\mathfrak{A} \models \beta[v]$;

- Dla $x \in X$, zachodzi $\mathfrak{A} \models (\forall x\ \alpha)[v]$ wtw, gdy dla każdego $a \in A$, zachodzi $\mathfrak{A} \models \alpha[v^a_x]$;
- Dla $R \in V_n$, zachodzi $\mathfrak{A} \models (\forall R\ \alpha)[v]$ wtw, gdy dla każdej relacji $B \subseteq A^n$, zachodzi $\mathfrak{A} \models \alpha[v^B_R]$;
- Dla $x \in X$ zachodzi $\mathfrak{A} \models (\exists x\ \alpha)[v]$ wtw, gdy istnieje $a \in A$ takie, że zachodzi $\mathfrak{A} \models \alpha[v^a_x]$;
- Dla $R \in V_n$ zachodzi $\mathfrak{A} \models (\exists R\ \alpha)[v]$ wtw, gdy istnieje relacja $B \subseteq A^n$ taka, że zachodzi $\mathfrak{A} \models \alpha[v^B_R]$.

Pojęcia *spełnialności, prawdziwości (w strukturze) oraz tautologii* definiuje się analogicznie jak dla języka pierwszego rzędu.

Formuła z Przykładu 13.1 ma zmienną wolną $R \in V_2$. Formuła ta jest spełniona w strukturze $\mathfrak{A}$ przez wartościowanie, które przyporządkowuje zmiennej R relację $B \subseteq A^2$ wtw, gdy B jest częściowym porządkiem, który daje się rozszerzyć do funkcji z A w A (a zatem wtw, gdy $B = I_A$).

Język drugiego rzędu jest bardziej wyrażalny niż pierwszego rzędu. Dla przykładu pokażemy, że własność dobrego ufundowania jest wyrażalna w języku drugiego rzędu.

Przykład 13.2 Niech $\leq$ będzie symbolem relacji dwuargumentowej z Σ^R_2. Niech α będzie formułą pierwszego rzędu wyrażającą własność struktury $\mathfrak{A}$, że $\leq^{\mathfrak{A}}$ jest częściowym porządkiem. Rozważmy następującą formułę

$$\alpha \wedge \forall R\ (\exists x\ R(x) \rightarrow \exists x\ (R(x) \wedge \forall y\ (R(y) \wedge y \leq x) \rightarrow x = y)).$$

Powyższa formuła wyraża własność struktury $\mathfrak{A}$, że $\leq^{\mathfrak{A}}$ jest częściowym porządkiem oraz, że każdy niepusty podzbiór ma element minimalny ze względu na $\leq^{\mathfrak{A}}$. Zatem na mocy Twierdzenia 8.1, relacja $\leq^{\mathfrak{A}}$ jest dobrze ufundowana.

Ze względu na dużą wyrażalność języka drugiego rzędu wiele własności języka pierwszego rzędu nie przenosi się na przypadek tego języka. Przykładowo twierdzenie o zwartości oraz twierdzenie Löwenheima, Skolema i Tarskiego nie zachodzą dla tego języka. Nie istnieje też żadna rozsądna aksjomatyzacja zbioru tautologii drugiego rzędu.

Zadania

13.1. Sprawdzić czy następująca formuła drugiego rzędu jest spełnialna oraz czy jest tautologią.
$\exists R \forall Q(\ \forall x \forall y (R(x,y) \rightarrow Q(x,y))\ \rightarrow\ \exists x \exists y (x \neq y \wedge Q(x,y) \wedge Q(y,x))\ )$.

13.2. Pokazać, że własność skończoności jest wyrażalna w języku drugiego rzędu.

13.3. Korzystając z powyższego zadania pokazać, że twierdzenie o zwartości nie zachodzi dla języka drugiego rzędu.