Wykłady ze Wstępu do Matematyki

Jacek Cichoń
WPPT, Politechnika Wrocławska

MAJ 2012

Spis treści

Wstęp

Książka zawiera dziewięć wykładów poświęconych omówieniu oraz uporządkowaniu podstawowych pojęć matematycznych. Ich treść odpowiada w przybliżeniu wykładom ze "*Wstępu do Matematyki*", które autor wielokrotnie prowadził dla studentów Instytutu Matematycznego Uniwersytetu Wrocławskiego oraz Wydziału Podstawowych Problemów Techniki Politechniki Wrocławskiej. Autor pragnie gorąco podziękować prof. B. Węglorzowi oraz prof W. Kordeckiemu za szereg uwag, które pomogły uporządkować i unowocześnić materiał. Dziękuję również studentom WPPT PWr za pomoc w eliminowaniu usterek z wcześniejszych wersji tej książki.

Główna część książki odpowiada zakresowi materiału który obowiązywał wszystkich studentów i ten zakres materiału powinien dobrze opanować każdy student informatyki i matematyki. Części książki umieszczone w dodatkach stanowią rozszerzenie podstawowego kursu.

1. W wykładzie pierwszym omawiamy podstawowe pojęcia Rachunku Zdań. Wykład opieramy na pojęciu *waluacji*, ze względu na liczne, zwłaszcza w informatyce, zastosowania uogólnień tego pojęcia. Głównym celem tego wykładu jest przegląd podstawowych tautologii oraz wprowadzeniu pojęcia reguły wnioskowania.

2. W wykładzie drugim zajmujemy się Rachunkiem Zbiorów. Rozważania opieramy o *Aksjomat Ekstensjonalności*. Pierwszym dowodzonym przez nas faktem jest *twierdzenie Russell'a* o nie istnieniu zbioru wszystkich zbiorów. Następnie omawiamy własności sumy, przekroju i różnicy zbiorów. Wszystkie dowody sprowadzamy do Rachunku Zdań.

3. W wykładzie trzecim zajmujemy się własnościami kwantyfikatorów W tym miejscu wykład traci nieco na precyzji. Interpretację kwantyfikatorów redukujemy do Rachunku Zbiorów. Z bardziej precyzyjnym wprowadzenie do Rachunku Predykatów studenci zapoznają się na wykładzie z Logiki Matematycznej lub Logiki Algorytmicznej. Elementem wymagającym szczególnej uwagi są uzasadnienia zależności pomiędzy wyrażeniami zbudowanymi z bloku dwóch kwantyfikatorów. W wykładzie tym omawiamy również pojęcie sumy i przekroju dowolnej rodziny zbiorów.

4. Wykład czwarty poświęcamy relacjom. Definiujemy podstawowe klasy relacji, w tym pojęcie funkcji. Zajmujemy się obrazami i przeciwobrazami zbio-

rów przez relacje. Omawiamy funkcje logiczne - pokazujemy, że standardowy zestaw spójników logicznych jest zupełny (synteza formuły odbywa się za pomocą tabeli wartości rozważanej funkcji). Następnie omawiamy indeksowane rodziny zbiorów oraz produkty kartezjańskie. W końcu wprowadzamy pojęcie funkcji charakterystycznej zbioru.

5. Wykład piąty poświęcony jest w całości relacjom równoważności. Pokazujemy w nim, jak startując z liczb naturalnych można zdefiniować liczby całkowite, wymierne i rzeczywiste.

6. Wykład szósty poświęcony jest częściowym porządkom. Po wprowadzeniu podstawowych pojęć omawiamy porządki na rodzinach funkcji. Celem tego fragmentu rozważań jest przybliżenie czytelnikom notacji $f = O(g)$. Następnie omawiamy liniowe porządki i porządek leksykograficzny na przestrzeni słów. Przechodzimy do prezentacji Lematu Kuratowskiego - Zorna i jego podstawowych konsekwencji. Wprowadzamy Aksjomat Wyboru. Pod koniec tego wykładu omawiamy pojęcie dobrego porządku.

7. W wykładzie poświęconym Indukcji Matematycznej pokazujemy jej równoważność z dobrym uporządkowaniem zbioru liczb naturalnych, omawiamy definicje rekurencyjne. Przypominamy pojęcie permutacji i wprowadzamy symbol Newtona. Rozważania kończymy zasadą Dirichleta.

8. W wykładzie ósmym omawiamy pojęcie równoliczności i nierówności mocy. Twierdzenie Cantora - Bernsteina wyprowadzamy za pomocą *Lematu Banacha*. Omawiamy zbiory przeliczalne i zbiory continuum. Głównym obszarem zainteresowań jest zbiór $\mathbb{N} \cup \{\aleph_0, 2^{\aleph_0}\}$, jednak pod koniec rozdziału wprowadzamy hierarchię liczb $\beth_n$ dla $n \in \mathbb{N}$.

9. Wykład dziewiąty poświęcony jest relacją ufundowanym, systemom przepisującym oraz drzewom. Tematy te umieszczone są w głównej części książki ze wzgledu na ich liczne zastosowania w informatyce.

10. W dodatku A znajduje się wprowadzenie do teorii algebr Boole'a. Rozpoczynamy od definicji, a kończymy na słabej wersji twierdzenia Stone'a o reprezentacji. W trakcie rozważań pojawia się pojęcie ciała zbiorów.

11. W dadatku B wprowadzamy pojęcie kraty i dowodzimy *twierdzenie Knastera-Tarskiego* o punkcie stałym. Za jego pomocą podajemy alternatywny dowód Lematu Banacha. Następnie omawiamy drzewa, dowodzimy twierdzenie Königa o istnieniu nieskończonej gałęzi. Na zakończenie wprowadzamy pojęcie tablic semantycznych dla rachunku zdań.

12. W dodatku C omawiamy system aksjomatów teorii mnogości Zermelo - Fraenkel'a i zagadnienia związane z niesprzecznością tej teorii.

13. W dodatku D omawiamy liczby porządkowe oraz liczby kardynalne. Rozważania kończymy omówieniem, jakim alefem może być liczba continuum.

14. W dodatku E znajdują się szkice rozwiązań lub wskazówki do trudniejszych zadań.

Z doświadczenia autora wynika, że pierwsze dziewięć wykładów można zrealizować w trakcie pierwszego semestru studiów informatycznych oraz matematycznych. Aby to osiągnąć należy wykład prowadzić stosunkowo szybko. Najbardziej obszernym pojęciowo jest wykład szósty, poświęcony częściowym porządkom. Należy go rozbić na co najmniej cztery godziny wykładowe.

Do każdego wykładu dołączone są ćwiczenia oraz zadania. Ćwiczenia są rutynowe i stosunkowo proste. Powinny być przerobione przez wszystkich studentów. Zadania są nieco trudniejsze i wymagają pewnego pomysłu. Oprócz tych zadań studenci powinni zostać zachęceni do zapoznania się ze wszystkimi zadaniami związanymi z tematami omawianymi na wykładzie z książki [6].

Jako literaturę pomocniczą do wykładów można polecić książki [4] oraz [7]. Studentom, którzy mogą czuć niedosyt formalizmu logicznego po trzecim wykładzie, można polecić książkę [1]. Jako literaturę pomocniczą do materiału omawianego w dodatkach można polecić pozycje [3], [5] oraz [2].

1 Rachunek Zdań

> Reductio ad absurdum, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.
>
> G. H. Hardy

Rachunek Zdań jest działem logiki matematycznej badającym związki pomiędzy zdaniami utworzonymi ze zmiennych zdaniowych za pomocą spójników logicznych. W klasycznym rachunku zdań - a takim właśnie rachunkiem zdań zajmować się będziemy podczas tego wykładu - przyjmuje się, że każdemu zdaniu można przypisać jedną z dwóch wartości logicznych - **prawdę** lub **fałsz**. W rozważaniach naszych treść zdań nie będzie miała żadnego znaczenia. Ważna będzie tylko ich wartość logiczna.

1.1 Zdania i Waluacje

Symbole $p_0, p_1, p_2, \ldots$ nazywać będziemy zmiennymi zdaniowymi. Symbole $\top$ i $\bot$ są stałymi; symbol $\top$ nazywamy zdaniem zawsze prawdziwe zaś $\bot$ nazywamy zdaniem zawsze fałszywym. Oprócz zmiennych zdaniowych rozważać będziemy spójniki logiczne: $\wedge$, $\vee$, $\neg$, $\rightarrow$, oraz $\leftrightarrow$. Spójnik $\wedge$ nazywamy *koniunkcją*, $\vee$ nazywamy *alternatywą*, $\neg$ nazywamy *negacją* bądź zaprzeczeniem. Kolejne dwa spójniki logiczne nazywamy *implikacją* i *równoważnością*. Do konstrukcji języka Rachunku Zdań potrzebujemy jeszcze dwóch symboli. Są nimi nawiasy. Pierwszy z nich, „(", nazywamy *nawiasem otwierającym* zaś drugi, „)", *nawiasem zamykającym*.

Określimy teraz pojęcie *zdania* Rachunku Zdań. Posłużymy się w tym celu tak zwaną techniką rekurencyjną.

Definicja 1.1 (Zdania)

1. *Zmienne zdaniowe oraz stałe $\top$ i $\bot$ są zdaniami.*
2. *Jeśli wyrażenia φ i ψ są zdaniami, to również zdaniami są następujące wyrażenia: $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$, $(\varphi \leftrightarrow \psi)$ i $\neg\varphi$.*
3. *Dowolne wyrażenie jest zdaniem, jeśli może zostać zbudowane ze zmiennych zdaniowych w wyniku zastosowania pewnej skończonej liczby reguł z punktu (2).*

Z powyższej definicji można wyprowadzić kilka podstawowych faktów o rodzinie wszystkich zdań.

Przykład 1.1 *Jako przykład pokażemy, że w każdym zdaniu występuje parzysta liczba nawiasów. Rozważmy mianowicie rodzinę Ω tych wszystkich wyrażeń, które mają parzystą ilość nawiasów. Wtedy rodzina zmiennych zdaniowych zawiera się w rodzinie Ω, bowiem zero jest liczbą parzystą. Zauważmy następnie, że jeśli wyrażenia φ i ψ są elementami rodziny Ω, czyli mają parzystą liczba nawiasów, to również wyrażenia $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $(\varphi \leftrightarrow \psi)$ i $\neg\varphi$ mają parzystą ilość nawiasów. Zatem każde zdanie jest elementem rodziny Ω, co kończy dowód.*

Wartościami logicznymi nazywamy symbole $\mathbb{0}$ i $\mathbb{1}$, które interpretujemy jako *fałsz* i *prawdę*. Na zbiorze wartości logicznych $\{\mathbb{0}, \mathbb{1}\}$ określamy działania $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ oraz $\neg$: za pomocą następującej tabelki:

$\mathbf{p}$	$\mathbf{q}$	$\mathbf{p} \wedge \mathbf{q}$	$\mathbf{p} \vee \mathbf{q}$	$\mathbf{p} \Rightarrow \mathbf{q}$	$\mathbf{p} \Leftrightarrow \mathbf{q}$	$\neg\mathbf{p}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$

Czytelnik powinien zwrócić uwagę na rozróżnienie miedzy spójnikami logicznymi $\wedge$, $\vee$, $\to$, $\leftrightarrow$, $\neg$ oraz działaniami $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ oraz $\neg$.

Definicja 1.2 ***Waluacją*** *nazywamy dowolny ciąg $\pi = (w_0, w_1, w_2, \ldots)$ wartości logicznych.*

Dla dowolnego zdania φ oraz dowolnej waluacji $\pi = (w_0, w_1, w_2, \ldots)$ możemy określić wartość $\pi(\varphi)$ waluacji π na φ. Proces ten nazywamy wartościowaniem zdania zdania φ na zadanej waluacji π.

Definicja 1.3 (Wartościowanie) *Niech π będzie waluacją. Dla dowolnej zmiennej zdaniowej p_i określamy $\pi(p_i) = w_i$. Jeśli φ oraz ψ są zdaniami i określone są już wartości $\pi(\varphi)$ oraz $\pi(\psi)$), to*

1. $\pi(\top) = \mathbb{1}$,
2. $\pi(\bot) = \mathbb{0}$,
3. $\pi(\varphi \wedge \psi) = \pi(\varphi) \wedge \pi(\psi)$,
4. $\pi(\varphi \vee \psi) = \pi(\varphi) \vee \pi(\psi)$,
5. $\pi(\varphi \to \psi) = \pi(\varphi) \Rightarrow \pi(\psi)$,
6. $\pi(\varphi \leftrightarrow \psi) = \pi(\varphi) \Leftrightarrow \pi(\psi)$,
7. $\pi(\neg\varphi) = \neg(\pi(\varphi))$.

Powyższa definicja może wyglądać na nieco skomplikowaną. Lecz tak w istocie nie jest. Stanie to się z pewnością jasne już po prześledzeniu pierwszego przykładu.

Przykład 1.2 *Niech $\pi = (\mathbb{1}, \mathbb{0}, \mathbb{1}, \mathbb{1}, \mathbb{1}, \mathbb{1}, \ldots)$ oraz niech $\varphi = ((p_0 \vee p_1) \wedge (\neg p_2))$. Wtedy*

$$\pi(\varphi) = \pi((p_0 \vee p_1) \wedge (\neg p_2)) = \pi(p_0 \vee p_1) \wedge \pi(\neg p_2) =$$
$$(\pi(p_0) \vee \pi(p_1)) \wedge \neg(\pi(p_2)) = (\mathbb{1} \vee \mathbb{0}) \wedge \neg(\mathbb{1}) = \mathbb{1} \wedge \mathbb{0} = \mathbb{0} \ .$$

Obliczenia te można zapisać trochę mniej formalnie, ale za to bardziej czytelnie

$$\pi(\varphi) = (\mathbb{1} \vee \mathbb{0}) \wedge (\neg\mathbb{1}) = \mathbb{1} \wedge \mathbb{0} = \mathbb{0} \ .$$

Definicja 1.4 *Zdanie φ nazywamy **tautologią**, co zapisujemy jako $\models \varphi$, jeśli $\pi(\varphi) = \mathbb{1}$ dla dowolnej waluacji π.*

Najprostszą tautologią jest oczywiście zdanie $\top$. Inny prosty przykład to zdanie $p_0 \vee \neg p_0$. Zauważmy, że do zbadania, czy dane zdanie jest waluacją wystarczy tylko ten fragment waluacji, który odpowiada zmiennym wchodzącym w skład analizowanego zdania. Ułatwia to znacznie badanie tego, czy dane zdanie jest waluacją i sprowadza to zagadnienie do znanej ze szkoły średniej metody zero-jedynkowej.

Przykład 1.3 *Pokażemy, że zdanie $((p_0 \vee p_1) \vee p_2) \leftrightarrow (p_0 \vee (p_1 \vee p_2))$ jest tautologią. Niech $\varphi = ((p_0 \vee p_1) \vee p_2)$ oraz $\psi = (p_0 \vee (p_1 \vee p_2))$. Rozważmy następującą tabelkę:*

p_0	p_1	p_2	$p_0 \vee p_1$	$p_1 \vee p_2$	φ	ψ	$\varphi \leftrightarrow \psi$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$

W tabelce tej mamy 8 wierszy, gdyż istnieje $8 = 2^3$ równych kombinacji wartości logicznych p_0, p_1 i p_2. W kolejnych kolumnach ustalonego wiersza prowadzone są wszystkie pomocnicze obliczenia, których celem jest wyznaczenie wartości leżącej w ostatniej kolumnie. Rozważane zdanie jest tautologią, gdyż w ostatniej kolumnie występują tylko wartości $\mathbb{1}$.

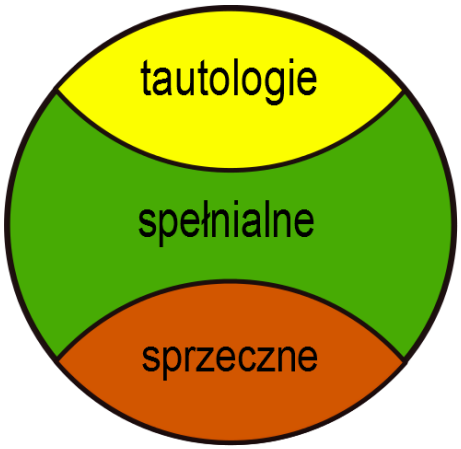
Zwróćmy uwagę na to, że metoda tabelek zero - jedynkowych określa automatyczną metodę badania tego, czy dane zdanie jest tautologią. Zagadnienia tego typu nazywamy *rozstrzygalnymi*. Jednak metoda ta dla zdań zbudowanych ze 100 zmiennych zdaniowych wymagałaby rozpatrzenia $2^{100} \approx 1.2 \cdot 10^{30}$ przypadków, co jest zadaniem znacznie przekraczającym moce obliczeniowe współczesnych komputerów. Nie wiadomo, czy istnieje istotnie szybszy algorytm rozstrzygający o danym zdaniu, czy jest ono tautologią.

Definicja 1.5 *Zdanie φ nazywamy **sprzecznym**, jeśli $\pi(\varphi) = \mathbb{0}$ dla dowolnej waluacji π.*

Zdania sprzeczne nazywane są czasem anty-tautologiami. Zauważmy, że zdanie ψ jest sprzeczne wtedy i tylko wtedy, gdy zdanie $\neg\psi$ jest tautologią. Podobnie, zdanie π jest tautologią wtedy i tylko wtedy, gdy zdanie $\neg\psi$ jest sprzeczne. Najprostszym przykładem zdania sprzecznego jest zdanie $\bot$. Innym prostym przykładem zdania sprzecznego jest $p_0 \wedge \neg p_0$.

Definicja 1.6 *Zdanie φ nazywamy **spełnialnym**, jeśli istnieje waluacja π taka, że $\pi(\varphi) = \mathbb{1}$.*

Zauważmy, że istnieją zdania, które są spełnialne, ale nie są tautologiami ani też zdaniami sprzecznymi.



Przykładami tautologii są zdania $p_0 \vee \neg p_0$ i $\top$. Przykładami zdań spełnialnych, które nie są tautologiami są p_0, p_1, $p_0 \vee p_1$, $p_0 \wedge p_1$, $p_0 \wedge (\neg p_1)$. Przykładami zdań sprzecznych są $p_0 \wedge (\neg p_0)$, $\bot$.

1.2 Przegląd Najważniejszych Tautologii

W rozdziale tym symbole p, q, r, s, t będą oznaczać dowolne zmienne zdaniowe. Rozważania rozpoczniemy od podstawowych własności koniunkcji oraz alternatywy. Zdania we wszystkich tabelkach zamieszczonych w tym rozdziale są tautologiami. Nie będziemy ich dowodzili. Pozostawiamy to czytelnikom jako proste ćwiczenie.

	Nazwa	**Tautologia**
1.	idempotentność	$(p \wedge p) \leftrightarrow p$
		$(p \vee p) \leftrightarrow p$
2.	przemienność	$(p \wedge q) \leftrightarrow (q \wedge p)$
		$(p \vee q) \leftrightarrow (q \vee p)$
3.	łączność	$(p \wedge (q \wedge r)) \leftrightarrow ((p \wedge q) \wedge r)$
		$(p \vee (q \vee r)) \leftrightarrow ((p \vee q) \vee r)$
4.	rozdzielność	$(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r)$
		$(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r)$

Przemienność jest własnością, którą czytelnik z pewnością zna w kontekście podstawowych działań arytmetycznych. Dodawanie i mnożenie liczb rzeczywistych są działaniami przemiennymi. Zwróćmy jednak uwagę na to, że potęgowanie liczb rzeczywistych nie jest operacją przemienną. Łączność jest własnością, którą również posiadają dodawanie i mnożenie liczb rzeczywistych. Jest to bardzo ciekawa własność, gdyż wynika z niej, że wynik działania nie zależy od pogrupowania podwyrażeń. W szczególności, możemy posługiwać się skrótem $p \wedge q \wedge r$, gdyż bez względu na to, jak w tym wyrażeniu rozłożymy nawiasy, to otrzymamy równoważne wyrażenie. Mnożenie liczb rzeczywistych jest rozdzielne względem dodawania, czyli $x \cdot (y + z) = x \cdot y + x \cdot z$. Jednakże dodawanie liczb rzeczywistych nie jest rozdzielne względem mnożenia.

	Nazwa	Tautologia
1.	prawo podwójnej negacji	$\neg(\neg p) \leftrightarrow p$
2.	prawo wyłączonego środka	$\neg(p \wedge \neg p)$
3.	prawo braku trzeciej możliwości	$p \vee \neg p$
4.	prawa de Morgana	$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
		$\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$

Prawa de Morgana pozwalają na wyrażenie alternatywy za pomocą koniunkcji oraz negacji: $(p \vee q) \leftrightarrow \neg(\neg p \wedge \neg q)$. W podobny sposób możemy wyrazić koniunkcję za pomocą alternatywy oraz negacji. Kolejna porcja ważnych tautologii dotyczy własności implikacji i równoważności.

	Nazwa	Tautologia
1.	przechodniość implikacji	$((p \to q) \wedge (q \to r)) \to (p \to r)$
2.	eliminacja implikacji	$(p \to q) \leftrightarrow (\neg p \vee q)$
3.	eliminacje równoważności	$(p \leftrightarrow q) \leftrightarrow ((p \to q) \wedge (q \to p))$
		$(p \leftrightarrow q) \leftrightarrow ((p \wedge q) \vee (\neg p \wedge \neg g))$

Każda tautologia generuje nieskończenie wiele innych tautologii. Wynika to następującego twierdzenia:

Twierdzenie 1.1 (O podstawianiu) *Załóżmy, że $\varphi(p_0, \ldots, p_n)$ jest tautologią oraz że $\psi_0, \ldots \psi_n$ są dowolnymi zdaniami. Wtedy zdanie $\varphi(\psi_0, \ldots, \psi_n)$ jest również tautologią.*

Dowód tego twierdzenia pozostawiamy czytelnikowi.

Definicja 1.7 *Mówimy, że zdania φ, ψ są równoważne, co zapisujemy $\varphi \equiv \psi$, jeśli $\models (\varphi \leftrightarrow \psi)$.*

Zauważmy, że $\varphi \equiv \psi$ wtedy i tylko wtedy, gdy dla dowolnej waluacji π zachodzi równość $\pi(\varphi) = \pi(\psi)$. W dalszych rozważaniach będziemy posługiwali się następującymi własnościami pojęcia równoważności zdań:

1. $\varphi \equiv \varphi$,
2. jeśli $\varphi \equiv \psi$, to $\psi \equiv \varphi$
3. jeśli $\varphi \equiv \psi$ oraz $\psi \equiv \eta$, to $\varphi \equiv \eta$
4. $\varphi \equiv \top$ wtedy i tylko wtedy, gdy $\models \varphi$,
5. $\varphi \equiv \bot$ wtedy i tylko wtedy, gdy $\models \neg\varphi$.

Pokażemy teraz, że zdania sprzeczne, jako zdania zawsze fałszywe, implikują dowolne inne zdania:

Twierdzenie 1.2 *Załóżmy, że φ jest zdaniem sprzecznym. Wtedy dla dowolnego zdania ψ zdanie $\varphi \to \psi$ jest tautologią.*

Dowód. Niech π będzie dowolną waluacją. Wtedy

$$\pi(\varphi \to \psi) = (\pi(\varphi) \Rightarrow \pi(\psi)) = (\mathbb{0} \Rightarrow \pi(\psi)) = \mathbb{1}$$

□

Uwaga. Z udowodnionego twierdzenia wynika, że jeśli w trakcie badania pewnego systemu formalnego natrafimy choćby raz na sprzeczność, to dyskwalifikuje ona całkowicie ten system.

Jak już zauważyliśmy, alternatywę możemy zdefiniować za pomocą negacji oraz koniunkcji. Z prawa eliminacji implikacji wynika, że implikację możemy zdefiniować za pomocą negacji oraz alternatywy. Zatem implikację można zdefiniować za pomocą negacji oraz koniunkcji. Podobna obserwacja zachodzi również dla równoważności. Skoro można ją zdefiniować za pomocą implikacji i koniunkcji, więc do jej zdefiniowania wystarcza tylko negacja oraz koniunkcja.

Inne Spójniki Logiczne

Istnieją dwa operatory logiczne, za pomocą których można zdefiniować wszystkie pozostałe operatory. Jednym z nich jest spójnik zwany *spójnikiem Pierce'a*, zdefiniowany jako

$$p \perp q \;=\; (\neg p \wedge \neg q).$$

Drugim z nich jest tak zwana kreska Sheffera zdefiniowana wzorem

$$p|q \;=\; (\neg p \vee \neg q).$$

Uwaga. Zauważmy, że $(p \perp q) \equiv \neg(p \vee q)$ oraz $(p|q) \equiv \neg(p \wedge q)$. Spójnik Pierce'a znany jest w informatyce pod nazwą NOR, zaś kreska Sheffera jako operacja NAND.

Bardzo pożyteczny jest również spójnik logiczny $\oplus$ zdefiniowany następująco:

$$p \oplus q \Leftrightarrow (\neg p \wedge q) \vee (p \wedge \neg q).$$

Odpowiada on, mniej więcej, konstrukcji językowej "albo" języka polskiego. Posiada on kilka interesujących własności, które czynią go przydatnym w informatyce do kodowania i dekodowania informacji.

1. $p \oplus p \equiv \perp$,
2. $p \oplus q \equiv q \oplus p$,
3. $(p \oplus q) \oplus r \equiv p \oplus (q \oplus r)$,
4. $p \oplus q \equiv \neg(p \leftrightarrow q)$.

Pierwsze dwie własności tego spójnika wynikają bezpośrednio z definicji. Trzecią własność, łączność, najprościej można pokazać za pomocą tabelki zero-jedynkowej. Czwarta własność wynika z praw de Morgana i z drugiego prawa eliminacji równoważności.

Uwaga. W informatyce spójnik logiczny "albo" znany jest pod nazwą **XOR**.

1.3 Metody Dowodzenia Twierdzeń

Większość twierdzeń matematycznych jest zbudowana z pewnej listy założeń oraz z tezy. Mają one postać implikacji

$$(\varphi_1 \wedge \ldots \wedge \varphi_n) \rightarrow \psi.$$

Zdania $\varphi_1, \ldots, \varphi_n$ nazywają się założeniami twierdzenia, a ψ jego tezą. W rozdziale tym omówimy kilka często spotykanych schematów rozumowań matematycznych. Z innymi schematami rozumowań spotkamy się w dalszych rozdziałach. Z formalnym pojęciem dowodu omówimy w dalszych rozdziałach tej książki.

Definicja 1.8 *Mówimy, że zdanie ψ wynika ze zdań $\varphi_1, \ldots, \varphi_n$, co zapisujemy jako*

$$\{\varphi_1, \ldots, \varphi_n\} \models \psi \,,$$

jeśli dla dowolnej waluacji π takiej, że $\pi(\varphi_1) = \mathbb{1}, \ldots, \pi(\varphi_n) = \mathbb{1}$ mamy również $\pi(\psi) = \mathbb{1}$.

Prawdziwe wyrażenia postaci $\{\varphi_1, \ldots, \varphi_n\} \models \psi$ nazywamy regułami wnioskowania.

Twierdzenie 1.3 *Następujące dwa zdania są równoważne*

1. $\{\varphi_1, \ldots, \varphi_n\} \models \psi$
2. $\models (\varphi_1 \wedge \ldots \wedge \varphi_n) \to \psi$

Dowód. $(1) \to (2)$. Załóżmy, że $\{\varphi_1, \ldots, \varphi_n\} \models \psi$. Musimy pokazać, że zdanie $(\varphi_1 \wedge \ldots \wedge \varphi_n) \to \psi$ jest tautologią. Niech π będzie dowolną waluacją. Z definicji operatora $\Rightarrow$ wynika, że jest $\pi(\alpha \to \beta) = \mathbb{0}$ tylko w przypadku $\pi(\alpha) = \mathbb{1}$ oraz $\pi(\beta) = \mathbb{0}$. Lecz jeśli $\pi(\varphi_1 \wedge \ldots \wedge \varphi_n)$, to założenia (1) wynika, że $\pi(\psi) = \mathbb{1}$.

$(2) \to (1)$. Załóżmy, że $\models (\varphi_1 \wedge \ldots \wedge \varphi_n) \to \psi$. Niech π będzie taką waluacją, że $\pi(\varphi_1) = \mathbb{1}, \ldots, \pi(\varphi_n) = \mathbb{1}$. Wtedy $\pi(\varphi_1 \wedge \ldots \wedge \varphi_n) = \mathbb{1}$. Ponownie, korzystając z założenia i definicji operatora $\Rightarrow$, otrzymujemy $\pi(\psi) = \mathbb{1}$. □

Oto kilka najważniejszych reguł wnioskowania:

Twierdzenie 1.4

1. $\{p\} \models p$,
2. $\{p, \neg p\} \models q$,
3. $\{p, q\} \models p \wedge q$,
4. $\{p \wedge q\} \models p$,
5. $\{p, p \to q\} \models q$ *(modus ponens)*,
6. $\{p \vee q, \neg p \vee q\} \models q$ *(rezolucja)*.

Interpretacja reguły $\{p, \neg p\} \models q$ jest następująca: ze sprzecznej rodziny zdań wyprowadzić możemy dowolne inne zdanie. Interpretacja reguły „modus ponens", zwanej również regułą odrywania, jest następująca: jeśli potrafię pokazać p oraz potrafię pokazać, że $p \to q$, to potrafię również pokazać zdanie q. Równoważną postacią reguły rezolucji jest reguła $\{p \to q, \neg p \to q\} \models q$.

Uwaga. Większość wykładów z logiki matematycznej stosuje regułę Modus Ponens jako podstawową regułę wnioskowania. Reguła rezolucji jest często stosowana w systemach automatycznego dowodzenia twierdzeń.

Metoda rezolucji dowodzenia twierdzeń bazuje na regule rezolucji oraz na następującej charakteryzacji relacji wynikania:

Twierdzenie 1.5 *Następujące dwa zdania są równoważne*

1. $\{\varphi_1, \ldots, \varphi_n\} \models \psi$
2. *rodzina zdań* $\varphi_1, \ldots, \varphi_n, \neg\psi$ *jest sprzeczna, czyli nie istnieje waluacja* π *taka, że* $\pi(\varphi_1) = \ldots = \pi(\varphi_n) = \pi(\neg\psi) = \mathbb{1}$

Dowód. $(1) \to (2)$. Załóżmy, że $\{\varphi_1, \ldots, \varphi_n\} \models \psi$. Rozważmy dowolną waluację π. Jeśli dla wszystkich $i = 1, \ldots n$ mamy $\pi(\varphi_i) = \mathbb{1}$, to z założenia wynika, że $\pi(\psi) = \mathbb{1}$ a więc $\pi(\neg\psi) = \mathbb{0}$.

$(2) \to (1)$. Załóżmy, że π jest taką waluacją, że $\pi(\varphi_1) = \ldots \pi(\varphi_n) = \mathbb{1}$. Wtedy $\pi(\neg\psi) = \mathbb{0}$, więc $\pi(\psi) = \mathbb{1}$. □

Dowody Wprost

Najprostsze dowody twierdzeń, zwane *dowodami wprost*, polegają na wywnioskowaniu tezy twierdzenia z jego założeń.

Przykład 1.4 *Rozważmy dowód następującego prostego twierdzenia o liczbach naturalnych:*

> *"jeśli liczby* n *i* m *są parzyste, to ich suma* $n + m$ *jest parzysta".*

(czyli: "suma dwóch liczb parzystych jest parzysta"). Założenie tego twierdzenie jest koniunkcją dwóch zdań: "n *jest liczbą parzystą" oraz "*m *jest liczbą parzystą". Załóżmy zatem, że oba te zdania są prawdziwe. Istnieją wtedy liczby* a *oraz* b *takie, że* $n = 2a$ *oraz* $m = 2b$*. Lecz wtedy* $n + m = 2a + 2b = 2(a + b)$*, zatem teza jest prawdziwa.*

Jest to typowy przykład rozumowanie "wprost.

Dowody Nie Wprost

Dowody nie wprost polegają na wykorzystaniu reguły

$$\{\neg q \to \neg p\} \models p \to q$$

Zaczynają się one od założenia, że teza jest fałszywa i pokazaniu, że z tego wynika fałszywość założenia.

Przykład 1.5 *Wykażemy prawdziwość następującego zdania o liczbach rzeczywistych:*

> *"jeśli średnia arytmetyczna liczb* x, y *jest większa od 1, to co najmniej jedna z tych liczb jest większa od 1".*

Twierdzenie to możemy zapisać następująco:

$$\big(\frac{x+y}{2} > 1\big) \to ((x > 1) \vee (y > 1)).$$

Załóżmy, że teza twierdzenia jest fałszywa, czyli, że prawdziwe jest zdanie $\neg((x > 1) \vee (y > 1))$*. Z prawa de Morgana wynika, że prawdziwa jest wówczas koniunkcja* $(\neg(x > 1)) \wedge (\neg(y > 1))$*, czyli, że prawdziwe jest zdanie* $(x \leq 1) \wedge (y \leq 1)$*. Lecz wtedy* $x + y \leq 2$*, zatem* $\frac{x+y}{2} \leq 1$*. Pokazaliśmy więc, że zaprzeczenie tezy implikuje zaprzeczenie założenia. Zatem twierdzenie zostało udowodnione.*

Dowody przez sprowadzenie do sprzeczności

Dowody przez *sprowadzenie do sprzeczności* są pewną odmianą dowodów nie wprost. Korzystają one z następującej reguły dowodzenia:

$$\{(\varphi \wedge \neg\psi) \to \bot\} \models \varphi \to \psi$$

Reguła ta jest poprawna, gdyż

$$((\varphi \wedge \neg\psi) \to \bot) \equiv \neg(\varphi \wedge \neg\psi) \vee \bot \equiv \neg(\varphi \wedge \neg\psi) \equiv \neg\varphi \vee \psi \equiv \varphi \to \psi.$$

Przykład 1.6 *Zanalizujemy dobrze z pewnością znany czytelnikowi dowód niewymierności liczby $\sqrt{2}$, czyli dowód zdania*

„jeśli $x^2 = 2$ to x jest liczbą niewymierną".

Zakładamy w nim, że

„$x^2 = 2$ i x jest liczbą wymierną"

i przedstawiamy liczbę x w postaci ułamka $x = \frac{n}{m}$ takiego, że $NWD(n, m) = 1$, gdzie $NDW(n, m)$ oznacza największy wspólny dzielnik liczb n i m. Po podniesieniu obu stron do kwadratu otrzymujemy równość $2 = \frac{n^2}{m^2}$, którą przekształcamy do postaci $2m^2 = n^2$. Z otrzymanej równości wynika, że n jest liczbą parzystą, możemy ją więc przestawić w postaci $n = 2k$. Po podstawieniu otrzymujemy równość $2m^2 = (2k)^2$, czyli $2m^2 = 4k^2$. Z równości tej wynika, że $m^2 = 2k^2$, z czego wnioskujemy, że m jest liczbą parzystą. Zatem $NWD(n, m) > 1$.

Z założeń „$x^2 = 2$ i x jest liczbą wymierną" wywnioskowaliśmy, że „istnieją liczby n i m takie, że $NWD(n, m) = 1$ i $NWD(n, m) > 1$". Założenie „$x^2 = 2$ i x jest liczbą wymierną" prowadzi więc do sprzeczności.

Dowody Przez Rozważenie Przypadków

Do dowodów niektórych twierdzeń skorzystać możemy z następującej postaci reguły rezolucji

$$\{p \to q, \neg p \to q\} \models q.$$

Przykład 1.7 *Pokażemy, że dla dowolnej liczb rzeczywistej x prawdziwa jest nierówność*

$$x \leq |x|.$$

Jeśli $x \geq 0$, to $|x| = x \leq x$. Jeśli $x < 0$, to $x < 0 \leq |x|$. Pokazaliśmy więc, że

$$(x \geq 0 \to x \leq |x||) \wedge (\neg(x \geq 0) \to x \leq |x|),$$

co kończy dowód.

Przykład 1.8 *Pokażemy, że dla dowolnych liczb rzeczywistych x oraz y prawdziwa jest nierówność*

$$|x + y| \leq |x| + |y|.$$

Jeśli $x+y \geq 0$ *to* $|x+y| = x+y \leq |x|+|y|$. *Jeśli* $x+y < 0$ *to* $|x+y| = -(x+y) = (-x)+(-y) \leq |x|+|y|$.
Pokazaliśmy więc, że

$$(x+y \geq 0 \to |x+y| \leq |x|+|y|) \wedge (\neg(x+y \geq 0) \to |x+y| \leq |x|+|y|),$$

co kończy dowód.

1.4 Notacja Polska

W definicji zdania rachunku zdań korzystaliśmy z nawiasów. Istnieje metoda zapisywania zdań bez ich użycia. Metodą tą wprowadził polski matematyk i logik Łukasiewicz i nazywana jest obecnie *notacją polską*. Pokażemy w jaki sposób można przekształcić zdanie zapisane za pomocą nawiasów w zdanie beznawiasowe. Posłużymy się metodą rekurencyjną.

Dla zmiennych zdaniowych p_i określimy $[p_i] = p_i$. Następnie definiujemy

1. $[\varphi \wedge \psi] = [\varphi][\psi]\wedge$
2. $[\varphi \vee \psi] = [\varphi][\psi]\vee$
3. $[\varphi \to \psi] = [\varphi][\psi] \to$
4. $[\varphi \leftrightarrow \psi] = [\varphi][\psi] \leftrightarrow$
5. $[\neg\varphi] = [\varphi]\neg$

Zastosujmy tę metodę dla prawa de Morgana $\neg(p\wedge q) \leftrightarrow (\neg p \vee \neg q)$. Mamy wtedy

$$[\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)] = [\neg(p \wedge q)][(\neg p \vee \neg q)] \leftrightarrow \ =$$

$$[p \wedge q]\neg[\neg p][\neg q]\vee \leftrightarrow \ = \ [p][q] \wedge \neg[p]\neg[q]\neg\vee \leftrightarrow \ = \ pq \wedge \neg p\neg q\neg\vee \leftrightarrow .$$

Otrzymane zdanie $pq \wedge \neg p\neg q\neg\vee \leftrightarrow$ jest nieco mniej czytelne dla człowieka niż oryginalne zdanie $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$. Jednak znacznie łatwiej jest napisać program komputerowy, który operuje na wyrażeniach zapisanych w notacji polskiej niż operujący na wyrażeniach zapisanych w notacji nawiasowej. Ponadto programy takie są bardzo efektywne. Metoda ta znalazła zastosowanie w kalkulatorach firmy Hewlett-Packard, w języku programowania Forth, stosuje się ją często w interpreterach. Warto zauważyć, że można ją stosować nie tylko do wyrażeń rachunku zdań. Z powodzeniem można ją używać do zapisu dowolnych wyrażeń arytmetycznych i algebraicznych.

1.5 Ćwiczenia i zadania

Ćwiczenie 1.1 *Pokaż, że dla dowolnych zmiennych zdaniowych p, q i r następujące zdania są tautologiami:*

1. $(p \wedge p) \leftrightarrow p$,
2. $(p \vee p) \leftrightarrow p$,
3. $(p \wedge q) \leftrightarrow (q \wedge p)$,
4. $(p \vee q) \leftrightarrow (q \vee p)$,
5. $(p \wedge (q \wedge r)) \leftrightarrow ((p \wedge q) \wedge r)$,
6. $(p \vee (q \vee r)) \leftrightarrow ((p \vee q) \vee r)$,
7. $(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r)$,
8. $(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r)$,
9. $\neg(\neg p) \leftrightarrow p$,
10. $\neg(p \wedge \neg p)$,
11. $p \vee \neg p$,
12. $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$,
13. $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$,
14. $((p \to q) \wedge (q \to r)) \to (p \to r)$,
15. $(p \to q) \leftrightarrow (\neg p \vee q)$,
16. $(p \leftrightarrow q) \leftrightarrow ((p \to q) \wedge (q \to p))$,
17. $(p \leftrightarrow q) \leftrightarrow ((p \wedge q) \vee (\neg p \wedge \neg g))$.

Ćwiczenie 1.2 *Pokaż, że dla dowolnych zmiennych zdaniowych p, q, r i s zdanie $p \wedge (q \wedge (r \wedge s)) \leftrightarrow ((p \wedge q) \wedge r) \wedge s))$ jest tautologią.*

Ćwiczenie 1.3 *Pokaż, że zdanie "Jeśli Jaś nie umie logiki, to jeśli Jaś umie logikę, to $1 + 1 = 3$" jest prawdziwe.*

Ćwiczenie 1.4 *Pokaż, że jeśli średnia arytmetyczna liczb $x_1, \ldots, x_n$ jest większa od liczby a, to co najmniej jedna z tych liczb jest większa od liczby a.*

Ćwiczenie 1.5 *Niech p oznacza zdanie „rok R jest podzielny przez 4", q - „rok R jest podzielny przez 100", i r - „rok R jest podzielny przez 400". Zapisz za pomocą zdań p, q i r zdanie „rok R jest przestępny".*

Ćwiczenie 1.6 *Twierdzenie Pitagorasa można sformułować w postaci implikacji:*

$$\angle(ACB) = 90^\circ \to AC^2 + CB^2 = AB^2 \ .$$

Przypomnij sobie dowód tego twierdzenia. Sformułuj twierdzenie odwrotne. Czy jest ono prawdziwe?

Ćwiczenie 1.7 *Sprawdź poprawność następujących rozumowań.*

1. *Gdyby Jan był żołnierzem, to byłby odważny. Lecz Jan nie jest żołnierzem. Zatem Jan jest tchórzem.*
2. *Jeśli $x+3 = \sqrt{3-x}$ to $x^2+6x+9 = 3-x$, więc $x = -6$ lub $x = -1$. Zatem liczby -6 oraz -1 są rozwiązaniami równania $x + 3 = \sqrt{3-x}$.*

Ćwiczenie 1.8 *Wyraź alternatywę, implikację oraz równoważność za pomocą negacji oraz koniunkcji. Wyraź koniunkcję, implikację oraz równoważność za pomocą negacji oraz alternatywy.*

Ćwiczenie 1.9 *Wyraź negację, koniunkcję, alternatywę, implikację oraz równoważność za pomocą spójnika Pierce'a.*

Ćwiczenie 1.10 *Wyraź negację, koniunkcję, alternatywę, implikację oraz równoważność za pomocą kreski Sheffera.*

Ćwiczenie 1.11 *Udowodnij łączność spójnika* $\triangle$.

Ćwiczenie 1.12 *Pokaż, że*
1. $\{p\} \models p$,
2. $\{p, q\} \models p \wedge q$,
3. $\{p, \neg p\} \models q$,
4. $\{p, p \to q\} \models q$, *(reguła Modus Ponens)*
5. $\{\alpha \vee p, \neg\alpha \vee q\} \models p \vee q$ *(reguła rezolucji).*

Ćwiczenie 1.13 *Zapisz w notacji polskiej następujące formuły:*
1. $((p \vee q) \vee r) \vee s$
2. $(p \vee q) \to (\neg r \wedge s)$
3. $(\neg(p \vee q)) \leftrightarrow (\neg p \wedge \neg q)$

Ćwiczenie 1.14 *Ile jest waluacji* $\pi : \{p_1, \ldots, p_{10}\} \to \{\mathbb{0}, \mathbb{1}\}$ *takich, że*
1. $\pi \models (p_1 \vee \ldots \vee p_{10})$,
2. $\pi \models p_1 \to (p_2 \vee \ldots \vee p_{10})$,
3. $\pi \models (p_1 \vee \ldots \vee p_5) \wedge (p_6 \vee \ldots \vee p_{10})$ *?*

Zadanie 1.1 *Pokaż, że każde zdanie rachunku zdań zawiera taką samą liczbę nawiasów otwierających co zamykających.*

Zadanie 1.2 *Pokaż, że jeśli zdanie jest zbudowane tylko ze stałych zdaniowych (czyli nie zawiera żadnej zmiennej zdaniowej), to jest ono tautologią lub zdaniem sprzecznym.*

Zadanie 1.3 *Pokaż, że jeśli* $\varphi(p_0, \ldots, p_n)$ *jest tautologią oraz że* $\psi_0, \ldots \psi_n$ *są dowolnymi zdaniami, to zdanie* $\varphi(\psi_0, \ldots, \psi_n)$ *jest również tautologią.*

Zadanie 1.4 *Niech* $\varphi_0 = p$ *oraz* $\varphi_{n+1} = (\varphi_n) \to p$ *dla liczb naturalnych* n. *Dla jakich liczb naturalnych* n *zdanie* φ_n *jest tautologią?*

Zadanie 1.5 (Liczby Catalana) *Niech* c_n *oznacza liczbę sposobów którymi można rozmieścić nawiasy w iloczynie* $x_1 \ldots x_n$. *Przyjmujemy, że* c_0*=0. Oczywiście* $c_1 = c_2 = 1$. *Wyznacz wartości* c_3 *i* c_4 *Pokaż, że*

$$c_n = \sum_{i=0}^{n} c_i c_{n-i}. \tag{1.1}$$

Zadanie 1.6 *Ile istnieje nierównoważnych formuł rachunku zdań zbudowanych ze zmiennych zdaniowych p, q?*

Zadanie 1.7 *Pokaż, że za pomocą koniunkcji i alternatywy nie można zdefiniować negacji. Pokaż, że za pomocą alternatywy i koniunkcji nie można zdefiniować implikacji*

Zadanie 1.8 *Pokaż, że liczba* $0.101001000100001000001\ldots$ *jest niewymierna. Przeprowadź analizę przedstawionego dowodu.*

Zadanie 1.9 *Na pewnej wyspie mieszka dwóch tubylców. Jeden z nich zawsze mówi prawdę, drugi - zawsze kłamie. Na wyspę dostał się wędrowiec. Stanął przed rozwidleniem dróg. Spotkał tubylca. Chce dowiedzieć się która z dwóch dróg doprowadzi go do stolicy. Może zadać tylko jedno pytanie. Jak powinien je sformułować?*

2 Zbiory

Zbiór oraz relację należenia $\in$ traktujemy jako pojęcia podstawowe. Oznacza to tyle, że nie będziemy zajmowali się tym czym jest zbiór ani czym jest relacja należenia, lecz zajmować się będziemy ich własnościami. Zbiór pusty oznaczać będziemy symbolem $\emptyset$. Zbiór liczb naturalnych, czyli zbiór $\{0, 1, 2, \ldots\}$ oznaczamy symbolem $\mathbb{N}$. Symbol $\mathbb{Z}$ oznacza zbiór liczb całkowitych, $\mathbb{Q}$ - zbiór liczb wymiernych zaś $\mathbb{R}$ oznacza zbiór liczb rzeczywistych. Symbol $\mathbb{C}$ oznacza zbiór liczb zespolonych. Negację symbolu należenia oznaczamy przez $\notin$, czyli wyrażenie $x \notin A$ należy traktować jako skróconą formę zapisu wyrażenia $\neg(x \in A)$.

Uwaga. Liczbę zero zaliczamy w tej książce do zbioru liczb naturalnych.

2.1 Aksjomat Ekstensjonalności

Rozważania tego wykładu rozpoczniemy od sprecyzowania tego, kiedy dwa zbiory są sobie równe.

Aksjomat 2.1 (Ekstensjonalności) *Dwa zbiory A i B są równe wtedy i tylko wtedy, gdy*

$$x \in A \leftrightarrow x \in B$$

dla dowolnego x.

Aksjomat ten można wysłowić następująco „***zbiory są równe jeśli mają te same elementy***". Można z niego wyprowadzić szereg interesujących wniosków. Pierwszy z nich dotyczy zbioru pustego, czyli takiego zbioru, do którego nie należy żaden element.

Wniosek 2.1 *Istnieje tylko jeden zbiór pusty.*

Dowód. Załóżmy, że $\emptyset_1$ i $\emptyset_2$ są zbiorami pustymi. Rozważmy dowolny x. Wtedy oba zdania $x \in \emptyset_1$ oraz $x \in \emptyset_2$ są fałszywe. Lecz $(\bot \leftrightarrow \bot) \equiv \top$, zatem zdanie

$$x \in \emptyset_1 \leftrightarrow x \in \emptyset_2$$

jest prawdziwe. A więc, na mocy Aksjomatu Ekstensjonalości, $\emptyset_1 = \emptyset_2$. □

Uwaga. Z ostatniego wniosku wynika, co chyba nie jest oczywiste, ze zbiór trolli jest równy zbiorowi elfów.

Definicja 2.1 *Niech Ω będzie dowolnym zbiorem.* ***Funkcją zdaniową*** *określoną dla elementów zbioru Ω nazywamy dowolne wyrażenie które każdemu elementowi $x \in \Omega$ jednoznacznie przypisuje wartość $\varphi(x)$ ze zbioru $\{\mathbb{1}, \mathbb{0}\}$.*

Jeśli $\Omega = \mathbb{N}$ to funkcjami zdaniowymi, są na przykład, $\psi_1(x)$ = "x jest liczbą parzystą", $\psi_2(x)$ = "x jest liczbą pierwszą".

Definicja 2.2 *Niech Ω będzie dowolnym zbiorem. Niech $\varphi(x)$ będzie funkcją zdaniową określoną dla elementów zbioru Ω. Wtedy przez $\{x \in \Omega : \varphi(x)\}$ oznaczamy taki zbiór C, że*

$$x \in C \leftrightarrow x \in \Omega \wedge \varphi(x).$$

Z operatorem tym, zwanym *operatorem wyróżniania*, spotykamy się w wielu konstrukcjach matematycznych. Na przykład, odcinek $[a, b]$ zbioru liczb rzeczywistych definiuje się jako $\{x \in \mathbb{R} : a \leq x \wedge x \leq b\}$. Zbiór liczb parzystych definiujemy jako $\{x \in \mathbb{N} : 2|x\}$, gdzie „|" oznacza symbol podzielności. Za pomocą operatora wyróżniania udowodnimy teraz pierwszy ciekawy fakt o zbiorach.

Twierdzenie 2.1 (Russel) *Nie istnieje zbiór wszystkich zbiorów.*

Dowód. Załóżmy, że V jest zbiorem wszystkich zbiorów. Rozważmy zbiór

$$A = \{x \in V : x \notin x\}.$$

Oczywiście $A \in V$, bo do zbioru V należą wszystkie zbiory. Lecz wtedy

$$A \in A \leftrightarrow (A \in V \wedge A \notin A) \leftrightarrow A \notin A.$$

Otrzymana sprzeczność kończy dowód. □

Uwaga. To właśnie z powodu Twierdzenia Russell'a operator wyróżniania stosujemy do konkretnego zbioru, czyli posługujemy się konstrukcją $\{x \in C : \varphi(x)\}$. Konstrukcja postaci $\{x : \varphi(x)\}$ prowadzić może do sprzeczności, gdyż jej wynikiem może nie być zbiór.

Uwaga. Pewien niepokój u czytelnika może budzić wyrażenie $x \notin x$. Wydawać się bowiem może, że nie ma zbiorów x takich, że $x \in x$, czyli, że formuła $x \notin x$ jest zawsze prawdziwa. Autor książki proponuje nie rozważać tej kwestii w tym miejscu. Jest ona bowiem, w pewnym sensie, nierozstrzygalna. Możemy założyć, że zbiory o własności $x \in x$ nie istnieją. A wtedy twierdzenie Russell'a jest oczywiste - nie może istnieć zbiór wszystkich zbiorów, gdyż gdyby istniał, to musiał by być swoim elementem. Przedstawiony wyżej dowód twierdzenia Russell'a jest „czysty" - nie korzysta z tego założenia. Czytelnikowi któremu te wyjaśnienia wydają się mało przekonywujące powinien zapoznać się z Aksjomatem Regularności omawianym w Dodatku C.

2.2 Operacje Mnogościowe

Dawnym polskim określeniem dzisiejszego pojęcia zbiór było słowo „*mnogość*". Jest ono nadal używane w terminologii matematycznej. W rozdziale tym zajmiemy się omówieniem podstawowych operacji mnogościowych na zbiorach, takich jak suma, przekrój oraz różnica.

Definicja 2.3 *Niech A i B będą zbiorami.*

1. ***Sumą** zbiorów A i B nazywamy taki zbiór C, że $x \in C \leftrightarrow (x \in A \vee x \in B)$ dla dowolnego x. Zbiór ten oznaczamy symbolem $A \cup B$.*
2. ***Przekrojem** zbiorów A i B nazywamy taki zbiór C, że $x \in C \leftrightarrow (x \in A \wedge x \in B)$. Zbiór ten oznaczamy symbolem $A \cap B$.*
3. ***Różnicą** zbiorów A i B nazywamy taki zbiór C, że $x \in C \leftrightarrow (x \in A \wedge x \notin B)$. Zbiór ten oznaczamy symbolem $A \setminus B$.*

Z Aksjomatu ekstensjonalności wynika, że powyższe operacje są poprawnie zdefiniowane, czyli, na przykład, że dla danych zbiorów A oraz B ich suma $A \cup B$ jest wyznaczona jednoznacznie.

W rozdziale tym omówimy podstawowe własności operacji wprowadzonych w Definicji 2.3. Wiele dowodów będziemy opuszczać, pozostawiając je czytelnikowi. Większość nich prowadzi się według pewnego ogólnego schematu, który przedstawimy teraz na konkretnym przykładzie.

Przykład 2.1 *Pokażemy, że operacja sumy jest przemienna, czyli, że $A \cup B = B \cup A$ dla dowolnych zbiorów A i B. Ustalmy zbiory A i B oraz rozważmy dowolny element x. Wtedy*

$$x \in A \cup B \equiv^{(1)} (x \in A \vee x \in B) \equiv^{(2)} (x \in B \vee x \in A) \equiv^{(2)} x \in B \cup A.$$

Zatem, dla dowolnego x mamy

$$x \in A \cup B \equiv x \in B \cup A,$$

a więc, na mocy Aksjomatu Ekstensjonalności, mamy $A \cup B = B \cup A$.

Przyjrzyjmy się powyższemu rozumowaniu. Zastosowaliśmy w nim uproszczony zapis szeregu równoważności. Zamiast w oddzielnych linijkach pisać $\varphi_1 \equiv \varphi_2$, $\varphi_2 \equiv \varphi_3$ oraz $\varphi_{n-1} \equiv \varphi_n$ zastosowaliśmy uproszczony zapis $\varphi_1 \equiv \varphi_2 \equiv \varphi_3 \ldots \equiv \varphi_n$. Pierwsza równoważność wynika z definicji operacji sumy. Druga równoważność wynika z przemienności alternatywy zastosowanej do zdań $p = (x \in A)$ oraz $q = (x \in B)$. Ostatnia równoważność ponownie wynika z definicji sumy. W podobny sposób można przeprowadzić dowody wielu innych faktów podanych w tym rozdziale. Pierwsza część takiego dowodu polega na przetłumaczeniu pewnego wyrażenia na język rachunku zdań. Następnie korzystamy z odpowiedniej tautologii. W ostatniej fazie wykonujemy odwrotne tłumaczenie zdania na wyrażenie rachunku zbiorów.

Uwaga. Przedstawiona metoda redukcji zagadnień z jednej dziedziny matematyki do zagadnień z innej dziedziny jest bardzo silnym narzędziem badawczym. Zastosował ją R. Descartes (Kartezjusz) który pokazał jak można redukować zagadnienia geometryczne do zagadnień analitycznych.

Przegląd najważniejszych własności wprowadzonych operacji rozpoczniemy od własności sumy i przekroju zbiorów. W poniższych tabelkach A, B i C oznaczają

dowolne zbiory.

idempotentność	$A \cap A = A$
	$A \cup A = A$
przemienność	$A \cap B = B \cap A$
	$A \cup B = B \cup A$
łączność	$A \cap (B \cap C) = (A \cap B) \cap C$
	$A \cup (B \cup C) = (A \cup B) \cup C$
rozdzielność	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Zauważmy również, że $A \cap \emptyset = \emptyset$ oraz $A \cup \emptyset = A$ dla dowolnego zbioru A. Zbiór pusty jest więc *elementem neutralnym* dodawania zbiorów.

Definicja 2.4 *Mówimy, że zbiór A zawiera się w zbiorze B ($A \subseteq B$) jeśli dla każdego x prawdziwa jest implikacja*

$$x \in A \to x \in B.$$

Zauważmy, że z Aksjomatu Ekstensjonalności wynika, że jeśli $A \subseteq B$ oraz $B \subseteq A$ to $A = B$. Aksjomat ten może więc być zapisany w postaci

$$A = B \leftrightarrow (A \subseteq B) \wedge (B \subseteq A).$$

Oto lista podstawowych własności inkluzji zbiorów:

zwrotność inkluzji	$A \subseteq A$
przechodniość inkluzji	$(A \subseteq B) \wedge (B \subseteq C) \to A \subseteq C$
własności sumy	$A \subseteq A \cup B$
	$(A \subseteq C) \wedge (B \subseteq C) \to A \cup B \subseteq C$
własności przekroju	$A \cap B \subseteq A$
	$(A \subseteq B) \wedge (A \subseteq C) \to A \subseteq B \cap C$
monotoniczność	$(A \subseteq B) \wedge (C \subseteq D) \to A \cup C \subseteq B \cup D$
	$(A \subseteq B) \wedge (C \subseteq D) \to A \cap C \subseteq B \cap D$

Dowody powyższych własności inkluzji różnią się od dowodów równości postaci $\Phi = \Psi$, gdzie Φ i Ψ są wyrażeniami algebry zbiorów. Spowodowane jest to tym, że inkluzja nie jest operacją na zbiorach lecz zależnością pomiędzy nimi. Dla przykładu naszkicujemy dowód przechodniości inkluzji.

Przykład 2.2 (Dowód przechodniości inkluzji) *Załóżmy, że $A \subseteq B$ i $B \subseteq C$. Rozważmy dowolny element $x \in A$. Z pierwszego założenia wynika, że $x \in B$. Lecz wtedy, z drugiej części założenia wynika, że $x \in C$. Zatem dla dowolnego elementu x jeśli zdanie $x \in A$ jest prawdziwe, to prawdziwe jest również zdanie $x \in C$. A więc $A \subseteq C$.*

Pokażemy teraz, że inkluzję można zdefiniować za pomocą operacji sumy oraz przekroju.

Twierdzenie 2.2 *Dla dowolnych zbiorów A i B następujące trzy zdania są równoważne:*

1. $A \subseteq B$,
2. $A \cap B = A$,
3. $A \cup B = B$.

Dowód. Pokażemy najpierw, że prawdziwa jest implikacja $(1) \to (2)$. Załóżmy, że $A \subseteq B$. Ponieważ $A \cap B \subseteq A$ dla dowolnych zbiorów A i B, wystarczy więc pokazać, że $A \subseteq A \cap B$. Niech więc $x \in A$. Z założenia wynika, że wtedy $x \in B$. Zatem oba zdania $x \in A$ i $x \in B$ są prawdziwe. Prawdziwa jest więc również ich koniunkcja $(x \in A) \wedge (x \in B)$. Pokazaliśmy więc, że $x \in A \cap B$, co kończy dowód implikacji $(1) \to (2)$.
Pokażemy teraz, że $(2) \to (3)$. Załóżmy, że $A \cap B = A$. Wtedy

$$A \cup B = (A \cap B) \cup B \subseteq B \cap B = B.$$

Druga inkluzja, czyli $B \subseteq A \cup B$, jest prawdziwa dla dowolnych zbiorów A i B. Pokazaliśmy więc prawdziwość implikacji $(2) \to (3)$.

Pokażemy teraz, że $(3) \to (1)$. Załóżmy, że $A \cup B = B$. Niech $x \in A$. Wtedy $x \in A \cup B$, a więc $x \in B$, co kończy dowód implikacji $(3) \to (1)$.

Pokazaliśmy więc, że implikacje $(1) \to (2)$, $(2) \to (3)$ oraz $(3) \to (1)$ są prawdziwe. Twierdzenie jest więc udowodnione. □

Zwróćmy uwagę na strukturę przeprowadzonego dowodu. Rozważaliśmy trzy zdania (1), (2) i (3). Pokazaliśmy, że prawdziwe są implikacje $(1) \to (2)$, $(2) \to (3)$ i $(3) \to (1)$. Łatwo można sprawdzić, że zdanie

$$((p \to q) \wedge (q \to r) \wedge (q \to r)) \to ((p \leftrightarrow q) \wedge (q \leftrightarrow r) \wedge (p \leftrightarrow r))$$

jest tautologią. Zatem wszystkie zdania (1), (2) i (3) są równoważne.

Uwaga. W celu udowodnienia równoważności trzech zdań należy pokazać $6 = 3 * 2$ implikacji. Metoda zastosowana w powyższym rozumowaniu redukuje tę liczbę do trzech implikacji. Zysk staje się tym bardziej widoczny im większą ilość równoważności mamy do pokazania. Jeśli do pokazania mamy równoważność n zdań, to bezpośrednia metoda wymaga $n(n-1)$ równoważności, zaś metoda oparta na uogólnieniu stosowanej wyżej metody wymaga przeprowadzenie tylko n rozumowań.

Zajmiemy się teraz pojęciem dopełnienia zbioru. Przypomnijmy (Twierdzenie 2.1), że nie istnieje zbiór wszystkich zbiorów. Dopełniać zbiory możemy tylko do ustalonego zbioru. Taki ustalony na pewien czas zbiór będziemy nazywać przestrzenią.

Definicja 2.5 *Niech Ω będzie ustalonym zbiorem oraz $A \subseteq \Omega$. Dopełnieniem zbioru A do przestrzeni Ω nazywamy zbiór $A^c = \Omega \setminus A$.*

Uwaga. W niektórych książkach dopełnienie zbioru A oznaczane jest przez A'. Można spotkać się również z notacją $-A$.

Ustalmy przestrzeń Ω oraz zbiory $A, B \subseteq \Omega$. Oto najważniejsze własności operacji dopełnienia do przestrzeni Ω.

inwolucyjność	$(A^c)^c = A$
różnica	$A \setminus B = A \cap B^c$
prawa de Morgana	$(A \cup B)^c = A^c \cap B^c$
	$(A \cap B)^c = A^c \cup B^c$
własności przestrzeni	$\emptyset^c = \Omega$
	$\Omega^c = \emptyset$
antymonotoniczność	$A \subseteq B \to B^c \subseteq A^c$

Twierdzenie 2.3 *Niech $\varphi(x)$ i $\psi(x)$ będą funkcjami zdaniowymi określonymi dla elementów przestrzeni Ω. Wtedy*

1. $\{x \in \Omega : \varphi(x)\}^c = \{x \in \Omega : \neg\varphi(x)\}$,
2. $\{x \in \Omega : \varphi(x) \wedge \psi(x)\} = \{x \in \Omega : \varphi(x)\} \cap \{x \in \Omega : \psi(x)\}$,
3. $\{x \in \Omega : \varphi(x) \vee \psi(x)\} = \{x \in \Omega : \varphi(x)\} \cup \{x \in \Omega : \psi(x)\}$.

Twierdzenie to wynika bezpośrednio z definicji operatora wyróżniania, definicji dopełnienia, przekroju i sumy oraz z Aksjomatu Ekstensjonalności.

Definicja 2.6 ***Różnicą symetryczną*** *zbiorów A i B nazywamy zbiór*

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Zauważmy, że $x \in A \triangle B \leftrightarrow (x \in A) \oplus (x \in B)$, gdzie $\oplus$ z prawej strony tego wyrażenia oznacza spójnik logiczny "albo" zdefiniowany w poprzednim wykładzie. Z tego powodu różnica symetryczna zbiorów dziedziczy własności tego spójnika. W szczególności $A \triangle \emptyset = A$, $A \triangle A = \emptyset$, $A \triangle B = B \triangle A$ oraz $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

Z wymienionych własności różnicy symetrycznej wynika, że $(A \triangle B) \triangle B = A$ dla dowolnych zbiorów A i B. Obserwację tę wykorzystać można do prostych metod kodowania informacji.

Definicja 2.7 *Parą elementów a i b nazywamy taki zbiór C, że $x \in C \leftrightarrow (x = a) \vee (x = b)$ dla dowolnego x. Zbiór ten oznaczamy symbolem $\{a, b\}$.*

Z Aksjomatu Ekstensjonalności wynika jednoznaczność operacji pary. Dla danego elementu a definiujemy $\{a\} = \{a, a\}$. Zbiór ten nazywamy *singletonem* elementu a. Ze zbioru pustego $\emptyset$, za pomocą operacji tworzenia singletonu, możemy skonstruować nieskończenie wiele różnych zbiorów. Są nimi $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}$, ... Za pomocą operacji pary oraz sumy definiować możemy trójki, czwórki itd. Na przykład, definujemy $\{a, b, c\} = \{a, b\} \cup \{c\}$.

Definicja 2.8 (Kuratowski) *Parą uporządkowaną elementów a i b nazywamy zbiór*

$$(a, b) = \{\{a\}, \{a, b\}\}\ .$$

Zauważmy, że jeśli $a = b$ to $(a, b) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$, a więc zbiór (a, a) jest jednoelementowy. Jeśli $a \neq b$ to $\{a\} \neq \{a, b\}$, więc wtedy zbiór (a, b) jest dwuelementowy. Podstawowa własność pary uporządkowanej zawarta jest w następującym twierdzeniu:

Twierdzenie 2.4 *Dla dowolnych elementów x, y, u i v mamy*

$$(x, y) = (u, v) \leftrightarrow (x = u) \wedge (y = v).$$

Dowód. Załóżmy, że $(x, y) = (u, v)$. Rozważmy dwa przypadki. Jeśli $x = y$, to (x, y) jest zbiorem jednoelementowym, więc również zbiór (u, v) musi być zbiorem jednoelementowym, z czego łatwo wynika, że $x = y = u = v$. Załóżmy teraz, że $x \neq y$. Wtedy również $u \neq v$. Z równości $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$ wynika, że $x = u$. Zatem $\{x, y\} = \{x, v\}$ a więc i $y = v$. □

Uwaga. Parę uporządkowaną można by określić inaczej. W niektórych rozważaniach tak też się czyni. Istotne jest tylko to aby dla pary uporządkowanej prawdziwe było Twierdzenie 2.4.

Definicja 2.9 ***Iloczynem kartezjańskim*** *zbiorów A i B nazywamy zbiór*

$$A \times B = \{(x, y) : x \in A \wedge y \in B\}.$$

Za pomocą iloczynu kartezjańskiego definiowane są skończenie wymiarowe przestrzenie euklidesowe. Na przykład, płaszczyznę $\mathbb{R}^2$ utożsamiamy ze zbiorem $\mathbb{R} \times \mathbb{R}$.

Pojęcie pary uporządkowanej uogólnia się na pojęcie n-ki uporządkowanej. Trójkę uporządkowaną definiujemy jako $(x, y, z) = ((x, y), z)$. Ogólnie, dla n>2 definiujemy

$$(x_1, \ldots, x_{n+1}) = ((x_1, \ldots, x_n), x_{n+1}).$$

Z twierdzenia 2.4 wynika, że

$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \leftrightarrow (x_1 = y_1) \wedge \ldots \wedge (x_n = y_n).$$

Definicję iloczynu kartezjańskiego dwóch zbiorów uogólniamy w następujący sposób na iloczyn kartezjański n zbiorów:

$$A_1 \times \ldots \times A_n = \{(x_1, \ldots, x_n) : x_1 \in A_1 \wedge \ldots \wedge x_n \in A_n\}$$

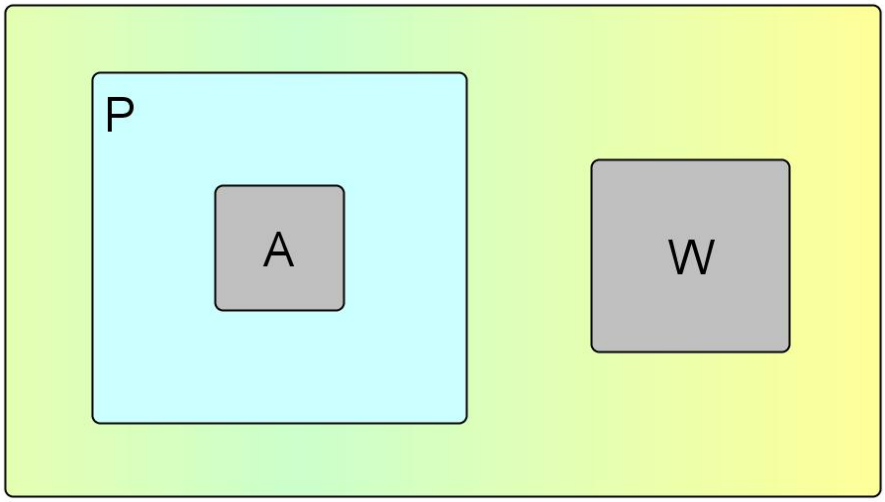
W szczególnym przypadku, gdy $A_1 = \ldots = A_n = A$ to zamiast $A \times \ldots \times A$ piszemy A^n. Trójwymiarową przestrzeń euklidesową utożsamiamy ze zbiorem $\mathbb{R}^3$.

Definicja 2.10 ***Zbiorem potęgowym*** *zbioru A nazywamy zbiór $P(A)$ złożony ze wszystkich podzbiorów zbioru A.*

Zbiór pusty jest podzbiorem dowolnego zbioru, zatem $\emptyset \in P(A)$ dla każdego zbioru A. Z inkluzji $A \subseteq A$ wynika, że $A \in P(A)$ dla każdego zbioru A. Zatem $\{\emptyset, A\} \subseteq P(A)$ dla dowolnego zbioru A.

2.3 Diagramy Venna

Pod koniec XIX wieku J. Venn upowszechnił prosty system obrazowania logicznych związków pomiędzy różnymi klasami obiektów. Diagram Venna jest prostokątem w którym narysowane są kółka reprezentujące grupy obiektów mających takie same własności. Na przykład, na następującym rysunku cały prostokąt reprezentuje "uniwersum" wszystkich zwierząt, obszar W reprezentuje wielbłądy, obszar P ptaki i region A albatrosy.



Na diagramie tym zaznaczone są trzy obserwacje:

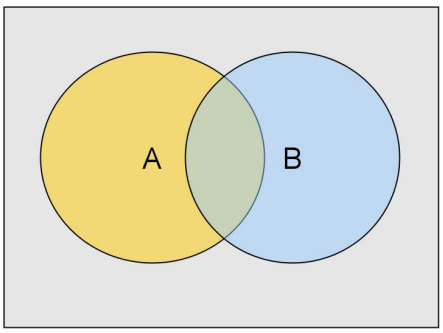
1. wszystkie albatrosy są ptakami,
2. żaden ptak nie jest wielbłądem,
3. żaden albatros nie jest wielbłądem.

Diagram ten służy do zilustrowania następującej reguły wnioskowania:

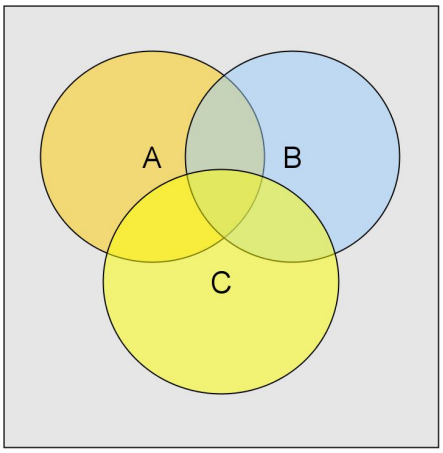
> z tego, że „*wszystkie A są P*" i „*żaden P nie jest W*" wynika, że „*żaden A nie jest W*",

co w języku zbiorów może być wyrażone następująco: jeśli $A \subseteq P$ oraz $P \cap W = \emptyset$ to $A \cap W = \emptyset$.

Diagramy te mogą służyć do sprawdzania czy dana równość pomiędzy wyrażeniami algebry zbiorów jest prawdziwa. Należy pamiętać o tym aby w przypadku sprawdzania tożsamości dla dwóch zbiorów, powiedzmy dla zbiorów A i B, wybrać takie zbiory aby $A \cap B \neq \emptyset$, $A \cap B^c \neq \emptyset$ $A^c \cap B \neq \emptyset$ i $A^c \cap B^c \neq \emptyset$. Taki układem są dwa przecinające się kółka:



Dla badania zależności pomiędzy trzema zbiorami należy zastosować takie zbiory A, B, C, dla których wszystkie przekroje $A^i \cap B^j \cap C^k$ są niepuste, gdzie $i, j, k \in \{0, 1\}$ oraz X^0 oznacza zbiór X zaś X^1 oznacza zbiór X^c. Takim układem są, na przykład, trzy kółka:



Dla większej ilości zmiennych trudno jest narysować odpowiedni układ zbiorów do testowania prawdziwości równości wyrażeń algebry zbiorów (patrz Rozdział A.7).

Uwaga. Diagramy Venna upowszechnił J. Venn. Jednakże podobnymi diagramami posługiwał się już w XVII wieku Gottfried Wilhelm Leibniz, który uważany jest za twórcę logiki symbolicznej. W księdze "*Opera Omnia*" Leonarda Eulera, znajduje się prawie taki sam rysunek jak ten, od którego rozpoczęliśmy ilustracje diagramów Venna. Tak więc Venn nie jest twórcą diagramów Venna, lecz ich popularyzatorem.

2.4 Ćwiczenia i zadania

Ćwiczenie 2.1 *Wyznacz $A \cap B$, $A \cup B$, $A \setminus B$ i $B \setminus A$ jeśli*
1. $A = \mathbb{R}$, $B = \mathbb{Q}$,
2. $A = \{n \in \mathbb{N} : 3|n\}$, $B = \{n \in \mathbb{N} : 5|n\}$,
3. $A = [0, 3]$, $B = (1, 2]$.

Ćwiczenie 2.2 *Pokaż, że dla dowolnych zbiorów A, B i C prawdziwe są następujące równości:*

1. $A \cap A = A$,
2. $A \cup A = A$
3. $A \cap B = B \cap A$,
4. $A \cup B = B \cup A$,
5. $A \cap (B \cap C) = (A \cap B) \cap C$,
6. $A \cup (B \cup C) = (A \cup B) \cup C$,
7. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
8. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Ćwiczenie 2.3 *Pokaż, że dla dowolnych zbiorów A, B i C prawdziwe są następujące zdania:*

1. $A \subseteq A$,
2. $(A \subseteq B) \wedge (B \subseteq C) \rightarrow A \subseteq C$,
3. $A \subseteq A \cup B$,
4. $(A \subseteq C) \wedge (B \subseteq C) \rightarrow A \cup B \subseteq C$,
5. $A \cap B \subseteq A$,
6. $(A \subseteq B) \wedge (A \subseteq C) \rightarrow A \subseteq B \cap C$,
7. $(A \subseteq B) \wedge (C \subseteq D) \rightarrow A \cup C \subseteq B \cup D$,
8. $(A \subseteq B) \wedge (C \subseteq D) \rightarrow A \cap C \subseteq B \cap D$.

Ćwiczenie 2.4 *Niech A i B będą podziorami ustalonej przestrzeni Ω. Pokaż, że*

1. $(A^c)^c = A$,
2. $A \setminus B = A \cap B^c$,
3. $(A \cup B)^c = A^c \cap B^c$,
4. $(A \cap B)^c = A^c \cup B^c$,
5. $\emptyset^c = \Omega$,
6. $\Omega^c = \emptyset$,
7. $A \subseteq B \rightarrow B^c \subseteq A^c$.

Ćwiczenie 2.5 *Pokaż, że $A \cup B$ jest najmniejszym (w sensie inkluzji) zbiorem zawierającym jednocześnie zbiory A oraz B. Sformułuj i udowodnij analogiczny fakt dla przekroju dwóch zbiorów.*

Ćwiczenie 2.6 *Pokaż, że $(A \setminus B) \setminus C = A \setminus (B \cup C)$ oraz $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$ dla dowolnych zbiorów A, B, i C.*

Ćwiczenie 2.7 *Rozwiąż równanie* $[0,1] \triangle X = [-1, \frac{1}{2})$.

Ćwiczenie 2.8 *Niech* $A = \{1,3,5\}$, $B = \{2,4\}$ *i* $C = \{1,5\}$. *Znajdź taki zbiór* X, *że* $(A \triangle X) \triangle B = C$.

Ćwiczenie 2.9 *Alicja i Bob przesyłają pomiędzy sobą informacje o podzbiorach zbioru* $\{1,\ldots,100\}$. *Do szyfrowania przesyłanych informacji stosują operację różnicy symetrycznej z podzbiorem wszystkich liczb pierwszych ze zbioru* $\{1,\ldots,100\}$. *Załóżmy, że Alicja chce przesłać Bobowi zbiór* $\{3,9,53\}$. *Wyznacz zaszyfrowany zbiór. Sprawdź, że Bob potrafi bezbłędnie odczytać przesłaną mu informację. Co jest potrzebne do złamania tej metody szyfrowania danych?*

Ćwiczenie 2.10 *Pokaż, że* $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.

Ćwiczenie 2.11 *Pokaż, że zbiory* $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\ldots$ *są parami różne.*

Ćwiczenie 2.12 *Czy iloczyn kartezjański jest operacją łączną? Czy jest przemienny?*

Ćwiczenie 2.13 *Pokaż, że dla dowolnych zbiorów* A, B *i* C *prawdziwe są następujące równości:*

1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$,
2. $(A \cap B) \times C = (A \times C) \cap (B \times C)$.

Ćwiczenie 2.14 *Pokaż, że* $A \subseteq B$ *wtedy i tylko wtedy, gdy* $P(A) \subseteq P(B)$.

Ćwiczenie 2.15 *Czy dla dowolnych zbiorów* A *i* B *prawdziwe są równości* $P(A) \cap P(B) = P(A \cap B)$ *i* $P(A) \cup P(B) = P(A \cup B)$*?*

Ćwiczenie 2.16 *Wyznacz zbiory* $P(\emptyset)$, $P(P(\emptyset))$, $P(\{a,b\})$ *i* $P(\{a,b,c\})$.

Ćwiczenie 2.17 *Niech* $A, B \subseteq \Omega$. *Opisz rodzinę wszystkich zbiorów które mogą zostać zdefiniowane ze zbiorów* A *i* B *za pomocą operacji sumy, przekroju i dopełnienia.*

Ćwiczenie 2.18 *Niech* $A = \{1,2,6,7,8\}$, $B = \{2,3,4,7,8\}$ *i* $C = \{4,5,6,7,8\}$. *Ile różnych zbiorów możesz zbudować za pomocą operacji* $\cup$, $\cap$, ^{c} *ze zbiorów* A, B *i* C*? Czy zbiór* $\{8\}$ *należy do tej rodziny zbiorów?*

Ćwiczenie 2.19 *Pokaż, ze dla dowolnych zbiorów* A *i* B *prawdziwa jest równoważność* $A = B \leftrightarrow A \setminus B = B \setminus A$.

Ćwiczenie 2.20 (Lewis Carroll) *Pokaż, że z następującego zbioru zdań*
(a) wszyscy moi synowie są szczupli,
(b) wszystkie moje zdrowe dzieci uprawiają sport,
(c) żadne moje dziecko które jest łakomczuchem nie jest szczupłe,
(d) żadna moja córka nie uprawia sportu
wynika, że "żadne moje zdrowe dziecko nie jest łakomczuchem".

Ćwiczenie 2.21 *Pokaż, że dla dowolnych zbiorów* A *i* B *mamy* $A \setminus (A \setminus (A \setminus B)) = A \setminus B$.

Ćwiczenie 2.22 *Zapisz w postaci "nawiasowej" następujące wyrażenia:* $ABC \cup \cup$ *oraz* $AB \cup C \cup$.

Zadanie 2.1 *Pokaż, że z Aksjomatu Ekstensjonalości wynika, że operacja sumy jest poprawnie określone. To znaczy, że jeśli* A *i* B *są dowolnymi zbiorami, to istnieje tylko jeden zbiór* C *taki, że* $x \in C \leftrightarrow (x \in A \vee x \in B)$. *To samo pokaż dla iloczynu i różnicy zbiorów.*

Zadanie 2.2 *Niech* $\varphi(x)$ *i* $\psi(x)$ *będą funkcjami zdaniowymi określonymi dla elementów przestrzeni* Ω. *Pokaż, że*

1. $\{x \in \Omega : \varphi(x)\}^c = \{x \in \Omega : \neg\varphi(x)\}$,
2. $\{x \in \Omega : \varphi(x) \wedge \psi(x)\} = \{x \in \Omega : \varphi(x)\} \cap \{x \in \Omega : \psi(x)\}$,
3. $\{x \in \Omega : \varphi(x) \vee \psi(x)\} = \{x \in \Omega : \varphi(x)\} \cup \{x \in \Omega : \psi(x)\}$.

Zadanie 2.3 *Niech* $S(x) = x \cup \{x\}$. *Niech* $x_0 = \emptyset$ *oraz* $x_{n+1} = S(x_n)$ *dla wszystkich liczb naturalnych* n. *Wyznacz* x_n *dla wszystkich* $n \leq 5$. *Pokaż, że jeśli* $n < m$ *to* $x_n \in x_m$.

Zadanie 2.4 *Pokaż, że* $A \times B = B \times A$ *wtedy i tylko wtedy, gdy* $A = B \vee A = \emptyset \vee B = \emptyset$.

Zadanie 2.5 *Pokaż, że dla każdego zbioru* A *zachodzi nierówność* $A \neq P(A)$.

Zadanie 2.6 *Pokaż, że nie istnieje taki zbiór* Ω, *że* $A \subseteq \Omega$ *dla dowolnego zbioru* A.

Zadanie 2.7 *Zbiór* A *nazywamy tranzytywnym jeśli* $x \subseteq A$ *dla dowolnego* $x \in A$. *Pokaż, że* $\emptyset$ *jest zbiorem tranzytywnym oraz, że jeśli* A *jest zbiorem tranzytywnym, to również zbiory* $P(A)$ *i* $A \cup \{A\}$ *są tranzytywne.*

3 Kwantyfikatory

Dział logiki matematycznej zajmujący się własnościami kwantyfikatorów nazywa się Rachunkiem Predykatów. Określa on poprawne metody wnioskowania w językach zawierających wyrażenia w których występują kwantyfikatory. W wykładzie tym omówimy tylko podstawowe własności kwantyfikatorów a mianowicie te które dają się sprowadzić do pewnych zagadnień mnogościowych. Z pełną wersją Rachunku Predykatów czytelnicy tej książki zetkną się na wykładach poświęconych Logice Algorytmicznej bądź też Logice Matematycznej.

3.1 Definicja kwantyfikatorów

Ustalmy **niepustą** przestrzeń Ω. Przypomnijmy, że φ jest *funkcją zdaniową* elementów przestrzeni Ω, jeśli dla każdego $a \in \Omega$ określona jest wartość $\varphi(a) \in \{\mathbb{0}, \mathbb{1}\}$. Przykładem funkcji zdaniowej dla $\Omega = \mathbb{R}$ są wyrażenia $\varphi(x) = (x > 0)$ i $\psi(x) = (3 \leq x \leq 5)$. Jeśli funkcja zdaniowa φ jest zapisana za pomocą symboli matematycznych, to nazywamy ją *formułą* jednej zmiennej. [1]

Definicja 3.1 *Niech φ będzie funkcją zdaniową elementów przestrzeni Ω. Wtedy*

1. *Zdanie $(\exists x)\varphi(x)$ jest prawdziwe, jeśli $\{x \in \Omega : \varphi(x)\} \neq \emptyset$.*
2. *Zdanie $(\forall x)\varphi(x)$ jest prawdziwe, jeśli $\{x \in \Omega : \varphi(x)\} = \Omega$.*

Wyrażenia $\exists$ oraz $\forall$ nazywamy się *kwantyfikatorami*. Pierwszy z nich nazywa się kwantyfikatorem *egzystencjalnym* (lub *szczegółowym*), drugi kwantyfikatorem *uniwersalnym* (lub *ogólnym*). W niektórych książkach używane są inne oznaczenia na kwantyfikatory. Oto kilka przykładów alternatywnych form zapisu kwantyfikatora ogólnego:

$$\bigwedge_x \varphi(x), \qquad (Ax)\varphi(x), \qquad (x)\varphi(x),$$

oraz kilka przykładów alternatywnych form zapisu kwantyfikatora szczegółowego:

$$\bigvee_x \varphi(x), \qquad (Ex)\varphi(x).$$

Załóżmy na chwilę, że rozważana przez nas przestrzeń Ω jest skończona. Niech $\Omega = \{\omega_1, \ldots, \omega_n\}$. Zauważmy, że wtedy

$$(\exists x)\varphi(x) \leftrightarrow \ (\varphi(\omega_1) \vee \ldots \vee \varphi(\omega_n))$$

[1] Sprawa ta zostanie omówiona bardziej starannie na wykładach z Logiki Matematycznej bądź z Logiki Algorytmicznej. Na razie ten poziom precyzji nam wystarczy.

oraz

$$(\forall x)\varphi(x) \leftrightarrow (\varphi(\omega_1) \wedge \ldots \wedge \varphi(\omega_n)).$$

Kwantyfikator egzystencjalny możemy więc traktować jako uogólnienie spójnika logicznego $\vee$. Podobnie kwantyfikator ogólny możemy traktować jako uogólnienie spójnika logicznego $\wedge$.

Przykład 3.1 *Niech* $\phi(x) = (x^2 = -1)$. *Jeśli* $\Omega = \mathbb{R}$ *to w dziedzinie tej zdanie* $(\exists x)\phi(x)$ *jest fałszywe, gdyż* $\{x \in \mathbb{C} : x^2 = -1\} = \emptyset$. *Jeśli zaś* $\Omega = \mathbb{C}$, *to w dziedzinie tej zdanie* $(\exists x)\phi(x)$ *jest prawdziwe, gdyż* $\{x \in \mathbb{C} : x^2 = -1\} = \{-i, i\}$.

3.2 Własności kwantyfikatorów

W części tej omówimy podstawowe własności kwantyfikatorów. Rozpoczniemy od analizy wyrażeń z jednym kwantyfikatorem. Potem omówimy własności wyrażeń rozpoczynających się od bloku kwantyfikatorów długości 2.

Definicja 3.2 *Niech* $\varphi(x)$ *będzie funkcją zdaniową elementów przestrzeni* Ω. ***Diagramem*** *funkcji zdaniowej* φ *nazywamy zbiór* $D_\varphi = \{a \in \Omega : \varphi(a)\}$.

Przypomnijmy, że z Twierdzenia 2.3 wynika natychmiast, że

1. $D_{\neg\varphi} = (D_\varphi)^c$,
2. $D_{\varphi\vee\psi} = D_\varphi \cup D_\psi$ oraz
3. $D_{\varphi\wedge\psi} = D_\varphi \cap D_\psi$.

Bezpośrednio z Definicji 3.1 oraz z Definicji 3.2 wynika, że jeśli $\varphi(x)$ jest funkcją zdaniową elementów przestrzeni Ω, to

1. Zdanie $(\exists x)\varphi(x)$ jest prawdziwe wtedy i tylko wtedy, gdy $D_{\varphi(x)} \neq \emptyset$.
2. Zdanie $(\forall x)\varphi(x)$ jest prawdziwe wtedy i tylko wtedy, gdy $D_{\varphi(x)} = \Omega$.

Twierdzenie 3.1 *Niech* φ *oraz* ψ *będą funkcjami zdaniowymi elementów przestrzeni* Ω. *Wtedy:*

1. $\neg(\exists x)\varphi(x) \leftrightarrow (\forall x)\neg\varphi(x)$,
2. $\neg(\forall x)\varphi(x) \leftrightarrow (\exists x)\neg\varphi(x)$,
3. $(\exists x)(\varphi(x) \vee \psi(x)) \leftrightarrow ((\exists x)\varphi(x) \vee (\exists x)\psi(x))$,
4. $(\exists x)(\varphi(x) \wedge \psi(x)) \rightarrow ((\exists x)\varphi(x) \wedge (\exists x)\psi(x))$,
5. $((\forall x)\varphi(x) \vee (\forall x)\psi(x)) \rightarrow (\forall x)(\varphi(x) \vee \psi(x))$,
6. $(\forall x)(\varphi(x) \wedge \psi(x)) \leftrightarrow ((\forall x)\varphi(x) \wedge (\forall x)\psi(x))$.

Pierwsze dwie równoważności nazywają się **prawami de Morgana dla kwantyfikatorów**. Równoważność (3) nazywa się rozdzielnością kwantyfikatora egzystencjalnego względem alternatywy a (5) - rozdzielnością kwantyfikatora uniwersalnego względem koniunkcji.

Dowód. W celu udowodnienia pierwszej równoważności zauważmy, że

$$\neg(\exists x)\varphi(x) \leftrightarrow \neg(D_\varphi \neq \emptyset) \leftrightarrow D_\varphi = \emptyset \leftrightarrow$$

$$D_\varphi^c = \Omega \leftrightarrow D_{\neg\varphi} = \Omega \leftrightarrow (\forall x)\neg\varphi(x).$$

Dowód drugiej równoważności przebiega podobnie jak pierwszej. Udowodnimy teraz trzecią równoważność. Zauważmy, że

$$(\exists x)(\varphi(x) \vee \psi(x)) \leftrightarrow D_{\varphi\vee\psi} \neq \emptyset \leftrightarrow D_\varphi \cup D_\psi \neq \emptyset$$

Zauważmy następnie, że suma dwóch zbiorów jest niepusta wtedy i tylko wtedy gdy choćby jeden z tych zbiorów jest niepusty. Zatem

$$(\exists x)(\varphi(x) \vee \psi(x)) \leftrightarrow D_\varphi \neq \emptyset \vee D_\psi \neq \emptyset,$$

a więc $(\exists x)(\varphi(x) \vee \psi(x)) \leftrightarrow ((\exists x)\varphi(x) \vee (\exists x)\psi(x))$. Pokażemy teraz czwartą część twierdzenia. Zauważmy najpierw, że

$$(\exists x)(\varphi(x) \wedge \psi(x)) \leftrightarrow D_{\varphi\wedge\psi} \neq \emptyset \leftrightarrow D_\varphi \cap D_\psi \neq \emptyset.$$

Zauważmy następnie, że jeśli przekrój dwóch zbiorów jest niepusty, to oba zbiory muszą być niepuste. Zatem

$$(\exists x)(\varphi(x) \wedge \psi(x)) \rightarrow (D_\varphi \neq \emptyset \wedge D_\psi \neq \emptyset),$$

a więc

$$(\exists x)(\varphi(x) \wedge \psi(x)) \rightarrow ((\exists x)\varphi(x) \wedge (\exists x)\psi(x)).$$

Dowód części (5) oraz (6) jest podobny do dowodów części (3) oraz (4). □

W punkcie (4) oraz (5) udowodnionego twierdzenia występują implikacje. Pokażemy teraz, że nie można ich zastąpić równoważnościami.

Przykład 3.2 *Niech $\Omega = \mathbb{N}$. Rozważmy formuły $\varphi(x) = 2|x$ oraz $\psi(x) = \neg(2|x)$, gdzie symbol $|$ oznacza podzielność bez reszty.*

Oba zdania $(\exists x)\varphi(x)$ oraz $(\exists x)\psi(x)$ są prawdziwe, gdyż $0 \in D_{\varphi(x)}$ oraz $1 \in D_{\psi(x)}$. Prawdziwa jest więc również ich koniunkcja $(\exists x)\varphi(x) \wedge (\exists x)\psi(x)$. Jednak zdanie $(\exists x)(\varphi(x) \wedge \psi(x))$ nie jest prawdziwe, gdyż $D_{\varphi(x)\wedge\psi(x)} = \emptyset$, bowiem nie istnieje liczba naturalna która jest jednocześnie parzysta i nieparzysta. Tak więc implikacji w trzecim punkcie ostatniego twierdzenia nie można zastąpić równoważnością.

Zauważmy, że każda liczba naturalna jest parzysta albo nieparzysta. Zatem zdanie $(\forall x)(\varphi(x) \vee \psi(x))$ jest prawdziwe. Lecz nie jest prawdą, że każda liczba jest parzysta. Podobnie nie jest prawdą, że każda liczba jest nieparzysta. Zatem $(\forall x)\varphi(x) \vee (\forall x)\psi(x)$ jest zdaniem fałszywym. Zatem i w punkcie (5) ostatniego twierdzenia implikacji nie można zastąpić równoważnością.

Załóżmy na chwilę, że przestrzeń Ω jest skończona. Niech $\Omega = \{\omega_1, \ldots, \omega_n\}$. Korzystając z łączności oraz przemienności spójnika $\vee$ mamy

$$(\exists x)(\varphi(x) \vee \psi(x)) \leftrightarrow \big((\varphi(\omega_1) \vee \psi(\omega_1)) \vee \ldots \vee (\varphi(\omega_n) \vee \psi(\omega_n))\big) \leftrightarrow$$
$$\big((\varphi(\omega_1) \vee \ldots \vee \varphi(\omega_n)) \vee (\psi(\omega_1) \vee \ldots \vee \psi(\omega_n))\big) \leftrightarrow \big((\exists x)\varphi(x) \vee (\exists x)\psi(x)\big) .$$

Widzimy więc, że tautologia $(\exists x)(\varphi(x) \vee \psi(x)) \leftrightarrow ((\exists x)\varphi(x) \vee (\exists x)\psi(x))$ dla przestrzeni skończonych wynika z łączności i przemienności alternatywy. Podobnie, tautologia $(\forall x)(\varphi(x) \wedge \psi(x)) \leftrightarrow ((\forall x)\varphi(x) \wedge (\forall x)\psi(x))$ dla przestrzeni skończonych jest konsekwencją łączności i przemienności koniunkcji.

Jeśli $\varphi(x)$ jest funkcją zdaniową określoną dla elementów przestrzeni Ω, to wyrażenia $(\forall x)\varphi(x)$ oraz $(\exists x)\varphi(x)$ są zdaniami, czyli takimi wyrażeniami, które są prawdziwe lub fałszywe. Możemy je traktować jako funkcje stałe, które każdemu elementowi rozważanej przestrzeni Ω przyporządkowują tą samą wartość logiczną. Oczywiście jeśli ψ jest zdaniem, to $(\forall x)\psi \leftrightarrow \psi$ oraz $(\exists x)\psi \leftrightarrow \psi$. Obserwację tą uogólnia następujące twierdzenie, którego dowód wynika bezpośrednio z Definicji 3.1.

Twierdzenie 3.2 *Niech $\varphi(x)$ będzie funkcją zdaniową oraz niech ψ będzie zdaniem. Wtedy*

1. $(\forall x)(\varphi(x) \vee \psi) \leftrightarrow (\forall x)\varphi(x) \vee \psi$.
2. $(\forall x)(\varphi(x) \wedge \psi) \leftrightarrow (\forall x)\varphi(x) \wedge \psi$.
3. $(\exists x)(\varphi(x) \vee \psi) \leftrightarrow (\exists x)\varphi(x) \vee \psi$.
4. $(\exists x)(\varphi(x) \wedge \psi) \leftrightarrow (\exists x)\varphi(x) \wedge \psi$.

Rozszerzymy teraz zakres naszych rozważań na funkcje zdaniowe dwóch zmiennych. Mówimy, że $\varphi(x, y)$ jest funkcją zdaniową elementów przestrzeni $\Omega \times \Omega$ jeśli dla dowolnych $(a, b) \in \Omega \times \Omega$ określona jest wartość $\varphi(a, b) \in \{\mathbb{0}, \mathbb{1}\}$. Podobnie jak poprzednio będziemy funkcje zdaniową $\varphi(x, y)$ nazywali formułą dwóch zmiennych jeśli jest zapisana za pomocą symboli matematycznych. Analogicznie określamy pojęcie diagramu dla formuły zdaniowej dwóch zmiennych: $D_\varphi = \{(a, b) \in \Omega \times \Omega : \varphi(a, b)\}$.

Niech $\varphi(x, y)$ będzie funkcją zdaniową elementów przestrzeni Ω^2. Zauważmy, że każde z wyrażeń $(\forall x)\varphi(x, y)$, $(\forall y)\varphi(x, y)$, $(\exists x)\varphi(x, y)$ oraz $(\exists y)\varphi(x, y)$ jest funkcją zdaniową jednej zmiennej. Do każdej z tych funkcji zdaniowych możemy dopisać z lewej strony jeden z czterech kwantyfikatorów $(\exists x)$, $(\exists y)$, $(\forall x)$ oraz $(\forall y)$. Otrzymamy w ten sposób kolekcję ośmiu zdań:

$$(\forall x)(\forall y)\varphi(x, y), \quad (\forall y)(\forall x)\varphi(x, y), \quad (\forall x)(\exists y)\varphi(x, y), \quad (\forall y)(\exists x)\varphi(x, y),$$

$$(\exists x)(\forall y)\varphi(x, y), \quad (\exists y)(\forall x)\varphi(x, y), \quad (\exists x)(\exists y)\varphi(x, y) \quad (\exists y)(\exists x)\varphi(x, y).$$

Zajmiemy się teraz omówieniem związków między tymi zdaniami. Interpretacja zdań $(\forall x)(\forall y)\varphi(x, y)$ oraz $(\forall y)(\forall x)\varphi(x, y)$ jest prosta. Mamy bowiem

$$(\forall x)(\forall y)\varphi(x, y) \leftrightarrow (\forall x)(\{y \in \Omega : \varphi(x, y)\} = \Omega) \leftrightarrow D_\varphi = \Omega^2,$$

oraz

$$(\forall y)(\forall x)\varphi(x,y) \leftrightarrow (\forall y)(\{z \in \Omega : \varphi(x,y)\} = \Omega) \leftrightarrow D_\varphi = \Omega^2.$$

Zatem zdania $(\forall x)(\forall y)\varphi(x,y)$ oraz $(\forall y)(\forall x)\varphi(x,y)$ są równoważne temu, że $D_\varphi = \Omega^2$. Ponadto widzimy, że $(\forall x)(\forall y)\varphi(x,y) \leftrightarrow (\forall y)(\forall x)\varphi(x,y)$.

W podobny sposób sprawdzamy, że

$$(\exists x)(\exists y)\varphi(x,y) \leftrightarrow D_\varphi \neq \emptyset$$

oraz

$$(\exists y)(\exists x)\varphi(x,y) \leftrightarrow D_\varphi \neq \emptyset.$$

Zatem zdania $(\exists x)(\exists y)\varphi(x,y)$ oraz $(\exists y)(\exists x)\varphi(x,y)$ są równoważne temu, że $D_\varphi \neq \emptyset$. Ponadto widzimy, że $(\exists x)(\exists y)\varphi(x,y) \leftrightarrow (\exists y)(\exists x)\varphi(x,y)$.

Wszystkie związki pomiędzy zdaniami zbudowanymi z jednej funkcji zdaniowej φ dwóch zmiennych oraz dwóch kwantyfikatorów przedstawione są na następującym diagramie:

$$\begin{array}{ccccc} & & (\exists x)(\forall y)\varphi & \to & (\forall y)(\exists x)\varphi & & \\ & \nearrow & & & & \searrow & \\ (\forall x)(\forall y)\varphi & & & & & & (\exists x)(\exists y)\varphi \\ & \searrow & & & & \nearrow & \\ & & (\exists y)(\forall x)\varphi & \to & (\forall x)(\exists y)\varphi & & \end{array} \tag{3.1}$$

Implikacja $(\forall x)(\forall y)\varphi(x,y) \to (\exists x)(\forall y)\varphi(x,y)$ wynika z tego, że przestrzeń Ω jest niepusta. Załóżmy bowiem, że zdanie $(\forall x)(\forall y)\varphi(x,y)$ jest prawdziwe oraz niech c będzie ustalonym elementem zbioru Ω. Z założenia wynika, że $D_\varphi = \Omega^2$, więc dla dowolnego $y \in \Omega$ mamy $\varphi(c,y) = \mathbb{1}$. Zatem $\{x \in \Omega : (\forall y)\varphi(x,y)\}$ jest zbiorem niepustym, gdyż należy do niego element c, a więc zdanie $(\exists x)(\forall y)\varphi(x,y)$ jest prawdziwe. Podobnie pokazujemy prawdziwość implikacji $(\forall x)(\forall y)\varphi(x,y) \to (\exists y)(\forall x)\varphi(x,y)$.

Załóżmy teraz, że prawdziwe jest zdanie $(\exists x)(\forall y)\varphi(x,y)$. Niech c będzie takim elementem zbioru Ω, że $(\forall y)\varphi(c,y)$. Wtedy dla każdego elementu $y_0 \in \Omega$ zbiór $\{x \in \Omega : \varphi(c,y_0)\}$ jest niepusty, gdyż należy do niego element c. Zatem dla każdego $y_0 \in \Omega$ zdanie $(\exists x)\varphi(x,y_0)$ jest prawdziwe, a więc $\{y \in \Omega : (\exists x)\varphi(x,y_0)\} = \Omega$, czyli zdanie $(\forall y)(\exists x)\varphi(x,y)$ jest prawdziwe. Pokazaliśmy więc, że implikacja $(\exists x)(\forall y)\varphi(x,y) \to (\forall y)(\exists x)\varphi(x,y)$ jest prawdziwa. Podobnie pokazujemy prawdziwość implikacji $(\exists y)(\forall x)\varphi(x,y) \to (\forall x)(\exists y)\varphi(x,y)$.

Załóżmy, że prawdziwe jest zdanie $(\forall y)(\exists x)\varphi(x,y)$. Niech d będzie elementem zbioru Ω Wtedy zdanie $(\exists x)\varphi(x,d)$ jest prawdziwe. Istnieje więc $c \in \Omega$ takie, że $\varphi(c,d) = \mathbb{1}$, a więc zdanie $(\exists x)(\exists y)\varphi(x,y)$ jest prawdziwe. Podobnie pokazujemy, że implikacja $(\forall x)(\exists y)\varphi(x,y) \to (\exists x)(\exists y)\varphi(x,y)$ jest prawdziwa dla dowolnej funkcji zdaniowej φ.

Można pokazać, że żadnej implikacji występującej w diagramie 3.1 nie można zastąpić równoważnością. Oto kilka przykładów ilustrujących ten fakt:

Przykład 3.3 *Niech $\Omega = \mathbb{R}$ oraz $\varphi(x,y) = (x < y)$. Wtedy zdanie $(\forall x)(\exists y)\varphi(x,y)$ jest prawdziwe, gdyż dla każdej liczby rzeczywistej x istnieje liczba od niej większa*

(jest nią, na przykład, liczba $x+1$). Zdanie $(\exists y)(\forall x)\varphi(x,y)$ jest zaś ewidentnie fałszywe, gdyż gdyby było prawdziwe to istniałaby liczba rzeczywista a taka, że dla każdej liczby rzeczywistej x mielibyśmy $x < a$. Implikacji

$$(\exists y)(\forall x)\varphi(x,y) \to (\forall x)(\exists y)\varphi(x,y)$$

nie można więc zastąpić równoważnością.

Przykład 3.4 *Niech $\Omega = [0,1]$ oraz niech $\varphi(x,y) = (x \geq y)$. Wtedy zdanie $(\exists x)(\forall y)\varphi(x,y)$ jest prawdziwe, gdyż liczba 1 jest największą liczbą w odcinku $[0,1]$. Zdanie $(\forall x)(\forall y)\varphi(x,y)$ jest zaś ewidentnie fałszywe. Implikacji*

$$(\forall x)(\forall y)\varphi(x,y) \to (\exists x)(\forall y)\varphi(x,y)$$

nie można więc zastąpić równoważnością.

Przykład 3.5 *Niech $\Omega = \{0,1\}$ oraz niech $\varphi(x,y) = (x = 1) \wedge (y = 1)$. Zdanie $(\exists x)(\exists y)\varphi(x,y)$ jest ewidentnie prawdziwe, lecz zdanie $(\forall y)(\exists x)\varphi(x,y)$ jest zaś fałszywe. Implikacji*

$$(\forall y)(\exists x)\varphi(x,y) \to (\exists x)(\exists y)\varphi(x,y)$$

nie można więc zastąpić równoważnością.

Do tej pory zajmowaliśmy się funkcjami zdaniowymi dwóch zmiennych. W podobny sposób możemy analizować funkcje zdaniowe n zmiennych dla dowolnego $n > 0$ oraz dłuższe bloki kwantyfikatorów. Na przykład, jeśli $\psi(x,y,z)$ jest funkcją zdaniową trzech zmiennych elementów przestrzeni Ω, to określamy

$$(\exists x)(\forall y)(\exists z)\psi(x,y,z) \leftrightarrow (\{a \in \Omega : (\forall y)(\exists z)\psi(a,y,z)\} \neq \emptyset)$$

W większości przypadków do analizy nawet bardzo skomplikowanych wyrażeń wystarczą nam omówione prawa dla funkcji zdaniowych dwóch zmiennych.

3.3 Kwantyfikatory ograniczone

W wielu sytuacjach w formułach opisujących własności ustalonej przestrzeni Ω odwołujemy się do wyróżnionych podzbiorów tej przestrzeni. Na przykład, w definicji ciągłości posługujemy się wyrażeniem $(\forall \varepsilon > 0)$, ograniczając zakres działania kwantyfikatora uniwersalnego do liczb rzeczywistych dodatnich. Konstrukcje takie nazywamy kwantyfikatorami ograniczonymi.

Definicja 3.3 *Niech A będzie podzbiorem, przestrzeni Ω oraz niech $\varphi(x)$ będzie funkcją zdaniową elementów przestrzeni Ω. Określamy*

1. $(\forall x \in A)\varphi(x) = (\forall x)(x \in A \to \varphi(x))$,
2. $(\exists x \in A)\varphi(x) = (\exists x)(x \in A \wedge \varphi(x))$.

Kwantyfikatory ograniczone mają podobne własności jak normalne kwantyfikatory. Pokażemy, dla przykładu, że prawdziwe jest dla nich prawo de Morgana.

Twierdzenie 3.3 (de Morgan) *Niech A będzie podzbiorem przestrzeni Ω oraz niech $\varphi(x)$ będzie funkcją zdaniową elementów przestrzeni Ω. Wtedy*

1. $\neg(\forall x \in A)\varphi(x) \leftrightarrow (\exists x \in A)(\neg\varphi(x))$,
2. $\neg(\exists x \in A)\varphi(x) \leftrightarrow (\forall x \in A)(\neg\varphi(x))$.

Dowód. Załóżmy, że A jest podzbiorem przestrzeni Ω oraz niech $\varphi(x)$ będzie funkcją zdaniową elementów przestrzeni Ω. Wtedy

$$\neg(\forall x \in A)\varphi(x) \equiv \neg(\forall x)(x \in A \to \varphi(x)) \equiv^{(2)} (\exists x)(\neg(x \in A \to \varphi(x))).$$

Równoważność (2) wynika z prawa de Morgan dla normalnych kwantyfikatorów. Z tautologii $(p \to q) \equiv (\neg p \vee q)$ oraz prawa de Morgana rachunku zdań wynika, że $\neg(p \to q) \equiv (p \wedge \neg q)$. Zatem

$$\neg(\forall x \in A)\varphi(x) \equiv (\exists x)(x \in A \wedge \neg\varphi(x))) \equiv (\exists x \in A)(\neg\varphi(x)).$$

Drugą część twierdzenia łatwo można wyprowadzić z części pierwszej. □

Pokażemy teraz kilka zastosowań omówionych własności kwantyfikatorów.

Przykład 3.6 *Funkcję $f : \mathbb{R} \mapsto \mathbb{R}$ nazywamy **jednostajnie ciągłą** jeśli*

$$(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x)(\forall y)(|x - y| < \delta \to |f(x) - f(y)| < \varepsilon).$$

Ponieważ prawdziwa jest implikacja $(\exists x)(\forall y)\varphi \to (\forall y)(\exists x)\varphi$, więc z jednostajnej ciągłości wynika, że

$$(\forall \varepsilon > 0)(\forall x)(\exists \delta > 0)(\forall y)(|x - y| < \delta \to |f(x) - f(y)| < \varepsilon).$$

Ponieważ

$$(\exists x)(\exists y)\varphi \leftrightarrow (\exists y)(\exists x)\varphi,$$

więc z jednostajnej ciągłości funkcji f wynika, że

$$(\forall x)(\forall \varepsilon > 0)(\exists \delta > 0)(\forall y)(|x - y| < \delta \to |f(x) - f(y)| < \varepsilon),$$

czyli, że funkcja f jest ciągła w każdym punkcie, czyli, po prostu, że jest ciągła. Pokazaliśmy więc, że jednostajna ciągłość pociąga ciągłość. Odwrotna implikacja nie jest prawdziwa. Przykładem na to jest funkcja $f(x) = x^2$ która jest ciągła, lecz nie jest jednostajnie ciągła na zbiorze $\mathbb{R}$.

Przykład 3.7 *Ciąg funkcji $f_n : \mathbb{R} \mapsto \mathbb{R}$ $(n \in \mathbb{N})$ nazywamy **jednostajnie zbieżnym** do funkcji f jeśli*

$$(\forall \varepsilon > 0)(\exists N \in \mathbb{N})(\forall n > N)(\forall x \in \mathbb{R})(|f_n(x) - f(x)| < \varepsilon).$$

Z prawa $(\forall x)(\forall y)\varphi \leftrightarrow (\forall y)(\forall x)\varphi \Leftrightarrow$ wynika, że jednostajna zbieżność ciągu (f_n) do funkcji f jest równoważna warunkowi

$$(\forall \varepsilon > 0)(\exists N \in \mathbb{N})(\forall x \in \mathbb{R})(\forall n > N)(|f_n(x) - f(x)| < \varepsilon),$$

Ponieważ prawdziwa jest implikacja

$$(\exists N \in \mathbb{N})(\forall x \in \mathbb{R})\varphi \to (\forall x \in \mathbb{R})(\exists N \in \mathbb{N})\varphi,$$

więc z jednostajnej zbieżności wynika, że

$$(\forall \varepsilon > 0)(\forall x \in \mathbb{R})(\exists N \in \mathbb{N})(\forall n > N)(|f_n(x) - f(x)| < \varepsilon),$$

Ponieważ

$$(\forall \varepsilon > 0)(\forall x \in \mathbb{R})\varphi \leftrightarrow (\forall x \in \mathbb{R})(\forall \varepsilon > 0)\varphi,$$

więc z jednostajnej zbieżności ciągu $(f_n)_{n\in\mathbb{N}}$ do funkcji f wynika, że

$$(\forall x \in \mathbb{R})(\forall \varepsilon > 0)(\exists N \in \mathbb{N})(\forall K > N)(|f_n(x) - f(x)| < \varepsilon),$$

*czyli, że ciąg $(f_n)_{n\in\mathbb{N}}$ jest **zbieżny punktowo** do funkcji f. Pokazaliśmy więc, że jednostajna zbieżność ciągu funkcji pociąga zbieżność punktową. Odwrotna implikacja nie jest prawdziwa. Przykładem na to jest ciąg funkcji $f_n(x) = \frac{x}{n+1}$ która jest punktowo zbieżny do funkcji stale równej zero, lecz nie jest do niej zbieżny jednostajnie.*

Przykład 3.8 *Rozważmy następującą grę. Bierze w niej udział dwóch graczy. Na początku mają położone na stole 30 zapałek. Na zmianę każdy z nich może wziąć jedną, dwie lub trzy zapałki. Wygra ten z nich, który weźmie ostatnią zapałkę. Opiszemy teraz matematyczny model tej gry. W tym celu zauważmy, że gra ta może trwać co nawyżej 30 ruchów. Będziemy ją modelowali jako ciągi 30 elementowe złożone z liczb $\{1, 2, 3\}$. Niech więc $\Omega = \{(x_1, \ldots, x_{30}) : (\forall i)(x_i \in \{1, 2, 3\})\}$. Dla $x \in \Omega$ definiujemy funkcję*

$$s(x) = \min\{i : \sum_{j=1}^{i} x_j \geq 30\}.$$

Funkcja s jest dobrze określona, gdyż $\sum_{i=1}^{30} x_i \geq 30$, a więc zbiór $\{i : \sum_{j=1}^{i} x_j \geq 30\}$ jest niepusty dla każdego elementu $x \in \Omega$. Rozważmy zdanie

$$\varphi = (\exists x_1)(\forall x_2) \ldots (\exists x_{29})(\forall x_{30})(\neg 2|s((x_1, \ldots, x_{30}))),$$

*gdzie $2|n$ oznacza, że n jest podzielne przez 2. Jeśli zdanie φ jest prawdziwe, to istnieje ruch gracza I (czyli liczba x_1), taki, że cokolwiek nie zrobi gracz II (czyli: dla dowolnej liczby x_2), ..., że $s((x_1, \ldots, x_{30}))$ jest liczbą nieparzystą, czyli, że w grze opisanej ciągiem $(x_1, \ldots, x_{30})$ gracz I wygrał. Oznacza to, że gracz pierwszy ma **strategię zwycięską** w tej grze, czyli, że istnieje metoda która zapewnia graczowi I odniesienie zwycięstwa. Oczywiście zdanie φ nie musi być prawdziwe. Lecz jeśli zdanie φ nie jest prawdziwe, to prawdziwa jest jest jego negacja. Na mocy prawa de Morgana zastosowanego 30 razy mamy:*

$$\neg\varphi \equiv (\forall x_1)(\exists x_2) \ldots (\forall x_{29})(\exists x_{30})(2|s((x_1, \ldots, x_{30}))).$$

*Prawdziwość tego zdania oznacza, że gracz II ma strategię zwycięską w rozważanej grze. Zwróćmy uwagę na to, że jedno ze zdań φ lub $\neg\varphi$ jest prawdziwe. A znaczy to, że gracz I ma strategie zwycięską lub gracz II ma strategię zwycięską w rozważanej grze. O takich grach mówimy, że są **zdeterminowane**.*

Rozważania z powyższego przykładu można uogólnić na wszystkie dwuosobowe skończone gry. Należy wprowadzić pojęcie zbioru dopuszczalnych ruchów $R(s)$, gdzie s jest ciągiem opisującym dotychczasowy przebieg gry. Zdanie opisujące istnienie strategii zwycięskiej dla pierwszego gracza przybiera postać

$$(\exists x_1 \in R(()))(\forall x_2 \in R((x_1))(\exists x_2 \in R((x_1, x_2)) \ldots ((x_1, \ldots, x_n)) \in A),$$

gdzie n oznacza maksymalną długość gry, $()$ oznacza ciąg pusty zaś A oznacza zbiór wszystkich przebiegów gry, które kończą się zwycięstwem pierwszego gracza. W celu wyznaczenia negacji tego zdania skorzystać należy z prawa de Morgana dla kwantyfikatorów ograniczonych.

3.4 Działania uogólnione

Rodziną zbiorów nazywamy zbiór, którego elementami są zbiory. Omówimy teraz metodę uogólnienia dwóch podstawowych działań mnogościowych, czyli operacji $\cup$ i $\cap$, na dowolne rodziny zbiorów.

Definicja 3.4 *Niech $\mathcal{A}$ będzie dowolna rodziną zbiorów.*

1. ***Sumą rodziny*** *$\mathcal{A}$ nazywamy taki zbiór $\bigcup\mathcal{A}$, że*

$$(\forall x)(x \in \bigcup\mathcal{A} \leftrightarrow (\exists X \in A)(x \in X)).$$

2. ***Przekrojem rodziny*** *$\mathcal{A}$ nazywamy taki zbiór $\bigcap\mathcal{A}$, że*

$$(\forall x)(x \in \bigcap\mathcal{A} \leftrightarrow (\forall X \in A)(x \in X)).$$

Niech A i B będą dowolnymi zbiorami. Rozważmy zbiór $\mathcal{A} = \{A, B\}$. Wtedy

$$x \in \bigcup\mathcal{A} \leftrightarrow (\exists X \in \{A, B\})(x \in X) \leftrightarrow x \in A \cup B,$$

oraz

$$x \in \bigcap\mathcal{A} \leftrightarrow (\forall X \in \{A, B\})(x \in X) \leftrightarrow x \in A \cap B.$$

Widzimy zatem, że $\bigcup\{A, B\} = A \cup B$ oraz $\bigcap\{A, B\} = A \cap B$. Wprowadzone działania są więc uogólnieniem standardowych działań mnogościowych. Podobnie, bez trudu możemy sprawdzić, że $\bigcup\{A, B, C\} = A \cup B \cup C$ oraz $\bigcap\{A, B, C\} = A \cap B \cap C$.

Zwróćmy uwagę na pewną subtelność. Otóż bez trudu możemy sprawdzić, że $\bigcup\emptyset = \emptyset$. Jednak $\bigcap\emptyset$ nie jest zbiorem! Rzeczywiście $x \in \bigcap\emptyset \leftrightarrow (\forall X \in \emptyset)(x \in X)$, czyli $x \in \bigcap\emptyset \leftrightarrow (\forall X)(X \in \emptyset \rightarrow x \in X)$. Zdanie $X \in \emptyset$ jest zdaniem fałszywym, więc implikacja $(X \in \emptyset \rightarrow x \in X)$ jest zdaniem prawdziwym dla dowolnego x. Pokazaliśmy więc, że $(\forall x)(x \in \bigcap\emptyset)$. Z Twierdzenia Russell'a wynika więc, że $\bigcap\emptyset$ nie jest zbiorem. **W związku z tym operator przekroju rodziny zbiorów stosować możemy tylko do rodzin niepustych.**

Twierdzenie 3.4 (de Morgan) *Niech $\mathcal{A}$ będzie niepustą rodziną podzbiorów przestrzeni Ω. Wtedy*

1. $(\bigcup\mathcal{A})^c = \bigcap\{X^c : X \in \mathcal{A}\}$,
2. $(\bigcap\mathcal{A})^c = \bigcup\{X^c : X \in \mathcal{A}\}$.

Dowód. Rozważmy dowolny $x \in \Omega$. Wtedy

$$x \in \left(\bigcup\mathcal{A}\right)^c \leftrightarrow \neg(x \in \bigcup\mathcal{A}) \leftrightarrow \neg(\exists X \in A)(x \in X) \leftrightarrow$$
$$(\forall X \in A)\neg(x \in X) \leftrightarrow (\forall X \in A)(x \in X^c) \leftrightarrow x \in \bigcap\{X^c : X \in \mathcal{A}\}.$$

Drugie prawo de Morgana dowodzi się podobnie do pierwszego. □

3.5 Ćwiczenia i zadania

Ćwiczenie 3.1 *Zapisz przy użyciu symboli* $0, 1, +, \cdot, \leq, |$ *oraz symboli logicznych następujące funkcje zdaniowe:*

1. x *jest liczbą parzystą,*
2. x *jest liczbą pierwszą,*
3. x *jest liczbą złożoną,*
4. $x = NWD(y, z)$*,*
5. *każde dwie liczby mają najmniejszą wspólną wielokrotność,*
6. *nie istnieje największa liczba pierwsza.*
7. *każda liczba parzysta większa od 2 jest sumą dwóch liczb pierwszych (hipoteza Goldbacha)*
8. *każda liczba naturalna jest sumą czterech kwadratów liczb naturalnych(twierdzenie Lagrange'a)*

Ćwiczenie 3.2 *Niech zakresem zmienności zmiennych będzie zbiór liczb rzeczywistych. Zapisz za pomocą symboli logicznych oraz symboli* $=$*,* $<$*,* $\leq$*,* $+$*,* $\cdot$ *i* $\mathbb{Q}$ *następujące formuły:*

1. *kwadrat każdej liczby jest nieujemny,*
2. *liczba* a *jest ograniczeniem górnym zbioru* A*,*
3. *liczba* a *jest kresem górnym zbioru* A*,*
4. *pomiędzy dowolnymi dwoma różnymi liczbami rzeczywistymi istnieje liczba wymierna,*
5. *funkcja f jest malejąca.*

Ćwiczenie 3.3 *Znajdź wykresy następujących formuł zmiennych* x *i* y*, o zakresie zmienności równym* $\mathbb{R}^2$*:* $x = y$*,* $x < y$*,* $x \leq y$*,* $x \cdot y < 1$*,* $|x \cdot y| < 1$*,* $(x \leq 0) \vee (x = y)$*,* $x \cdot y < 1 \rightarrow x \cdot y = 1$*.*

Ćwiczenie 3.4 *Udowodnij wszystkie implikacje występujące w Diagramie 3.1. Pokaż, że żadnej implikacji występującej w tym diagramie nie można zastąpić równoważnością.*

Ćwiczenie 3.5 *Zapisz zdanie "g jest granicą ciągu* $(a_n)_{n\in\mathbb{N}}$*". Pokaż, że liczba* 1 *nie jest granicą ciągu* $a_n = \frac{1}{n+1}$*.*

Ćwiczenie 3.6 *Niech formuła* $r(x, y)$ *oznacza, że* x *jest rodzicem* y*, niech* $m(x)$ *oznacza, że* x *jest mężczyzną. Zdefiniuj za pomocą formuł* r *oraz* m *następujące formuły:*

1. *"x jest bratem y"*
2. *"x jest kuzynką y"*

3. *"x jest pradziadkiem y"*

Ćwiczenie 3.7 *Dla każdej liczby rzeczywistej t niech $A_t = \{(x, tx) : x \in \mathbb{R}\}$. Niech $\mathcal{A} = \{A_t : t \in \mathbb{R}\}$. Wyznacz zbiór $\bigcup \mathcal{A}$.*

Ćwiczenie 3.8 *Pokaż, że dla dowolnych dwóch rodzin zbiorów $\mathcal{A}$ i $\mathcal{B}$ zachodzi równość $\bigcup(\mathcal{A} \cup \mathcal{B}) = \bigcup \mathcal{A} \cup \bigcup \mathcal{B}$.*

Ćwiczenie 3.9 *Załóż że Ω jest zbiorem skończonym i niech $\Omega = \{\omega_1, \ldots, \omega_n\}$. Pokaż, że*

1. $(\forall x)(\forall y)\psi(x, y) \leftrightarrow \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n} \psi(\omega_i, \omega_j)$,
2. $(\forall y)(\forall x)\psi(x, y) \leftrightarrow \bigwedge_{j=1}^{n} \bigwedge_{i=1}^{n} \psi(\omega_i, \omega_j)$,
3. $(\forall x)(\exists y)\psi(x, y) \leftrightarrow \bigwedge_{i=1}^{n} \bigvee_{j=1}^{n} \psi(\omega_i, \omega_j)$,
4. $(\forall y)(\exists x)\psi(x, y) \leftrightarrow \bigwedge_{j=1}^{n} \bigvee_{i=1}^{n} \psi(\omega_i, \omega_j)$,
5. $(\exists x)(\forall y)\psi(x, y) \leftrightarrow \bigvee_{i=1}^{n} \bigwedge_{j=1}^{n} \psi(\omega_i, \omega_j)$,
6. $(\exists y)(\forall x)\psi(x, y) \leftrightarrow \bigvee_{j=1}^{n} \bigwedge_{i=1}^{n} \psi(\omega_i, \omega_j)$,
7. $(\exists x)(\exists y)\psi(x, y) \leftrightarrow \bigvee_{i=1}^{n} \bigvee_{j=1}^{n} \psi(\omega_i, \omega_j)$,
8. $(\exists y)(\exists x)\psi(x, y) \leftrightarrow \bigvee_{j=1}^{n} \bigvee_{i=1}^{n} \psi(\omega_i, \omega_j)$.

Zadanie 3.1 *Rozstrzygnij, który z graczy ma strategię zwycięską w grze „trzech zapałek" zaczynającą się od 30 zapałek. Opisz tę strategię.*

Zadanie 3.2 *Pokaż, że jeśli $a, b \in A$ to $(a, b) \in P(P(A))$. Wykorzystaj tę obserwację do zdefiniowanie iloczynu kartezjańskiego dwóch zbiorów A i B za pomocą operacji zbioru potęgowego oraz wyróżniania.*

Zadanie 3.3 *Określmy następujące dwa kwantyfikatory stosowane do liczb naturalnych: $(\forall^\infty n)\psi(n) \leftrightarrow (\exists k \in \mathbb{N})(\forall n > k)\psi(n)$ oraz $(\exists^\infty n)\psi(n) \leftrightarrow (\forall k \in \mathbb{N})(\exists n > k)\psi(n)$. Sformułuj i udowodnij prawa de Morgana dla tych kwantyfikatorów. Pokaż, że dla dowolnej formuły ψ zdanie $(\forall^\infty n)\psi(n) \to (\exists^\infty n)\psi(n)$ jest prawdziwe. Sformułuj przy pomocy tych kwantyfikatorów pojęcie granicy ciągu oraz pojęcie punktu skupienia. Bezpośrednio z własności tych kwantyfikatorów pokaż, że granica ciągu jest jego punktem skupienia.*

Zadanie 3.4 *Pokaż, że dla każdego zbioru A zachodzi równość $A = \bigcup P(A)$.*

Zadanie 3.5 *Niech zakresem zmienności zmiennych będzie zbiór liczb całkowitych. Zapisz za pomocą symboli logicznych oraz symboli $+$, $\cdot$ predykat „$x \geq 0$". Wskazówka: Zapoznaj się z twierdzeniem Lagrange'a o sumach czterech kwadratów.*

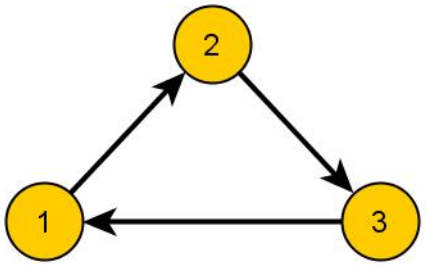
Zadanie 3.6 * *Niech zakresem zmienności zmiennych będzie zbiór liczb naturalnych. Pokaż, że za pomocą symboli 0, 1, $+$ oraz $|$ można zdefiniować predykat „$x \cdot y = z$" (symbol $|$ oznacza podzielność bez reszty). Wskazówka: Zdefiniuj najpierw predykat $(\exists y)(x = y^2)$. Przydać ci się mogą następujące tożsamości: $(x + y)^2 = x^2 + xy + xy + y^2$, $NWD(x, x+1) = 1$ oraz $x^2 + x = NWW(x, x+1)$, gdzie NWD oznacza największy wspólny dzielnik, NWW oznacza najmniejszą wspólną wielokrotność.*

4 Relacje i Funkcje

Relacje są najprostszym i zarazem podstawowym sposobem modelowania pojęcia zależności pomiędzy różnymi obiektami. Za pomocą tego pojęcia definiuje się, na przykład, pojęcie funkcji oraz grafu. Za pomocą relacji modeluje się współczesne bazy danych.

Definicja 4.1 *Zbiór R nazywamy **relacją** jeśli istnieje taki zbiór X, że $R \subseteq X \times X$.*

W szczególności, każdy podzbiór płaszczyzny $\mathbb{R}^2$ jest relacją. Inaczej mówiąc, relacją nazywamy dowolny zbiór par uporządkowanych. Istnieje wiele sposobów wizualizacji relacji. Rozważmy, na przykład, zbiór $X = \{1, 2, 3\}$ oraz relację $R = \{(1, 2), (2, 3), (3, 1)\}$. Relację tą możemy przedstawić w postaci strzałek



łączących elementy zbioru. Strzałka biegnąca od elementu a do elementu b oznacza, że $(a, b) \in R$. Metodę tę omówimy dokładniej przy omawianiu częściowych porządków.

Czasami zamiast $(x, y) \in R$ będziemy pisali xRy lub $R(x, y)$. Są to różne formy stwierdzenia tego samego faktu - że para uporządkowana (x, y) jest elementem relacji R.

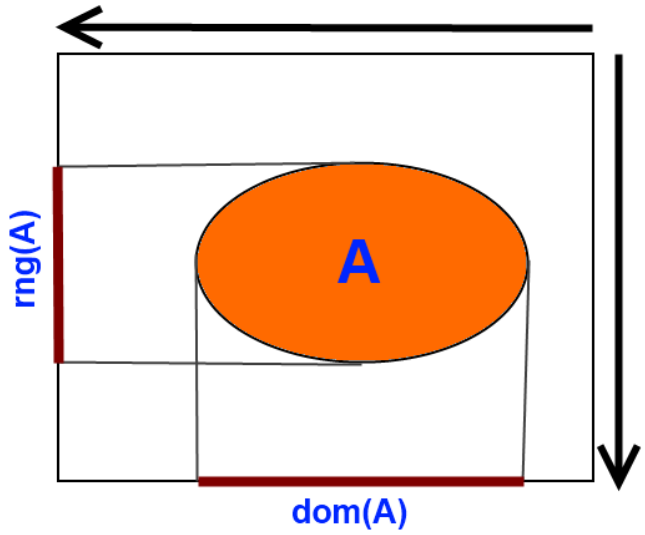
Przykład 4.1 *Niech* $\mathrm{LEQ} = \{(x, y) \in \mathbb{R}^2 : (\exists z \in \mathbb{R})(y = x + z^2)\}$. *Jak łatwo sprawdzić*

$$(x, y) \in \mathrm{LEQ} \leftrightarrow x \leq y.$$

Definicja 4.2 *Niech R będzie relacją.*

1. ***Dziedziną** relacji R nazywamy zbiór $dom(R) = \{x : (\exists y)((x, y) \in R)\}$.*
2. ***Obrazem** relacji R nazywamy zbiór $rng(R) = \{y : (\exists x)((x, y) \in R)\}$.*

Zauważmy, że zachodzi inkluzja $R \subseteq dom(R) \times rng(R)$. Obraz relacji nazywany jest czasami zbiorem wartości relacji. Suma $dom(R) \cup rng(R)$ nazywana jest czasem *polem* relacji R. Mówimy, że relacja R jest określona na zbiorze X lub, że jest określona dla elementów zbioru X, jeśli $R \subset X \times X$.



Rysunek 4.1: Dziedzina i obraz relacji A

4.1 Podstawowe Klasy Relacji

Zdefiniujemy teraz kilka własności relacji, które będą odgrywały ważną rolę w dalszych rozważaniach.

Definicja 4.3 *Niech R będzie relacją.*

1. *R jest relacją **przechodnią**, jeśli* $(\forall x)(\forall y)(\forall z)((x,y) \in R \wedge (y,z) \in R \rightarrow (x,z) \in R)$.
2. *R jest relacją **zwrotną** na zbiorze X jeśli* $(\forall x \in X)((x,x) \in R)$.
3. *R jest relacją **symetryczną** jeśli* $(\forall x)(\forall y)(((x,y) \in R \rightarrow (y,x) \in R))$.
4. *R jest relacją **słabo antysymetryczną** jeśli* $(\forall x)(\forall y)((x,y) \in R \wedge (y,x) \in R \rightarrow x = y)$.

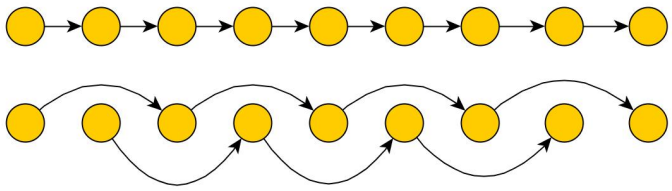
Przykładem relacji przechodniej jest rozważana już klasyczna nierówność pomiędzy liczbami rzeczywistymi. Inną ważną relacją przechodnią jest relacja podzielności w liczbach naturalnych. Relacja $\leq$ w zbiorze liczb rzeczywistych jest również zwrotna na $\mathbb{R}$. Najmniejszą relacją zwrotną na zbiorze X, o dziedzinie równej X, jest relacja $Id_X = \{(x,x) : x \in X\}$, zwana identycznością na zbiorze X. Relacją symetryczną jest na przykład relacja $W = \{(x,y) \in \mathbb{R}^2 : |x| = |y|\}$. Relacja $\leq$ dla liczb rzeczywistych jest również relacją słabo antysymetryczną. Relacja W nie jest słabo antysymetryczna.

Definicja 4.4 *Niech R i S będą relacjami.*

1. $R \circ S = \{(x, z) : (\exists y)(x, y) \in S \wedge (y, z) \in R\}$.
2. $R^{-1} = \{(y, x) : (x, y) \in R\}$.

Operację $\circ$ nazywamy *złożeniem* relacji zaś relację R^{-1} nazywamy relacją *odwrotną* do relacji R. Operację $^{-1}$ interpretować możemy jako odwrócenie kierunku strzałek w diagramie relacji R. Wprowadzone wyżej klasy relacji można opisać za pomocą powyższych operacji. Relacja R jest przechodnia wtedy i tylko wtedy, gdy $R \circ R \subseteq R$. Relacja R jest symetryczna wtedy i tylko wtedy, gdy $R = R^{-1}$. Relacja R jest słabo antysymetryczna wtedy i tylko wtedy, gdy $R \cap R^{-1} \subseteq Id_{dom(R)}$. Zwrotność relacji na swojej dziedzinie oznacza, że $Id_{dom(R) \cup rng(R)} \subseteq R$.

Przykład 4.2 *Niech $R = \{(n, n+1) : n \in \mathbb{N}\}$. Wtedy $(x, z) \in R \circ R \leftrightarrow (\exists y)((x, y) \in R \wedge (y, z) \in R) \leftrightarrow (\exists y)(y = x + 1 \wedge z = y + 1) \leftrightarrow z = x + 2$, zatem $R \circ R = \{(x, x + 2) : x \in \mathbb{N}\}$.*



Rysunek 4.2: Relacja R oraz $R \circ R$ z Przykładu 4.2

.

Twierdzenie 4.1 *Niech R, S i T będą dowolnymi relacjami. Wtedy*

1. $(R \circ S) \circ T = R \circ (S \circ T)$,
2. $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$,
3. $(R^{-1})^{-1} = R$.

Dowód. Niech x, y będą ustalonymi elementami. Wtedy

$$(x, y) \in (R \circ S) \circ T \leftrightarrow (\exists z)((x, z) \in T \wedge (z, y) \in R \circ S) \leftrightarrow$$
$$(\exists z)(\exists v)((x, z) \in T \wedge ((z, v) \in S \wedge (v, y) \in R)).$$

Podobnie

$$(x, y) \in R \circ (S \circ T) \leftrightarrow (\exists v)((x, v) \in S \circ T \wedge (v, y) \in R) \leftrightarrow$$
$$(\exists v)(\exists z)(((x, z) \in T \wedge (z, v) \in S) \wedge (v, y) \in R).$$

Równość (1) wynika więc z łączności koniunkcji i przemienności kwantyfikatora egzystencjalnego. Równość (2) wynika z następującego ciągu równoważności:

$$(x, y) \in (R \circ S)^{-1} \leftrightarrow (y, x) \in R \circ S \leftrightarrow (\exists v)((y, v) \in S \wedge (v, x) \in R) \leftrightarrow$$
$$(\exists v)((v, y) \in S^{-1} \wedge (x, v) \in R^{-1}) \leftrightarrow (x, y) \in S^{-1} \circ R^{-1}.$$

Równość (3) jest zaś oczywista.

□

Złożenie relacji nie jest operacją przemienną: na przykład $\{(0,1)\} \circ \{(1,2)\} = \emptyset$ lecz $\{(1,2)\} \circ \{(0,1)\} = \{(0,2)\}$.

Uwaga. To, że złożenie relacji nie jest przemienne nie powinno dziwić. Efekt założenia skarpetki i następnie założenia buta jest inny od założenia buta i następnie założenia skarpetki.

Reprezentacja Macierzowa

Ustalmy skończony zbiór $X = \{x_1, \ldots, x_n\}$. Rozważać będziemy relacje $R \subseteq X \times X$. Dla każdej takiej relacji określamy macierz wartości logicznych $M(R) = (m_{ij})_{i,j=1,\ldots n}$ o wartościach

$$m_{ij} = \begin{cases} \mathbb{1} & : \quad (i,j) \in R \\ \mathbb{0} & : \quad (i,j) \notin R \end{cases}$$

Reprezentacja macierzowa relacji jest szczególnie wygodna w algorytmach informatycznych, zwłaszcza, gdy zbiór X nie jest zbyt duży. Symetria relacji R oznacza, że $(\forall i,j)(m_{ij} = m_{ji})$. Zwrotność relacji R na zbiorze X oznacza, że $(\forall i)(m_{ii} = \mathbb{1})$. Złożeniem $A \circ B$ dwóch macierzy o wartościach logicznych $A = (a_{ij})_{i,j=1,\ldots n}$ i $B = (b_{ij})_{i,j=1,\ldots n}$ nazywamy macierz $C = (c_{ij})_{i,j=1,\ldots n}$ której elementy zadane są wzorem

$$c_{ik} = \bigvee_{j=1}^{n} (a_{ij} \wedge b_{jk}).$$

Twierdzenie 4.2 *Dla dowolnych relacji R i S na zbiorze X zachodzi równość*

$$M(R \circ S) = M(S) \circ M(R).$$

Dowód. Niech $M(R) = (r_{ij})$, $M(S) = (s_{ij})$ oraz $M(R \circ S) = (t_{ij})$. Wtedy

$$t_{ik} = \mathbb{1} \leftrightarrow (x_i, x_k) \in R \circ S \leftrightarrow (\exists j)((x_i, x_j) \in S \wedge (x_j, x_k) \in R) \leftrightarrow$$
$$(\exists j)(s_{ij} = \mathbb{1} \wedge r_{jk} = \mathbb{1}) \leftrightarrow \bigvee_{j=1}^{n} (s_{ij} \wedge r_{jk}) = \mathbb{1},$$

co kończy dowód. □

Niech $A = (a_{ij})_{i,j=1,\ldots n}$ i $B = (b_{ij})_{i,j=1,\ldots n}$ będą macierzami logicznymi. Będziemy mówili, że B dominuje A ($A \preceq B$) jeśli $\mathbf{IMP}(a_{ij}, b_{ij}) = \mathbb{1}$ [1] dla wszystkich par i, j. Z udowodnionego twierdzenia wynika, że relacja $R \subseteq X \times X$ jest przechodnia wtedy i tylko wtedy, gdy $M(R) \circ M(R) \preceq M(R)$. Jeśli relacja R jest przechodnia i zwrotna na X, to $M(R \circ R) = M(R)$.

[1] **IMP** oznacza działanie na wartościach logicznych zdefiniowane w rozdziale pierwszym

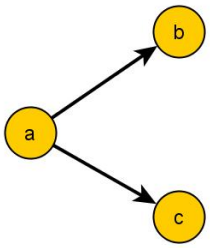
4.2 Funkcje

Przegląd różnych typów relacji rozpoczniemy od sprecyzowania jednego z najważniejszych pojęć matematycznych, jakim jest pojęcie funkcji. Pojęcie to długo, bo aż do połowy XIX wieku, używane było bez precyzyjnej definicji. Interpretowano je jako "*przyporządkowanie*" elementom jednego zbioru elementów drugiego zbioru. Precyzyjną i bardzo ogólną definicję funkcji podano dopiero na gruncie teorii mnogości. I tą definicją się teraz zajmiemy.

Definicja 4.5 *Relację f nazywamy **funkcją**, jeśli*

$$(\forall x)(\forall y_1)(\forall y_2)\left(((x,y_1)\in f \wedge (x,y_2)\in f) \rightarrow y_1 = y_2\right) .$$

Relacja R przedstawiona na rysunku



nie jest funkcją, gdyż $(a,b)\in R$, $(a,c)\in R$ zaś $b\neq c$.

Funkcja w pojęciu teoriomnogościowym jest tożsama ze swoim wykresem. W niektórych sytuacjach trzeba jednak zwracać uwagę na to, czy o funkcji myślimy jako o przyporządkowaniu, czy też jako o podzbiorze odpowiedniego iloczynu kartezjańskiego.

Przykład 4.3 *Rozważmy relację $h = \{(x,y)\in\mathbb{R}^2 : x\cdot y = 1\}$. Relację tą interpretujemy jako funkcją zadaną wzorem $y=\frac{1}{x}$. Oczywiście $dom(h)=\mathbb{R}\setminus\{0\}$ oraz $rng(h)=\mathbb{R}\setminus\{0\}$.*

Jeśli f jest funkcją oraz $x\in dom(f)$ to istnieje element y takie, że $(x,y)\in f$ i taki y jest tylko jeden. Oznaczamy go symbolem $f(x)$. Załóżmy, że f i g są funkcjami oraz $dom(f)=dom(g)$. Równość $f=g$ zachodzi wtedy i tylko wtedy, gdy $(\forall x\in dom(f))(f(x)=g(x))$. Ta prosta uwaga wynika z oczywistej równości $f=\{(x,f(x)) : x\in dom(f)\}$.

Często stosowany jest zapis $f : X\rightarrow Y$, który oznacza, że f jest funkcją, $dom(f)=X$ oraz $rng(f)\subseteq Y$. Gdy $dom(f)\subseteq\mathbb{R}$ to funkcję nazywa się *funkcją zmiennej rzeczywistej*. Gdy zaś $rng(f)\subseteq\mathbb{R}$ to f nazywa się *funkcją rzeczywistą*.

Załóżmy, że $f : X\rightarrow Y$ oraz $g : Y\rightarrow Z$. Wtedy $g\circ f$ jest funkcją, $g\circ f : X\rightarrow Z$ oraz $g\circ f(x)=g(f(x))$ dla każdego $x\in X$. Widzimy więc, że wprowadzona operacja złożenia relacji, po zastosowaniu do funkcji pokrywa się ze znaną, standardową, definicją złożenia funkcji. Łatwo również sprawdzić, że jeśli f i g są dowolnymi funkcjami, to $g\circ f$ jest również funkcją. Dziedziną jej jest zbiór $\{x\in dom(f) : f(x)\in dom(g)\}$.

Definicja 4.6 *Funkcję f nazywamy **injekcją** bądź **różnowartościową** jeśli*

$$(\forall x_1, x_2 \in dom(f))(f(x_1) = f(x_2) \to x_1 = x_2).$$

Z tautologii $(p \to q) \leftrightarrow (\neg q \to \neg q)$ wynika, że funkcja f jest injekcją wtedy i tylko wtedy, gdy $(\forall x_1, x_2 \in dom(f))(x_1 \neq x_2 \to f(x_1) \neq f(x_2))$. Ta charakteryzacja różnowartościowości jest przydatna w wielu zadaniach. Zapis $f : X \xrightarrow{1-1} X$ oznacza, że f jest injekcją ze zbioru X w zbiór Y.

Twierdzenie 4.3 *Funkcja f jest injekcją tedy i tylko wtedy, gdy f^{-1} jest funkcją.*

Dowód. Załóżmy, że f jest funkcją injekcją. Niech $(x, y_1) \in f^{-1}$ oraz $(x, y_2) \in f^{-1}$. Wtedy $(y_1, x) \in f$ oraz $(y_2, x) \in f$, czyli $f(y_1) = f(y_2)$. Z różnowartościowości funkcji f wynika, że $y_1 = y_2$, a więc pokazaliśmy, że f^{-1} jest funkcją.
Załóżmy teraz, że f^{-1} jest funkcją. Załóżmy, że $f(x_1) = f(x_2) = a$. Wtedy $(x_1, a) \in f$ oraz $(x_2, a) \in f$, a więc $(a, x_1) \in f^{-1}$ oraz $(a, x_2) \in f^{-1}$. Lecz f^{-1} jest funkcją, więc $x_1 = x_2$, a zatem funkcja f jest injekcją. □

Przypomnijmy, że dla dowolnego zbiory X przez Id_X oznaczyliśmy relację $\{(x, x) : x \in X\}$. Jest ona funkcją i nazywamy ją identycznością na zbiorze X. Niech f będzie funkcją injekcją. Jest jasne, że $dom(f^{-1}) = rng(f)$ oraz $rng(f^{-1}) = dom(f)$. Ponadto, łatwo można sprawdzić, że $f^{-1} \circ f = Id_{dom(f)}$ oraz $f \circ f^{-1} = Id_{rng(f)}$. Funkcję f^{-1} nazywa się funkcją *odwrotną* do funkcji f.

Twierdzenie 4.4 *Złożenie dwóch injekcji jest injekcją.*

Dowód. Załóżmy, że f i g są injekcjami. Niech $a, b \in dom(f)$ będą takie, że $f(a) \in dom(g)$, $f(b) \in dom(g)$ oraz $g \circ f(a) = g \circ f(b)$. Wtedy $g(f(a)) = g(f(b))$, a więc z różnowartościowości funkcji g wnioskujemy, że $f(a) = f(b)$, co z kolei implikuje, że $a = b$. □

Definicja 4.7 *Funkcję $f : A \to B$ nazywamy **surjekcją** jeśli $rng(f) = B$.*

Definicja 4.8 *Funkcję $f : A \to B$ nazywamy **bijekcją** jeśli jest jednocześnie injekcją i surjekcją.*

Zapis $f :\xrightarrow{na} Y$ oznacza, że f jest surjekcją ze zbioru X na zbiór Y, a zapis $f :\xrightarrow[1-1]{na} Y$ oznacza, że f jest bijekcją ze zbioru X na zbiór Y.

Twierdzenie 4.5 *Złożenie dwóch surjekcji jest surjekcją.*

Dowód. Załóżmy, że $f : A \to B$ i $g : B \to C$ są surjekcjami. Niech $c \in C$. Ponieważ g jest surjekcją, więc istnieje taki element $b \in B$, że $g(b) = c$. Ponieważ f jest surjekcją, więc istnieje $a \in A$ takie, że $f(a) = b$. Wtedy $g \circ f(a) = g(f(a)) = g(b) = c$, co kończy dowód. □

Z Twierdzeń 4.4 i 4.5 otrzymujemy następujący bardzo pożyteczny wniosek.

Wniosek 4.1 *Złożenie dwóch bijekcji jest bijekcją.*

Zauważmy, że jeśli $f : A \to B$, to f jest relacją o dziedzinie równej A i przeciwdziednienie zawartej w zbiorze B, czyli $f \subseteq A \times B$, a więc $f \in P(A \times B)$.

Definicja 4.9 *Niech A i B będą dowolnymi zbiorami. Symbolem B^A oznaczamy zbiór wszystkich funkcji ze zbioru A w zbiór B, czyli*

$$B^A = \{f \in P(A \times B) : f : A \to B\}.$$

Zauważmy, że $\mathbb{R}^{\mathbb{N}}$ jest dobrze znanym obiektem. Jest to mianowicie zbiór wszystkich ciągów liczb rzeczywistych. Zbiór $\mathbb{R}^{\mathbb{R}}$ jest rodziną wszystkich funkcji rzeczywistych o dziedzinie równej całemu zbiorowi $\mathbb{R}$.

4.3 Funkcje Logiczne

Funkcje $f : \{\mathbb{0}, \mathbb{1}\}^n \to \{\mathbb{0}, \mathbb{1}\}$ nazywamy n-argumentowymi *funkcjami logicznymi*. Rozważane w pierwszym rozdziale tej książki działania logiczne **AND**, **OR**, **IMP**, **IFF** są 2-argumentowymi funkcjami logicznymi. Działanie **NOT** jest 1-argumentową funkcją logiczną. Dowolne zdanie Rachunku Zdań możemy traktować jako funkcje logiczną. Niech bowiem $\varphi(p_1, \ldots, p_n)$ będzie zdaniem zbudowanym tylko ze zmiennych $p_1, \ldots, p_n$. Związaną z nim funkcję logiczną F_φ określamy za pomocą waluacji:

$$F_\varphi((w_1, \ldots, w_n)) = \overrightarrow{(w_1, \ldots, w_n)}(\varphi).$$

Okazuje się, że środki Rachunku Zdań są tak silne, że za ich pomocą potrafimy wyrazić dowolną funkcję logiczną.

Twierdzenie 4.6 *Niech $n \in \mathbb{N}$ oraz $f : \{\mathbb{0}, \mathbb{1}\}^n \to \{\mathbb{0}, \mathbb{1}\}$. Istnieje wtedy zdanie $\varphi(p_1, \ldots, p_n)$ rachunku zdań takie, że $f = F_\varphi$.*

Dowód. Zauważmy, że jeśli funkcja f jest tożsamościowo równa zero, to $f = F_{p_1 \wedge \neg p_1}$, gdyż $p_1 \wedge \neg p_1$ jest antytautologią, a więc dla dowolnej waluacji $\overrightarrow{w}$ mamy $\overrightarrow{w}(p_1 \wedge \neg p_1) = \mathbb{0}$. Załóżmy zatem, że funkcja f nie jest tożsamościowo równa zero. Dla każdej waluacji $w \in \{\mathbb{0}, \mathbb{1}\}^n$ niech a_w będzie koniunkcją $(z_1 \wedge \ldots \wedge z_n)$, gdzie

$$z_i = \begin{cases} p_i & : \quad w_i = \mathbb{1} \\ \neg p_i & : \quad w_i = \mathbb{0} \end{cases}$$

Zauważmy, że dla dowolnej waluacji $v \in \{\mathbb{0}, \mathbb{1}\}^n$ mamy $v(a_w) = \mathbb{1} \leftrightarrow v = w$. Formułę φ określamy następująco

$$\varphi = \bigvee \{a_w : w \in \{\mathbb{0}, \mathbb{1}\}^n \wedge f(w) = \mathbb{1}\}.$$

Wtedy dla dowolnej waluacji $v \in \{\mathbb{0}, \mathbb{1}\}^n$ mamy

$$v(\varphi) = \mathbb{1} \leftrightarrow (\exists w)(f(w) = \mathbb{1} \wedge v(a_w) = \mathbb{1}) \leftrightarrow$$
$$(\exists w)(f(w) = \mathbb{1} \wedge v = w) \leftrightarrow f(v) = \mathbb{1},$$

a więc $F_\varphi = f$. □

Warto zauważyć, że w dowodzie ostatniego twierdzenia zbudowaliśmy szukaną formułę tylko za pomocą alternatyw, koniunkcji oraz negacji.

Przykład 4.4 *Rozważmy funkcję logiczną f trzech zmiennych, czyli określoną na zbiorze $\{\mathbb{0}, \mathbb{1}\} \times \{\mathbb{0}, \mathbb{1}\} \times \{\mathbb{0}, \mathbb{1}\}$ zadaną następującą tabelą*

p	q	r	f
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$
$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$

Funkcja ta nie jest tożsamościowo równa wartości $\mathbb{0}$. *Wartość* $\mathbb{1}$ *przyjmuje tylko w dwóch wierszach. Stosując metodą zastosowaną w dowodzie ostatniego twierdzenia otrzymujemy formułę*

$$\varphi = (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r)$$

dla której mamy $F_\varphi = f$.

4.4 Obrazy i Przeciwobrazy

W części tej omówimy najpierw pojęcie obrazu zbioru przez zadaną relację a następnie zajmiemy się omówieniem własności obrazów i przeciwobrazów dla funkcji.

Definicja 4.10 *Niech* R *będzie dowolną relacją oraz niech* A *będzie dowolnym zbiorem.* ***Obrazem*** *zbioru* A *przez relację* R *nazywamy zbiór*

$$R[A] = \{y : (\exists x \in A)((x, y) \in R)\}.$$

Zbiór $R[A]$ interpretujemy jako zbiór tych wszystkich elementów do których można dojść w jednym kroku ze zbioru A za pomocą strzałek (połączeń) z relacji R.

Twierdzenie 4.7 *Niech* R *będzie dowolną relacją oraz niech* A, B *będą dowolnymi zbiorami. Wtedy*

1. $R[A \cup B] = R[A] \cup R[B]$,
2. $R[A \cap B] \subseteq R[A] \cap R[B]$.

Dowód. Niech y będzie dowolnym elementem. Wtedy

$$\begin{gathered} y \in R[A \cup B] \leftrightarrow \\ (\exists x \in A \cup B)((x, y) \in R) \leftrightarrow (\exists x)((x \in A \cup B) \wedge (x, y) \in R) \leftrightarrow \\ (\exists x)((x \in A \vee x \in B) \wedge (x, y) \in R) \leftrightarrow \\ (\exists x)(x \in A \wedge (x, y) \in R) \vee (x \in B \wedge (x, y) \in R)) \leftrightarrow \\ (\exists x)(x \in A \wedge (x, y) \in R) \vee (\exists x)(x \in B \wedge (x, y) \in R)) \leftrightarrow \\ y \in R[A] \vee y \in R[B] \leftrightarrow y \in R[A] \cup R[B], \end{gathered}$$

co kończy dowód równości (1). Następnie

$$y \in R[A \cap B] \leftrightarrow$$
$$(\exists x \in A \cap B)((x,y) \in R) \leftrightarrow (\exists x)((x \in A \cap B) \wedge (x,y) \in R) \leftrightarrow$$
$$(\exists x)((x \in A \wedge (x,y) \in R) \wedge (x \in B \wedge (x,y) \in R)) \rightarrow$$
$$(\exists x)(x \in A \wedge (x,y) \in R) \wedge (\exists x)(x \in B \wedge (x,y) \in R) \leftrightarrow$$
$$(y \in R[A] \wedge y \in R[B]) \leftrightarrow y \in R[A] \cap R[B],$$

co kończy dowód inkluzji (2).
W dowodzie (1) skorzystaliśmy z rozdzielczości kwantyfikatora egzystencjalnego względem alternatywy. W dowodzie (2) skorzystaliśmy z implikacji $(\exists x)(\varphi(x) \wedge \psi(x)) \rightarrow ((\exists x)\varphi(x) \wedge (\exists x)\psi(x))$. □

Przykład 4.5 *Niech $R = \{(a,c),(b,c)\}$, gdzie $a \neq b$, $A = \{a\}$ oraz $B = \{b\}$. Wtedy $R[A \cap B] = R[\emptyset] = \emptyset$, lecz $R[A] \cap R[B] = \{c\} \cap \{c\} = \{c\}$. Zatem inkluzji z punktu (2) ostatniego twierdzenia nie można zastąpić równością.*

Pojęcie obrazu zbioru przez relację ma swój dualny odpowiednik, a mianowicie "przeciwobraz zbioru przez relację", który definiuje się wzorem

$$\overleftarrow{R}[A] = \{x : (\exists y \in A)((x,y) \in R\}.$$

Zauważmy, że $\overleftarrow{R}[A] = R^{-1}[A]$, więc operacja ta ma takie same własności co operacja obrazu. Sytuacja jednak ulega pewnej zmianie, gdy rozważane relacje fą funkcjami, gdyż wtedy

$$x \in f^{-1}[A] \leftrightarrow (\exists y \in A)((y,x) \in f^{-1}) \leftrightarrow (\exists y \in A)((x,y) \in f) \leftrightarrow f(x) \in A.$$

Twierdzenie 4.8 *Niech f będzie dowolną funkcją oraz niech A, B będą dowolnymi zbiorami. Wtedy*

1. $f^{-1}[A \cup B] = f^{-1}[A] \cup f^{-1}[B]$,
2. $f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$,
3. $f^{-1}[rng(f) \setminus A] = dom(f) \setminus f^{-1}[A]$.

Dowód. Pierwsza równość zachodzi dla dowolnej relacji. Udowodnimy więc drugą. Niech x będzie dowolnym elementem. Wtedy

$$x \in f^{-1}[A \cap B] \leftrightarrow (f(x) \in A \cap B) \leftrightarrow (f(x) \in A) \wedge (f(x) \in B) \leftrightarrow$$
$$(x \in f^{-1}[A] \wedge x \in f^{-1}[B]) \leftrightarrow x \in f^{-1}[A] \cap f^{-1}[B],$$

co kończy dowód (2). Rozważmy teraz $x \in dom(f)$. Wtedy

$$x \in f^{-1}[rng(f) \setminus A] \leftrightarrow f(x) \in rng(f) \setminus A \leftrightarrow \neg(f(x) \in A),$$

co kończy dowód (3). □

Definicja 4.11 *Niech f będzie dowolną funkcją oraz niech A będzie dowolnym zbiorem. **Obcięciem** funkcji f do zbioru A nazywamy relację $f \restriction A = f \cap (A \times rng(f))$.*

Jeśli f jest funkcją to $f \restriction A$ też jest funkcją. Jeśli $f : X \rightarrow Y$ oraz $A \subseteq X$ to $f \restriction A : A \rightarrow Y$. Ogólniej: $dom(f \restriction A) = dom(f) \cap A$.

4.5 Indeksowane Rodziny Zbiorów

Indeksowaną rodziną zbiorów nazywamy dowolną funkcję której wartościami są zbiory. Niech $\mathcal{F}$ będzie taka funkcją oraz niech $dom(F) = T$. Zbiór $F(t)$ oznacza się zwykle przez F_t zaś samą funkcję $\mathcal{F}$ przez $(F_t)_{t\in T}$.

Uwaga. Powyższa konwencja stosowana jest powszechnie w analizie matematycznej, gdzie liczbowe ciągi nieskończone, czyli funkcje z liczb naturalnych w zbiór liczb rzeczywistych, oznacza się przez $(a_n)_{n\in\mathbb{N}}$.

Bezpośrednio z definicji sumy oraz przekroju dowolnej rodziny zbiorów wynika następujące twierdzenie:

Twierdzenie 4.9 *Niech $\mathcal{F} = (F_t)_{t\in T}$ będzie indeksowaną rodziną zbiorów oraz niech x będzie dowolnym elementem. Wtedy*

1. $x \in \bigcup \mathcal{F} \leftrightarrow (\exists t \in T)(x \in F_t)$,
2. $x \in \bigcap \mathcal{F} \leftrightarrow (\forall t \in T)(x \in F_t)$.

Obiekt $\bigcap \mathcal{F}$ jest zbiorem wtedy i tylko wtedy, gdy $\mathcal{F}$ jest rodziną niepustą. Stosowane są oznaczenia $\bigcup_{t\in T} F_t$ na $\bigcup \mathcal{F}$ oraz $\bigcap_{t\in T} F_t$ na $\bigcap \mathcal{F}$. W wielu dziedzinach matematyki istotną rolę odgrywają rodziny zbiorów indeksowane zbiorem liczb naturalnych, zwane ciągami zbiorów. Dla takich rodzin rozważa się dwie specjalne operacje:

$$\liminf_{n\in\mathbb{N}} F_n = \bigcup_n \bigcap_{k>n} F_k$$

oraz

$$\limsup_{n\in\mathbb{N}} F_n = \bigcap_n \bigcup_{k>n} F_k.$$

Pierwszą operację nazywa się *granicą dolną* zaś drugą *granicą górną* rodziny zbiorów $(F_n)_{n\in\mathbb{N}}$. Dla dowolnej rodziny $(F_n)_{n\in\mathbb{N}}$ prawdziwe są następujące zawierania

$$\bigcap_{n\in\mathbb{N}} F_n \subseteq \liminf_{n\in\mathbb{N}} F_n \subseteq \limsup_{n\in\mathbb{N}} F_n \subseteq \bigcup_{n\in\mathbb{N}} F_n.$$

Jeśli $\liminf_{n\in\mathbb{N}} F_n = \limsup_{n\in\mathbb{N}} F_n$, to ciąg $(F_n)_{n\in\mathbb{N}}$ nazywany jest ciągiem zbieżnym i wspólną wartość granicy dolnej i granicy górnej oznacza się przez $\lim_{n\in\mathbb{N}} F_n$.

4.6 Produkty Kartezjańskie

W rozdziale 2 omówiliśmy operację iloczynu kartezjańskiego dwóch zbiorów. Pokażemy teraz jak można uogólnić to pojęcie na dowolną rodzinę zbiorów.

Definicja 4.12 *Niech $(A_t)_{t\in T}$ będzie indeksowaną rodziną zbiorów.* ***Produktem kartezjańskim*** *tej rodziny nazywamy zbiór*

$$\prod_{t\in T} A_t = \{f : f \textit{ jest funkcją } \wedge\, dom(f) = T \wedge (\forall t \in T)(f(t) \in A_t)\}.$$

Jeśli istnieje taki zbiór A, że dla wszystkich $t \in T$ mamy $A_t = A$, to wtedy produkt kartezjański $\prod_{t\in T} A_t$ jest równy zbiorowi A^T.

Załóżmy teraz, że zbiór indeksujący T jest zbiorem skończonym. Niech mianowicie $T = \{1, \ldots, n\}$. Wtedy

$$\prod_{t\in T} A_t = \{\{(1, x_1), \ldots, (n, x_n)\} : x_1 \in A_1 \wedge \ldots \wedge x_n \in A_n\}.$$

Z drugiej strony

$$A_1 \times \ldots A_n = \{(x_1, \ldots, x_n) : x_1 \in A_1 \wedge \ldots \wedge x_n \in A_n\}.$$

Zbiory te są oczywiście różne, jednak istnieje naturalna bijekcja pomiędzy nimi. Jest nią mianowicie funkcja f określona wzorem

$$f((x_1, \ldots, x_n)) = \{(1, x_1), \ldots, (n, x_n)\}.$$

Obserwacja ta pokazuje, że produkt kartezjański rodziny zbiorów jest uogólnieniem pojęcia iloczynu kartezjańskiego zbiorów.

4.7 Funkcje Charakterystyczne

Ustalmy przestrzeń Ω. Omówimy teraz metodę reprezentowania podzbiorów przestrzeni Ω za pomocą funkcji z przestrzeni Ω w zbiór $\{0, 1\}$.

Definicja 4.13 ***Funkcją charakterystyczną*** *zbioru $A \subseteq \Omega$ nazywamy funkcję $\mathbf{1}_A : \Omega \to \{0, 1\}$ określoną wzorem*

$$\mathbf{1}_A(x) = \begin{cases} 1 & : \quad x \in A \\ 0 & : \quad x \notin A \end{cases}$$

Zauważmy, że $\mathbf{1}_A^{-1}[\{1\}] = A$. Niech $f : \Omega \to \{0, 1\}$. Połóżmy $A = f^{-1}[\{1\}]$. Wtedy dla dowolnego $x \in \Omega$ mamy

$$x \in A \leftrightarrow f(x) \in \{1\} \leftrightarrow f(x) = 1 \leftrightarrow \mathbf{1}_A(x) = 1.$$

Zatem każda funkcja $f : \Omega \to \{0, 1\}$ jest funkcją charakterystyczną pewnego podzbioru przestrzeni Ω.

Twierdzenie 4.10 *Niech $A, B \subseteq \Omega$. Wtedy*

1. $\mathbf{1}_A = \mathbf{1}_B \leftrightarrow A = B$,
2. $\mathbf{1}_{A^c} = 1 - \mathbf{1}_A$,
3. $\mathbf{1}_{A\cap B} = \min\{\mathbf{1}_A, \mathbf{1}_B\}$,
4. $\mathbf{1}_{A\cup B} = \max\{\mathbf{1}_A, \mathbf{1}_B\}$,

Dowód. Załóżmy, że $\mathbf{1}_A = \mathbf{1}_B$ Wtedy dla dowolnego $x \in \Omega$ mamy

$$x \in A \leftrightarrow \mathbf{1}_A(x) = 1 \leftrightarrow \mathbf{1}_B = 1 \leftrightarrow x \in B\ ,$$

a więc A=B. Odwrotna implikacja z punktu (1) jest oczywista. Niech teraz x będzie ustalonym elementem przestrzeni Ω. Wtedy

$$(\mathbf{1}_{A^c} = 1) \leftrightarrow (x \in A^c) \leftrightarrow \neg(x \in A) \leftrightarrow \neg(\mathbf{1}_A(x) = 1) \leftrightarrow$$
$$(\mathbf{1}_A(x) = 0) \leftrightarrow (1 - \mathbf{1}_A(x) = 1) \leftrightarrow ((1 - \mathbf{1}_A)(x) = 1)\ .$$

Równość (2) została więc pokazana. Następnie

$$\mathbf{1}_{A\cap B}(x) = 1 \leftrightarrow (x \in A \cap B) \leftrightarrow$$
$$(x \in A \wedge x \in B) \leftrightarrow (\mathbf{1}_A(x) = 1 \wedge \mathbf{1}_B(x) = 1) \leftrightarrow$$
$$(\min\{\mathbf{1}_A(x), \mathbf{1}_B(x)\} = 1) \leftrightarrow (\min\{\mathbf{1}_A, \mathbf{1}_B\}(x) = 1)\ .$$

Równość (4) pokazuje się podobnie jak równość (3). □

Metoda reprezentowania zbiorów za pomocą funkcji o wartościach w zbiorze $\{0, 1\}$ wykorzystywana jest czasem do reprezentowania zbiorów w informatyce. Jest to bardzo wygodna metoda, zwłaszcza gdy przestrzeń Ω jest stosunkowo mała. Funkcje te nazywają się mapami bitowymi.

Metoda ta jest również podstawą tak zwanej „*teorii zbiorów rozmytych*", w której zbiory opisywane są jako funkcje ze zbioru Ω o wartościach w odcinku $[0, 1]$. Funkcje $f : \Omega \to \{0, 1\}$ nazywane są w tej teorii *zbiorami klasycznymi*. Wzory pojawiające się w Twierdzeniu 4.10 są jedną z metod określania działań mnogościowych na zbiorach rozmytych.

4.8 Ćwiczenia i zadania

Ćwiczenie 4.1 *Podaj przykład relacji która jest symetryczna, ale nie jest zwrotna ani przechodnia.*

Ćwiczenie 4.2 *Pokaż, że relacja R jest przechodnia wtedy i tylko wtedy, gdy $R \circ R \subseteq R$.*

Ćwiczenie 4.3 *Pokaż, że relacja R jest symetryczna wtedy i tylko wtedy, gdy $R^{-1} = R$.*

Ćwiczenie 4.4 *Niech $R = \{(n, n + 1) : n \in \mathbb{N}\}$. Wyznacz najmniejszą relację przechodnią na zbiorze $\mathbb{N}$ zawierającą relację R.*

Ćwiczenie 4.5 *Niech f będzie funkcją różnowartościową. Pokaż, że wtedy dla dowolnych zbiorów A i B mamy $f[A \cap B] = f[A] \cap f[B]$. Sformułuj i udowodnij twierdzenie odwrotne.*

Ćwiczenie 4.6 *Niech f będzie funkcją. Pokaż, że następujące dwa zdania są równoważne:*

1. $(\forall A, B)(f[A \setminus B] = f[A] \setminus f[B])$,

2. *f jest injekcją*

Ćwiczenie 4.7 *Wyznacz zbiory $\emptyset^\emptyset$, $X^\emptyset$ oraz $\emptyset^X$, gdzie X jest dowolnym zbiorem niepustym.*

Ćwiczenie 4.8 *Niech $R = \{(x, y) \in \mathbb{R}^2 : |x| = |y|\}$ oraz $Q = \{(x, y) \in \mathbb{R}^2 : y = sin(x)\}$. Narysuj wykres relacji $R \circ Q$.*

Ćwiczenie 4.9 *Niech f będzie funkcją i A dowolnym zbiorem. Pokaż, że $f \restriction A$ jest również funkcją i $dom(f \restriction A) = dom(f) \cap A$.*

Ćwiczenie 4.10 *Niech f i g będą funkcjami. Pokaż, że $f \cup g$ jest funkcją wtedy i tylko wtedy, gdy $f \restriction (dom(f) \cap dom(g)) = g \restriction (dom(f) \cap dom(g))$.*

Ćwiczenie 4.11 *Znajdź bijekcje pomiędzy następującymi parami zbiorów:*

- $\mathbb{N}$ *i* $\mathbb{Z}$,
- $(0, 1)$ *i* $(3, 5)$,
- $(0, 1)$ *i* $\mathbb{R}$,
- $(0, 1)$ *i* $\mathbb{R}^+$,
- $[0, 1]$ *i* $[0, 1)$.

Ćwiczenie 4.12 *Niech $f : \mathbb{R}^2 \to \mathbb{R}^2$ będzie funkcją zadaną wzorem $f((x, y)) = (x + y, x - y)$. Czy odwzorowanie f jest injekcją? Czy f jest surjekcją? Znajdź $f[\mathbb{R} \times \{0\}]$, $f[L]$ oraz $f^{-1}[L]$, gdzie L jest prostą zadaną równaniem $y = x + 1$.*

Ćwiczenie 4.13 *Niech $(A_t)_{t\in T}$ będzie rodziną zbiorów i niech f będzie funkcją. Pokaż, że*

- $f[\bigcup_{t\in T} A_t] = \bigcup_{t\in T} f[A_t]$,
- $f[\bigcap_{t\in T} A_t] \subseteq \bigcap_{t\in T} f[A_t]$,
- $f^{-1}[\bigcup_{t\in T} A_t] = \bigcup_{t\in T} f^{-1}[A_t]$,
- $f^{-1}[\bigcap_{t\in T} A_t] = \bigcap_{t\in T} f^{-1}[A_t]$.

Ćwiczenie 4.14 *Pokaż, że dla podzbiorów A, B przestrzeni Ω zachodzą następujące wzory: $\chi_{A\cap B} = \chi_A \cdot \chi_B$, $\chi_{A\cup B} = 1 - (1 - \chi_A) \cdot (1 - \chi_B)$*

Zadanie 4.1 *Niech $f : \{\mathbb{0}, \mathbb{1}\}^{10} \to \{\mathbb{0}, \mathbb{1}\}$ będzie funkcją tożsamościowo równą $\mathbb{1}$. Zastosuj do funkcji f uniwersalną metodę wyznaczenia zdania φ takiego, że $f = F_\varphi$ i wyznacz jego długość uwzględniając ilość zmiennych zdaniowych, spójników i nawiasów.*

Zadanie 4.2 *Ile istnieje nierównoważnych formuł rachunku zdań zbudowanych ze zmiennych zdaniowych $p_1, \ldots, p_n$?*

Zadanie 4.3 *Niech $(F_n)_{n\in\mathbb{N}}$ będzie dowolnym ciągiem zbiorów. Pokaż, że*

$$x \in \liminf_{n\in\mathbb{N}} F_n$$

wtedy i tylko wtedy, gdy $(\forall^\infty n)(x \in F_n)$ oraz $x \in \limsup_{n\in\mathbb{N}} F_n$ wtedy i tylko wtedy, gdy $(\exists^\infty n)(x \in F_n)$ (patrz zadanie 3.3). Udowodnij, korzystając z powyższych obserwacji, że

$$\bigcap_{n\in\mathbb{N}} F_n \subseteq \liminf_{n\in\mathbb{N}} F_n \subseteq \limsup_{n\in\mathbb{N}} F_n \subseteq \bigcup_{n\in\mathbb{N}} F_n \ .$$

Zadanie 4.4 *Ustalmy zbiory A, B i C. Niech $A_{3n} = A$, $A_{3n+1} = B$ oraz $A_{3n+2} = C$ dla $n \in \mathbb{N}$. Wyznacz $\liminf_{n\in\mathbb{N}} A_n$, $\limsup_{n\in\mathbb{N}} A_n$. Kiedy ciąg $(A_n)_{n\in\mathbb{N}}$ jest zbieżny?*

Zadanie 4.5 *Niech $(A_{(i,j)})_{(i,j)\in I\times J}$ będzie dowolną indeksowaną rodziną zbiorów. Pokaż, że*

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

Zadanie 4.6 *Niech $\mathcal{F}$ będzie dowolna rodziną funkcji. Pokaż, że $\bigcup\mathcal{F}$ jest funkcją wtedy i tylko wtedy, gdy*

$$(\forall f, g \in \mathcal{F})(f \cup g \textit{ jest funkcją}) \ .$$

(patrz Ćwiczenie 4.10).

Zadanie 4.7 *Załóżmy, że $(A_n)_{n\in\mathbb{N}}$ jest rodziną zbiorów parami rozłącznych. Pokaż, że wtedy $\limsup_{n\in\mathbb{N}} A_n = \emptyset$.*

Zadanie 4.8 *Załóżmy, że $(A_n)_{n\in\mathbb{N}}$ jest malejącą rodziną zbiorów, czyli, że*

$$A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots$$

oraz, że $\bigcap_{n\in\mathbb{N}} A_n = \emptyset$. Pokaż, że wtedy

$$A_0 = \bigcup_{n\in\mathbb{N}} (A_n \setminus A_{n+1}).$$

Zadanie 4.9 *Funkcję logiczną f nazywamy nazywamy monotoniczną jeśli zmiana dowolnego argumentu z $\mathbf{F}$ na $\mathbf{T}$ nie powoduje zmiany wartości funkcji z $\mathbf{T}$ na $\mathbf{F}$. Pokaż, że jeśli f jest monotoniczną funkcją logiczną, to jest ona funkcją stałą lub może zostać przedstawiona jako formuła zbudowana wyłącznie ze zmiennych oraz spójników $\wedge$ i $\vee$.*

Zadanie 4.10 *Niech R będzie relacją symetryczną na zbiorze $\{1,2,3,4,5,6\}$. Pokaż, że istnieje taki trójelementowy podzbiór A zbioru $\{1,2,3,4,5,6\}$ taki, że $(\forall x, y \in A)(x \neq y \to (x,y) \in R)$ lub, że istnieje taki trójelementowy podzbiór B zbioru $\{1,2,3,4,5,6\}$ taki, że $(\forall x, y \in B)(x \neq y \to (x,y) \notin R)$.*

5 Relacje równoważności

Proces abstrakcji polega na wyznaczeniu istotnych i odrzuceniu nieistotnych cech rozpatrywanej kolekcji obiektów. Kiedy zajmujemy się barwą obiektów pomijamy ich kształty i identyfikujemy dwa obiekty, gdy mają ten sam kolor. W ten sposób zajmujemy się tylko barwami i traktujemy je jako samodzielne obiekty. W arytmetyce utożsamiamy se sobą ułamki $1/2$ i $2/4$ - są to różne obiekty, ale mają tę samą wartość. W geometrii, podobieństwo trójkątów służy nam do wyróżnienia klas trójkątów prostokątnych, równobocznych i równoramiennych. Trójkąty o bokach 3,4 i 5 oraz 6, 8 i 10 są oczywiście różnymi obiektami, lecz uważamy je za podobne, gdyż stosunki odpowiednich boków w obu trójkątach są takie same.

Abstrakcja jest czynnością niezbędną do klasyfikacji obiektów, która zastosowana do istot żywych prowadzi do podziału ich na królestwa, gromady, klasy, rzędy, rodzaje i gatunki.

Uwaga. Bardzo ważną sprawą w procesie abstrakcji jest odróżnienie cech istotnych od nieistotnych. Jeśli zwierzęta będziemy klasyfikowali ze względu na ilość nóg oraz kwestię posiadania opierzenia, do możemy dojść do wniosku, że człowiek to nieopierzone, dwunożne zwierze. Tropem tym kilka tysięcy lat temu poszedł Arystoteles.

Matematycznym narzędziem służącym do modelowania procesu abstrakcji są relacje równoważności.

Definicja 5.1 *Relację $R \subseteq X \times X$ nazywamy relacją **równoważności** na zbiorze X jeśli jest zwrotna na zbiorze X, symetryczna i przechodnia.*

Najmniejszą relacją równoważności na zbiorze X jest relacja równości, czyli zbiór $Id_X = \{(x, x) : x \in X\}$. Największą relacją równoważności na zbiorze X jest zaś relacja $X \times X$. Przed przystąpieniem do analizowania własności tych relacji podamy kilka przykładów. Pierwszy z nich ma bardzo ogólny charakter.

Przykład 5.1 *Niech $f : X \to Y$. Na zbiorze X określamy relację $ker(f) = \{(x, y) \in X^2 : f(x) = f(y)\}$. Nazywamy ją **jądrem funkcji** f. Zwrotność tej relacji wynika z tego, że $f(x) = f(x)$ dla dowolnego $x \in X$. Jeśli $f(x) = f(y)$, to oczywiście $f(y) = f(x)$, z czego wynika symetria relacji $ker(f)$. W końcu, jeśli $f(x) = f(y)$ i $f(y) = f(z)$ to $f(x) = f(z)$, a więc relacja ta jest przechodnia.*

Drugi przykład ma charakter algebraiczny.

Przykład 5.2 *Niech n będzie ustaloną dodatnią liczbą naturalną. Na zbiorze liczb całkowitych $\mathbb{Z}$ określmy relacje $\equiv_n$ wzorem*

$$x \equiv_n y \leftrightarrow n|x-y,$$

gdzie $|$ oznacza relację podzielności w liczbach całkowitych. Ponieważ $n|0$, więc rozważana relacja jest zwrotna. Jeśli $n|x-y$ to również $n|-(x-y)$, czyli $n|y-x$, czyli relacja ta jest symetryczna. Załóżmy teraz, że $x \equiv_n y$ oraz $y \equiv_n z$. Wtedy istnieją takie liczby całkowite k i l, że $x-y = k \cdot n$ oraz $y-z = l \cdot n$. Wtedy

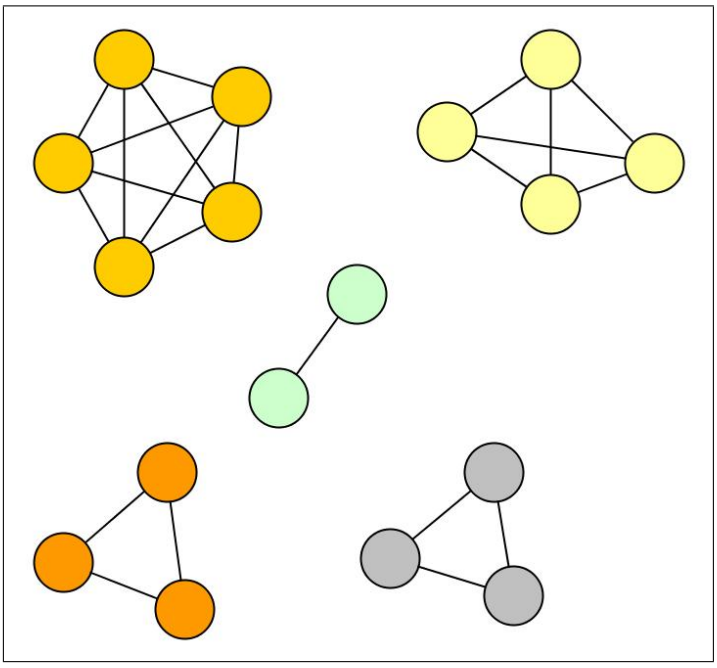
$$x - z = (x-y) + (y-z) = k \cdot n + l \cdot n = (k+l) \cdot n,$$

więc $x \equiv_n z$. Zatem relacja $\equiv_n$ jest przechodnia.

Definicja 5.2 *Niech ϱ będzie relacją równoważności na zbiorze X oraz niech $a \in X$.* ***Klasą abstrakcji*** *elementu a względem relacji ϱ nazywamy zbiór*

$$[a]_\varrho = \{x \in X : a \,\varrho\, x\}.$$

Klasa abstrakcji $[a]_\varrho$ elementu a nazywana jest również warstwą w relacji ϱ elementu przez a.



Twierdzenie 5.1 (O abstrakcji) *Załóżmy, że ϱ jest relacją równoważności na zbiorze X. Wtedy*

1. $(\forall x \in X)(x \in [x]_\varrho)$,
2. $(\forall x, y \in X)(x \varrho y \to [x]_\varrho = [y]_\varrho)$,
3. $(\forall x, y \in X)(\neg(x \varrho y) \to [x]_\varrho \cap [y]_\varrho = \emptyset)$.

Dowód. Niech $x \in X$. Wtedy $x \varrho x$ więc $x \in [x]_\varrho$. Załóżmy teraz, że $x, y \in X$ oraz $x \varrho y$. Rozważmy dowolne element $z \in [x]_\varrho$. Wtedy $x \varrho z$. Z symetrii rozważanej relacji wynika, że $y \varrho z$, a więc, z przechodniości relacji ϱ mamy $y \varrho z$, czyli $z \in [y]_\varrho$. Pokazaliśmy więc, że $[x]_\varrho \subseteq [y]_\varrho$. Inkluzję $[y]_\varrho \subseteq [x]_\varrho$ pokazuje się podobnie. Załóżmy teraz, że $x, y \in X$ oraz $[x]_\varrho \cap [y]_\varrho \neq \emptyset$. Niech $z \in [x]_\varrho \cap [y]_\varrho$. Wtedy $x \varrho z$ i $y \varrho z$, więc $x \varrho z$ oraz $z \varrho y$. Z przechodniości rozważanej relacji wynika, że $x \varrho y$, co kończy dowód twierdzenia. □

Definicja 5.3 *Niech ϱ będzie relacją równoważności na zbiorze X. **Przestrzenią ilorazową** relacji ϱ nazywamy zbiór X/ϱ = $\{[x]_\varrho : x \in X\}$.*

Ustalmy zbiór X oraz relację równoważności ϱ na X. Niech $f : X \to X/\varrho$ będzie funkcją określoną wzorem $f(x) = [x]_\varrho$. Wtedy $\varrho = ker(f)$. Widzimy więc, że Przykład 5.1 jest uniwersalny. Dla każdej relacji równoważności ϱ istnieje taka funkcja f, że $\varrho = ker(f)$.

Przykład 5.3 *Rozważmy ponownie relację $\equiv_n$ z przykładu 5.2. Dla dowolnej liczby całkowitej k mamy*

$$[k]_{\equiv_n} = \{x \in \mathbb{Z} : n | k - x\}.$$

Przypomnijmy, że dla dowolnej liczby całkowitej k istnieją takie liczby l i r, że $k = n \cdot l + r$ i $0 \leq r < n$. Lecz wtedy $k - r = n \cdot l$, więc $n|k - r$. Zatem dla każdej liczby całkowitej k istnieje taka liczba naturalna $r \in \{0, \ldots, n-1\}$, że $k \equiv_n r$, czyli $[k]_{\equiv_n} = [r]_{\equiv_n}$. Zatem

$$\mathbb{Z}/\equiv_n = \{[0]_{\equiv_n}, [1]_{\equiv_n}, \ldots, [n-1]_{\equiv_n}\}.$$

Elementami warstwy $[0]_{\equiv_n}$ są wszystkie liczby podzielne przez n. Następnie $[1]_{\equiv_n} = \{kn + 1 : k \in \mathbb{Z}\}$, $[2]_{\equiv_n} = \{kn + 2 : k \in \mathbb{Z}\}$ itd.

5.1 Rozbicia

Omówimy jeszcze jeden sposób opisywania relacji równoważności.

Definicja 5.4 *Rodzinę zbiorów $\mathcal{A}$ nazywamy **rozbiciem** lub **partycją** zbioru Ω jeśli $\bigcup \mathcal{A} = \Omega$, $(\forall A \in \mathcal{A})(A \neq \emptyset)$ oraz $(\forall A, B \in \mathcal{A})(A \neq B \to A \cap B = \emptyset)$.*

Przykładem rozbicia zbioru $\mathbb{R}$ jest rodzina $\{(-\infty, 0), \{0\}, (0, +\infty)\}$. Ma ono trzy elementy: zbiór liczb ujemnych, zbiór złożony z zera (czyli singleton zera) oraz zbiór liczb dodatnich.

Niech $\mathcal{A}$ będzie dowolnym rozbiciem zbioru Ω. Określmy relację równoważności $\sim_\mathcal{A}$ wzorem

$$x \sim_\mathcal{A} y \leftrightarrow (\exists X \ \in \mathcal{A})(x \in X \wedge y \in X).$$

Łatwo sprawdzić, że $\sim_\mathcal{A}$ jest relacją równoważności na zbiorze Ω oraz, że $\Omega/\sim_\mathcal{A} = \mathcal{A}$. Z Twierdzenia 5.1 wynika, że jeśli ϱ jest relacją równoważności na zbiorze X, to X/ϱ jest rozbiciem zbioru X. Istnieje więc wzajemna odpowiedniość pomiędzy relacjami równoważnościami na zbiorze Ω a rozbiciami zbioru Ω.

5.2 Konstruowanie obiektów matematycznych

Relacje równoważności wykorzystywane są do konstruowania wielu obiektów matematycznych. Rozważmy odcinek $[0,1]$. Określmy na nim następującą relację równoważności $\approx = \{(x,x) : x \in [0,1]\} \cup \{(0,1),(1,0)\}$. Jeśli $x \in (0,1)$, to $[x] = \{x\}$ oraz $[0] = [1] = \{0,1\}$. Relacja ta zlepia więc końce odcinka $[0,1]$. Wynik operacji $[0,1]/\approx$ możemy więc utożsamiać z okręgiem. Konstrukcję tę możemy opisać trochę prościej. Niech mianowicie $fr : \mathbb{R} \to [0,1)$ będzie funkcją określoną wzorem

$$fr(x) = y \leftrightarrow (y \in [0,1)) \wedge (\exists k \in \mathbb{Z})(x = k + y).$$

Wtedy rozważaną przed chwilą relację możemy zdefiniować wzorem

$$x \approx y \leftrightarrow fr(x) = fr(y).$$

Rozważmy teraz zbiór $[0,1] \times [0,1]$ oraz relację $\cong$ określoną wzorem

$$(x,y) \cong (x',y') \leftrightarrow (fr(x) = fr(x') \wedge y = y') \ .$$

Po chwili zastanowienia powinno być jasne dla czytelnika, że przestrzeń ilorazową $[0,1] \times [0,1]/\cong$ utożsamiać możemy z walcem.

Głównym celem tego rozdziału jest pokazanie jak startując z liczb naturalnych[1] można otrzymać liczby całkowite, następnie jak z liczb całkowitych można zbudować liczby wymierne i w końcu, z liczb wymiernych, liczby rzeczywiste.

Konstrukcja liczb całkowitych

Niech $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ będzie funkcją określoną wzorem $f(x,y) = x - y$. Rozważmy relację $\sim$

$$(x,y) \sim (x',y') \leftrightarrow f(x,y) = f(x',y')$$

określoną na iloczynie kartezjańskim $\mathbb{N} \times \mathbb{N}$. Jest to, na mocy rozważań z Przykładu 5.1, relacja równoważności. Zauważmy, że relację tę możemy zdefiniować w sposób równoważny wzorem

$$(x,y) \sim (x',y') \leftrightarrow x + y' = x' + y \ , \tag{5.1}$$

a więc do zdefiniowania jej nie potrzebujemy liczb całkowitych. Bez trudu sprawdzić możemy, że odwzorowanie

$$\psi : ((\mathbb{N} \times \mathbb{N})/\sim) \ \to \mathbb{Z} : [(n,m)]_\sim \mapsto n - m$$

jest bijekcją. Zatem liczby całkowite możemy zbudować z liczb naturalnych za pomocą relacji równoważności zdefiniowanej wzorem 5.1.

Konstrukcja liczb wymiernych

Rozważmy teraz funkcją $g : \mathbb{Z} \times (\mathbb{N} \setminus \{0\}) \to \mathbb{Q}$ określoną wzorem $g(k,n) = \frac{k}{n}$ oraz rozważmy relację $\approx$

$$(k,n) \approx (k',n') \leftrightarrow g(k,n) = g(k',n').$$

[1] „Liczby naturalne stworzył dobry Bóg, resztę wymyślili ludzie.” - Leopold Kronecker (1823-1891). Dziś już wiemy, że liczby naturalne można zbudować ze zbioru pustego.

Jest to relacja równoważności na zbiorze $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$. Łatwo sprawdzić, że odwzorowanie

$$\psi : ((\mathbb{Z} \times (\mathbb{N} \setminus \{0\}))/\approx) \ \to \mathbb{Q} : [(k,n)]_\approx \mapsto \frac{k}{n}$$

jest bijekcją. Zauważmy również, że

$$(k,n) \approx (k',n') \leftrightarrow kn' = k'n \ .$$

Widzimy więc, że liczby wymierne możemy skonstruować z liczb całkowitych oraz z liczb naturalnych za pomocą powyższej relacji równoważności.

Konstrukcja liczb rzeczywistych

Rozważmy zbiór C wszystkich ciągów podstawowych liczb wymiernych, czyli niech

$$C = \{f \in \mathbb{Q}^{\mathbb{N}} : (\forall k \in \mathbb{N})(\exists N \in \mathbb{N})(\forall n,m > N)(|f(n) - f(m)| < \frac{1}{1+k})\}.$$

Z wykładu z Analizy Matematycznej wiemy, że każdy ciąg podstawowy liczb rzeczywistych jest ciągiem zbieżnym. Niech $L : C \to \mathbb{R}$ będzie funkcją określoną wzorem $L((q_n)_{n\in\mathbb{N}}) = \lim_n q_n$. Na zbiorze C określamy relację $\sim$ wzorem

$$r \sim s \leftrightarrow L(r) = L(s) \ .$$

Jest to relacja równoważności. Ponadto funkcja

$$\psi : (C/\sim) \ \to \mathbb{R} : [(q_n)_{n\in\mathbb{N}}]_\sim \mapsto L((q_n)_{n\in\mathbb{N}})$$

jest bijekcją, gdyż dla każdej liczby rzeczywistej x istnieje ciąg liczb wymiernych zbieżny go x. Łatwo można sprawdzić, że

$$f \sim g \leftrightarrow (\forall k \in \mathbb{N})(\exists N \in \mathbb{N})(\forall n > N)(|f(n) - g(n)| < \frac{1}{k+1}).$$

Widzimy więc, że liczby rzeczywiste można skonstruować z liczb wymiernych oraz z liczb naturalnych za pomocą powyższej relacji równoważności.

Uwaga. Alternatywną metodę konstrukcji zbioru liczb rzeczywistych przedstawił Dedekind. Oparta jest ona na pojęciu przekrojów Dedekinda. Są nimi pary uporządkowane (A,B) niepustych podzbiorów zbioru liczb wymiernych $\mathbb{Q}$ takich, że $A \cup B = \mathbb{Q}$ oraz $(\forall a \in A)(\forall b \in B)(a < b)$. Zbiór A nazywamy klasą dolną zaś zbiór B klasą górną przekroju (A,B). Bez trudu można sprawdzić, że istnieją trzy rodzaje przekrojów:

1. w klasie dolnej istnieje liczba największa, a w klasie górnej nie istnieje liczba najmniejsza.
2. w klasie górnej istnieje liczba najmniejsza, a w klasie dolnej nie istnieje liczba największa.
3. w klasie górnej nie istnieje liczba najmniejsza, a w klasie dolnej nie istnieje liczba największa.

Przekroje pierwszego rodzaju są więc postaci $D_q = ((-\infty, q], (q, \infty))$ a drugiego rodzaju są postaci $G_q = ((-\infty, q), [q, \infty))$, gdzie $q \in \mathbb{Q}$ a przedział oznacza oczywiście przedział w zbiorze liczb wymiernych. Przekroje takie utożsamiamy z liczbą wymierną q. Przekroje trzeciego rodzaju interpretujemy jako liczby niewymierne. Przekładem takiego przekroju jest para

$$(\{x \in \mathbb{Q} : x < 0 \vee (x > 0 \wedge x^2 < 2\}, \{x \in \mathbb{Q} : x > 0 \wedge x^2 > 2\}),$$

którą interpretujemy jako $\sqrt{2}$. Liczby rzeczywiste interpretujemy jako zbiór wszystkich przekrojów Dedekinda po utożsamieniu przekrojów D_q z G_q.

5.3 Ćwiczenia i zadania

Ćwiczenie 5.1 *Pokaż, że następujące relacje są relacjami równoważności na zbiorze X i wyznacz ich klasy abstrakcji:*

- $X = \mathbb{N}^2$; $(x, y) \approx (a, b) \leftrightarrow x + y = a + b$,
- $X = \mathbb{N}^2$; $(x, y) \approx (a, b) \leftrightarrow max\{x, y\} = max\{a, b\}$,
- $X = \mathbb{R}$; $x \approx y \leftrightarrow (\exists t \neq 0)(tx = y)$,
- $X = \mathbb{R}$; $x \approx y \leftrightarrow (\exists t > 0)(tx = y)$,
- $X = \mathbb{R}^2$; $x \approx y \leftrightarrow (\exists t \neq 0)(tx = y)$,
- $X = \mathbb{R}^2$; $x \approx y \leftrightarrow (\exists t > 0)(tx = y)$.

Ćwiczenie 5.2 *Dla $(x_1, x_2), (y_1, y_2) \in [0, 1]^2$ określamy relację*

$$(x_1, x_2) \sim (y_1, y_2) \leftrightarrow fr(x_1) = fr(y_1) \wedge fr(x_2) = fr(y_2),$$

gdzie fr jest funkcją określoną w podrozdziale 5.2. Pokaż, że $\sim$ jest relacją równoważności. Wyznacz jej klasy abstrakcji.

Ćwiczenie 5.3 *Pokaż, że relacja $\approx$ określona na zbiorze $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ w konstrukcji zbioru liczb wymiernych ze zbioru liczb całkowitych jest relacją równoważności.*

Ćwiczenie 5.4 *Ile jest relacji równoważności na zbiorze $\{1, 2, 3\}$? Ile jest różnych rozbić zbioru $\{1, 2, 3, 4\}$?*

Ćwiczenie 5.5 *Na zbiorze $[0, 8)^2$ określamy następującą relację równoważności*

$$(a, b) \approx (c, d) \leftrightarrow [a] = [c] \wedge [b] = [d],$$

gdzie $[x]$ oznacza część całkowitą liczby x. Niech

$$T = \{(n, m) \in \{0, 1, 2, 3, 4, 5, 6, 7, 8\}^2 : 2|n + m\}.$$

Narysuj zbiór

$$\bigcup_{(n,m)\in T} [(n, m)]_{\approx}.$$

Ćwiczenie 5.6 *Na zbiorze liczb całkowitych $\mathbb{Z}$ określamy relacje $x \equiv y \leftrightarrow 3|(x+2y)$ oraz $x \simeq y \leftrightarrow 5|x^2 - y^2$. Czy są to relacje równoważności?*

Ćwiczenie 5.7 *Opisz klasy abstrakcji relacji $\approx$ na zbiorze liczb rzeczywistych $\mathbb{R}$ zadanej formułą*

$$x \approx y \leftrightarrow (x - y \in \mathbb{Z}).$$

Ćwiczenie 5.8 *Na zbiorze $\mathbb{N} \times \mathbb{N}$ określamy relacją równoważności $\approx$ formułą*

$$(x, y) \approx (x', y') \leftrightarrow \max\{x, y\} = \max\{x', y'\}\ .$$

Ile elementów ma klasa abstrakcji $[(0, 20)]_{\approx}$?

Ćwiczenie 5.9 *Pokaż, że jeśli ϱ i η są relacjami równoważności na zbiorze Ω, to również $\varrho \cap \eta$ jest relacją równoważności na zbiorze Ω. Opisz klasy abstrakcji relacji $\varrho \cap \eta$.*

Ćwiczenie 5.10 *Ustalmy liczbę $x \in \mathbb{R}$. Pokaż, że $\left(\frac{\lfloor (n+1)x \rfloor}{n+1}\right)_{n\in\mathbb{N}}$ jest ciągiem liczb wymiernych zbieżnym do liczby x, gdzie $\lfloor z \rfloor$ oznacza część całkowitą liczby rzeczywistej z.*

Zadanie 5.1 *Niech $\mathcal{G} = (G, \cdot)$ będzie grupą oraz niech $H \subseteq G$ będzie podgrupą grupy $\mathcal{G}$. Na zbiorze G określamy relację $\sim_H$ wzorem*

$$x \sim_H y \leftrightarrow xy^{-1} \in H.$$

Pokaż, że $\sim_H$ jest relacją równoważności. Opisz jej klasy abstrakcji.

Zadanie 5.2 *Pokaż, że przekrój dowolnej rodziny relacji równoważności na zbiorze X jest relacją równoważności na zbiorze X. Na zbiorze $\mathbb{N} \times \mathbb{N}$ określamy relacje ϱ i η wzorami $(n, m)\varrho(n', m') \leftrightarrow n = n'$ oraz $(n, m)\eta(n', m') \leftrightarrow m = m'$. Wyznacz najmniejszą relację równoważności zawierającą relację $\varrho \cup \eta$.*

Zadanie 5.3 (Konstrukcja Dedekinda) *Na zbiorze przekrojów Dedekinda $\mathcal{D}$ określamy relację*

$$(A, B) \leq (C, D) \leftrightarrow A \subseteq C$$

oraz działania:

1. $(A, B) + (C, D) = (A + B, C + D)$, *gdzie* $X + Y = \{x + y : x \in X \wedge y \in Y\}$,
2. $-(A, B) = (-B, -A)$, *gdzie* $-X = \{-x : x \in X\}$,
3. $(A, B) \cdot (C, D) = (\mathbb{Q} \setminus (B \cdot D), B \cdot D)$, *gdzie* $X \cdot Y = \{xy : x \in X \wedge y \in Y\}$.

Pokaż, że tak określone działania są poprawne, czyli, że, na przykład, jeśli (A, B) i (C, D) są przekrojami Dedekinda, to również $(A + B, C + D)$ jest przekrojem Dedekinda. Pokaż, że tak określone działania uogólniają działania na zbiorze liczb wymiernych, czyli, że, na przykład, $D_q + D_r = D_{q+r}$ oraz $-D_q = G_{-q}$.

Zadanie 5.4 *Omów metodę konstruowania ciała liczb zespolonych z ciała liczb rzeczywistych.*

6 Częściowe Porządki

W tym rozdziale rozważymy kolejną ważną klasę relacji. Uogólniają one zarówno porządek na liczbach rzeczywistych jak i relację inkluzji określoną na rodzinie podzbiorów danego zbioru. Jest to więc bardzo obszerna klasa relacji.

Definicja 6.1 *Relację $R \subseteq X \times X$ nazywamy **częściowym porządkiem** na zbiorze X jeśli R jest relacją zwrotną na zbiorze X, przechodnią i słabo antysymetryczną. Parę (X, R) nazywamy częściowym porządkiem jeśli R jest częściowym porządkiem na zbiorze X.*

Przykładem częściowego porządku jest klasyczna słaba nierówność $\leq$ na zbiorze liczb rzeczywistych. Zwróćmy uwagę na to, że ostra nierówność $<$ na $\mathbb{R}$ nie jest zwrotna, więc nie jest częściowym porządkiem. Bardzo często łącznie z częściowym porządkiem $\leq$ rozważać będziemy relacje $<$ zdefiniowaną wzorem $x < y \leftrightarrow (x \neq y) \wedge (x \leq y)$.

Przykład 6.1 *Niech Ω będzie ustalonym zbiorem. Rozważmy relację inkluzji obciętą do podzbiorów zbioru Ω, czyli relację $R = \{(X, Y) : X \subseteq Y\}$. Bezpośrednio o podstawowych własności inkluzji wynika, że para $(P(\Omega), R)$, którą będziemy oznaczać przez $\mathcal{P}(\Omega)$, jest częściowym porządkiem.*

Przykład 6.2 *Rozważmy relacje podzielności $|$ w zbiorze dodatnich liczb naturalnych. Bezpośrednio z definicji podzielności wynika, że para $(\mathbb{N} \setminus \{0\}, |)$ jest częściowym porządkiem. Zauważmy jednak, że relacja podzielności na zbiorze liczb całkowitych nie jest częściowym porządkiem, gdyż na przykład $-1|1$ oraz $1| - 1$, lecz $1 \neq -1$, a więc relacja ta nie jest słabo antysymetryczna na zbiorze $\mathbb{Z}$.*

Definicja 6.2 *Niech $R \subseteq X \times X$ będzie dowolną relacją oraz niech A będzie dowolnym podzbiorem zbioru X. **Obcięciem** relacji R do zbioru A nazywamy relację $R \restriction A = R \cap (A \times A)$.*

Bez trudu możemy sprawdzić, że jeśli $(X, \leq)$ jest częściowym porządkiem i $A \subseteq X$ to również $(A, \leq \restriction A)$ jest częściowym porządkiem.

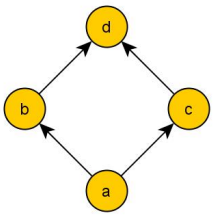
Definicja 6.3 *Mówimy, że dwa częściowe porządki $(X, \leq)$ i $(Y, \preceq)$ są **izomorficzne** jeśli istnieje bijekcja $f : X \to Y$ taka, że*

$$(\forall x, y \in X)(x \leq y \leftrightarrow f(x) \preceq f(y)).$$

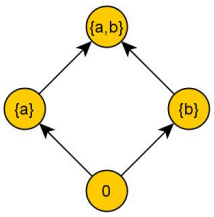
O porządkach izomorficznych mówimy, że są podobne. Rozważmy częściowy porządek

$$\preceq = \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (a, d), (b, d), (c, d)\}$$

na zbiorze $\{a, b, c, d\}$. Możemy go przedstawić za pomocą rysunku



Na rysunku tym nie umieściliśmy strzałek wynikających ze zwrotności relacji $\preceq$ oraz strzałek wynikających z przechodniości, czyli strzałki prowadzącej od elementy a do elementu d. Zauważmy, że wszystkie strzałki skierowane są do góry strony. Takie rysunki nazywane są *diagramami Hassego* częściowego porządku. Rozważmy teraz porządek $(P(\{a, b\}), \subseteq)$. Oto jego diagram Hassego:



Widzimy, że diagramy Hassego tych porządków są identyczne. Wynika to z tego, że oba porządki $(\{a, b, c, d\}, \preceq)$ oraz $(P(\{a, b\}), \subseteq)$ są izomorficzne. Izomorfizmem jest funkcja $f = \{(a, \emptyset), (a, \{a\}), (c, \{b\}), (d, \{a, b)\}$.

Pokażemy teraz, że inkluzja jest w pewnym sensie uniwersalnym częściowym porządkiem. Precyzuje to następujące twierdzenie:

Twierdzenie 6.1 *Niech $(X, \leq)$ będzie częściowym porządkiem. Wtedy istnieje rodzina $\mathcal{A} \subseteq P(X)$ taka, że porządki $(X, \leq)$ oraz $(\mathcal{A}, \subseteq \restriction \mathcal{A})$ są izomorficzne.*

Dowód. Dla każdego $x \in X$ określmy $f(x) = \{y \in X : y \leq x\}$. Wtedy $f : X \to P(X)$. Pokażemy, że funkcja f jest różnowartościowa. Załóżmy bowiem, że $x, y \in X$ oraz $f(x) = f(y)$. Wtedy $x \in f(x) = f(y)$, więc $x \leq y$. Podobnie pokazujemy, że $y \leq x$. Zatem $x = y$. Podobnie łatwo pokazujemy, że $f(x) \subseteq f(y) \leftrightarrow x \leq y$. Niech więc $A = rng(f)$. Wtedy f jest izomorfizmem pomiędzy $(X, \leq)$ oraz $(\mathcal{A}, \subseteq \restriction \mathcal{A})$. □

6.1 Wyróżnione elementy

W rozdziale tym omówimy pojęcie elementów najmniejszych, minimalnych, największych oraz maksymalnych.

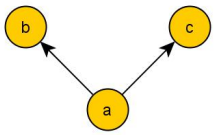
Definicja 6.4 *Niech $(X, \leq)$ będzie częściowym porządkiem oraz niech $a \in X$.*

1. *a jest elementem $\leq$-**największym**, jeśli $(\forall x \in X)(x \leq a)$.*
2. *a jest elementem $\leq$-**najmniejszym**, jeśli $(\forall x \in X)(a \leq z)$.*

3. *a jest elementem $\leq$-**maksymalnym**, jeśli* $\neg(\exists x \in X)(a \leq x \wedge a \neq x)$.

4. *a jest elementem $\leq$-**minimalnym**, jeśli* $\neg(\exists x \in X)(x \leq a \wedge a \neq x)$.

Zauważmy, że jeśli a jest elementem $\leq$-największym to jest również $\leq$-maksymalnym. Rzeczywiście, załóżmy, że a jest $\leq$-największym. Jeśli $a \leq x$, to ze słabej antysymetrii relacji $\leq$ i z tego, że $x \leq a$ wynika, że $x = a$. Podobnie pokazać możemy, że każdy element najmniejszy jest elementem minimalnym. Rozważmy częściowy porządek o następującym diagramie Hassego:



Elementy b i c są maksymalne w tym porządku. Relacja ta nie ma elementu największego. Element a jest najmniejszy, a więc jest również elementem minimalnym.

Przykład 6.3 *Niech a będzie dowolnym obiektem, który nie należy do zbioru $\mathbb{Z}$. Rozważmy następujący częściowy porządek R określony na zbiorze $\Omega = \{a\} \cup \mathbb{Z}$:*

$$R = \{(a, a)\} \cup \{(x, y) \in \mathbb{Z}^2 : x \leq y\}.$$

Wtedy a jest jedynym R-minimalnym i jedynym R-maksymalnym elementem. W częściowym porządku (Ω, R) nie ma elementów najmniejszych ani największych.

Przykład 6.4 *Rozważmy następujący częściowy porządek $\preceq$ na płaszczyźnie $\mathbb{R}^2$:*

$$(x, y) \preceq (x', y') \leftrightarrow (x \leq x') \wedge (y \leq y').$$

Sprawdzenie, że tak określona relacja jest częściowym porządkiem nie sprawia żadnych trudności. Niech teraz $K = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$ będzie kulą jednostkową. Rozważmy częściowy porządek $(K, \preceq \restriction K)$. Elementami maksymalnymi w tym porządku są elementy zbioru $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1 \wedge x \geq 0 \wedge y \geq 0\}$.

Rozważany w powyższym przykładzie porządek częściowy na zbiorze $\mathbb{R}^2$ jest szczególnym przypadkiem porządku produktowego.

Definicja 6.5 *Niech $((X_t, \leq_t))_{t \in T}$ będzie rodziną częściowych porządków. **Produktem** $\prod_{t \in T}((X_t, \leq_t))$ nazywamy częściowy porządek $\leq$ na zbiorze $\prod_{t \in T} X_t$ określony wzorem*

$$f \leq g \leftrightarrow (\forall t \in T)(f(t) \leq_t g(t)).$$

Twierdzenie 6.2 *Niech $((X_t, \leq_t))_{t \in T}$ będzie rodziną częściowych porządków. Wtedy ich produkt $\prod_{t \in T}((X_t, \leq_t))$ jest częściowym porządkiem.*

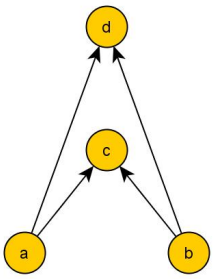
Dowód. Niech $f \in \prod_{t \in T} X_t$. Wtedy $(\forall t \in T)(f(f) \leq_t f(t))$, więc $f \leq f$. Relacja $\leq$ jest więc zwrotna. Jeśli $f, g \in \prod_{t \in T} X_t$ oraz $f \leq g$ i $g \leq f$, to $(\forall t \in T)(f(f) \leq_t g(t))$ oraz $(\forall t \in T)(f(f) \leq_t g(t))$, a więc $(\forall t \in T)((f(f) \leq_t f(t)) \wedge (g(t) \leq_t f(t))$. Zatem $(\forall t \in T)(f(t) = g(t))$, a więc $f = g$. Relacja $\leq$ jest więc słabo antysymetryczna. Niech następnie $f, g, h \in \prod_{t \in T} X_t$ oraz $f \leq g$ i $g \leq h$. Wtedy $(\forall t \in T)(f(f) \leq_t g(t))$ oraz $(\forall t \in T)(g(f) \leq_t h(t))$, a więc $(\forall t \in T)((f(f) \leq_t h(t))$. Zatem $f \leq h$. Pokazaliśmy więc, że relacja $\leq$ jest relacją przechodnią.

□

Przykład 6.5 *Rozważmy dowolny niepusty zbiór T. Na zbiorze $\{0,1\}$ określamy naturalny porządek $\leq$ dziedziczony z liniowego porządku prostej rzeczywistej $\mathbb{R}$. Dla każdego $t \in T$ niech $X_t = \{0,1\}$ oraz $\leq_t = \leq$. Rozważmy porządek produktowy $\leq^*$ na $\{0,1\}^T = \prod_{t\in T} X_t$. Okazuje się, że porządki $(\{0,1\}^T, \leq^*)$ oraz $(P(T), \subseteq)$ są izomorficzne. Funkcją ustalającą izomorfizm pomiędzy nimi jest przyporządkowanie $\psi : P(T) \to \{0,1\}^T$ podzbiorowi $A \subseteq T$ funkcji charakterystycznej χ_A.*

Definicja 6.6 *Niech $(X, \leq)$ będzie częściowym porządkiem oraz niech $A \subseteq X$ będzie zbiorem niepustym. Element $a \in X$ nazywamy **kresem górnym** zbioru A jeśli jest najmniejszym ograniczeniem górnym zbioru A, czyli jeśli $(\forall x \in A)(x \leq a)$ oraz $(\forall b \in X)((\forall x \in A)(x \leq b) \to a \leq b)$.*

Kres górny nie musi istnieć. Rozważmy, na przykład, następujący porządek



Ograniczeniami górnymi zbioru $\{a, b\}$ są oczywiście elementy c i d. Lecz w tym przykładzie są one nieporównywalne. Nie istnieje więc najmniejsze ograniczenie górne zbioru $\{a, b\}$. Kres górny może nie istnieć również z innych powodów. Rozważmy, na przykład, częściowy porządek $(\mathbb{N}, \leq)$. Wtedy zbiór $A = \mathbb{N}$ nie ma ograniczenia górnego, gdyż w zbiorze liczb naturalnych nie ma elementu największego. Istnieją jednak częściowe porządki w których każdy niepusty podzbiór zbiór ma kres górny. Są nimi na przykład porządki postaci $\mathcal{P}(X)$. Kresem górnym rodziny $\mathcal{A} \subseteq P(X)$ jest oczywiście zbiór $\bigcup \mathcal{A}$. Kres górny zbioru A, o ile istnieje, oznaczany jest symbolem $\sup(A)$ i nazywany jest również supremum zbioru A.

Dualnym pojęciem do kresu górnego jest pojęcie kresu dolnego. Mówimy, że element $a \in X$ jest kresem dolnym zbioru A jeśli jest największym ograniczeniem dolnym zbioru A, czyli jeśli $(\forall x \in A)(a \leq x)$ oraz $(\forall b \in X)((\forall x \in A)(b \leq x) \to b \leq a)$. Element taki, oczywiście o ile istnieje, oznaczany jest symbolem $\inf(A)$ i nazywany jest infimum zbioru A.

Uwaga. Bardzo ważną własnością liczb rzeczywistych jest to, że każdy ograniczony podzbiór $\mathbb{R}$ ma kres górny oraz kres górny. Własność ta charakteryzuje zbiór liczb rzeczywistych w następującym sensie: jeśli struktura $(K, +, \cdot, 0, 1, \leq)$ jest ciałem uporządkowanym takim, że każdy ograniczony jego podzbiór ma kres górny, to ciało to jest izomorficzne z liczbami rzeczywistymi.

6.2 Porządki na rodzinach funkcji

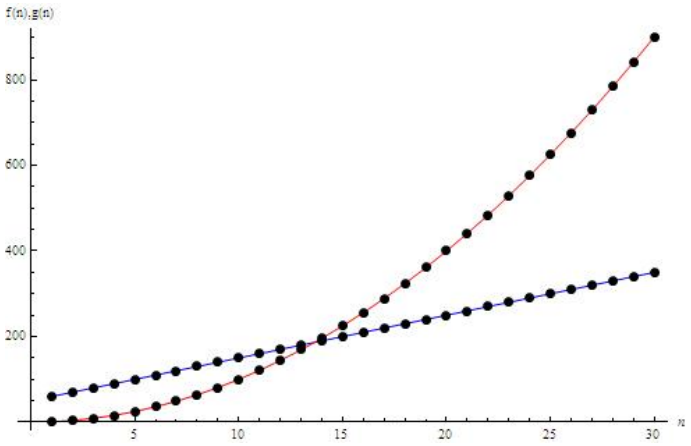
W badaniach złożoności obliczeniowej często mamy do czynienia z zagadnieniem porównywania tempa wzrostu funkcji ze zbioru $\mathbb{R}^{\mathbb{N}}$.

Definicja 6.7 *Dla ciągów $f, g \in \mathbb{R}^{\mathbb{N}}$ określamy*

$$f \trianglelefteq g \leftrightarrow (\exists C > 0)(\exists N \in \mathbb{N})(\forall n > N)(|f(n)| \leq C \cdot |g(n)|)$$

Relacja $f \trianglelefteq g$ jest często zapisywana jako $\mathbf{f = O(g)}$. Stosowane jest również oznaczenie $\mathbf{g = \Omega(f)}$. Nieformalnie mówiąc, prawdziwość relacji $f = O(g)$ oznacza, że funkcja f rośnie najwyżej, z dokładnością do stałej, tak szybko jak funkcja g.

Oczywiście $f \trianglelefteq f$ dla każdej funkcji $f \in \mathbb{R}^{\mathbb{N}}$. Łatwo można zauważyć, że rela-



Rysunek 6.1: Wykresy funkcji $f(n) = 50 + 10 \cdot n$, $g(n) = n^2$. Zachodzi między nimi zależnośc $f = O(g)$.

cja $\trianglelefteq$ jest przechodnia. Nie jest zaś ona słabo-antysymetryczna, o czym świadczy następujący przykład:

Przykład 6.6 *Niech $f(n) = n$ oraz $g(n) = 2n$. Wtedy $f \trianglelefteq g$ oraz $g \trianglelefteq f$.*

Definicja 6.8 *Strukturę (X, R) nazywamy **preporządkiem** jeśli R jest relacją zwrotną na zbiorze X i przechodnią.*

Struktura $(\mathbb{R}^{\mathbb{N}}, \trianglelefteq)$ jest więc preporządkiem. Pokażemy teraz że z dowolnego preporządku można w bardzo naturalny sposób skonstruować częściowy porządek.

Twierdzenie 6.3 *Załóżmy, że $(X, \sqsubseteq)$ jest preporządkiem. Niech*

$$x \equiv y \leftrightarrow (x \sqsubseteq y) \wedge (y \sqsubseteq x)\}.$$

Wtedy relacja

$$\preceq \quad = \{([a]_{\equiv}, [b]_{\equiv}) : a \in X \wedge b \in X \wedge a \sqsubseteq b\}$$

jest częściowym porządkiem na przestrzeni ilorazowej $X/\equiv$.

Dowód. Zauważmy najpierw, że jeśli $a \equiv a'$, $b \equiv b'$ oraz $a \sqsubseteq b$, to również $a' \sqsubseteq b'$. Ta obserwacja służy do stwierdzenia, że definicja relacji $\preceq$ jest poprawna, czyli, że nie zależy od wyboru reprezentantów klas abstrakcji.

Zwrotność i przechodniość relacji $\preceq$ wynika bezpośrednio ze zwrotności i przechodniości relacji $\sqsubseteq$. Załóżmy, że $[a]_\equiv \preceq [b]_\equiv$ oraz $[b]_\equiv \preceq [a]_\equiv$. Wtedy $a \sqsubseteq b$ oraz $b \sqsubseteq a$, a więc $a \equiv b$, czyli $[a]_\equiv = [b]_\equiv$. Zatem $\preceq$ jest relacją słabo-antysymetryczną. □

Metodę zastosowaną w powyższej konstrukcji można określić lakonicznie jako "*zlepienie kontrprzykładów na słabą-antysymetrię relacji* $\sqsubseteq$". Idąc tropem Twierdzenia 6.3 wprowadzimy teraz relację $\equiv_\Theta$ na zbiorze ciągów $\mathbb{R}^\mathbb{N}$:

Definicja 6.9 *Dla dowolnych $f, g \in \mathbb{R}^\mathbb{N}$ definiujemy*

$$f \equiv_\Theta g \leftrightarrow (f \trianglelefteq g) \wedge (g \trianglelefteq f)$$

Relacja równoważności $f \equiv_\Theta g$ jest często zapisywana jako $\mathbf{f = \Theta(g)}$ Jeśli $\mathbf{f = \Theta(g)}$, to mówimy, że funkcje f, g mają takie samo tempo wzrostu. Z Twierdzenia 6.3 wynika, że

$$[f]_{\equiv_\Theta} \trianglelefteq [g]_{\equiv_\Theta} \leftrightarrow f \trianglelefteq g$$

jest częściowym porządkiem na przestrzeni ilorazowej $\mathbb{R}^\mathbb{N} / \equiv_\Theta$.

Przykład 6.7 *Niech $n < m$ będą liczbami naturalnymi. Wtedy dla każdego $x > 1$ mamy $x^n < x^m$. Zatem $x^n \trianglelefteq x^m$. Chcemy pokazać, że $\neg(x^n \equiv_\Theta x^m)$. W tym celu wystarczy zauważyć, że jeśli $x^m < C \cdot x^n$, to $x^{m-n} < C$, a więc nierówność $x^m < C \cdot x^n$ zachodzi tylko dla skończonej ilości argumentów. Zatem*

$$x^1 \triangleleft x^2 \triangleleft x^3 \triangleleft \ldots x^n \triangleleft x^{n+1} \triangleleft \ldots,$$

gdzie $f \triangleleft g$ oznacza, że $f \trianglelefteq g$ oraz $\neg(f \equiv_\Theta g)$.

Przykład 6.8 *Rozważmy dowolny wielomian $w(x) = a_0 + a_1 x + \ldots + a_k x^k$ stopnia k. Wtedy $|w(x)| \leq \sum_{i=0}^k |a_i||x|^i$. Niech $C = \sum_{i=0}^k |a_i|$. Wtedy $|w(x)| \leq C \cdot k \cdot x^k$ dla $x \geq 1$. Zatem $w \trianglelefteq x^k$. Z drugiej strony*

$$w(x) = a_k \cdot x^k \cdot (\frac{a_0}{a_k x^k} + \frac{a_1}{a_k x^{k-1}} \ldots \frac{a_{k-1}}{a_k x} + 1).$$

Istnieje takie N że

$$|\frac{a_0}{a_k x^k} + \frac{a_1}{a_k x^{k-1}} \ldots \frac{a_{k-1}}{a_k x}| < 1$$

dla wszystkich $x > N$. Zatem dla dostatecznie dużych x mamy $|w(x)| \leq 2 \cdot |a_k| \cdot x^k$, czyli $w \trianglelefteq x^k$. Pokazaliśmy więc, że jeśli w jest wielomianem stopnia k-tego, to $w(x) \equiv_\Theta x^k$.

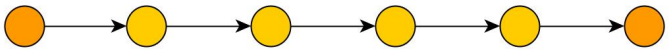
6.3 Liniowe Porządki

Zajmiemy się teraz ważną podklasę częściowych porządków. Uogólnia ona własności standardowych porządków na zbiorach $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{R}$.

Definicja 6.10 *Częściowy porządek $(X, \leq)$ nazywamy **liniowym porządkiem**, jeśli*

$$(\forall x, y \in X)(x \leq y \vee y \leq x).$$

Warunek występujący w definicji liniowego porządku nazywa się *spojnością* relacji. Oczywistymi przykładami liniowych porządków są już wspomniane struktury $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$.



Tak wyglądają skończone linowe porządki na zbiorze sześcio elementowym. Na rysunku nie umieściliśmy strzałek wynikających ze zwrotności oraz przechodniości.

Zauważmy, że w liniowych porządkach pojęcia elementów największych i maksymalnych oraz najmniejszych i minimalnych pokrywają się. Ponadto, jeśli $(X, \leq)$ jest liniowym porządkiem oraz $Y \subseteq X$, to $(Y, \leq \restriction Y)$ jest również porządkiem liniowym.

Porządek Leksykograficzny

Ustalmy niepusty zbiór Ω, który nazywać będziemy alfabetem. *Przestrzenią słów* nad alfabetem Ω nazywamy zbiór

$$\Omega^* = \bigcup_{n \in \mathbb{N}} \Omega^{\{0,\ldots,n-1\}}.$$

Jego elementy nazywamy słowami nad alfabetem Ω. Do zbioru tego zaliczamy również *słowo puste*, oznaczane symbolem ε. Zbiór Ω^* nazywany jest otoczką Kleeniego zbioru Ω.

Na przestrzeni słów istnieje naturalny częściowy porządek określony wzorem

$$\sigma \leq \eta \leftrightarrow \sigma \subseteq \eta.$$

Najmniejszym elementem w porządku $(\Omega^*, \leq)$ jest oczywiście słowo puste. Długość słowa σ oznaczamy przez $|\sigma|$. Jeśli $\sigma \leq \eta$ to $|\sigma| \leq |\eta|$. Na zbiorze Ω^* określona jest naturalna operacja zwana konkatenacją.

Definicja 6.11 *Niech $\sigma : \{0, \ldots, n\} \to \Omega$ oraz $\eta : \{0, \ldots, m\} \to \Omega$ będą słowami z Ω^*. Konkatenacją (złożeniem) słów σ i η nazywamy słowo*

$$\sigma\eta = \sigma \cup \{((i + n + 1, \eta(i)) : i < m\}.$$

Inaczej mówiąc, słowo $\sigma\eta$ powstaje w wyniku dopisania do końca słowa σ kolejnych liter słowa η, czyli, na przykład

$$(a, b, a, b, c)(x, x, y, z) = (a, b, a, b, c, x, x, y, z)\ .$$

Konkatencję słów σ i η oznacza się czasem symbolem $\sigma^\frown\eta$. Oczywiście $\sigma\varepsilon = \varepsilon\sigma = \sigma$ dla dowolnego słowa σ. Zauważmy, że dla słów $\sigma, \eta \in \Omega^*$ zachodzi następująca równoważność

$$\sigma \subseteq \eta \leftrightarrow (\exists \delta \in \Omega^*)(\eta = \sigma\delta).$$

Jeśli $\eta = \sigma\delta$, to mówimy, że σ jest prefiksem słowa η. Z tego powodu rozważany porządek $\leq$ nazywa się porządkiem prefiksowym na zbiorze słów. Pokażemy teraz w jaki sposób można ten porządek rozszerzyć do porządku liniowego.

Definicja 6.12 *Niech $\preceq$ będzie porządkiem liniowym alfabetu Ω.* ***Porządkiem leksykograficznym*** *generowanym przez porządek $\preceq$ nazywamy porządek $\preceq_{lex}$ na przestrzeni słów Ω^* określony wzorem*

$$\sigma \preceq_{lex} \eta \leftrightarrow (\sigma \leq \eta) \vee (\exists n \in dom(\sigma \cap \eta))(\sigma(n) \prec \eta(n) \wedge (\forall k < n)(\sigma(k) = \eta(k))).$$

Bezpośrednio z definicji wynika, że, porządek leksykograficzny rozszerza porządek prefiksowy na przestrzeni słów, czyli, że jeśli $\sigma \leq \eta$ to $\sigma \preceq_{lex} \eta$.

Twierdzenie 6.4 *Jeśli $\preceq$ jest porządkiem liniowym na alfabecie Ω , to porządek leksykograficzny $\preceq_{lex}$ jest porządkiem liniowym na przestrzeni słów Ω^*.*

Dowód. Dla dowolnego $\sigma \in \Omega^*$ mamy $\sigma \leq \sigma$, więc $\preceq_{lex}$ jest relacją zwrotną. Dla potrzeb tylko tego dowodu oznaczmy przez $pr(\sigma, \eta)$ najmniejszą taką liczbę naturalną n, że $\sigma(n) \neq \eta(n)$. Jeśli taka liczba n nie istnieje to położymy $pr(\sigma, \eta) = -1$. Zauważmy, że

$$pr(\sigma, \eta) < 0 \leftrightarrow (\sigma \preceq \eta) \vee (\eta \preceq \sigma).$$

Ponadto

$$\sigma \preceq_{lex} \eta \leftrightarrow (\sigma \leq \eta) \vee (\sigma(pr(\sigma, \eta)) \prec \eta(pr(\sigma, \eta))).$$

Załóżmy teraz, że $\sigma, \eta \in \Omega^*$ oraz $\sigma \preceq_{lex} \eta$ i $\eta \preceq_{lex} \sigma$. Niech $k = pr(\sigma, \eta)$. Jeśli $k = -1$, to $\sigma \leq \eta$ oraz $\eta \leq \sigma$, więc $\sigma = \eta$. Załóżmy więc, że $k > 0$. Wtedy $\sigma(k) \prec \eta(k)$ oraz $\eta(k) \prec \sigma(k)$, co jest niemożliwe. Relacja $\preceq_{lex}$ jest więc słabo-antysymetryczna.

Niech $\sigma, \eta, \rho \in \Omega^*$ oraz $\sigma \preceq_{lex} \eta$ i $\eta \preceq_{lex} \sigma$. Niech $k = pr(\sigma, \eta)$ i $l = pr(\eta, \rho)$. Załóżmy najpierw, że $k < 0$, czyli, że $\sigma \leq \eta$. Jeśli również $l < 0$ to $\eta \leq \rho$, więc $\sigma \leq \rho$, a zatem $\sigma \preceq_{lex} \rho$. Jeśli $l \geq 0$ i $l \geq |\sigma|$ to $\sigma \leq \rho$, jeśli zaś $l \geq 0$ i $l < |\sigma|$ to $[r(\sigma, \rho) = l > 0$. Załóżmy więc, że $k > 0$. Jeśli $l < 0$ to $pr(\sigma, \rho) = k > 0$. Jeśli zaś $l > 0$ to $pr(\sigma, \rho) = \min\{pr(\sigma, \eta), pr(\eta, \rho)\} > 0$. Relacja $\preceq_{lex}$ jest więc przechodnia.

Rozważmy teraz dowolne $\sigma, \eta \in \Omega^*$. Niech $k = pr(\sigma, \eta)$. Jeśli $k < 0$ to $\sigma \preceq_{lex} \eta$ lub $\eta \preceq_{lex} \sigma$. Jeśli zaś $k > 0$ to $\sigma(k) \prec \eta(k)$ lub też $\eta(k) \prec \sigma(k)$. W pierwszym przypadku $\sigma \preceq_{lex} \eta$ a w drugim $\eta \preceq_{lex} \sigma$. Relacja $\preceq_{lex}$ jest więc liniowym porządkiem zbioru Ω^*. □

Przykład 6.9 *Rozważmy zbiór liter $\Omega = \{A, B, C, D\}$ uporządkowany liniowy w sposób $A < B < C < D$. Rozważmy teraz porządek leksykograficzny na rodzinie słów $\{A, B, C, D\}^*$. Oto kilka nierówności:*

$$A < AA < AAA < \ldots < B < BA < BB < BBB < BC \ldots .$$

Widzimy, że rozważany porządek jest porządkiem słownikowym, czyli w tej właśnie kolejności uporządkowane są słowa w typowych słownikach i encyklopediach.

6.4 Lemat Kuratowskiego-Zorna

Niech $(X, \leq)$ będzie częściowym porządkiem. Podzbiór $A \subseteq X$ nazywamy *łańcuchem* jeśli relacja $\leq \restriction A$ jest liniowym porządkiem. Inaczej mówiąc, zbiór A jest łańcuchem, jeśli $(\forall a, b \in A)(a \leq b \vee b \leq a)$. Element $a \in X$ nazywamy *ograniczeniem górnym* zbioru A jeśli $(\forall x \in A)(x \leq a)$.

Następujące twierdzenie przyjmujemy na razie bez dowodu. W dalszej części tego wykładu omówimy środki które są niezbędne do jego udowodnienia.

Twierdzenie 6.5 (Lemat Kuratowskiego-Zorna) *Niech $(X, \leq)$ będzie takim częściowym porządkiem, że dla każdego łańcucha $A \subseteq X$ istnieje ograniczenie górne zbioru A. Wtedy w częściowym porządku $(X, \leq)$ istnieje element maksymalny.*

Lemat Kuratowskiego-Zorna będziemy oznaczać w dalszych rozważaniach przez $\mathbf{LKZ}$. Niech $\mathcal{A} = (A_t)_{t \in T}$ będzie dowolną rodziną zbiorów. Mówimy, że $\mathcal{A}$ jest rodziną zbiorów niepustych, jeśli $(\forall t \in T)(A_t \neq \emptyset)$. Mówimy również, że $\mathcal{A}$ jest rodziną zbiorów *parami rozłącznych* jeśli $(\forall s, t \in T)((s \neq t) \rightarrow (A_s \cap A_t = \emptyset)$. Każde rozbicie jakiegoś zbioru jest rodziną zbiorów parami rozłącznych i odwrotnie, każda rodzina $\mathcal{A}$ zbiorów niepustych parami rozłącznych jest rozbiciem zbioru $\bigcup \mathcal{A}$. Zbiór S nazywamy *selektorem* rodziny zbiorów $(A_t)_{t \in T}$, jeśli $(\forall t \in T)(\exists x)(S \cap A_t = \{x\})$ oraz $S \subseteq \bigcup_{t \in T} A_t$.

Aksjomat 6.1 *Aksjomatem Wyboru nazywamy następujące zdanie:*

„każda rodzina zbiorów niepustych parami rozłącznych ma selektor”.

Aksjomat wyboru oznaczany jest przez $\mathbf{AC}$[1]. Odgrywa on istotną rolę w wielu rozumowaniach matematycznych. Potrzebny jest on, na przykład, do udowodnienia tego, że definicje Heinego i Cauchy'ego ciągłości funkcji są równoważne. Konieczny jest również do dowodu tego, że każda przestrzeń liniowa posiada bazę. Pokażemy teraz jedną z równoważnych wersji $\mathbf{AC}$.

Twierdzenie 6.6 *Następujące zdania są równoważne:*

1. $\mathbf{AC}$*,*
2. *dla dowolnej rodziny $(A_t)_{t \in T}$ zbiorów niepustych produkt $\prod_{t \in T} A_t$ jest zbiorem niepustym.*

Dowód. Załóżmy najpierw że Aksjomat Wyboru jest prawdziwy oraz niech $(A_t)_{t \in T}$ będzie dowolną zbiorów niepustych. Rozważmy rodzinę zbiorów $\mathcal{B} = \{\{t\} \times A_t : t \in T\}$. Jest to rodzina zbiorów niepustych. Z Aksjomatu Wyboru wynika, że istnieje jakiś selektor S rodziny $\mathcal{B}$. Każdy selektor rodziny $\mathcal{B}$ jest elementem $\prod_{t \in T} A_t$.
Załóżmy teraz, że prawdziwe jest zdanie (2) oraz, że $(A_t)_{t \in T}$ jest rodziną zbiorów niepustych, parami rozłącznych. Niech $f \in \prod_{t \in T} A_t$. Wtedy zbiór $rng(f)$ jest selektorem rodziny $(A_t)_{t \in T}$. □

Pokażemy teraz pierwsze zastosowanie Lematu Kuratowskiego-Zorna.

Twierdzenie 6.7 *Lemat Kuratowskiego-Zorna implikuje Aksjomat Wyboru.*

[1] AC jest skrótem od “Axiom of Choice”

Dowód. Niech $(A_t)_{t\in T}$ będzie rodziną zbiorów niepustych parami rozłącznych. Niech $S = \bigcup_{t\in T} A_t$. Rozważmy zbiór

$$P = \{X \in P(S) : (\forall t \in T)(A_t \cap X = \emptyset \vee (\exists x)(A_t \cap X = \{x\})).$$

Pokażemy najpierw, że częściowy porządek $(P, \subseteq\restriction P)$ spełnia założenia Lematu Kuratowskiego - Zorna. Niech $A \subseteq P$ będzie łańcuchem. Wtedy $(\forall X \in A)(X \subseteq \bigcup A)$. Wystarczy więc pokazać, że $\bigcup A \in X$. Załóżmy, że istnieją takie $t \in T)$ oraz elementy x i y takie, że $x \neq y$ oraz $\{x, y\} \subseteq A_t$. Niech $X \in A$ oraz $Y \in A$ będą takie, że $x \in X$ oraz $y \in Y$. Lecz A jest liniowo uporządkowany przez zawieranie. Zatem $X \subseteq Y$ lub $Y \subseteq X$. Gdyby prawdziwy był pierwszy przypadek, to $x, y \in Y$, a więc $\{x, y\} \subseteq Y \cap A_t$, co jest niemożliwe. Podobnie wykluczamy przypadek drugi. Tak więc oba przypadki są niemożliwe. Zatem $\bigcup A \in P$.

Pokazaliśmy więc, że porządek $(P, \subseteq\restriction P)$ spełnia założenia Lematu Kuratowskiego - Zorna. Niech $S \in P$ będzie jego elementem maksymalnym. Pokażemy, że $(\forall t \in T)(\exists x)(A_t \cap S = \{x\})$. Załóżmy bowiem, że istnieje takie $t_0 \in T$, że $A_{t_0} \cap S = \emptyset$. Weźmy dowolny element $x_0 \in A_{t_0}$ i rozważmy zbiór $S' = S \cup \{x_0\}$. Wtedy również $S' \in P$, co jest sprzeczne z tym, że S jest elementem maksymalnym. □

6.5 Dobre porządki

Dobre porządki są szczególnymi porządkami liniowymi, których własności są dosyć zbliżone do własności naturalnego porządku liczb naturalnych.

Definicja 6.13 *Porządek liniowy $(X, \leq)$ nazywamy dobrym porządkiem, jeśli*

$$(\forall A \subseteq X)(A \neq \emptyset \to (\exists a \in A)(\forall x \in A)(a \leq x)).$$

Inaczej mówiąc, porządek liniowy jest dobrym porządkiem jeśli każdy jego niepusty podzbiór ma element najmniejszy. W szczególności, jeśli za podzbiór weźmiemy cały zbiór X, to widzimy, że w dobrym porządku, o ile jest on niepusty, musi istnieć element najmniejszy.

Rozważmy teraz dowolny element a dobrego porządku $(X, \leq)$. Załóżmy, że a nie jest elementem największym. Wtedy zbiór $\{x \in X : a < x\}$ jest niepusty, a więc ma element najmniejszy. Zatem istnieje najmniejszy element większy od elementu a. Powyższa własność wyraźnie odróżnia zbiór liczb wymiernych od dobrych porządków. Jeśli bowiem $a \in \mathbb{Q}$ i $b \in \mathbb{Q}$ jest dowolną liczbą większą od a, to liczba $\frac{a+b}{2}$ jest większa od a i mniejsza od b. W liczbach wymiernych żadna liczba nie ma bezpośrednio po niej większej liczby. Ta sama uwaga dotyczy zbioru liczb rzeczywistych $\mathbb{R}$.

Twierdzenie 6.8 *Każdy skończony liniowy porządek jest dobrym porządkiem.*

Dowód. Załóżmy że A jest niepustym podzbiorem takiego porządku. Rozważmy dowolny element a_0 ze zbioru A. Jeśli a_0 nie jest elementem najmniejszym zbioru A, to w zbiorze A istnieje element a_1 mniejszy od a_0. Gdyby a_1 nie był elementem najmniejszym, to w zbiorze A znaleźlibyśmy element a_3 mniejszy od a_2. Gdyby powyższa procedura niegdy się nie skończyła, to zbudowalibyśmy nieskończony ciąg różnych elementów zbioru A. A to jest sprzeczne ze skończonością rozważanego porządku.

□

Przykładem dobrego porządku jest oczywiście $(\mathbb{N}, \leq)$. Porządek ten charakteryzuje się tym, że jest nieskończony oraz, że dla każdego $n \in \mathbb{N} \setminus \{0\}$ istnieje element bezpośrednio mniejszy od n, czyli taki, że pomiędzy nim a n nie ma żadnego innego elementu. Dla liczby $n > 0$ takim elementem jest oczywiście liczba naturalna $n - 1$. Mówimy, że dobry porządek $(X, \preceq)$ ma typ porządkowy ω jeśli jest on izomorficzny z $(\mathbb{N}, \leq)$.

Przykład 6.10 *Niech $X = \{1 - \frac{1}{n+1} : n \in \mathbb{N}\}$. Rozważmy obcięcie $\leq \restriction X$ naturalnego porządku ze zbioru liczb rzeczywistych do zbioru X. Wtedy funkcja $f(n) = 1 - \frac{1}{n+1}$ określa izomorfizm pomiędzy $(\mathbb{N}, \leq)$ i zbiorem $(X, \leq \restriction X)$. Zatem częściowy porządek $(X, \leq \restriction X)$ ma typ porządkowy ω.*

Twierdzenie 6.9 *Załóżmy, że $(W_1, \leq_1)$, $(W_2, \leq_2)$ są dobrymi porządkami oraz, że $W_1 \cap W_2 = \emptyset$. Niech*

$$\leq = \leq_1 \cup (W_1 \times W_2) \cup \leq_2 .$$

Wtedy $\leq$ jest dobrym porządkiem na zbiorze $W_1 \cup W_2$.

Dowód. Niech A będzie niepustym podzbiorem $W_1 \cap W_2$. Jeśli $A \cap W_1 \neq \emptyset$, to w A istnieje $\leq_1$-minimalny element. W przeciwnym razie $A \cap W_2 \neq \emptyset$ i wtedy $\leq_2$-minimalny element zbioru A jest jego $\leq$-minimalnym elementem. □

Zbudowany w tym twierdzeniu porządek powstał przez ustawienie wszystkich elementów zbioru W_2 za elementami zbioru W_1.

Przykład 6.11 *Niech $X = \{1 - \frac{1}{n+1} : n \in \mathbb{N}\}$ będzie zbiorem rozważanym w poprzednim przykładzie oraz niech $Y = \{2 - \frac{1}{n+1} : n \in \mathbb{N}\}$. Oczywiście $(Y, \leq \restriction X)$. Konstrukcja z poprzedniego twierdzenia zastosowana do porządków X i Y daje nam porządek izomorficzny z $(X \cup Y, \restriction (X \cup Y))$. Jest to więc dobry porządek. Typ porządkowy tego zbioru oznaczamy przez $\omega + \omega$.*

Twierdzenie 6.10 *Załóżmy, że $(X, \leq_1)$ i $(Y, \leq_2)$ są dobrymi porządkami. Wtedy relacja $\leq$ określona na zbiorze $X \times Y$ określona wzorem*

$$(x, y) \leq (x', y') \leftrightarrow (x <_1 x') \vee (x = x' \wedge y \leq_2 y')$$

jest dobrym porządkiem.

Dowód. Sprawdzenie tego, że relacja $\leq$ jest częściowym porządkiem na zbiorze $X \times Y$ pozostawiamy czytelnikowi jako proste zadanie. Niech A będzie niepustym podzbiorem zbioru $X \times Y$. Pokażemy w jaki sposób możemy znaleźć $\leq$-najmniejszy element zbioru A. Niech $A_1 = \{x \in X : (\exists y)((x, y) \in A\}$. Wtedy A_1 jest niepustym elementem zbioru X. Niech a będzie $\leq_1$ najmniejszym elementem zbioru A. Niech następnie $B = \{y \in Y : (a, y) \in A\}$. Wtedy B jest niepustym podzbiorem zbioru Y. Niech b będzie $\leq_2$-najmniejszym elementem zbioru B. Wtedy para (a, b) jest najmniejszym elementem zbioru A. □

Z ostatniego twierdzenia wynika, że na zbiorze $\mathbb{N} \times \mathbb{N}$ istnieje naturalny dobry porządek. Ustawia on elementy w następującej kolejności

$$(0,0) \leq (0,1) \leq (0,2) \leq \ldots \leq (1,0) \leq (1,1) \leq (1,2) \leq \ldots \leq (2,0) \leq \ldots$$

Typ porządkowy $\mathbb{N} \times \mathbb{N}$ z powyższym porządkiem oznaczamy symbolem $\omega \cdot \omega$.

Twierdzenie 6.11 *Jeśli $(X, \leq)$ jest dobrym porządkiem, to nie istnieje funkcja $f : \mathbb{N} \to X$ taka, że $f(n+1) < f(n)$ dla wszystkich liczb naturalnych n.*

Dowód. Załóżmy, że $f : \mathbb{N} \to X$ jest taką funkcją, że $(\forall n \in \mathbb{N})(f(n+1) < f(n))$. Niech $A = rng(f)$. Wtedy A jest zbiorem niepustym. Posiada więc element $\leq$-najmniejszy. Niech a będzie takim elementem. Wtedy $a = f(n)$ dla pewnej liczby naturalnej n. Lecz $f(n+1) < a$ oraz $f(n+1) \in A$, co jest sprzeczne z wyborem elementu a. □

Przykład 6.12 *Rozważmy następującą funkcję która dla zadanych argumentów A i B wyznacza ich największy wspólny dzielnik:*

```
function NWD(A,B:integer):integer;
begin
  while A<>B do
  if A>B then A:= A-B
         else B:= B-A;
  NWD:= A;
end;
```

Łatwo można uzasadnić, że jeśli algorytm ten skończy swoje działanie, to da w wyniku największy wspólny dzielnik liczb A i B. Wynika to mianowicie z tego, że $NWD(A, A)$ = A oraz, że jeśli $A > B$ to $NWD(A, B) = NWD(A - B, B)$. Pokażemy, że dla dowolnych dwóch liczb naturalnych A i B algorytm ten skończy swoje działanie po skończonej liczbie kroków. Rozważmy porządek $\preceq$ określony na $\mathbb{N} \times \mathbb{N}$ wzorem

$$(n, m) \preceq (n'm') \leftrightarrow (n < n') \vee (n = n \wedge m \leq m').$$

Z Twierdzenia 6.10 wynika, że jest on dobrym porządkiem na $\mathbb{N} \times \mathbb{N}$. Załóżmy, że algorytm ten na pewnej parze liczb naturalnych (A, B) nie kończy swojego działania. Niech (A_n, B_n) oznacza wartość zmiennych (A, B) w n-tym kroku iteracji. Wtedy $(A_{n+1}, B_{n+1}) \prec (A_n, B_n)$ dla każdego $n \in \mathbb{N}$, co jest sprzeczne z Twierdzeniem 6.11.

Aksjomat 6.2 *Zasadą dobrego uporządkowania nazywamy zdanie*

„na każdym zbiorze istnieje dobry porządek”.

Zasadę dobrego uporządkowania będziemy oznaczać w dalszych rozważaniach symbolem **WO** [2].

Twierdzenie 6.12 *Zasada dobrego uporządkowania implikuje Aksjomat Wyboru.*

Dowód. Niech $\mathcal{A} = (A_t)_{t\ inT}$ będzie dowolną rodziną zbiorów niepustych, parami rozłącznych. Niech $U = \bigcup_{t \in T} A_t$. Z Zasady dobrego uporządkowania wynika istnienie dobrego porządku $\preceq$ na zbiorze U. Za pomocą tego porządku zdefiniujemy selektor rodziny $\mathcal{A}$. W tym celu definiujemy funkcję $f : T \to U$

$$f(t) = \preceq - \text{najmniejszy element zbioru } A_t.$$

Z rozłączności rodziny $\mathcal{A}$ wynika, że zbiór $rng(f)$ jest szukanym selektorem. □

[2] WO jest skrótem od „Well-Ordering Principle”

Przyjrzyjmy się teraz rozważanym do tej pory zdaniom **AC**, **LKZ** oraz **WO**. Pokazaliśmy do tej pory, że $\mathbf{WO} \to \mathbf{AC}$ oraz, że $\mathbf{LKZ} \to \mathbf{AC}$. Okazuje się, że są one równoważne.

Twierdzenie 6.13 *Zdania* **AC**, **LKZ** *i* **WO** *są równoważne.*

Nie będziemy dowodzili teraz tego twierdzenia, gdyż nie posiadamy jeszcze dostatecznie silnych środków. Naturalny jego dowód wykorzystuje technikę indukcji pozaskończonej i jest przedstawiony w Dodatku D tej książki.

6.6 Ćwiczenia i zadania

Ćwiczenie 6.1 *Pokaż, że jeśli w częściowym porządku istnieje element największy, to jest on jedynym elementem największym i jest elementem maksymalnym*

Ćwiczenie 6.2 *Pokaż, że jeśli R i S sa częściowymi porządkami, to ich przekrój $R \cap S$ też jest częściowym porządkiem. Czy ich suma $R \cup S$ musi być częściowym porządkiem?*

Ćwiczenie 6.3 *Pokaż, że $(\mathbb{N} \setminus \{0\}, |)$ jest częściowym porządkiem. Znajdź w nim element najmniejszy. Znajdź elementy minimalne w częściowym porządku $(\mathbb{N} \setminus \{0, 1\}, |)$.*

Ćwiczenie 6.4 *Dla danych liczb $n, m \in \mathbb{N}$ podaj przykład częściowego porządku który ma dokładnie n elementów minimalnych oraz m elementów maksymalnych.*

Ćwiczenie 6.5 *Niech (X, R) będzie częściowym porządkiem. Pokaż, że relacja R^{-1} jest również częściowym porządkiem na zbiorze X. Jakie są związki pomiędzy elementami maksymalnymi, minimalnymi, największymi i najmniejszymi w tych dwóch częściowych porządkach?*

Ćwiczenie 6.6 *Pokaż, że porządki $(P(A), \subseteq)$ i $(\{0,1\}^A, \leq^*)$, gdzie $f \leq^* g \leftrightarrow (\forall a \in A)(f(a) \leq g(a))$, są izomorficzne.*

Ćwiczenie 6.7 *Na zbiorze $\mathbb{R}^2$ rozważamy relację $\preceq$ zadaną formułą*

$$((x, y) \preceq (x'y')) \leftrightarrow (x \leq x') \wedge (y \leq y') \,.$$

Pokaż, że relacja ta jest częściowym porządkiem. Niech $K = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$. Wyznacz elementy minimalne zbioru K. Dla ustalonego punktu $(a, b) \in \mathbb{R}^2$ wyznacz zbiory $\{(x, y) \in \mathbb{R}^2 : (a, b) \leq (x, y)\}$, $\{(x, y) \in \mathbb{R}^2 : (x, y) \leq (a, b)\}$ oraz $\{(x, y) \in \mathbb{R}^2 : \neg((a, b) \leq (x, y)) \wedge \neg((x, y) \leq (a, b))\}$.

Ćwiczenie 6.8 *Rozważmy częściowy porządek $(\mathbb{R}, \leq)$. Niech $A, B \subseteq \mathbb{R}$ będą zbiorami ograniczonymi. Pokaż, że $\inf(A) = -\sup(\{-a : a \in A\})$ oraz $\sup(\{a + b : a \in A \wedge b \in B\}) = \sup(A) + \sup(B)$.*

Ćwiczenie 6.9 *Niech $\Omega = \{a, b\}$ oraz niech X będzie zbiorem wszystkich słów z Ω^* długości nie większej niż 3. Wypisz elementy tego zbioru w porządku leksykograficznym.*

Ćwiczenie 6.10 *Pokaż, że $x^n \lhd 2^x$ dla dowolnej liczny naturalnej n. Pokaż, że w częściowym porządku $(\mathbb{R}^{\mathbb{N}}/ \equiv_\Theta, \trianglelefteq)$ nie istnieją elementy maksymalne.*

Ćwiczenie 6.11 *Rozważamy częściowy porządek $(\{2, \ldots, 30\}, |)$, gdzie $|$ oznacza relację podzielności. Ile jest elementów minimalnych oraz ile jest elementów maksymalnych w tym częściowym porządku?*

Ćwiczenie 6.12 *Niech Ω będzie niepustym zbiorem. Na zbiorze słów Ω^* definiujemy relację $\sigma \approx \eta \leftrightarrow |\sigma| = |\eta|$, gdzie $|x|$ oznacza długość słowa x. Pokaż, że $\approx$ jest relacją równoważności. Wyznacz jej klasy abstrakcji.*

Zadanie 6.1 *Pokaż, że dla dowolnej liczby naturalnej n istnieje zbiór liczb naturalnych T taki, że częściowe porządki $(P(\{1, .., n\}), \subseteq)$ oraz $(T, |)$ są izomorficzne*

Zadanie 6.2 *Niech L_1 oznacza zbiór wszystkich zdań zbudowanych z jednej zmiennej zdaniowej p. Na zbiorze L_1 określamy relację $\varphi \leq \psi \leftrightarrow \models (\varphi \to \psi)$. Pokaż, że $\leq$ jest preporządkiem. Niech $\equiv$ będzie relacją równoważności wyznaczoną przez ten preporządek (patrz Twierdzenie 6.3) oraz niech $\preceq$ będzie częściowym porządkiem na $L_1/ \equiv$ wyznaczonym przez $\leq$. Pokaż, że porządek $(L_1/ \equiv, \leq)$ jest izomorficzny z porządkiem $\mathcal{P}(\{0, 1\})$.*

Zadanie 6.3 *Zbadaj tempa wzrostu funkcji wymiernych w porządku $\trianglelefteq$ zdefiniowanym formułą $(f \trianglelefteq g) \leftrightarrow (f = O(g))$.*

Zadanie 6.4 *Czy porządek $\trianglelefteq$ z poprzedniego zadania jest liniowy? Pokaż, że jeśli $f \lhd g$ to istnieje funkcja h taka, że $f \lhd h \lhd g$.*

Zadanie 6.5 *Załóżmy, że $(X, \leq)$ jest dobrym porządkiem o następujących własnościach: nie ma w nim elementu największego, dla każdego elementu, z wyjątkiem najmniejszego, istnieje element bezpośrednio go poprzedzający. Pokaż, że porządek $(X, \leq)$ jest izomorficzny z liczbami naturalnymi z naturalnym porządkiem.*

Zadanie 6.6 *Załóżmy, że $f : A \to B$ jest surjekcją. Pokaż, korzystając z Aksjomatu Wyboru, że istnieje taka funkcja $g : B \to A$, że $(\forall y \in B)(f(g(y)) = y)$.*

Zadanie 6.7 *Niech $(x_n, y_n)_{n\in\mathbb{N}}$ będzie dowolnym ciągiem liczb naturalnych. Pokaż, że istnieją liczby $n, m \in \mathbb{N}$ takie, że $n < m$ oraz $x_n \leq x_m$ i $y_n \leq y_m$.*

Zadanie 6.8 *Podaj przykład injekcji $f : \{0, 1\}^* \times \{0, 1\}^* \to \{0, 1\}^*$.*

Zadanie 6.9 *W którym momencie dowodu równoważności definicji ciągłości Heinego i Cauchy'ego korzystamy z Aksjomatu Wyboru?*

Zadanie 6.10 *Na zbiorze $X = \mathbb{R}^2$ rozważamy relację równoważności określoną wzorem $x \approx y \leftrightarrow (\exists t \neq 0)(tx = y)$. Znajdź selektor rodziny $X/ \approx$.*

Zadanie 6.11 *Pokaż, że w każdej przestrzeni liniowej istnieje baza. Wskazówka: skorzystaj z Lematu Kuratowskiego Zorna.*

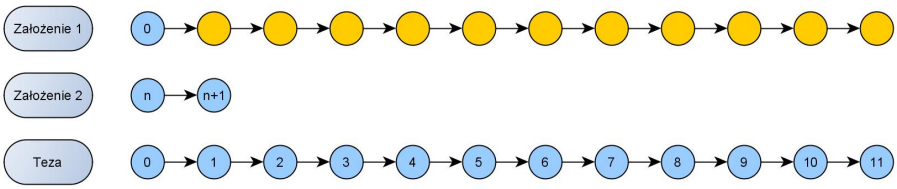
Zadanie 6.12 *Niech $(X, \leq)$ będzie częściowym porządkiem. Pokaż, że istnieje porządek liniowy $\preceq$ na zbiorze X taki, że $\leq \quad \subseteq \quad \preceq$.*

7 Indukcja Matematyczna

W trakcie tego wykładu omówimy różne warianty indukcji matematycznej oraz ich zastosowania do badania mocy zbiorów skończonych. Ten dział matematyki nazywa się Kombinatoryka Skończoną.

Twierdzenie 7.1 (Zasada Indukcji Matematycznej) *Niech $\varphi(x)$ będzie funkcją zdaniową określoną dla liczb naturalnych. Wtedy jeśli $\varphi(0)$ oraz $(\forall n \in \mathbb{N})(\varphi(n) \to \varphi(n+1))$, to $(\forall n \in \mathbb{N})\varphi(n)$.*

Dowód. Załóżmy, że $\varphi(0)$ oraz $(\forall n \in \mathbb{N})(\varphi(n) \to \varphi(n+1))$, oraz, że istnieje takie n, że $\neg\varphi(n)$. Niech $A = \{x \in \mathbb{N} : \neg\varphi(x)\}$. Zbiór A jest niepusty, gdyż $n \in A$. Ponieważ $(\mathbb{N}, \leq)$ jest dobrym porządkiem, więc w zbiorze A istnieje element najmniejszy. Niech nim będzie liczba a. Wtedy $a \neq 0$, gdyż zdanie $\varphi(0)$ z założenia jest prawdziwe. Zatem $a > 0$. Niech $b = a - 1$. Wtedy $b \notin A$, gdyż a jest najmniejszym elementem zbioru A. A więc zdanie $\varphi(b)$ jest prawdziwe. Lecz wtedy, na mocy założenia o φ zdanie $\varphi(b+1)$ również prawdziwe. Lecz $b+1 = a$, więc zdanie $\varphi(a)$ jest prawdziwe, co jest sprzeczne z tym, że $a \in A$. □



Z Zasady Indukcji Matematycznej można wyprowadzić szereg jej form pokrewnych. Na przykład, "jeśli $\varphi(a)$ oraz $(\forall n \in \mathbb{N})(\varphi(n) \to \varphi(n+1))$, to $(\forall n \geq a)\varphi(n)$" lub "jeśli $\varphi(0) \wedge \varphi(1)$ oraz $(\forall n \in \mathbb{N})(\varphi(n) \to \varphi(n+2))$, to $(\forall n \in \mathbb{N})\varphi(n)$". A oto inna forma Zasady Indukcji Matematycznej: "jeśli $\varphi(0)$ oraz $(\forall n \in \mathbb{N})((\forall k < n)\varphi(n) \to \varphi(n))$, to $(\forall n \in \mathbb{N})\varphi(n)$".

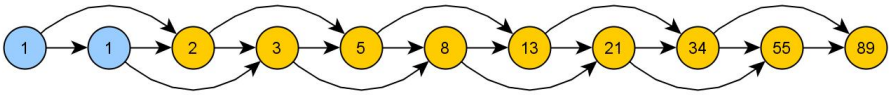
Zdarzają się rozumowania oparte o jeszcze bardziej skomplikowany schemat: "jeśli $\varphi(0,0)$ oraz z prawdziwości zdania $\varphi(n,m)$ wynika prawdziwość zdań $\varphi(n+1,m)$ oraz $\varphi(n,m+1)$, to wtedy dla wszystkich liczb naturalnych n, m zdanie $\varphi(n,m)$ jest prawdziwe".

7.1 Definicje rekurencyjne

Dużą klasę funkcji o dziedzinie równej $\mathbb{N}$ definiuje się za pomocą następującego schematu:

1. określamy wartość funkcji dla liczby $n = 0$,
2. zakładając, że wyznaczone są już wartości $f(0), \ldots f(n)$ określa się metodę wyznaczenia wartości $f(n+1)$.

Przykładem takiej funkcji jest *silnia*. Zdefiniować ją możemy mianowicie następująco: przyjmujemy, że $0! = 1$ oraz określamy $(n+1)! = n! \cdot (n+1)$. Rozważmy inny przykład. *Ciągiem Fibonacciego* nazywamy ciąg $(F_n)_{n\geq 1}$ określony następująco: $F_0 = F_1 = 1$ oraz $F_n = F_{n-2} + F_{n-1}$. Liczby F_n nazywamy liczbami Fibbonacciego. Wzór ten pozwala nam wyznaczyć wartości F_n dla każdego konkretnego n. Na przykład $F_2 = F_0 + F_1 = 1 + 1 = 2$, $F_3 = F_1 + F_2 = 1 + 2 = 3$, $F_4 = F_2 + F_3 = 2 + 3 = 5$ itd. Zauważmy, że w pierwszym przypadku do wyznaczenia wartości $f(n+1)$ wystarczała nam znajomość wartości $f(n)$. W drugim zaś przypadku potrzebowaliśmy znajomość wartości $f(n)$ oraz $f(n-1)$.



Przypomnijmy, że przez $\Omega^\star$ oznaczamy zbiór wszystkich skończonych ciągów elementów zbioru Ω. Sformułujemy teraz i udowodnimy twierdzenie, które gwarantuje nam poprawność tego typu definicji.

Twierdzenie 7.2 *Niech Λ oraz B są niepustymi zbiorami. Niech $f : \Lambda \to B$ oraz $g : \Lambda \times B^\star \times \mathbb{N} \to B$. Wtedy istnieje dokładnie jedna funkcja $h : \Lambda \times \mathbb{N} \to B$ taka, że*

$$\begin{cases} h(a,0) & = & f(a) \\ h(a,n+1) & = & g(a,(h(a,0),\ldots,h(a,n)),n) \end{cases}$$

Dowód. Oznaczmy przez $\mathcal{F}$ rodzinę złożoną wszystkich funkcji x o następujących własnościach:

1. $dom(x) \subseteq \Lambda \times \mathbb{N}$,
2. $rng(x) \subseteq B$,
3. $(a,n) \in dom(x) \to (\forall k < n)((a,k) \in dom(x))$,
4. $(a,0) \in dom(x) \to x((a,0)) = f(a)$,
5. $(a,n+1) \in dom(x) \to x((a,n+1)) = g(a,(x(a,0),\ldots,x(a,n)),n)$.

Indukcją względem n przy ustalonym $a \in \Lambda$ pokażemy najpierw, że $(\forall a \in \Lambda)(\forall n \in \mathbb{N})(\exists x \in \mathcal{F})((a,n) \in dom(x))$. Ustalmy bowiem $a \in \Lambda$. Wtedy $\{((a,0), f(a))\} \in \mathcal{F}$. Załóżmy teraz, że istnieje $x \in PS$ taki, że $(a,n) \in dom(x)$. Niech $y = x \restriction (\{(a,0),\ldots,(a,n)\})$. Wtedy $y \in \mathcal{F}$ oraz

$$y \cup \{(a,n+1), g(a,(x(a,0),\ldots,x(a,n)),n)\} \in \mathcal{F}.$$

Zatem w zbiorze $\mathcal{F}$ istnieje taki element z, że $(a,n+1) \in dom(z)$.

Indukcją względem n przy ustalonym $a \in \Lambda$ pokazujemy następnie, że jeśli $x, y \in \mathcal{F}$ oraz $(a,n) \in dom(x) \cap dom(x)$ to $x(a,n) = y(a,n)$. Ustalmy zatem $a \in \Lambda$. Teza jest oczywiście prawdziwa dla $n = 0$. Załóżmy następnie, że teza jest prawdziwa

dla wszystkich liczb $i \leq n$. Niech $(a, n+1) \in dom(x) \cap dom(y)$. Wtedy $(a, i) \in dom(x) \cap dom(y)$ dla wszystkich $i \leq n$. Z założenia indukcyjnego wynika, że

$$x(a, n+1) = g(a, (x(a,0), \ldots, x(a,n)), n) =$$

$$g(a, (y(a,0), \ldots, y(a,n)), n) = y(a, n+1)$$

Z drugiej własności rodziny $\mathcal{F}$ wynika, że $h = \bigcup \mathcal{F}$ jest funkcją a z pierwszej własności, że $dom(h) = \Lambda \times \mathbb{N}$. Ponadto h spełnia własności (3) i (4), a więc jest szukaną funkcją.

Jednoznaczność wynika zaś z tego, że jeśli h_1 i h_2 są funkcjami spełniającymi warunki twierdzenia, to $h_1 \in \mathcal{F}$ i $h_2 \in \mathcal{F}$, a więc zachodzi dla nich druga z udowodnionych własności rodziny (F). □

Przykład 7.1 *Niech $S : \mathbb{N} \to \mathbb{N}$ będzie następnikiem, czyli funkcją określoną wzorem $S(n) = n + 1$. W następujący sposób można zdefiniować dodawanie w liczbach naturalnych:*

1. $a + 0 = a$,
2. $a + (n + 1) = S(a + n)$

Funkcja ta (dodawanie) powstaje według schematu omówionego wyżej. Funkcją f jest $Id_{\mathbb{N}}$. Funkcja g jest zdefiniowana wzorem $g(a, (x_0, \ldots, x_n), n) = S(x_n)$.

Przykład 7.2 *W następujący sposób można zdefiniować mnożenie w liczbach naturalnych:*

1. $a \cdot 0 = 0$,
2. $a \cdot (n + 1) = a \cdot n + a$

Funkcja ta (mnożenia) również powstaje według schematu omówionego wyżej. Funkcją f jest stale równa zeru. Funkcja g jest zaś zdefiniowana wzorem

$$g(a, (x_0, \ldots, x_n), n) = x_n + a.$$

Przykład 7.3 *W następujący sposób można zdefiniować potęgowanie w liczbach naturalnych:*

1. $a^0 = 1$,
2. $a^{n+1} = a^n \cdot a$

Uogólnienie powyższych przykładów prowadzi do w naturalny sposób do konstrukcji rodziny funkcji pierwotnie rekurencyjnych, które są najprostszymi funkcjami obliczalnymi. Badaniem ich własności zajmuje się Teoria Obliczalności.

7.2 Zbiory skończone

W rozdziale tym zajmować się będziemy zbiorami skończonymi. Rozpoczniemy od wprowadzenia pojęcia równoliczności.

Definicja 7.1 *Mówimy, że zbiory A i B są **równoliczne**, co zapisujemy jako $|A| = |B|$, jeśli istnieje bijekcja $f : A \to B$.*

Rownoliczność dwóch zbiorów jest formalizacją pojęcia "posiadanie takiej samej ilości elementów". Zauważmy, że każdy zbiór jest równoliczny z samym sobą, gdyż identyczność $Id_A = \{(x, x) : x \in A\}$ jest bijekcją. Jeśli $|A| = |B|$, to istnieje bijekcja $f : A \to B$. Wtedy funkcja $f^{-1} : B \to A$ jest również bijekcją, a więc $|B| = |A|$. Przypomnijmy, że złożenie bijekcji jest bijekcją, a więc jeśli $|A| = |B|$ oraz $|B| = |C|$ to $|A| = |C|$. Tak więc pojęcie równoliczności posiada te same własności, co relacja równoważności: jest zwrotne, symetryczne i przechodnie. Nie jest jednak relacją z powodu twierdzenia Russela (patrz Twierdzenie 2.1).

Będziemy mówili, że zbiór A jest skończony, jeśli istnieje liczba naturalna n oraz elementy a_1,...,a_n takie, że $A = \{a_1, \ldots, a_n\}$. Bardziej formalnie ujmuje to następująca definicja.

Definicja 7.2 *Mówimy, że zbiór A jest mocy $n \in \mathbb{N}$, co zapisujemy $|A| = n$, jeśli istnieje bijekcja $f : \{0, \ldots, n-1\} \xrightarrow[1-1]{na} A$.*

W szczególności, zdanie $|A| = 0$ jest równoważne temu, że $A = \emptyset$. Podobnie, $|A| = 1$ wtedy i tylko wtedy, gdy istnieje element a taki, że $A = \{a\}$. Zbiór A nazywamy **skończonym**, jeśli $|A| = n$ dla pewnej liczby naturalnej n a liczbę n nazywamy jego mocą.

Warto zauważyć, że jeśli $|A| = n$ oraz istnieje bijekcja $g : A \to B$, to również $|B| = n$. Rzeczywiście, jeśli $f : \{0, \ldots, n\} \to A$ jest bijekcją, to superpozycja $g \circ f : \{0, \ldots, n\} \to B$ jest również bijekcją.

Lemat 7.1 *Załóżmy, że $n \in \mathbb{N}$, $|A| = n$ oraz, że $B \subseteq A$ i $B \neq A$. Wtedy istnieje liczba naturalna $k < n$ taka, że $|B| = k$.*

Dowód. Dla liczby $n = 0$ rozważane zdanie jest prawdziwe, gdyż zbiór pusty nie posiada właściwych podzbiorów. Załóżmy zatem, że zdanie jest prawdziwe dla zbiorów n elementowych i rozważmy dowolny zbiór $A = \{a_0, \ldots, a_n\}$. Niech $B \subseteq A$ oraz $B \neq A$. Jeśli $a_n \notin B$ to $B \subseteq \{1_n, \ldots, a_{n-1}\}$ i teza wynika łatwo z założenia indukcyjnego. Jeśli $a_n \in B$ to założenie indukcyjne należy wykorzystać do pary zbiorów $\{a_0, \ldots, a_{n-1}\}$ oraz $B' = A \cap \{a_0, \ldots, a_{n-1}\}$. □

Wniosek 7.1 *W każdym skończonym częściowym porządku istnieją elementy minimalne i maksymalne.*

Dowód. Udowodnimy tylko pierwszą część tezy, czyli pokażemy że w każdym skończonym częściowym porządku istnieje element minimalny. Dowód drugiej części tezy jest podobny do przedstawionego dowodu części pierwszej. Dla zbiorów jednoelementowych teza jest oczywiście prawdziwa. Załóżmy zatem, że teza jest prawdziwa dla wszystkich porządków na zbiorach k-elementowych dla wszystkich $k \leq n$. Rozważmy częściowy porządek $\preceq$ na zbiorze A mocy $n + 1$. Niech $a \in A$. Jeśli a jest

elementem $\preceq$-minimalnym to teza jest prawdziwa. Załóżmy zatem, że a nie jest elementem $\preceq$-minimalnym. Rozważmy obcięcie porządku $\preceq$ do zbioru $A' = \{x \in A : x \prec a\}$. Wtedy $a \notin A$, więc zbiór A' ma co najwyżej n elementów. W porządku $(A', \preceq)$ istnieje więc element minimalny. Jest on oczywiście elementem minimalnym w porządku $(A, \preceq)$. □

Wniosek 7.2 *W każdym skończonym liniowym porządku istnieją elementy najmniejsze i największe.*

Dowód. Teza wynika z poprzedniego wniosku oraz z tego, że w liniowym porządku elementy minimalne i najmniejsze oraz maksymalne i największe pokrywają się. □

Wniosek 7.3 (O sortowaniu topologicznym) *Niech $(X, \leq)$ będzie skończonym częściowym porządkiem. Istnieje wtedy liniowy porządek $\preceq$ na zbiorze X taki, że $\leq \subset \preceq$.*

Dowód. Twierdzenie to jest prawdziwe dla częściowych porządków jednoelementowych, gdyż na nich istnieje tylko jeden porządek częściowy, który jest jednocześnie porządkiem liniowym. Załóżmy więc, że twierdzenie to jest prawdziwe dla wszystkich porządków n - elementowych i niech $(X, \leq)$ będzie częściowym porządkiem takim, że zbiór X ma $n+1$ elementów. Niech a będzie $\leq$-minimalnym elementem zbioru X oraz niech $Y = X \setminus \{a\}$. Wtedy zbiór Y ma n-elementów. Istnieje więc porządek liniowy $\preceq_Y$ rozszerzający $\leq \restriction Y$. Szukanym liniowym porządkiem na zbiorze X jest

$$\preceq \quad = (\{a\} \times Y) \cup \preceq_Y .$$ □

Twierdzenie 7.3 uogólnić można na dowolne, również nieskończone, częściowe porządki. Przed przystąpieniem do sformułowania i udowodnienia następnego twierdzenia zauważmy, że jeśli $|A| = n$ oraz $b \notin A$ to $|A \cup \{b\}| = n+1$. Rzeczywiście, jeśli $f : \{0, \ldots, n-1\} \to A$ jest bijekcją, to funkcja $g = f \cup \{(n, b)\}$ jest bijekcją pomiędzy zbiorami $\{0, \ldots, n\}$ oraz $A \cup \{b\}$.

Twierdzenie 7.3 *Załóżmy, że A i B są zbiorami skończonymi.*

1. *Jeśli $A \cap B = \emptyset$ to $|A \cup B| = |A| + |B|$,*
2. $|A \times B| = |A| \cdot |B|$,
3. $|A^B| = |A|^{|B|}$,
4. $|P(A)| = 2^{|A|}$.

Dowód. Dowody punktów (1), (2) i (3) przeprowadzimy indukcja względem mocy zbioru B. Jeśli $B = \emptyset$ to $|A \cup B| = |A| = |A| + 0 = |A| + |B|$. Załóżmy, że równość $|A \cup B| = |A| + |B|$ zachodzi dla wszystkich zbiorów B mocy n rozłącznych ze zbiorem A. Niech B będzie zbiorem rozłącznym z A takim, że $|B| = n+1$. Ustalmy element $b \in B$ oraz niech $B' = B \setminus \{b\}$. Wtedy $|B'| = n$ oraz

$$|A \cup B| = |A \cup (B' \cup \{b\})| = |(A \cup B') \cup \{b\}| = |(A \cup B')| + 1 =$$

$$(|A| + |B'|) + 1 = |A| + (|B'| + 1) = |A| + |B|.$$

Zatem, na mocy Zasady indukcji matematycznej, wzór $|A \cup B| = |A| + |B|$ jest prawdziwy dla wszystkich rozłącznych par zbiorów skończonych A i B.

Zauważmy, że $|A \times \emptyset| = |\emptyset| = 0$, a więc wzór $|A \times B| = |A| \cdot |B|$ jest prawdziwy jeśli $|B| = 0$. Załóżmy więc, że $|A \times B| = |A| \cdot |B|$ dla wszystkich zbiorów B mocy n. Niech $|B| = n + 1$. Ustalmy element $b \in B$ oraz niech $B' = B \setminus \{b\}$. Wtedy

$$A \times B = A \times (B' \cup \{b\}) = (A \times B') \cup (A \times \{b\}).$$

Zbiory $A \times B'$ oraz $A \times \{b\}$ są rozłączne oraz $|A \times \{b\}| = |A|$. Zatem

$$|A \times B| = |A \times B'| + |A \times \{b\}| = |A| \cdot n + |A| = |A| \cdot (n + 1) = |A| \cdot |B|.$$

Udowodnimy teraz równość $|A^B| = |A|^{|B|}$. Zauważmy najpierw, że

$$\emptyset^B = \begin{cases} \{\emptyset\} & : B = \emptyset \\ \emptyset & : B \neq \emptyset \end{cases}$$

Zatem dowodzony wzór jest prawdziwy, jeśli A jest zbiorem pustym (przypomnijmy, że $0^0 = 1$). Możemy więc zakładać, że A jest zbiorem niepustym. Jeśli B jest zbiorem pustym, to $A^B = \{\emptyset\}$, więc wtedy $|A^B| = 1$, co jest zgodne z tym, że $n^0 = 1$ dla dowolnej liczby naturalnej n.
Załóżmy więc, że równość $|A^B| = |A|^{|B|}$ jest prawdziwa dla wszystkich zbiorów B mocy n. Niech $|B| = n + 1$. Ustalmy element $b \in B$ i niech $B' = B \setminus \{b\}$. Zdefiniujemy odwzorowanie $\psi : A^B \to A^{B'} \times A$ wzorem

$$\psi(f) = (f \restriction B', f(b)).$$

Zauważmy, że jeśli $\psi(f) = \psi(g)$ to $f = g$. Rzeczywiście, załóżmy, że $\psi(f) = \psi(g)$ i rozważmy dowolny element $x \in B$. Jeśli $x = b$ to z równości $(f \restriction B', f(x)) = (g \restriction B', g(x))$ wynika, że $f(x) = g(x)$. Jeśli zaś $x \neq b$ to wtedy $x \in dom(f \restriction B')$ oraz $f \restriction B'(x) = g \restriction B'(x)$, więc $f(x) = g(x)$. Zatem $f = g$. Odwzorowanie g jest więc injekcją. Pokażemy, że ψ jest również surjekcją. Niech $(\alpha, a) \in A^{B'} \times A$. Połóżmy $f = \alpha \cup \{(b, a)\}$. Wtedy $f \in A^B$ oraz $\psi(f) = (\alpha, a)$. Zatem ψ jest bijekcją. Widzimy więc, że $|A^B| = |A^{B'} \times A| = |A^{B'}| \cdot |A| = |A|^n \cdot |A| = |A|^{n+1} = |A|^{|B|}$.

Ostatni punkt twierdzenia udowodnimy indukcją matematyczną względem ilości elementów zbioru A. Jeśli $A = \emptyset$ to $P(A) = \{\emptyset\}$ więc wtedy $|P(A)| = 1 = 2^0 = 2^{|A|}$. Załóżmy więc, że teza jest prawdziwa dla dowolnego n-elementowego zbioru A. Niech $|A| = n + 1$, $a \in A$ oraz $A' = A \setminus \{a\}$. Wtedy

$$P(A) = \{X \in P(A) : a \in X\} \cup \{X \in P(A) : a \notin X\} =$$

$$\{X \cup \{a\} : X \in P(A')\} \cup P(A').$$

Zbiory $\{X \cup \{a\} : X \in P(A')\}$ i $P(A')$ są rozłączne oraz $|\{X \cup \{a\} : X \in P(A')\}| = |P(A')|$. Zatem $|P(A)| = |P(A')| + |P(A')| = 2^{|A'|} + 2^{|A'|} = 2^{|A'|+1} = 2^{|A|}$, co kończy dowód twierdzenia. □

7.3 Permutacje

Permutacją zbioru A nazywamy dowolną bijekcję $f : A \to A$. Zbiór wszystkich permutacji zbioru A oznaczamy symbolem $Sym(A)$. Łatwo można pokazać, że jeśli A i B są zbiorami skończonymi o tej samej ilości elementów, to również zbiory $Sym(A)$ i $Sym(B)$ są tej samej mocy. Rozważania zbioru permutacji dla zbiorów skończonych można więc ograniczyć do badania permutacji zbiorów postaci $\{1, \ldots, n\}$ dla liczb naturalnych n.

Każdą permutację $\pi \in Sym(\{1, \ldots, n\})$ możemy jednoznacznie przedstawić w postaci ciągu $(\pi(1), \pi(2), \ldots, \pi(n))$. W ciągu tym każda liczba ze zbioru $\{1, \ldots, n\}$ występuje dokładnie jeden raz.

Twierdzenie 7.4 *Dla każdej liczby naturalnej $n \geq 1$ prawdziwa jest równość*

$$|Sym(\{1, \ldots, n\})| = n! \, .$$

Dowód. Równość $|Sym(\{1, \ldots, n\})| = n!$ jest oczywiście prawdziwa dla liczby $n = 1$. Załóżmy więc, że jest ona prawdziwa dla liczby n. Rozważmy dowolną permutację $\pi \in Sym(\{1, \ldots, n\})$. Liczbę $n+1$ możemy wstawić do ciągu $(\pi(1), \pi(2), \ldots, \pi(n))$ dokładnie na $n + 1$ sposobów: $(n + 1, \pi(1), \ldots, \pi(n))$, $(\pi(1), n + 1, \ldots, \pi(n))$, $\ldots$, $(\pi(1), \ldots, \pi(n), n + 1)$. Zatem

$$|Sym(\{1, \ldots, n+1\})| = |Sym(\{1, \ldots, n\})| \cdot (n+1) = n! \cdot (n+1) = (n+1)!$$

□

Funkcja silnia jest bardzo szybko rosnąca. W wielu zastosowaniach konieczne jest oszacowanie wartości $n!$. Przydatna do tego celu jest formuła Stirlinga:

$$n! \simeq \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

Dowód tej formuły przeprowadzić można środkami analitycznymi. Nie będzie omawiany w tej książce. Pewna przybliżona postać tej formuły może być wyprowadzona stosunkowo elementarnymi środkami.

7.4 Symbol Newtona

Symbolem Newtona nazywamy wyrażenie

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

gdzie $k, n \in \mathbb{N}$ oraz $k \leq n$. Bezpośrednio z definicji wynika, że $\binom{n}{0} = \binom{n}{n} = 1$ oraz $\binom{n}{k} = \binom{n}{n-k}$ oraz że $\binom{n}{1} = \binom{n}{n-1} = n$. Jedna z najważniejszych własności symbolu Newtona jest następująca równość, zwana równością Pascala:

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1},$$

która jest prawdziwa dla dowolnych $k < n$. Oto jej dowód:

$$\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} =$$

$$\frac{n!}{k!(n-k-1)!}\left(\frac{1}{n-k}+\frac{1}{k+1}\right)=\frac{n!}{k!(n-k-1)!}\cdot\frac{n+1}{(n-k)(k+1)}=$$
$$\frac{(n+1)!}{(k+1)!(n-k)!}=\binom{n+1}{k+1}.$$

Przyjrzyjmy się teraz nieco dokładniej podzbiorom danego zbioru skończonego. Dla dowolnym zbioru A oraz liczby naturalnej k niech

$$[A]^k=\{X\in P(A):|X|=k\}.$$

Mówiąc inaczej, zbiór $[A]^k$ jest rodziną wszystkich k-elementowych podzbiorów zbioru A.

Twierdzenie 7.5 *Niech A będzie zbiorem skończonym, $|A|=n$ oraz niech $k\leq n$. Wtedy*

$$|[A]^k|=\binom{n}{k}.$$

Dowód. Dowód przeprowadzimy indukcją względem ilości elementów zbioru A. Dla zbioru pustego oczywiście mamy $|[A]^0|=|\{\emptyset\}|=1=\binom{0}{0}$. Załóżmy zatem, że dowodzony wzór jest prawdziwy dla wszystkich zbiorów A mocy n. Rozważmy dowolny zbiór A mocy $n+1$. Zauważmy, że $|[A]^{n+1}|=|\{A\}|=1$. Zajmować się będziemy od tej pory tylko przypadkiem $k\leq n$. Ustalmy element $a\in A$ i nich $B=A\setminus\{a\}$. Wtedy

$$[A]^k=\{X\in[A]^k:a\in X\}\cup\{X\in[A]^k:x\notin X\}.$$

Zbiory $\{X\in[A]^k:a\in X\}$ i $\{X\in[A]^k:x\notin X\}$ są rozłączne. Ponadto $\{X\in[A]^k:x\notin X\}=[B]^k$. Zauważmy następnie, że $\{X\in[A]^k:a\in X\}$ = $\{X\cup\{a\}:X\in[B]^{k-1}\}$, więc $|\{X\in[A]^k:a\in X\}|=|[B]^{k-1}|$. Zatem

$$|[A]^k|=|[B]^{k-1}|+|[B]^k|=\binom{n}{k-1}+\binom{n}{k}=\binom{n+1}{k},$$

co kończy dowód twierdzenia. □

Niech A będzie zbiorem skończonym mocy n. Wtedy zbiór $P(A)$ możemy przedstawić jako rozłączną sumę $\bigcup_{i=0}^{n}[A]^i$. Zatem

$$2^n=\sum_{i=0}^{n}\binom{n}{i}.$$

Alternatywny dowód tej tożsamości oparty jest na własnościach wzoru Newtona i jest sformułowany w ćwiczeniach do tego rozdziału.

7.5 Zasada Dirichleta

Zasada indukcji matematycznej może byś sformułowana na wiele równoważnych sposobów. Jedną z jej postaci jest tak zwana zasada szufladkowa Dirichletta. Sformułujemy ją w postaci twierdzenia.

Twierdzenie 7.6 (Zasada Dirichleta) *Jeśli $n < m$ są liczbami naturalnymi to nie istnieje iniekcja ze zbioru $\{1, \ldots, m\}$ w zbiór $\{1, \ldots, n\}$.*

Dowód. Zauważmy, że wystarczy pokazać, że dla każdej liczby naturalnej n nie istnieje injekcja ze zbioru $\{1, \ldots, n+1\}$ w zbiór $\{1, \ldots, n\}$. Zdanie to będziemy dowodzić indukcją względem liczby naturalnej n. Dla $n = 1$ teza jest oczywista. Załóżmy, że jest ona prawdziwa dla liczby n. Niech $f : \{1, \ldots, n+2\} \to \{1, \ldots, n+1\}$ oraz niech $a = f(n+2)$. Określmy funkcję $g : \{1, \ldots, n+1\} \to \{1, \ldots, n\}$ za pomocą wzoru

$$g(k) = \begin{cases} f(k) - 1 & : f(k) > a \\ f(k) & : f(k) < a \end{cases}$$

Z założenia indukcyjnego wynika, że istnieją $x, y \in \{1, \ldots, n+1\}$ takie, że $x \neq y$ i $g(x) = g(y)$. Rozważmy cztery przypadki. Jeśli $f(x), f(y) < a$ to wtedy $g(x) = f(x)$ oraz $g(y) = f(y)$, wiec $f(x) = f(y)$. Jeśli $f(x), f(y) > a$ to $g(x) = f(x) - 1$ oraz $g(y) = f(y) - 1$, więc ponownie mamy $f(x) = f(y)$. Trzeci przypadek $f(x) < a, f(y) > a$ jest niemożliwy, gdyż wtedy mielibyśmy $g(x) = f(x) < a \leq f(y) - 1 = g(y)$. Podobnie niemożliwy jest przypadek przypadek $f(x) > a, f(y) < a$. Zatem we wszystkich możliwych przypadkach okazało się, że funkcja f nie jest różnowartościowa. □

Uwaga. Zasada Dirichletta nazywana jest czasem "*zasadą gołębnika*", gdyż można ją sformułować następująco: „*jeśli n+1 gołębi wejdzie do n gołębników, to w pewnym gołębniku znajdą się co najmniej dwa gołębie*".

Uwaga. Z Zasady Dirichletta można wywnioskować, że we Wrocławiu istnieją dwie osoby, które mają taką samą ilość włosów na głowie. Ta stosunkowo łatwa do udowodnienia obserwacja jest niezwykle trudna do bezpośredniej weryfikacji.

Przykład 7.4 *Załóżmy, że $\mathcal{A} \subseteq P(\{1, \ldots, n\})$ jest zbiorem mocy większej od 2^{n-1}. Pokażemy, że istnieją dwa różne zbiory $X, Y \in \mathcal{A}$ takie, że $X \subseteq Y$. Niech $f : \mathcal{A} \to P(\{1, \ldots, n-1\})$ będzie funkcja określoną wzorem $f(X) = X \cap \{1, \ldots, n-1\}$. Istnieją wiec dwa różne elementy $X, Y \in \mathcal{A}$ takie, że $f(X) = f(Y)$. Wtedy $X \subset Y$ lub $Y \subset X$, gdyż zbiory X i Y różnią się tylko na elemencie n.*

Nieskończony wariant Zasady Dirichleta brzmi następująco: „*jeśli suma skończonej ilości zbiorów jest nieskończona, to jeden ze składników sumy jest nieskończony*".

7.6 Ćwiczenia i zadania

Ćwiczenie 7.1 *Niech $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ będzie funkcją określoną wzorem:*

$$\begin{aligned} h(x, 0) &= 1 \\ h(x, y+1) &= x^{h(x,y)} \end{aligned}$$

Wyznacz wartości $h(3, 3)$, $h(4, 4)$ oraz $h(5, 5)$.

Ćwiczenie 7.2 *Niech F_n będzie n-tym wyrazem ciągu Fibbonacciego. Pokaż, że*

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right].$$

Ćwiczenie 7.3 *Pokaż, że w każdym skończonym częściowym porządku istnieje element maksymalny.*

Ćwiczenie 7.4 *Pokaż, że dla dowolnych dwóch zbiorów skończonych A i B zachodzi równość*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Uogólnij ten wzór na trzy i cztery zbiory.

Ćwiczenie 7.5 *Niech $\mathcal{A} = \{A \in P(\{1, \ldots, 10\}) : 2 \leq |A| \leq 7\}$. Ile jest elementów minimalnych oraz ile jest elementów maksymalnych w częściowym porządku $(\mathcal{A}, \subseteq)$?*

Ćwiczenie 7.6 *Pokaż, że dla dowolnych liczb rzeczywistych x, y oraz dla dowolnej liczny naturalnej $n > 0$ zachodzi równość*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} ,$$

zwana wzorem dwumianowym Newtona.

Ćwiczenie 7.7 *Korzystając ze wzoru Newtona wyznacz następujące sumy:*

$$\sum_{i=0}^{n} \binom{n}{i}, \ \sum_{i=0}^{n} (-1)^i \binom{n}{i}, \ \sum_{i=0}^{n} 2^i \binom{n}{i}, \ \sum_{i=0}^{n} i \binom{n}{i}.$$

Wskazówka: do wyznaczenia ostatniej sumy skorzystaj z tego, że $\binom{n}{i} = \binom{n}{n-i}$.

Ćwiczenie 7.8 *Pokaż, że jeśli skończony porządek ma tylko jeden element maksymalny, to jest on elementem największym.*

Ćwiczenie 7.9 *Za pomocą formuły Stirlinga oszacuj liczbę $\binom{n}{[\frac{n}{2}]}$, gdzie $[x]$ oznacza część całkowitą liczby x.*

Ćwiczenie 7.10 *Pokaż, że jeśli $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ jest injekcją, to funkcja f jest również surjekcją.*

Ćwiczenie 7.11 *Pokaż, że jeśli $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ jest surjekcją, to funkcja f jest również injekcją.*

Ćwiczenie 7.12 *Pokaż, że jeśli w trójkącie równobocznym o boku 2 rozmieścimy dowolnie pięć punktów, to dwa z nich są odległe nie więcej niż o 1.*

Ćwiczenie 7.13 *Pokaż, że w każdej szóstce liczb ze zbioru $\{1, ..., 10\}$ istnieją dwie liczby których suma jest nieparzysta.*

Ćwiczenie 7.14 *Udowodnij nieskończony wariant Zasady Dirichleta.*

Ćwiczenie 7.15 *Załóżmy, że każdy punkt płaszczyzny ma kolor czerwony lub biały. Pokaż, że istnieje prostokąt którego wszystkie wierzchołki mają ten sam kolor.*

Ćwiczenie 7.16 *Niech $x_1, \ldots, x_n$ będzie ciągiem liczb całkowitych. Pokaż, że suma pewnej liczby kolejnych wyrazów tego ciągu jest podzielna przez liczbę n.*

Ćwiczenie 7.17 *Czy szachownicę z usuniętymi naprzeciwległymi narożnikami można pokryć kostkami domina o powierzchni równej dwóm kwadratom szachownicy?*

Ćwiczenie 7.18 *Wyznacz liczbę przekątnych w n-kącie wypukłym.*

Ćwiczenie 7.19 *Ile jest relacji zwrotnych, symetrycznych, słabo antysymetrycznych na zbiorze n elementowym?*

Ćwiczenie 7.20 *Pokaż, że istnieją dwie potęgi liczby 3 których róznica dzieli się przez 1997. Pokaż, że istnieje potęga liczby 3, której rozwinięcie dziesiętne kończy się cyframi 001.*

Ćwiczenie 7.21 *Ile jest relacji które są jednocześnie zwrotne i symetryczne na zbiorze $\{1, 2, ..., n\}$?*

Ćwiczenie 7.22 *Relację R nazywamy antysymetryczną, jeśli $(\forall x, y)((x, y) \in R \rightarrow (x, y) \notin R)$. Ile jest relacji antysymetrycznych na zbiorze n - elementowym?*

Ćwiczenie 7.23 *Relację R nazywamy żałosną, jeśli $(\forall x, y)((x, y) \in R \rightarrow x = y)$. Ile jest relacji żałosnych na zbiorze n - elementowym?*

Ćwiczenie 7.24 *Niech $S = \{X \subseteq \{1, ..., 9\} : |X|$ jest liczbą parzystą$\}$. Jaka jest moc rodziny zbiorów S ?*

Zadanie 7.1 *Pokaż, że*

$$\big(\psi(2) \wedge (\forall n)(\psi(n) \rightarrow \psi(2n)) \wedge (\forall n > 2)(\psi(n) \rightarrow \psi(n-1)\big) \rightarrow (\forall n \geq 2)\psi(n)$$

Zadanie 7.2 *Uogólnij wzór $|A \cup B| = |A| + |B| - |A \cap B|$ na dowolną skończoną liczbę zbiorów.*

Zadanie 7.3 *Niech $\Sigma = \{a, b\}$. Niech s_n oznacza liczbę ciągów z Σ^n w których nie występują dwie kolejne litery a, czyli takich w których nie występuje ciąg aa. Wyznacz liczby s_n.*

Zadanie 7.4 *Korzystając z Zasady Indukcji Matematycznej pokaż, że $(\mathbb{N}, \leq)$ jest dobrym porządkiem.*

Zadanie 7.5 *Korzystając z tego, że $\ln n! = \sum_{i=1}^{n} \ln i$ oraz ze wzoru $\int \ln x dx = x(\ln x - 1) + C$ wyznacz samodzielnie przybliżenie liczby $n!$.*

Zadanie 7.6 *Funkcją Ackermana nazywamy funkcję A określoną wzorem:*

$$A(m,n) = \begin{cases} n+1 & : m = 0 \\ A(m-1,1) & : n = 0 \\ A(m-1, A(m, n-1)) & : n > 0 \wedge m > 0 \end{cases}$$

Wyznacz wartości funkcji Ackermana dla małych wartości n i m. Pokaż, że definicja tej funkcji jest poprawna, czyli, że można w skończonej liczbie kroków wyznaczyć wartość $A(n, m)$ dla dowolnych liczb naturalnych ni m.

Zadanie 7.7 *Funkcją McCarthy'ego nazywamy funkcję f_{91} określoną wzorem:*

$$f_{91}(m) = \begin{cases} n - 10 & : n > 100 \\ f_{91}(f_{91}(n + 11)) & : n \leq 100 \end{cases}$$

Pokaż, że dla każdej liczby naturalnej n funkcja $f_{91}(n)$ jest określona i wyznacz wartości funkcji $f_{91}(n)$ dla dowolnego $n \in \mathbb{N}$.

Zadanie 7.8 *Niech $A \subseteq \{1, 2, ..., 2n\}$ będzie zbiorem o mocy $|A| > n$. Pokaż, że istnieją dwie różne liczby $a, b \in A$ takie, że a dzieli b.*

Zadanie 7.9 *Niech $x_1, \ldots, x_{mn+1}$ będzie ciągiem liczb rzeczywistych. Pokaż, że z ciągu tego można wybrać podciąg rosnący długości $m + 1$ lub podciąg malejący długości $n + 1$.*

Zadanie 7.10 *Niech $\mathcal{A} \subseteq P(\{1, ..., n\}) \setminus \{\emptyset\}$ będzie taką rodziną zbiorów, że $|\mathcal{A}| > \frac{n}{2}$. Pokaż, że istnieją wtedy dwa różne zbiory $A, B \in \mathcal{A}$ takie, że $\neg(A \subseteq B) \wedge \neg(B \subseteq A)$.*

8 Teoria mocy

W poprzednim wykładzie wprowadziliśmy pojęcie równoliczności (patrz Definicja 7.1) oraz mocy zbioru skończonego. W tym wykładzie rozważania z poprzedniego wykładu uogólnimy na dowolne zbiory. Zauważmy na wstępie, że zbiory $\mathbb{N}$ oraz $\mathbb{N} \setminus \{0\}$ są równoliczne. Jedną z bijekcji pomiędzy tymi zbiorami jest funkcja $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ określona wzorem $f(n) = n + 1$. Zbiór nieskończony może być więc równoliczny ze swoim podzbiorem właściwym. Spostrzeżenie to pewnie by zdziwiło Euklidesa, lecz znał je już Galileusz.

Rozpoczniemy od sformułowania kilka ogólnych twierdzeń o własnościach pojęcia równoliczności.

Twierdzenie 8.1 *Załóżmy, że* $|A| = |C|$, $|B| = |D|$, $A \cap B = \emptyset$ *oraz* $C \cap D = \emptyset$. *Wtedy* $|A \cup B| = |C \cup B|$.

Dowód. Niech $f : A \to C$ oraz $g : B \to D$ będą bijekcjami. Wtedy $f \cup g$ jest bijekcją pomiędzy $A \cup B$ i $C \cup D$. □

Twierdzenie 8.2 *Załóżmy, że* $|A| = |C|$, $|B| = |D|$. *Wtedy* $|A \times B| = |C \times B|$.

Dowód. Niech $f : A \to C$ oraz $g : B \to D$ będą bijekcjami. Dla $(x, y) \in A \times B$ określamy $\psi((x, y)) = (f(x), g(x))$. Wtedy ψ jest bijekcją pomiędzy zbiorami $A \times B$ oraz $C \times B$. □

Twierdzenie 8.3 *Załóżmy, że* $|A| = |B|$. *Wtedy* $|P(A)| = |P(B)|$.

Dowód. Niech $f : A \to B$ będzie bijekcją. Wtedy odwzorowanie $\psi(X) = f[X]$ jest bijekcją pomiędzy zbiorami $P(A)$ i $P(B)$. □

Twierdzenie 8.4 $|P(A)| = |\{0, 1\}^A|$.

Dowód. Dla każdego zbioru $X \subseteq A$ niech χ_X oznacza funkcję charakterystyczną zbioru X (patrz Rozdział 4.7). Odwzorowanie $\psi : P(A) \to \{0, 1\}^A$ określone wzorem $\psi(X) = \chi_X$ jest szukaną bijekcją. □

Twierdzenie 8.5 *Załóżmy, że* $|A| = |C|$, $|B| = |D|$. *Wtedy* $|A^B| = |C^D|$.

Dowód. Niech $f : A \to C$ oraz $g : B \to D$ będą bijekcjami. Dla funkcji $x \in A^B$ kładziemy $\psi(x) = g \circ x \circ f^{-1}$. Wtedy ψ jest bijekcja pomiędzy zbiorami A^B i C^D. □

Twierdzenie 8.6 *Załóżmy, że zbiory* B *i* C *są rozłączne. Wtedy dla dowolnego zbioru* A *mamy* $|A^{B \cup C}| = |A^B \times A^C|$.

Dowód. Dla każdej funkcji $x \in A^{B \cup C}$ kładziemy

$$\psi(x) = (x \restriction B, x \restriction C).$$

Odwzorowanie ψ jest bijekcją pomiędzy zbiorami $A^{B \cup C}$ i $A^B \times A^C$. □

Zauważmy, że twierdzenie to jest uogólnieniem wzoru $a^{b+c} = a^b a^c$, który prawdziwy jest dla dowolnych liczb rzeczywistych a, b, c, gdzie $a > 0$.

Twierdzenie 8.7 *Dla dowolnych zbiorów A, B i C mamy $|(A^B)^C| = |A^{B \times C}|$.*

Dowód. Dla każdej funkcji $x \in (A^B)^C$ kładziemy

$$\psi(x) = \{((b, c), x(c)(b)) : (b, c) \in B \times C\}.$$

Odwzorowanie ψ jest bijekcją pomiędzy zbiorami $(A^B)^C$ oraz $A^{B \times C}$. □

Ostatnie twierdzenie jest uogólnieniem tożsamości $(a^b)^c = a^{bc}$ prawdziwej dla dowolnych liczb rzeczywistych a, b, c, o ile $a > 0$.

8.1 Twierdzenia Cantora

Zajmiemy się teraz porównywaniem ilości elementów dowolnych zbiorów.

Definicja 8.1 *Mówimy, że moc zbioru A jest mniejszej lub równej od mocy zbioru B, co zapisujemy jako $|A| \leq |B|$, jeśli istnieje injekcja $f : A \to B$.*

Oczywiście, jeśli $|A| = |B|$ to $|A| \leq |B|$. Zatem, w szczególności, $|A| \leq |A|$ dla dowolnego zbioru A. Z tego, że złożenie injekcji jest injekcją wynika, że jeśli $|A| \leq |B|$ i $|B| \leq |C|$ to $|A| \leq |C|$.

Definicja 8.2 *Mówimy, że zbiór A jest mocy mniejszej od zbioru B, co zapisujemy jako $|A| < |B|$, jeśli $|A| \leq |B|$ oraz $\neg|A| = |B|$.*

Twierdzenie 8.8 (Cantor) *Dla każdego zbioru A prawdziwa jest nierówność $|A| < |P(A)|$.*

Dowód. Odwzorowanie $f : A \to P(A)$ określone wzorem $f(x) = \{x\}$ jest injekcją, a zatem $|A| \leq |P(A)|$. Rozważmy teraz dowolne odwzorowanie $F : A \to P(A)$. Niech $T = \{x \in A : x \notin F(x)\}$. Wtedy $T \in P(A)$. Załóżmy, że $T = F(a)$ dla pewnego $a \in A$. Lecz wtedy

$$a \in T \leftrightarrow a \in F(a) \leftrightarrow a \notin F(a) \leftrightarrow a \notin T.$$

Otrzymaliśmy sprzeczność, która pokazuje, że $T \notin rng(F)$. Zatem F nie jest surjekcją. □

Dokładniejsza analiza powyższego dowodu pokazuje, że dla dowolnego zbioru A nie istnieje surjekcja $F : A \to P(A)$.

Z Twierdzenia 8.8 wynika, że $|\mathbb{N}| < |P(\mathbb{N}))| < |P(P(\mathbb{N})))| < \ldots$. Istnieje więc nieskończenie wiele nieskończonych i różnych pod względem mocy zbiorów. Istnieje więc nieskończenie wiele nieskończoności.

Przykład 8.1 *Metoda wykorzystana w dowodzie twierdzenia Cantora nosi nazwę „rozumowania przekątniowego". Aby zdać sobie sprawę z tego dlaczego nosi ona taką nazwę zastosujemy ją do zbioru $\mathbb{N}$. Niech $f : \mathbb{N} \to P(\mathbb{N})$ będzie dowolną funkcją. Rozważmy następujący zbiór $diag(f) = \{(n,m) \in \mathbb{N} \times \mathbb{N} : m \in f(n)\}$ i niech $\Delta = \{(n,n) \in \mathbb{N} \times \mathbb{N} : (n,n) \in diag(f)\}$. Zbiór Δ składa się z tych elementów przekątnej $Id_{\mathbb{N}}$ które należą do zbioru $diag(f)$. Zbiór T zbudowany w dowodzie Twierdzenia Cantora, który nie należy do obrazu funkcji f, jest równy w rozważanym przypadku zbiorowi $\{n \in \mathbb{N} : (n,n) \notin \Delta\}$. Funkcja charakterystyczna tego zbioru spełnia następującą tożsamość*

$$\chi_T(n) = 1 - \chi_{diag(f)}(n,n).$$

Przykład 8.2 *Oto jeszcze jeden przykład rozumowania przekątniowego. Pokażemy mianowicie, że $|\mathbb{N}| < |\mathbb{N}^{\mathbb{N}}|$. Nierówność $|\mathbb{N}| \leq |\mathbb{N}^{\mathbb{N}}|$ jest łatwa do zauważenia, gdyż odwzorowanie które przyporządkowuje liczbie naturalne n funkcję stale równą n jest injekcją. Załóżmy teraz, że $F : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$. Niech $g \in \mathbb{N}^{\mathbb{N}}$ będzie funkcją określoną wzorem*

$$g(n) = F(n)(n) + 1.$$

Wtedy $g \neq F(n)$ każdego $n \in \mathbb{N}$, gdyż $g(n) \neq F(n)(n)$, a więc $g \notin rng(F)$.

Kolejnym celem naszych rozważań jest twierdzenie Cantora - Bernsteina. Przed jego sformułowaniem udowodnimy pomocniczy lemat, który ma zastosowania w wielu innych rozważaniach.

Lemat 8.1 (Banach) *Niech $f : A \to B$ i $g : B \to A$ będą injekcjami. Wtedy istnieją zbiory A_1, A_2, B_1, B_2 o następujących własnościach:*

1. *$A_1 \cup A_2 = A$, $A_1 \cap A_2 = \emptyset$,*
2. *$B_1 \cup B_2 = B$, $B_1 \cap B_2 = \emptyset$,*
3. *$f[A_1] = B_1$, $g[B_2] = A_2$.*

Dowód. Niech $f : A \to B$ i $g : B \to A$ będą injekcjami. Rozważmy odwzorowanie $\psi : P(A) \to P(A)$ określone wzorem

$$\psi(X) = A \setminus g[B \setminus f[X]].$$

Niech $(A_t)_{t \in T}$ będzie dowolną rodziną podzbiorów zbioru A. Z różnowartościowości odwzorowania g wynika, że

$$\psi[\bigcup_{t\in T} A_t] = A \setminus g[B \setminus f[\bigcup_{t\in T} A_t]] = A \setminus g[B \setminus \bigcup_{t\in T} f[A_t]] =$$

$$A \setminus g[\bigcap_{t\in T} (B \setminus f[A_t]) = A \setminus \bigcap_{t\in T} g[B \setminus f[A_t]] =$$

$$\bigcup_{t\in T} (A \setminus g[B \setminus f[A_t]]) = \bigcup_{t\in T} \psi(A_t).$$

Rozważmy teraz zbiór $\Omega = \emptyset \cup \psi(\emptyset) \cup \psi(\psi(\emptyset)) \cup \ldots$. Z udowodnionej wyżej własności odwzorowania ψ wynika, że

$$\psi(\Omega) = \psi(\emptyset) \cup \psi(\psi(\emptyset)) \cup \psi(\psi(\psi(\emptyset))) \cup \ldots = \Omega.$$

Niech $A_1 = \Omega$, $A_2 = A \setminus A_1$, $B_1 = f[A_1]$ i $B_2 = B \setminus B_1$. Wtedy

$$A_1 = \psi(A_1) = A \setminus g[B \setminus f[A_1]] = A \setminus g[B \setminus B_1] = A \setminus g[B_2]$$

więc

$$A_2 = A \setminus A_1 = A \setminus (A \setminus g[B_2]) = g[B_2],$$

co kończy dowód twierdzenia. □

Twierdzenie 8.9 (Cantor-Bernstein) *Jeśli* $|A| \leq |B|$ *oraz* $|B| \leq |A|$ *to* $|A| = |B|$.

Dowód. Załóżmy, że $|A| \leq |B|$ oraz $|B| \leq |A|$. Niech $f : A \to B$ oraz $g : B \to A$ będą injekcjami. Z Lematu Banacha wynika, że istnieją rozbicia $\{A_1, A_2\}$ zbioru A i $\{B_1, B_2\}$ zbioru B takie, że $f[A_1] = B_1$ oraz $g[B_2] = A_2$. Zatem $|A_1| = |B_1|$ i $|A_2| = |B_2|$, a więc na mocy Twierdzenia 8.1 otrzymujemy tezę. □

8.2 Zbiory przeliczalne

Najmniejszą nieskończonością jest ta którą posiadają liczby naturalne. Będziemy mówili, że zbiór A jest mocy $\aleph_0$ jeśli $|A| = |\mathbb{N}|$.

Uwaga. Symbol $\aleph$ jest pierwszą literą alfabetu języka hebrajskiego. Wymawia się ją "alef".

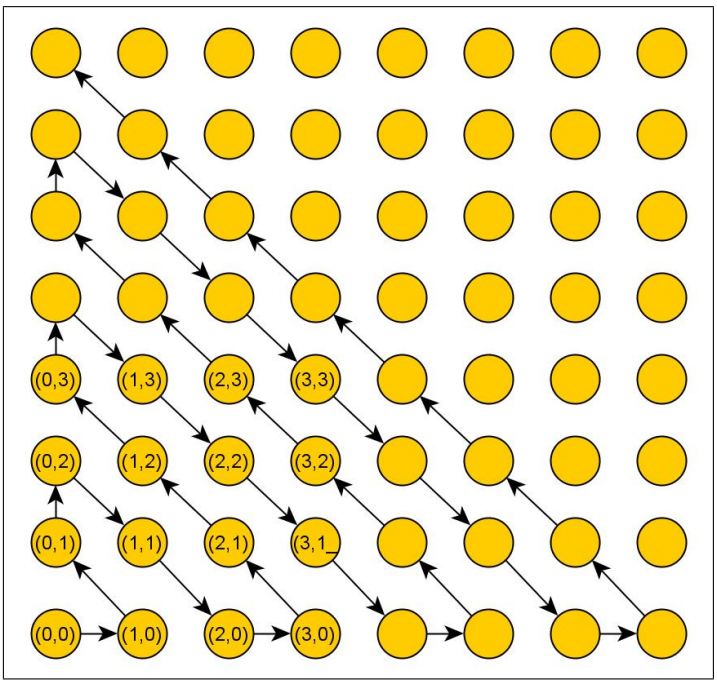
Przykład 8.3 *Zbiór liczb całkowitych jest mocy* $\aleph_0$*, czyli* $|\mathbb{Z}| = \aleph_0$*. Jedna z bijekcji pomiędzy zbiorami* $\mathbb{N}$ *oraz* $\mathbb{Z}$ *jest funkcja* $f : \mathbb{N} \to \mathbb{Z}$ *zadana wzorem* $f(n) = (-1)^n \left[\frac{n+1}{2}\right]$*, gdzie* $[x]$ *oznacza część całkowitą liczby* x*. Oto tabelka z kilkoma początkowymi wartościami funkcji* f*:*

n	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	...
f(n)	*0*	*-1*	*1*	*-2*	*2*	*-3*	*3*	*-4*	...

Twierdzenie 8.10 $|\mathbb{N} \times \mathbb{N}| = \aleph_0$

Dowód. Niech $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ będzie funkcją określoną wzorem $f((n, m)) = 2^n(2m + 1) - 1$. Zauważmy, że jeśli $f((n, m)) = f((n', m'))$ to $2^n(2m + 1) = 2^{n'}(2m' + 1)$, więc $2^n = 2^{n'}$ oraz $2m + 1 = 2m' + 1$, a więc funkcja f jest różnowartościowa. Rozważmy teraz dowolną liczbę naturalna a. Istnieją wtedy takie liczby naturalne n i m, że $a + 1 = 2^n(2m + 1)$. Wtedy $f((n, m)) = 2^n(2m + 1) - 1 = (a + 1) - 1 = a$. Zatem f jest bijekcją pomiędzy zbiorami $\mathbb{N} \times \mathbb{N}$ oraz $\mathbb{N}$. □

Inną bijekcję pomiędzy zbiorami $\mathbb{N} \times \mathbb{N}$ oraz $\mathbb{N}$ można zobaczyć, jeśli przyjrzy się następującemu rysunkowi:



Definicja 8.3 *Zbiór A nazywamy przeliczalnym jeśli $A = \emptyset$ lub istnieje surjekcja ze zbioru $\mathbb{N}$ na zbiór A.*

Oczywiście każdy zbiór mocy $\aleph_0$ jest przeliczalny. Zbiór pusty jest z samej definicji przeliczalny. Jeśli zaś $A = \{a_0, \ldots, a_n\}$ to funkcja

$$f(k) = \begin{cases} a_k & : k \leq n \\ a_n & : k > n \end{cases}$$

przekształca zbiór liczb naturalnych na zbiór A. Tak więc każdy zbiór skończony jest przeliczalny. Pokażemy, że prawdziwa jest również odwrotna implikacja.

Twierdzenie 8.11 *Zbiór A jest przeliczalny wtedy i tylko wtedy, gdy A jest skończony lub $|A| = \aleph_0$.*

Dowód. Załóżmy, że $f : \mathbb{N} \xrightarrow{na} A$ oraz, że A nie jest zbiorem skończonym. Niech $k_0 = 0$ oraz $k_{n+1} = min(\{m \in \mathbb{N} : f(m) \notin \{f(k_i) : i \leq n\})$. Poprawność definicji ciągu $(k_n)_{n\in\mathbb{N}}$ wynika z tego, że A jest zbiorem nieskończonym. Niech $g(n) = f(k_n)$. Wtedy $g : \mathbb{N} \to A$ jest szukaną surjekcją. □

Wniosek 8.1 *Jeśli A i B są zbiorami przeliczalnymi, to $A \times B$ jest zbiorem przeliczalnym.*

Dowód. Możemy oczywiście założyć, że zbiory A i B są niepuste. Niech $f : \mathbb{N} \to A$ i $g : \mathbb{N} \to B$ będą surjekcjami. Niech $F : \mathbb{N} \times \mathbb{N} \to A \times B$ będzie funkcją określoną wzorem $F((n, m)) = (f(n), g(m))$. Funkcja ta jest oczywiście surjekcją na $A \times B$. Niech następnie $\psi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ będzie bijekcją, której istnienie wykazaliśmy w Twierdzeniu 8.10. Wtedy $F \circ \psi$ jest surjekcją ze zbioru $\mathbb{N}$ na zbiór $A \times B$. □

Pokażemy teraz, że suma przeliczalnej rodziny zbiorów przeliczalnych jest zbiorem przeliczalnym.

Wniosek 8.2 *Jeśli $(A_n)_{n\in\mathbb{N}}$ jest rodziną zbiorów przeliczalnych, to $\bigcup_{n\in\mathbb{N}} A_n$ jest zbiorem przeliczalnym.*

Dowód. Niech $(A_n)_{n\in\mathbb{N}}$ będzie rodziną zbiorów przeliczalnych. Możemy założyć że każdy z tych zbiorów jest niepusty. Niech $f_n : \mathbb{N} \to A_n$ będą surjekcjami. Niech $F : \mathbb{N} \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n$ będzie funkcją zdefiniowana wzorem $F(n, m) = f_n(m)$. Jest jasne, że D jest surjekcją. Niech następnie $\psi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ będzie bijekcją Wtedy $F \circ \psi$ jest surjekcją ze zbioru $\mathbb{N}$ na zbiór $\bigcup_{n\in\mathbb{N}} A_n$. □

Zauważmy, że jeśli A jest zbiorem przeliczalnym i istnieje surjekcja ze zbioru A na zbiór B, to B jest również zbiorem przeliczalnym.

Przykład 8.4 *Zbiory $\mathbb{Z}$ oraz $\mathbb{N}$ są przeliczalne. Zatem, na mocy wniosku 8.1, ich iloczyn kartezjański $\mathbb{Z} \times \mathbb{N}$ jest również przeliczalny. Funkcja $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ określoną wzorem $f(k, n) = \frac{k}{n+1}$ jest surjekcją. Zatem zbiór liczb wymiernych $\mathbb{Q}$ jest przeliczalny.*

Wniosek 8.3 *Jeśli Ω jest zbiorem przeliczalnym, to zbiór słów Ω^* jest również zbiorem przeliczalnym*

Dowód. Niech Ω będzie zbiorem przeliczalnym. Dla każdego $n \in \mathbb{N}$ niech

$$\Omega^n = \Omega^{\{0,\ldots,n-1\}}.$$

Na mocy Wniosku 8.1 każdy ze zbiorów Ω^n jest przeliczalny, przeliczalna jest więc i ich suma $\Omega^* = \bigcup_{n\in\mathbb{N}} \Omega^n$. □

Przykład 8.5 *Liczbę rzeczywistą a nazywamy **liczbą algebraiczną**, jeśli istnieje wielomian $w[x]$ o współczynnikach całkowitych, który nie jest tożsamościowo równy zeru, taki, że $w(a) = 0$. Na przykład, liczba $\sqrt{2}$ jest algebraiczna, gdyż jest ona pierwiastkiem nietrywialnego wielomianu $w(x) = x^2+0\cdot x-2$ o współczynnikach całkowitych. Zbiór $\mathbb{Z}^*$ jest przeliczalny. Dla każdego ciągu $a = (a_0, \ldots, a_n) \in \mathbb{Z}^*$ niech*

$$w_a(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0$$

oraz $Z_a = \{x \in \mathbb{R} : w_a(x) = 0\}$. Jeśli a nie jest ciągiem tożsamościowo równym zero, to wielomian w_a ma tylko skończenie wiele pierwiastków, czyli zbiór Z_a jest skończony dla takich ciągów. Niech D oznacza zbiór tych ciągów ze zbioru $\mathbb{Z}^*$ dla których wielomian w_a nie jest tożsamościowo równe zeru. Zbiór D jest oczywiście zbiorem przeliczalnym. Tak więc zbiór $\bigcup_{a\in D} Z_a$ jest również przeliczalny. Pokazaliśmy więc, że zbiór wszystkich liczb algebraicznych jest zbiorem przeliczalnym.

8.3 Zbiory mocy continuum

Zbiór A nazywamy zbiorem mocy *continuum* ($|A| = \mathfrak{c}$), jeśli jest równoliczny ze zbiorem liczb rzeczywistych. Zauważmy, że jeśli $a, b \in \mathbb{R}$ i $a < b$ to odcinek (a, b) jest równoliczny ze zbiorem $\mathbb{R}$. Jedną z funkcji ustalających taką równoliczność jest funkcja $f(x) = \tan(\pi\frac{x-a}{b-a} - \frac{\pi}{2})$, gdzie $\tan(x)$ oznacza funkcję tangens.

Twierdzenie 8.12 $|P(\mathbb{N})| = \mathfrak{c}$

Dowód. Pokażemy najpierw, że $|\mathbb{R}| \leq |P(\mathbb{N})|$. Z Twierdzenia 8.3 wynika, że wystarczy pokazać prawdziwość nierówności $|\mathbb{R}| \leq |P(\mathbb{Q})|$. Szukanym zanurzeniem jest odwzorowanie f określone wzorem $f(x) = \{q \in \mathbb{Q} : q < x\}$. Jego różnowartościowość wynika z gęstości zbioru liczb wymiernych w liczbach rzeczywistych.
Pokażemy teraz, że istnieje injekcja $f : \{0,1\}^{\mathbb{N}} \to \mathbb{R}$, co na mocy Twierdzenia 8.3 pokaże, że $|P(\mathbb{N})| \leq |\mathbb{R}|$. Jest nią mianowicie funkcja

$$f(a) = \sum_{i=0}^{\infty} \frac{a(i)}{3^n}.$$

Jest ona dobrze określona, gdyż dla dowolnego $a \in \{0,1\}^{\mathbb{N}}$ zachodzi nierówność $\sum_{i=0}^{\infty} \frac{a(i)}{3^n} \leq \sum_{i=0}^{\infty} \frac{1}{3^n} = \frac{3}{2}$. Załóżmy, że $a, b \in \{0,1\}^{\mathbb{N}}$ oraz $a \neq b$. Niech $n = min\{k \in \mathbb{N} : a(k) \neq b(k)\}$. Możemy założyć, że $a(n) = 0$ i $b(n) = 1$. Niech $c = \sum_{i=0}^{n-1} \frac{a(i)}{3^n}$. Wtedy

$$f(a) = c + \sum_{i=n+1}^{\infty} \frac{a(i)}{3^n} \leq c + \sum_{i=n+1}^{\infty} \frac{1}{3^n} = c + \frac{1}{2} \cdot \frac{1}{3^n} < c + \frac{1}{3^n} \leq f(b).$$

Zatem odwzorowanie f jest różnowartościowe. Pokazaliśmy więc, że $|\mathbb{R}| \leq |P(\mathbb{N})|$ oraz $|P(\mathbb{N}) \leq |\mathbb{R}|$. Z Twierdzenia Cantora-Bernsteina wynika, że $|\mathbb{R}| = |P(\mathbb{N})|$. □

Wniosek 8.4 (Cantor) $|\mathbb{N}| < |\mathbb{R}|$

Dowód. Z Twierdzenia Cantora wynika, że $|\mathbb{N}| < |P(\mathbb{N})|$. Z poprzedniego twierdzenia mamy zaś $|P(\mathbb{N})| = |\mathbb{R}|$. □

Powyższy wniosek możemy zapisać w postaci $\aleph_0 < \mathfrak{c}$.

Przykład 8.6 *W poprzednim rozdziale pokazaliśmy, że zbiór liczb algebraicznych jest przeliczalny. W tym rozdziale pokazaliśmy, że zbiór liczb rzeczywistych jest nieprzeliczalny. Istnieją więc liczby rzeczywiste, które nie są liczbami algebraicznymi. Liczby takie nazywamy* ***liczbami przestępnymi****. Pokazać można, jednak zupełnie innymi technikami, że są nimi stałe π oraz e.*

Wniosek 8.5 (Cantor) $|\mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$

Dowód. Niech $\mathbb{Z}^- = \{x \in \mathbb{Z} : x < 0\}$. Wtedy

$$|\mathbb{R}| = |\{0,1\}^{\mathbb{N}}| = |\{0,1\}^{\mathbb{Z}}| = |(\{0,1\}^{\mathbb{N} \cup \mathbb{Z}^-}| = |\{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{Z}^-}| =$$
$$|\{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}| = |\mathbb{R} \times \mathbb{R}|.$$ □

Uwaga. Udowodnione właśnie twierdzenie można sformułować następująco: na płaszczyźnie istnieje tyle samo punktów co na prostej rzeczywistej. Obserwacja ta wzbudziła wiele kontrowersji wśród matematyków pod koniec XIX wieku.

Uwaga. Bijekcję pomiędzy prostą i płaszczyzną można stosunkowo łatwo skonstruować, bez korzystania z żadnych pomocniczych twierdzeń.

W podobny sposób można pokazać, że zbiór wszystkich ciągów rzeczywistych $|\mathbb{R}^{\mathbb{N}}|$ jest mocy continuum. Z twierdzenia Cantora - Bernsteina wynika, że $|\mathbb{R}| =$

$|\mathbb{R}^2| = |\mathbb{R}^3| = \ldots = |\mathbb{R}^{\mathbb{N}}|$. Warto również zauważyć, że $|\mathbb{R}^{\mathbb{R}}| \geq |\{0,1\}^{\mathbb{R}}| = |P(\mathbb{R})| > |\mathbb{R}|$, a więc moc zbioru wszystkich funkcji z liczb rzeczywistych w liczby rzeczywiste jest większa od continuum.

8.4 Algebra mocy

Pojęcie równoliczności zbiorów zostało wprowadzone w Definicji 7.1. Stwierdziliśmy tam, że pojęcie te posiada te same własności, co relacja równoważności, czyli jest zwrotne, symetryczne i przechodnie. Nie jest jednak relacją, gdyż jej polem jest klasa wszystkich zbiorów, która nie jest zbiorem. Sytuacja z równolicznością staje się znacznie prostsza, jeśli prawdziwy jest Aksjomat Wyboru, gdyż wtedy każda moc jest jednoznacznie wyznaczona przez pewne obiekty, które nazywają się liczbami kardynalnymi. Pojęcie to zostanie omówione w Dodatku B.

Do tej pory zajmowaliśmy się tylko ograniczoną kolekcją mocy. Były nimi liczby naturalne, $\aleph_0$ oraz $\mathfrak{c}$. W rozdziale tym zajmować się będziemy rodziną mocy, które możemy zdefiniować z wymienionych mocy za pomocą operacji dodawania, mnożenia i potęgowania.

Definicja 8.4 *Niech κ i λ będą mocami oraz niech $|X| = \kappa$ i $|Y| = \lambda$. Wtedy*

1. $\kappa + \lambda = |(X \times \{0\}) \cup (Y \times \{1\})|$,
2. $\kappa \cdot \lambda = |X \times Y|$,
3. $\kappa^\lambda = |X^Y|$.

Z twierdzeń sformułowanych na początku tego wykładu wynika, że definicje te są poprawne, czyli, że nie zależą od wyboru zbiorów X i Y do reprezentowania rozważanych mocy.

Rozważymy teraz kilka przykładów, których celem jest pokazanie w jaki sposób można przeprowadzać obliczenia na mocach.

Przykład 8.7 *Rozważmy zbiór $\mathbb{Z}^- = \{x \in \mathbb{Z} : x < 0\}$. Wtedy $|Z| = \aleph_0$. Zatem $\aleph_0 + \aleph_0 = |\mathbb{Z}^- \cup \mathbb{N}| = |\mathbb{Z}| = \aleph_0$. Z twierdzenia 8.10 wynika, że $\aleph_0 \cdot \aleph_0 = |\mathbb{N} \times \mathbb{N}| = \aleph_0$. Zatem $\aleph_0 + \aleph_0 = \aleph_0$ oraz $\aleph_0 \cdot \aleph_0 = \aleph_0$.*

Przykład 8.8 *Z Twierdzeń 8.4 oraz 8.12 wynika, że $\mathfrak{c} = |P(\mathbb{N})| = |\{0,1\}^{\mathbb{N}}| = 2^{\aleph_0}$. Z Twierdzenia Cantora otrzymujemy zaś nierówność $\aleph_0 < \mathfrak{c}$. Wniosek 8.5 możemy zaś zapisać w postaci $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$. Zauważmy następnie, że*

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

Zauważmy też, że $\mathfrak{c} \leq \mathfrak{c} + \mathfrak{c} \leq \mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$. Z twierdzenia Cantora - Bendixona otrzymujemy równość: $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$. Jest jasne, że $\mathfrak{c} \leq \mathfrak{c} + \aleph_0 \leq \mathfrak{c} + \mathfrak{c} = \mathfrak{c}$. Ponownie stosując twierdzenie Cantora - Bendixona otrzymujemy równość $\mathfrak{c} + \aleph_0 = \mathfrak{c}$.

Przykład 8.9 *Niech $\mathfrak{f} = 2^{\mathfrak{c}}$. Z Twierdzenia Cantora wynika, że $\mathfrak{f} > \mathfrak{c}$. Zauważmy, że*

$$\mathfrak{c}^{\mathfrak{c}} = \left(2^{\aleph_0}\right)^{\mathfrak{c}} = 2^{\aleph_0 \cdot \mathfrak{c}} = 2^{\mathfrak{c}} = \mathfrak{f},$$

zatem liczba kardynalna $\mathbf{f}$ *jest mocą rodziny wszystkich funkcji z liczb rzeczywistych w liczby rzeczywiste. Zauważmy następnie, że*

$$\mathbf{f} \cdot \mathbf{f} = 2^{\mathfrak{c}} \cdot 2^{\mathfrak{c}} = 2^{\mathfrak{c}+\mathfrak{c}} = 2^{\mathfrak{c}} = \mathbf{f}.$$

Z nierówności $\mathbf{f} \leq \mathbf{f} + \mathbf{f} \leq \mathbf{f} \cdot \mathbf{f}$ *wynika zaś, że* $\mathbf{f} + \mathbf{f} = \mathbf{f}$.

Niech $\beth_0 = \aleph_0$ oraz[1] $\beth_{n+1} = 2^{\beth_n}$ dla wszystkich liczb naturalnych n. Zauważmy, że $\beth_1 = \mathbf{c}$. Z Twierdzenia Cantora wynika, że ciąg mocy $\beth_n$ jest ostro rosnący, czyli, że

$$\beth_0 = \aleph_0 < \beth_1 = \mathbf{c} < \beth_2 < \beth_3 < \beth_4 < \dots$$

Niech teraz X_n będą takimi zbiorami, że $|X_n| = \beth_n$. Rozważmy zbiór $Y = \bigcup_{n\in\mathbb{N}}(X_n \times \{n\})$. Łatwo można sprawdzić, że dla każdego $n \in \mathbb{N}$ zachodzi ostra nierówność $\beth_n < |Y|$. Widzimy, że hierarchia mocy nie wyczerpuje się liczbami $\beth_n$. Moc tak zdefiniowanego zbioru Y oznaczamy przez $\beth_\omega$. Startując od liczby $\beth_\omega$ możemy za pomocą podobnej konstrukcji zbudować kolejny rosnący ciąg mocy:

$$\beth_0 < \beth_1 < \dots < \beth_\omega < \beth_{\omega+1} < \beth_{\omega+2} < \dots$$

W miejscu tym nasuwa się naturalne pytanie: czy zdefiniowany ciąg mocy $(\beth_n)_{n\in\mathbb{N}}$ jest w jakimś sensie zupełny? W szczególności można się pytać, czy istnieje zbiór A taki, że $\beth_0 < |A| < \beth_1$, czyli taki, że $\aleph_0 < |A| < \mathfrak{c}$?

Aksjomat 8.1 *Hipotezą Continuum nazywamy zdanie*

$$(\forall A)(A \subseteq \mathbb{R} \to (|A| \leq \aleph_0 \vee |A| = \mathfrak{c})).$$

Hipotezy Continuum nie można udowodnić ani też nie można udowodnić jej negacji na gruncie standardowej teorii zbiorów. O zdaniach takich mówimy, że są niezależne od teorii zbiorów. Innym przykładem takiego zdania jest Aksjomat Wyboru. Zagadnienia te będą szerzej omówione w Dodatkach do tej książki.

8.5 Funkcje obliczalne

Wyobraźmy sobie komputer z językiem programowania, którego jedynym typem zmiennych jest zmienne które mogą przyjmować dowolne wartości ze zbioru liczb naturalnych. W popularnym języku programowania C przybliżeniem tego typu jest unsigned int, z tym, że w naszym komputerze nie nakładamy żadnych ograniczeń na ich rozmiar. W języku tym występują stałe, podstawienia, pętle. Do konstrukcji wyrażeń arytmetycznych możesz posługiwać się operatorami $+$, $-$, $*$, $/$, z tym że dzielenie oznacza dzielenie całkowito-liczbowe, czyli

$$(c = a/b) \leftrightarrow (\exists k)(0 \leq k < b \wedge a = c \cdot b + k)\ .$$

W naszym języku programowania istnieją instrukcje czytania wartości zmiennych (read(x)) oraz wyświetlania wartości zmiennych (write(x)). Zakładamy ponadto, że każdy program napisany w tym języku programowania wszystkie instrukcje czytania wykonuje na początku swojego działania, oraz, że po wykonaniu instrukcji zapisania

[1] Symbol $\beth$ jest drugą literą alfabetu hebrajskiego, wymawianą jako "bet".

wartości dowolnej zmiennej kończy swoje działanie.

Uwaga. Z bardziej precyzyjną definicję modelu obliczeń czytelnik zapozna się wykładach ze Złożoności Obliczeniowej lub z Teoretycznych Podstaw Informatyki.

Definicja 8.5 *Funkcja f taka, że $dom(f) \subseteq \mathbb{N}^k$ oraz $rng(f) \subseteq \mathbb{N}$ jest **obliczalna** jeśli istnieje program $\mathcal{P}$ o następujących własnościach:*

1. *na początku działania czyta on wartości zmiennych $x_1, \ldots, x_k$;*
2. *jeśli $(n_1, \ldots, n_k) \in dom(f)$, to po skończonej liczbie kroków obliczeń program $\mathcal{P}$ zwraca wartość $f(n_1, \ldots, n_k)$;*
3. *jeśli $(n_1, \ldots, n_k) \notin dom(f)$, to program $\mathcal{P}$ nigdy nie zatrzymuje się.*

Przykładem funkcji obliczalnej jest, na przykład, funkcja $f(x, y) = x + y$, gdyż oblicza ją następujący program

```
read(x1);
read(x2);
y = x1+x2;
write(y);
```

Mówiąc mniej precyzyjniej, funkcja f jest obliczalna, jeśli istnieje program, który ją wyznacza. Niech Σ będzie zbiorem wszystkich znaków które możemy użyć do pisania programów w naszym języku. Zbiór Σ jest zbiorem skończonym.

Twierdzenie 8.13 *Zbiór wszystkich funkcji obliczalnych jest zbiorem mocy $\aleph_0$.*

Dowód. Zauważmy, że każdy program jest skończonym ciągiem elementów ze zbioru Σ, czyli jest elementem zbioru Σ^*. Na mocy wniosku 8.3 mamy $|\Sigma^*| = \aleph_0$. Zatem zbiór wszystkich programów jest mocy $\aleph_0$. Tak więc i zbiór wszystkich funkcji obliczalnych jest mocy $\aleph_0$. □

Funkcję $f : \mathbb{N}^k \to \mathbb{N}$ nazywamy **nieobliczalną**, jeśli nie jest funkcją obliczalną.

Wniosek 8.6 *Istnieje nieobliczalna funkcja $f : \mathbb{N} \to \mathbb{N}$.*

Dowód. Przypomnijmy, że $|\mathbb{N}^{\mathbb{N}}| = {\aleph_0}^{\aleph_0} = \mathfrak{c}$. Z poprzedniego twierdzenie wynika, że zbiór $\{f \in \mathbb{N}^{\mathbb{N}} : f \quad \text{jest obliczalna}\}$ jest przeliczalny. Z nierówności $\aleph_0 < \mathfrak{c}$ wynika, że zbiór

$$\mathbb{N}^{\mathbb{N}} \setminus \{f \in \mathbb{N}^{\mathbb{N}} : f \quad \text{jest obliczalna}\}$$

jest niepusty. □

Warto tutaj podkreślić, większość funkcji ze zbioru $\mathbb{N}$ w zbiór $\mathbb{N}$ jest nieobliczalna. Wynika to z tego, że jeśli zbiór A ma moc continuum zaś $B \subseteq A$ jest zbiorem przeliczalnym, to $|A \setminus B| = \mathfrak{c}$.

8.6 Ćwiczenia i zadania

Ćwiczenie 8.1 *Znajdź bijekcję pomiędzy następującymi parami zbiorów:*

1. $(-\pi/2, \pi/2)$ *i* $\mathbb{R}$,
2. $(0, 1)$ *i* $(2, 5)$,
3. $(0, \infty)$ *i* $\mathbb{R}$,
4. $[0, 1]$ *i* $[0, 1)$.

Ćwiczenie 8.2 *Pokaż, że każdy niezdegenerowany odcinek prostej rzeczywistej jest mocy continuum.*

Ćwiczenie 8.3 *Pokaż, że zbiór punktów płaszczyzny o obu współrzędnych wymiernych jest zbiorem przeliczalnym.*

Ćwiczenie 8.4 *Pokaż, że dowolna rodzina parami rozłącznych odcinków liczb rzeczywistych jest przeliczalna. Wskazówka: skorzystaj z tego, że liczby wymierne są gęste w zbiorze liczb rzeczywistych oraz, że zbiór liczb wymiernych jest przeliczalny.*

Ćwiczenie 8.5 *Pokaż, że dowolna rodzina parami rozłącznych niepustych kółek na płaszczyźnie jest przeliczalna.*

Ćwiczenie 8.6 *Pokaż, że* $n \cdot \aleph_0 = (\aleph_0)^n = \aleph_0$ *dla każdej liczby naturalnej* $n > 0$. *Wyznacz liczbę* $\aleph_0^{\aleph_0}$.

Ćwiczenie 8.7 *Jaka jest moc zbioru wszystkich ciągów liczb rzeczywistych zbieżnych do zera? Jaka jest moc zbioru wszystkich ciągów liczb całkowitych zbieżnych do zera?*

Ćwiczenie 8.8 *Pokaż, że zbiór wszystkich funkcji ciągłych z liczb rzeczywistych w liczby rzeczywiste jest mocy continuum. Wskazówka: pokaż, że jeśli* $f, g : \mathbb{R} \to \mathbb{R}$ *są takimi funkcjami ciągłymi, że* $f \restriction \mathbb{Q} = g \restriction \mathbb{Q}$ *to* $f = g$.

Ćwiczenie 8.9 *Pokaż, że zbiór wszystkich bijekcji ze zbioru liczb naturalnych w zbiór liczb naturalnych jest mocy continuum.*

Ćwiczenie 8.10 *Jaka może być moc zbioru* $A \setminus B$ *jeśli* A *i* B *są zbiorami mocy* $\aleph_0$*? Jaka może być moc zbioru* $A \setminus B$ *jeśli* A *i* B *są zbiorami mocy* $\mathbf{c}$*?*

Ćwiczenie 8.11 *Niech* $f : \mathbb{N} \to \mathbb{N}$. *Pokaż, że* $|rng(f)| = \aleph_0$ *lub istnieje taka liczba naturalna* n*, że* $|f^{-1}(n)| = \aleph_0$.

Ćwiczenie 8.12 *Pokaż, że jeśli* $|A| = |B|$ *to* $|Sym(A)| = |Sym(B)|$.

Ćwiczenie 8.13 *Jaka jest moc zbioru* $\{X \subset \mathbb{N} : |X| < \aleph_0\}$*? Jaka jest moc zbioru* $\{X \subset \mathbb{R} : |X| < \aleph_0\}$*? Jaka jest moc zbioru* $\{X \subset \mathbb{R} : |X| \leq \aleph_0\}$*?*

Ćwiczenie 8.14 *Pokaż, że funkcja* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *określona wzorem* $f(x, y) = x^y$ *jest obliczalna.*

Ćwiczenie 8.15 *Niech p_n oznacza n-tą liczbę pierwszą. Pokaż, że funkcja $f(n) = p_n$ jest obliczalna.*

Ćwiczenie 8.16 *Niech $f : \mathbb{N} \to \mathbb{N}$ będzie funkcją obliczalną. Pokaż, że zbiór programów obliczających funkcję f jest mocy $\aleph_0$.*

Ćwiczenie 8.17 *Pokaż, że zbiór nieobliczalnych funkcji $f : \mathbb{N} \to \mathbb{N}$ jest mocy continuum.*

Zadanie 8.1 *Jaka jest moc zbioru $\{(x, y) \in \mathbb{Q}^2 : x^2 + y^2 = 1\}$?*

Zadanie 8.2 *W którym miejscu dowodu tego, że suma przeliczalnej rodziny zbiorów jest przeliczalna, korzysta się z Aksjomatu Wyboru ?*

Zadanie 8.3 *Wyznacz wartości $\beth_n + \beth_m$, $\beth_n \cdot \beth_m$ oraz $\beth_n^{\beth_m}$ dla wszystkich liczb naturalnych n i m.*

Zadanie 8.4 *Ile można narysować parami rozłącznych liter "L" na płaszczyźnie?. Ile można narysować parami rozłącznych liter "T" na płaszczyźnie?*

Zadanie 8.5 *Niech $f : \mathbb{R} \to \mathbb{R}$ będzie funkcją monotoniczna. Pokaż, że zbiór punktów nieciągłości funkcji f jest przeliczalny.*

Zadanie 8.6 *Jak dużej mocy może być rodzina $\mathcal{A} \subseteq P(\mathbb{N})$ taka, że $(\forall A, B \in \mathcal{A})(A \subseteq B \vee B \subseteq A)$?.*

Zadanie 8.7 (Cantor) *Liniowy porządek $(L, \leq)$ nazywamy gęstym, jeśli*

$$(\forall a, b \in L)(a < b \to (\exists c \in L)(a < c < b)).$$

Pokaż, że każdy przeliczalny liniowy gęsty porządek bez elementu największego i najmniejszego jest izomorficzny z porządkiem $(\mathbb{Q}, \leq)$.

Zadanie 8.8 *Niech $(A_n)_{n\in\mathbb{N}}$ będzie dowolną rodziną zbiorów mocy $\aleph_0$. Pokaż, że istnieje rodzina nieskończonych, parami rozłącznych zbiorów $(B_n)_{n\in\mathbb{N}}$ taka, że $B_n \subseteq A_n$ dla wszystkich n.*

Zadanie 8.9 *Niech $(A_n)_{n\in\mathbb{N}}$ będzie dowolną rodziną nieskończonych podzbiorów zbiorów $\mathbb{N}$. Pokaż, że istnieje taki podzbiór S zbioru $\mathbb{N}$, że*

$$(\forall n \in \mathbb{N})(|A_n \cap S| = |A_n \setminus S| = \aleph_0).$$

Zadanie 8.10 *Niech $\{f_n : n \in N\}$ będzie dowolną rodziną funkcji ze zbioru $\mathbb{N}^{\mathbb{N}}$. Znajdź taką funkcję $g \in \mathbb{N}^{\mathbb{N}}$ taką, że $(\forall n)(\forall^\infty k)(f_n(k) < g(k))$ (kwantyfikator $\forall^\infty$ został zdefiniowany w zadaniu 3.3).*

Zadanie 8.11 *Dla zbiorów $A, B \in P(\mathbb{N})$ określamy relację $A \subseteq^* B \leftrightarrow |A \setminus B| < \aleph_0$. Pokaż, że $\subseteq^*$ jest preporządkiem. Załóżmy, że $(A_n)_{n\in\mathbb{N}}$ jest taką rodziną nieskończonych podzbiorów $\mathbb{N}$, że $(\forall n \in \mathbb{N})(A_{n+1} \subseteq^* A_n)$. Pokaż, że istnieje taki nieskończony podzbiór B zbioru liczb naturalnych, że $(\forall n \in \mathbb{N})(B \subseteq^* A_n)$.*

Zadanie 8.12 *Pokaż, że istnieje rodzina $\mathcal{A}$ nieskończonych podzbiorów zbioru liczb naturalnych mocy continuum taka, że dla dowolnych dwóch różnych $A, B \in \mathcal{A}$ przekrój $A \cap B$ jest skończony.*

Zadanie 8.13 *Pokaż, korzystając z Aksjomatu Wyboru, że jeśli A jest zbiorem nieskończonym (czyli, że $(\forall n \in \mathbb{N})(\neg|A| = n)$), to istnieje injekcja $f : \mathbb{N} \to A$.*

Zadanie 8.14 (twierdzenie Ramseya) *Niech $R \subseteq \mathbb{N}^2$ będzie relacją symetryczną. Pokaż, że istnieje nieskończony podzbiór A zbioru $\mathbb{N}$ taki, że $(\forall x, y \in A)(x \neq y \to (x, y) \in R)$ lub istnieje nieskończony podzbiór A zbioru $\mathbb{N}$ taki, że $(\forall x, y \in A)(x \neq y \to (x, y) \notin R)$.*

Zadanie 8.15 *Niech $\mathcal{S}$ będzie nieprzeliczalną rodziną zbiorów skończonych. Pokaż, że istnieje skończony zbiór Δ oraz nieprzeliczalna podrodzina $\mathcal{T} \subseteq \mathcal{S}$ taka, że $(\forall x, y \in \mathcal{T})(x \neq y \to x \cap y = \Delta)$.*

Zadanie 8.16 (Peano) *Pokaż, że istnieje funkcja ciągła surjekcja $f : [0, 1] \to [0, 1]^2$.*

9 Drzewa i Relacje Ufundowane

W rozdziale tym rozważać będziemy trzy ważne klasy częściowych porządków: relacje ufundowane, systemy przepisujące oraz drzewa. .

9.1 Relacje Ufundowane

Relacje ufundowane są naturalnym uogólnieniem pojęcia dobrego porządku.

Definicja 9.1 *Binarną relację $E \subseteq X \times X$ nazywamy **ufundowaną** jeśli dla dowolnego niepustego zbioru $A \subseteq X$ istnieje takie $a \in A$, że $(\forall x \in A)(\neg(xEa))$.*

Zauważmy, że jeśli $(X, \leq)$ jest dobrym porządkiem oraz zdefiniujemy

$$x < y \leftrightarrow (x \leq y) \wedge x \neq y) \ ,$$

to relacja $<$ jest ufundowana. Od relacji ufundowanej nie wymagamy aby była liniowym porządkiem. Nie wymagamy nawet aby była ona częściowym porządkiem. Relacje ufundowane nazywane są również czasami relacjami noetherowskimi.

Twierdzenie 9.1 *Niech E będzie relacją na zbiorze X. Wtedy następujące zdania są równoważne:*

1. *relacja E jest ufundowana;*
2. *nie istnieje ciąg $(a_n)_{n\in\mathbb{N}}$ elementów zbioru X taki, że*

$$(\forall n \in \mathbb{N})(a_{n+1}Ea_n) \ .$$

Dowód. (1) $\rightarrow$ (2). Załóżmy, że $(A_n)_{n\in\mathbb{N}}$ jest takim ciągiem elementów zbioru X że, $(\forall n \in \mathbb{N})(a_{n+1}Ea_n)$. Niech $A = \{a_n : n \in \mathbb{N}\}$. Rozważmy dowolny element $a \in A$. Jest takie $n \in \mathbb{N}$, że $a = a_n$. Lecz wtedy $a_{n+1} \in A$ oraz $a_{n+1}Ea$, co jest sprzeczne z założeniem.
(2) $\rightarrow$ (1). Niech teraz $A \subseteq X$ oraz $A \neq \emptyset$. Załóżmy, że $(\forall a \in A)(\exists b \in A)(bEa)$. Niech $C : A \rightarrow A$ będzie taką funkcją, że $(\forall a \in A)(C(a)Ea)$. Niech $a_0 \in A$. Indukcją względem $n \in \mathbb{N}$ definiujemy $a_{n+1} = C(a_n)$. Wtedy $(a_n)_{n\in\mathbb{N}}$ jest takim nieskończonym ciągiem elementów zbioru A takim, że $(\forall n \in \mathbb{N})(a_{n+1}Ea_n)$. Otrzymaliśmy sprzeczość z założeniem. □

W drugiej części powyższego dowodu wykorzystaliśmy Aksjomat Wyboru. W wielu konkretnych przypadkach, na przykład, gdy zbiór X jest przeliczalny, można go wyeliminować.

Następujące kryterium jest często wykorzystywane w praktyce do pokazywania, że dana relacja jest ufundowana.

Twierdzenie 9.2 *Niech E będzie relacją na zbiorze X. Załóżmy, że istnieje dobry porządek $(K, \preceq)$ funkcja $f : X \to K$ taka, że*

$$(\forall x, y \in X)(yEx \to f(x) \prec f(x)) .$$

Wtedy relacja E jest ufundowana.

Dowód. Niech A będzie dowolnym niepustym podzbiorem zbioru X. Wtedy $f[A]$ jest niepustym podzbiorem zbioru K, zatem ma najmniejszy element. Niech $m = \min_{\preceq}(f[A])$. Weźmy $a \in A$ takie, że $f(a) = m$. Wtedy $(\forall x \in A)(\neg xEa)$, gdyż, gdyby istniał $x \in A$ taki, że xEa, to element $f(x)$ byłby elementem zbioru $f[A]$ $\preceq$-mniejszym od elementu m, co nie jest możliwe. □

Prawdziwe jest również twierdzenie odwrotne do powyższego twierdzenia: jeśli relacja E na zbiorze X jest ufundowana, to istnieje dobry porządek $(K, \preceq)$ oraz funkcja $f : X \to K$ taka, że $(\forall x, y \in X)(xEy \to f(x) \prec f(y))$. Jednakże dowód tego twierdzenia wymaga użycia aparatu indukcji pozaskończonej i z tego powodu nie będziemy go tutaj podawali (patrz Zadanie D.22).

9.2 Systemy Przepisujące

Systemy przepisujące służą jako prototyp wielu formalnych modeli obliczeń.

Definicja 9.2 *Systemem przepisującym nazywamy parę $(X, \to)$ taką, że $\to$ jest relacją na zbiorze X.*

Ciąg $x_0, x_1, \ldots x_k$ elementów systemu przepisującego $(X, \to)$ taki, że

$$x_0 \to x_1 \to x_2 \to \ldots \to x_k$$

nazywamy *skończonym obliczeniem*. Ciąg $(x_n)_{n\in\mathbb{N}}$ nazywamy *nieskończonym obliczeniem*, jeśli dla każdego $n \in \mathbb{N}$ mamy $x_n \to x_{n+1}$ Element $x \in X$ nazywamy elementem *końcowym*, jeśli nie istnieje $y \in X$ taki, że $x \to y$.

Definicja 9.3 *Mówimy, że system przepisującym $(X, \to)$ ma własność stopu jeśli że relacja $\to^{-1}$ jest ufundowana.*

T Twierdzenia 9.1 wynika, że system przepisujący ma własność stopu, jeśli nie ma w nich nieskończonych obliczeń. Niech $(X, \to)$ będzie systemem przepisującym. Funkcję $f : X \to \mathbb{N}$ nazywamy *funkcją kontrolną* systemu, jeśli $f : X \to \mathbb{N}$ oraz

$$(\forall x, y \in X)\,((x \to y) \to (f(x) > f(y))) .$$

Z Twierdzenia 9.2 wynika, że jeśli system przepisujący ma funkcję kontrolną, to ma własność stopu.

Przykład 9.1 *Niech Ω będzie ustalonym alfabetem. Określmy*

$$R = \{(xaay, xy) : x, y \in \Omega^* \wedge a \in \Omega\} .$$

Para (Ω^*, R) jest systemem przepisującym. Zauważmy, że funkcja $f(x) = |x|$ jest jego funkcją kontrolną. Zatem system ten ma własność stopu. System ten może służyć do modelowania procesu usuwania duplikatów z ciągu znaków.

Przykład 9.2 *Niech Ω będzie ustalonym alfabetem zawierającym symbol _. Niech*

$$R = \{(x\_\_y, x\_y) : x, y \in \Omega^*\} \cup \{(\_x, x) : x \in \Omega^*\} \cup \{(x\_, x) : x \in \Omega^*\}$$

Para (Ω^*, R) jest systemem przepisującym. Podobnie jak w poprzednim przykładzie funkcja $f(x) = |x|$ jest jego funkcją kontrolną. Zatem system ten ma własność stopu. System ten modeluje proces usuwania zbędnych spacji z ciągu znaków.

Ustalmy system przepisujący $(X, \to)$ oraz rozważmy relację $\to^+$ zdefiniowaną następująco:

$$(x \to^+ y) \leftrightarrow \text{ istnieje obliczenie od x do y .}$$

Łatwo zauważyć, że relacja $\to^+$ jest najmniejszą relacją przechodnią (patrz Def. 4.3) zawierającą relację $\to$.

Definicja 9.4 *1. System przepisujący $(X, \to)$ jest słabo konfluentny jeśli*

$$(\forall x, y, z)((x \to y \wedge x \to z) \to (\exists w)(y \to^+ w \wedge z \to^+ w))$$

2. System przepisujący $(X, \to)$ jest konfluentny jeśli

$$(\forall x, y, z)((x \to^+ y \wedge x \to^+ z) \to (\exists w)(y \to^+ w \wedge z \to^+ w))$$

Twierdzenie 9.3 (Newman) *Załóżmy, że system $R = (X, \to)$ przepisujący ma własność stopu. Wtedy R jest słabo konfluentny wtedy i tylko wtedy, gdy jest konfluentny.*

Dowód. Rozważmy zbiór $A = \{x \in X :\}$ Jeśli $A = X$, to twierdzenie jest udowodnione. Załóżmy zatem, że zbiór $X \setminus A$ jest niepusty oraz niech b będzie □

Definicja 9.5 *Niech $\mathcal{R} = (X, \to)$ będzie systemem przepisującym. Funkcję zdaniową $\varphi(x)$ o dziedzinie X nazywamy niezmiennikiem systemu $\mathcal{R}$ jeśli*

$$(\forall x, y \in X)(((x \to y) \to (\varphi(x) \leftrightarrow \varphi(y))) \ .$$

Zauważmy, że jeśli $\varphi(x)$ jest niezmiennikiem systemu $\mathcal{R}$ oraz $x_0, x_1, \ldots x_k$ jest obliczeniem w $\mathcal{R}$, to $\varphi(x) \leftrightarrow \varphi(y)$.

Przykład 9.3 *(Grecka Urna). W urnie znajduje się 150 czarnych oraz 75 białych kul. Wybieramy z urny dwie kule: jeśli są one tego samego koloru, to do urny wkładamy czarną kulę; jeśli są różne, to do urny wkładamy białą kule. Proces powtarzamy tak długo jak się da.*

Proces ten możemy wymodelować jako system przepisujący. Niech $X = \{1, 2, 3, \ldots\}^2$. Niech $(x, y) \in X$. Liczbę x interpretujemy jako liczbę czarnych kul zaś y jako liczbę białych kul w urnie. Proces wyjmowania i wkładania kul możemy wymodelować jako następująca relację:

$$\begin{aligned} \to \quad = &\{((x, y), (x-1, y)) : x \geq 2\} \cup \{((x, y), (x, y-2)) : y \geq 2\} \cup \\ &\{((x, y), (x-1, y)) : x \geq 1 \wedge y \geq 1\} \ . \end{aligned}$$

Niech $f : X \to \mathbb{N}$ będzie funkcją określoną wzorem $f(x, y) = x + y$. Łatwo sprawdzić, że jest to funkcja kontrolna systemu $(X, \to)$. Zatem system ten ma własność stopu. Stanami końcowymi są pary $(1, 0)$ oraz $(0, 1)$. Zatem każde nieporzedłużalne obliczenie musi zakończyć się w jednym z tych stanów.

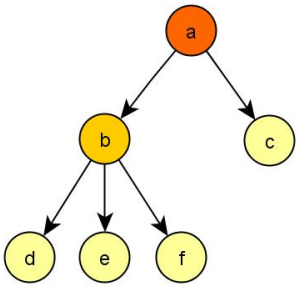
Niech $\varphi((x,y)) = (2|y)$. Każde przekształcenie nie zmienia liczby białych kul lub zmniejsza ją o 2. Zatem φ jest niezmiennikiem naszego systemu. Jeśli (a,b) jest stanem końcowym obliczenia zaczynającego się od pary $(150,75)$, to $\varphi((a,b)) = \varphi((150,75)$. Lecz 75 jest liczbą nieparzystą. Zatem i liczba b musi być nieprzysta. Czyli stanem końcowym musi być para $(0,1)$. Zatem na końcu zostanie jedna biała kula.

9.3 Drzewa

Zajmiemy się teraz klasą częściowych porządków, które służą do modelowania wielu obiektów matematycznych oraz informatycznych. Rozpoczniemy od ogólnej definicji.

Definicja 9.6 ***Drzewem*** *nazywamy częściowy porządek $(T,\leq)$ z elementem najmniejszym w którym dla dowolnego $a \in T$ zbiór $\{y \in T : y \leq a\}$ jest skończonym zbiorem liniowo uporządkowanym przez relację $\leq$.*

Przykład drzewa znajduje się na następującym rysunku:



Elementem najmniejszym, zwanym *korzeniem* w tym drzewie jest element a. Elementy drzewa nazywamy są *wierzchołkami*. W naszym przykładzie wierzchołkami są elementy zbioru $\{a,b,c,d,e,f\}$. Jeśli T jest drzewem oraz $x \in T$, to element $y \in T$ nazywamy *następnikiem* elementu x jeśli $x < y$ oraz nie istnieje element $u \in T$ taki, że $x < u < y$. Następniki nazywamy również *dziećmi*. Zbiór dzieci elementu $x \in T$ oznaczamy przez $scc(x)$. W powyższym przykładzie mamy $scc(a) = \{b,c\}$, $scc(b) = \{d,e\}$ oraz $scc(c) = scc(d) = scc(e) = \emptyset$. Element x drzewa T nazywamy liściem jeśli $scc(x) = \emptyset$. W naszym przykładzie liśćmi są elementy c, d, e i f. Elementy drzewa, które nie są liściami nazywamy *wierzchołkami wewnętrznymi* drzewa.

Wysokością elementu $t \in T$ nazywamy liczbę

$$lh(t) = |\{x \in T : x < t\}| .$$

Zauważmy, że $lh(x) = 0$ wtedy i tylko wtedy, gdy x jest korzeniem. Niech $n \in \mathbb{N}$. Wtedy n-tym piętrem drzewa T nazywamy zbiór $T_n = \{x \in T : lh(x) = n\}$. Liczbę $lh(T) = \sup\{n : T_n \neq \emptyset\}$ nazywamy wysokością drzewa T. Jeśli zbiór $\{n : T_n \neq \emptyset\}$ jest nieograniczony, to mówimy, że T jest drzewem o nieskończonej wysokości. Zauważmy, że

$$T = \bigcup_{n \geq 0} T_n .$$

Przykład 9.4 ***Drzewem słów*** *na zbiorze Ω nazywamy taki niepusty podzbiór $T \subseteq \Omega^*$, że jeśli $w \in T$ oraz $v \in \Omega^*$ i v jest prefiksem w, to $v \in T$. Każde drzewo słów jest drzewem. Niech T będzie drzewem słów na zbiorze Ω. Korzeniem drzewa T jest słowo puste ε. Zauważmy, że $scc(w) = \{wa : a \in \Omega \wedge wa \in T\}$ dla $w \in T$. Wysokością węzła $w \in T$ jest długość ciągu w.*

Funkcję $f : \mathbb{N} \to T$ nazywamy *nieskończoną gałęzią* drzewa T jeśli $(\forall n \in \mathbb{N})(f(n) \in T_n)$ oraz $(\forall n \in \mathbb{N})(f(n) < f(n+1))$.

Przykład 9.5 *Niech $T = \{0,1\}^*$. Wtedy T jest drzewem słów na zbiorze Ω oraz każda funkcja $f \in \{0,1\}^{\mathbb{N}}$ jest jego nieskończoną gałęzią.*

Twierdzenie 9.4 (König) *Każde drzewo nieskończone o skończonych piętrach ma nieskończoną gałąź.*

Dowód. Niech T będzie drzewem spełniającym założenia twierdzenia. Niech $f(0)$ będzie jego wierzchołkiem. Indukcyjnie zdefiniujemy wartości funkcji $f(n)$ w taki sposób, aby zbiór $\{x \in T : f(n) \leq x\}$ był nieskończony oraz aby $f(n) \in T_n$. Z nieskończoności drzewa T wynika, że element $f(0)$ ma tę własność. Załóżmy zatem, że $f(n)$ ma również tę własność. Ze skończoności piętra T_{n+1} wynika, że element $f(n)$ ma skończenie wiele dzieci. Ponadto

$$\{x \in T : f(n) \geq x\} = \{f(n)\} \cup \bigcup_{a \in scc(f(n))} \{x \in T : f(n) \leq x\}.$$

Istnieje więc $a \in scc(f(n))$ takie, że zbiór $\{x \in T : a \leq x\}$ jest nieskończony. Ustalamy takie a oraz kładziemy f(n+1) = a. □

Przykład 9.6 *Niech $\Omega = \mathbb{N}$ oraz niech $T = \{\varepsilon\} \cup \{n0^n : n \in \mathbb{N}\}$, gdzie przez 0^n oznaczamy ciąg długości n złożony z samych zer. Wtedy T jest nieskończonym drzewem słów bez nieskończonej gałęzi, czyli $[T] = \emptyset$. Jednak dla każdego $n \in \mathbb{N}$ istnieje element $w \in T$ taki, że $rnk(w) \geq n$. Zatem T jest drzewem o nieskończonej wysokości. Przykład ten pokazuje, że założenie skończoności pięter w twierdzeniu Königa jest potrzebne.*

Drzewa Binarne

Zajmować się będziemy teraz tylko drzewami skończonymi.

Definicja 9.7

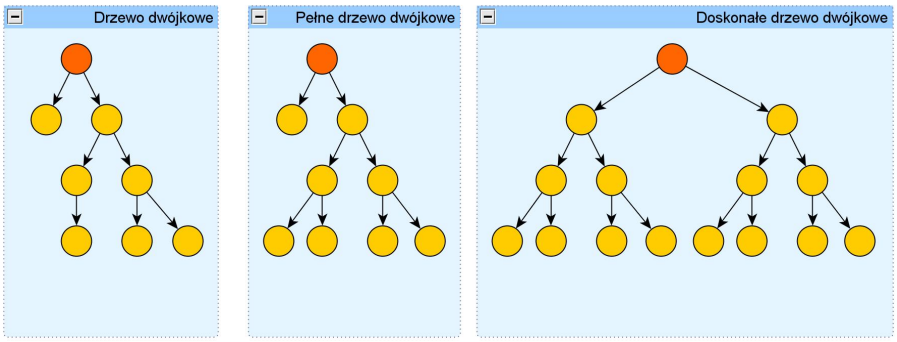
1. ***Drzewem binarnym*** *nazywamy drzewo w którym każdy wierzchołek ma co najwyżej dwójkę dzieci*
2. ***Pełnym drzewem binarnym*** *nazywamy drzewo w którym każdy wierzchołek ma zero lub dwójkę dzieci.*
3. ***Doskonałym drzewem binarnym*** *jest pełne drzewo binarne w którym każdy liść na taka samą wysokość.*

Przykładem doskonałego drzewa binarnego wysokości n jest zbiór $\{w \in \{0,1\}^* : |w| \leq n\}$. Niech T będzie dowolnym drzewem doskonałym o wysokości n. Wtedy

$|T_0| = 1$ oraz jeśli $i + 1 \leq n$, to $|T_{i+1}| = 2 \cdot |T_i|$. A z tego wynika, że $|T_k| = 2^k$ dla wszystkich $k \in \{0, \ldots, n\}$. Zatem drzewo T ma 2^n liści. Następnie

$$|T| = \sum_{i=0}^{n} |T_i| = \sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \,,$$

więc drzewo doskonałe o wysokości n ma $2^{n+1} - 1$ wierzchołków.



Twierdzenie 9.5 *Jeśli T jest pełnym drzewem binarym to T ma $\frac{1}{2}(|T| + 1)$ liści oraz $\frac{1}{2}(|T| - 1)$ węzłów wewnętrznych.*

Dowód. Twierdzenie to udowodnimy indukcją matematyczną. Zauważmy, że jest ono prawdziwe jeśli $|T| = 1$. Załóżmy teraz, że jest ono prawdziwe dla wszystkich takich drzew T, że $|T| < n$. Rozważmy drzewo T takie, że $|T| = n > 1$. Niech a, b będą dziećmi korzenia drzewa T oraz $T_a = \{x \in T : x \geq a\}$ i $T_b = \{x \in T : x \geq b\}$. Wtedy $|T_a| < n$ oraz $|T_b| < n$. Do drzew T_a i T_b możemy więc stosować założenie indukcyjne. Niech L_a i L_b oznaczają zbiory liści w drzewach T_a i T_b. Wtedy, na mocy założenia indukcyjnego, $|L_a| = \frac{1}{2}(|T_a| + 1)$ oraz $|L_b| = \frac{1}{2}(|T_b| + 1)$. Ponadto $L_a \cap L_b = \emptyset$. Niech L oznacza zbiór liści w drzewie T. Wtedy $L = L_a \cup L_b$. Zatem

$$|L| = |L_a| + |L_b| = \frac{1}{2}(|T_a| + 1) + \frac{1}{2}(|T_b| + 1) = \frac{1}{2}(|T_b| + |T_b| + 2) \,.$$

Zauważmy, że $|T| = |T_a| + |T_b| + 1$, więc

$$|L| = \frac{1}{2}(|T_b| + |T_b| + 2) = \frac{1}{2}(|T| + 1) \,.$$

Pierwsza część twierdzenia została więc pokazana. Liczba węzłów wewnętrznych drzewa T jest równa

$$|T| - |L| = |T| - \frac{1}{2}(|T| + 1) = \frac{1}{2}(2|T| - (|T| + 1)) = \frac{1}{2}(|T| - 1) \,,$$

co kończy dowód. □

Rozważania tego rozdziału zakończymy twierdzeniem wykorzystywanym, między innymi, w Teorii Informacji do badania optymalnych metod kodowania.

Twierdzenie 9.6 (Kraft) *Niech $L_1, \ldots, L_k$ będą wysokościami liści w drzewie binarnym. Wtedy*

$$\sum_{i=1}^{k} \frac{1}{2^{L_i}} \leq 1 \,. \tag{9.1}$$

Odwrotnie, jeśli liczby naturalne $L_1, \ldots, L_k$ spełniają nierówność (9.1), to istnieje drzewo binarne T, które ma liście o rzędach $L_1, \ldots, L_k$.

Dowód. (1) Załóżmy, liczby $L_1, \ldots, L_k$ są wysokościami liści w drzewie dwójkowym T. Niech $L = \max\{L_1, \ldots, L_k\}$. Rozszerzmy drzewo T do doskonałego drzewa binarnego wysokości L. Poniżej liścia o rzędzie L_i dodaliśmy zbiór Z_i liści w drzewie T' mocy 2^{L-L_i}. Ponadto, jeśli $i \neq j$ to $Z_i \cap Z_j = \emptyset$. Oczywiście $|Z_1 \cup \ldots \cup Z_k| \leq 2^L$. Zatem

$$\sum_{i=1}^{k} 2^{L-L_i} \leq 2^L \,,$$

czyli $\sum_{i=1}^{k} 2^{-L_i} \leq 1$.

(2) Załóżmy teraz, że liczby $L_1, \ldots, L_k$ spełniają nierówność (9.1). Możemy założyć, że $L_1 \leq \ldots \leq L_k$. Niech, podobnie jak poprzednio, $L = \max\{L_1, \ldots, L_k\}$. Rozważmy doskonałe drzewo binarne T wysokości L. Niech $T_1 = T$ Znajdźmy element x_1 w drzewie T_1 o wysokości L_1 i usuńmy z drzewa T_1 wszystkie elementy mniejsze od x_1. Otrzymane drzewo oznaczmy przez T_2. Powtórzmy ten proces dla $i = 2, \ldots, k$. Jeśli uda na się ten proces, czyli jeśli dla każdego $i = 2, \ldots, k$ znajdziemy choćby jeden element w drzewie T_i, to twierdzenie jest udowodnione. Załóżmy więc, że $a \leq k$ oraz, że znaleźliśmy już elementy $x_1, \ldots, x_{a-1}$. W oryginalnym drzewie T na poziomie L_a znajduje się 2^{L_a} elementów. Z drzewa T usunęliśmy z poziomu L_a

$$\sum_{i=1}^{a-1} 2^{L_a - L_i}$$

elementów. Zauważmy, że $\sum_{i=1}^{a} \frac{1}{2^{L_i}} \leq 1$, czyli $1 \geq \sum_{i=1}^{a-1} \frac{1}{2^{L_i}} + \frac{1}{2^{L_a}}$ czyli $2^{L_a} \geq \sum_{i=1}^{a-1} \frac{L_a}{2^{L_i}} + 1$ więc

$$\sum_{i=1}^{a-1} 2^{L_a - L_i} < 2^{L_a} \,.$$

Zatem w drzewie T_a istnieje element rzędu L_a, czyli nasza konstrukcja jest prawidłowa. □

9.4 Ćwiczenia i zadania

Ćwiczenie 9.1 *Pokaż, że każde pełne drzewo binarne ma nieparzystą liczbę wierzchołków.*

Ćwiczenie 9.2 *Niech T będzie drzewem binarnym wysokości h. Pokaż, że $h + 1 \leq |T| \leq 2^{h+1} - 1$.*

Ćwiczenie 9.3 *Niech T będzie drzewem binarnym. Pokaż, że $\log_2(|T|) - 1 < lh(T) < |T|$.*

Ćwiczenie 9.4 *Pokaż, że system przepisujący z przykładu 9.1 ma własność stopu.*

Ćwiczenie 9.5 *(Grecka Urna). W urnie znajduje się* 150 *czarnych oraz* 75 *białych kul. Wybieramy z urny dwie kule: jeśli są one tego samego koloru, to do urny wkładamy czarną kulę; jeśli są różne, to do urny wkładamy białą kule. Proces powtarzamy tak długo jak się da. Wymodeluj ten proces jako system przepisujący, pokaż, że ma on własność stopu oraz wyznacz kolor ostatniej kuli.*

A Algebry Boole'a

Algebry Boole'a są klasą struktur matematycznych które znajdują zastosowanie w wielu dziedzinach matematyki oraz informatyki: w logice matematycznej, w rachunku zbiorów, w teorii miary, w projektowaniu sieci elektrycznych.

Przed zdefiniowaniem algebr Boole'a dokonamy kilka ustaleń. *Działaniem binarnym* na zbiorze A nazywamy dowolną funkcję $f : A \times A \to A$. *Działaniem unarnym* nazywamy zaś dowolne odwzorowanie $g : A \to A$. Strukturą algebraiczną nazywamy zbiór z ustalonymi działaniami oraz wyróżnionymi elementami. Przekładem struktury jest pierścień liczb całkowitych $(\mathbb{Z}, +, \cdot, 0, 1)$, ciało liczb rzeczywistych $(\mathbb{R}, +, \cdot, 0, 1)$ oraz grupa permutacji $(Sym(n), \circ)$ zbioru $\{1, \ldots, n\}$ ze składaniem.

Definicja A.1 *Strukturę $\mathcal{A} = (A, \vee, \wedge, -, 0, 1)$ nazywamy **algebrą Boole'a** jeśli $0, 1 \in A$, $0 \neq 1$, $\wedge$ i $\vee$ są działaniami binarnymi na zbiorze A, $\neg$ jest działaniem unarnym na zbiorze A oraz*

$1a.$	$x \vee y = y \vee x$	$1b.$	$x \wedge y = y \wedge x$
$2a.$	$x \vee (y \vee z) = (x \vee y) \vee z$	$2b.$	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$
$3a.$	$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$	$3b.$	$(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$
$4a.$	$x \vee 0 = x$	$4b.$	$x \wedge 1 = x$
$5a.$	$x \vee (-x) = 1$	$5b.$	$x \wedge (-x) = 0$

dla dowolnych $x, y, z \in A$. Zbiór A nazywamy uniwersum algebry $\mathcal{A}$

Widzimy, że jeśli $(A, \vee, \wedge, -, 0, 1)$ jest algebrą Boole'a to działania $\vee$ i $\wedge$ są przemienne, łączne oraz wzajemnie rozdzielne. Działanie $\vee$ nazywamy *sumą*, $\wedge$ - *iloczynem* zaś $-$ nazywamy *dopełnieniem*.

Przykład A.1 *Niech A będzie dowolnym zbiorem. Wtedy struktura*

$$\mathcal{P}(A) = (P(A), \cup, \cap, ^c, \emptyset, A)$$

jest algebrą Boole'a. Zerem tej algebry Boole'a jest zbiór pusty zaś jedynką - zbiór A.

Przykład A.2 *Struktura $\mathcal{B} = (\{\mathbb{0}, \mathbb{1}\}, \vee, \wedge, \neg, \mathbb{0}, \mathbb{1})$, gdzie $\mathbb{0}$ oraz $\mathbb{1}$ oznaczają wartości logiczne "fałsz" i "prawda", zaś $\vee$, $\wedge$ i $\neg$ są standardowymi spójnikami logicznymi, jest algebrą Boole'a.*

Przykład A.3 *Na zbiorze $\{\mathbb{0}, \mathbb{1}\}^n = \mathcal{B} \times \ldots \mathcal{B}$ n definiujemy działania boolowskie pochodzące z działań w algebrze $\mathcal{B}_2$:*

$$(x_1, \ldots, x_n) \vee (y_1, \ldots, y_n) = (x_1 \vee y_1, \ldots, x_n \vee y_n),$$

$$(x_1, \ldots, x_n) \wedge (y_1, \ldots, y_n) = (x_1 \wedge y_1, \ldots, x_n \wedge y_n)$$

oraz

$$-(x_1, \ldots, x_n) = (\neg x_1, \ldots, \neg x_n).$$

Za zero przyjmujemy ciąg $\mathbf{0} = (\mathbb{0}, \ldots, \mathbb{0})$ *zaś za jedynkę ciąg* $\mathbf{1} = (\mathbb{1}, \ldots, \mathbb{1})$. *Struktura* $\mathcal{B}_n = (\{\mathbb{0}, \mathbb{1}\}^n, \vee, \wedge, \mathbf{0}, \mathbf{1})$ *jest algebrą Boole'a mocy* 2^n.

Przykład A.4 *Niech* $\mathcal{L}$ *oznacza zbiór wszystkich zdań Rachunku Zdań. Na zbiorze tym określamy relację równoważności:*

$$(\varphi \approx \psi) \leftrightarrow \models (\varphi \leftrightarrow \psi).$$

Na elementach przestrzeni ilorazowej określamy działania:

- $[\varphi] \wedge [\psi] = [\varphi \wedge \psi]$
- $[\varphi] \vee [\psi] = [\varphi \vee \psi]$
- $-[\varphi] = [\neg\varphi]$

Poprawność tych określeń wynika z tautologii, które omawialiśmy w pierwszym wykładzie. Za zero przyjmiemy klasę abstrakcji $\mathbf{0} = [p_0 \wedge (\neg p_0)]$ *(mogliśmy tutaj wziąć tutaj dowolną antytaulogię) zaś za jedynkę weźmiemy klasę abstrakcji* $\mathbf{1} = [p_0 \vee (\neg p_0)]$. *Struktura*

$$(\mathcal{L}/\approx, \vee, \wedge, -, \mathbf{0}, \mathbf{1})$$

jest algebrą Boole'a, zwaną algebrą Lindenbauma.

Twierdzenie A.1 *Niech* $(A, \vee, \wedge, -, 0, 1)$ *będzie algebrą Boole'a. Wtedy dla dowolnych* $a, b \in A$ *mamy:*

1. $a \vee a = a$, $a \wedge a = a$,
2. $a \vee 1 = 1$, $a \wedge 0 = 0$,
3. $a \vee b = b \leftrightarrow a \wedge b = a$.

Dowód. Bezpośrednio z aksjomatów algebry Boole'a wynika, że

$$a = a \vee 0 = a \vee (a \wedge -a) = (a \vee a) \wedge (a \vee -a) = (a \vee a) \wedge 1 = a \vee a.$$

Podobnie

$$a = a \wedge 1 = a \wedge (a \vee -a) = (a \wedge a) \vee (a \wedge -a) = (a \vee a) \vee 0 = a \wedge a,$$

co kończy dowód równości (1). Następnie

$$a \vee 1 = a \vee (a \vee -a) = (a \vee a) \vee -a = a \vee -a = 1$$

oraz

$$a \wedge 0 = a \wedge (a \wedge -a) = (a \wedge a) \wedge -a = a \wedge -a = 0,$$

co kończy dowód równości (2).
Załóżmy teraz, że $a \vee b = b$ wtedy

$$a \wedge b = a \wedge (a \vee b) = (a \wedge a) \vee (a \wedge b) = a \vee (a \wedge b) = (a \wedge 1) \vee (a \wedge b) =$$

$$a \wedge (1 \vee b) = a \wedge 1 = a.$$

Jeśli zaś $a \wedge b = a$, to

$$a \vee b = (a \wedge b) \vee b = (a \vee b) \wedge (b \vee b) = (a \vee b) \wedge b = (a \vee b) \wedge (0 \vee b) =$$

$$(a \wedge 0) \vee b = 0 \vee b = b.$$ □

W każdej algebrze Boole'a można w naturalny sposób zdefiniować częściowy porządek.

Definicja A.2 *Niech* $(A, \vee, \wedge, -, 0, 1)$ *będzie algebrą Boole'a. Kładziemy*

$$a \leq b \leftrightarrow a \wedge b = a. \tag{A.1}$$

Z ostatniego twierdzenia wynika, że $a \leq b \leftrightarrow a \vee b = b$. Z Twierdzenia 2.2 wynika, że w algebrach Boole'a postaci $\mathcal{P}(X)$ relacja ta pokrywa się z relacją inkluzji obciętej do rodziny podzbiorów zbioru X.

Twierdzenie A.2 *Relacja* $\leq$ *na algebrze Boole'a* $(A, \vee, \wedge, -, 0, 1)$ *zdefiniowana wzorem A.1 jest częściowym porządkiem na zbiorze A. Najmniejszym elementem w tym porządku jest 0, zaś największym element jest 1.*

Dowód. Nierówność $a \leq a$ wynika z równości $a \wedge a = a$. Załóżmy teraz, że $a \leq b$ oraz $b \leq a$. Wtedy $a \wedge b = a$ oraz $a \wedge b = b$ więc $a = b$. Zatem relacja $\leq$ jest słabo-antysymetryczna. Załóżmy teraz, że $a \leq b$ oraz $b \leq c$ Wtedy

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a,$$

Zatem relacja $\leq$ jest przechodnia. Ponieważ $0 \wedge a = 0$ dla dowolnego $a \in A$, więc 0 jest $\leq$-najmniejszym elementem A. Z równości $a \wedge 1 = a$ wynika, że 1 jest $\leq$-największym elementem zbioru A. □

Bezpośrednio z definicji relacji $\leq$ w algebrze Boole'a wynika szereg jej dodatkowych własności. Na przykład, bez trudu możemy pokazać pewien wariant monotoniczności. Mianowicie jeśli $a \leq b$ oraz $c \leq d$ to $a \wedge c \leq b \wedge d$. Rzeczywiście, założenie można zapisać w postaci $a \wedge b = a$ i $c \wedge d = c$, więc $(a \wedge c) \wedge (b \wedge d) = (a \wedge b) \wedge (c \wedge d) = a \wedge c$ a więc $a \wedge c \leq b \leq d$. Podobnie, z nierówności $a \leq b$ oraz $c \leq d$ wynika, że $a \vee c \leq b \vee d$.

Wniosek A.1 *Niech* $(A, \vee, \wedge, -, 0, 1)$ *będzie algebrą Boole'a. Wtedy dla dowolnego* $a \in A$ *mamy*

$$(\forall x \in A)(x = -a \leftrightarrow (a \vee x = 1) \wedge (a \wedge x = 0)).$$

Dowód. Implikacja w jedną stronę jest oczywista, gdyż wynika bezpośrednio z określenia algebry Boole'a. Załóżmy zatem, że $x \in A$, $a \vee x = 1$ oraz $a \wedge x = 0$. Z pierwszej równości wynika, że $(a \wedge -a) \vee (x \wedge -a) = -a$, czyli, że $x \wedge -a = -a$, więc $-a \leq x$. Z drugiej równości wynika, że $(a \vee -a) \wedge (x \vee -a) = -a$, czyli $x \vee -a = -a$, czyli, że $x \leq -a$. Ze słabej antysymetrii relacji $\leq$ wynika równość $x = -a$, która kończy dowód. □

Wniosek A.2 *Niech* $(A, \vee, \wedge, -, 0, 1)$ *będzie algebrą Boole'a. Wtedy dla dowolnych* $a, b \in A$ *mamy:*

1. $-(-a) = a$,
2. $-(a \vee b) = (-a) \wedge (-b)$,
3. $-(a \wedge b) = (-a) \vee (-b)$.

Dowód. Zauważmy, że zarówno a jak i element $--a$ spełniają formułę $(-a \vee x = 1) \wedge (-a \wedge x = 0)$. Z poprzedniego wniosku wynika więc, że $a = -(-a)$.
Zauważmy następnie, że

$$((-a) \wedge (-b)) \wedge (a \vee b) = ((-a) \wedge (-b) \wedge a) \vee ((-a) \wedge (-b) \wedge b) = 0 \vee 0 = 0.$$

Podobnie, bez trudu pokazujemy, że $((-a) \wedge (-b)) \vee (a \vee b) = 1$, co na mocy poprzednio wniosku pokazuje, że $-(a \vee b) = (-a) \wedge (-b)$.
Ostatnią równość pokazuje się podobnie jak poprzednią. □

Ostatnie dwie równości ostatniego wniosku nazywają się, oczywiście, prawami de Morgana algebr Boole'a.

Definicja A.3 *Niech* $\mathcal{A} = (A, \vee, \wedge, -, 0^A, 1^A)$ *oraz* $\mathcal{B} = (B, +, \cdot, -, 0^B, 1^B)$ *będą algebrami Boole'a. Bijekcję* $f : A \to B$ *nazywamy izomorfizmem algebr* $\mathcal{A}$ *i* $\mathcal{B}$ *jeśli* $f(x \vee y) = f(x) + f(y)$, $f(x \wedge y) = f(x) \cdot f(y)$, $f(-x) = -f(x)$, $f(0^A) = 0^B$ *oraz* $f(1^A) = 1^B$.

Przykład A.5 *Łatwo sprawdzić, że dowolna dwuelementowa algebra Boole'a jest izomorficzna z algebrą* $\mathcal{B}_2$ *z Przykładu A.2.*

Widzimy więc, że z dokładnością do izomorfizmu istnieje dokładnie jedna dwuelementowa algebra Boole'a.

Przykład A.6 *Algebra* $\mathcal{B}_n$ *jest izomorficzna z algebrą* $P(\{1, \ldots, n\})$.

Definicja A.4 *Niech* $(A, \vee, \wedge, -, 0^A, 1^A)$ *będzie algebrą Boole'a. Element* $a \in A$ *nazywamy* ***atomem*** *jeśli* $a > 0$ *oraz nie istnieje element* $b \in A$ *taki, że* $0 < b < a$.

Łatwo można sprawdzić, że element a jest atomem wtedy i tylko wtedy gdy jest elementem minimalnym w częściowym porządku $(A \setminus \{0\}, \leq)$. W algebrach postaci $\mathcal{P}(X)$ atomami są oczywiście singletony $\{a\}$ elementów $a \in X$. Jednakże nie wszystkie algebry Boole'a posiadają atomy. Jest jasne, że przykładów algebr bez atomów należy szukać wśród algebr nieskończonych, gdyż w każdym skończonym porządku poniżej dowolnego elementu istnieje element minimalny.

Przykład A.7 *Niech* S *będzie rodziną wszystkich podzbiorów odcinka* $[0, 1)$ *postaci*

$$[a_0, b_1) \cup \ldots \cup [a_n, b_n)$$

gdzie $0 \leq a_0 < b_0 < \ldots < a_n < b_n \leq 1$. *Do rodziny tej zaliczamy również zbiór pusty. Rodzina ta jest zamknięta na przekroje i dopełnienia. Struktura* $(S, \cup, \cap, ^c, \emptyset, [0, 1))$ *jest więc algebrą Boole'a. Algebra ta nie posiada atomów.*

A.1 Ciała zbiorów

Omówimy teraz pewną klasę rodzin zbiorów, które odgrywają istotną rolę nie tylko w badaniach algebr Boole'a, lecz są również podstawowymi obiektami badań teorii miary oraz probabilistyki.

Definicja A.5 *Rodzinę $\mathcal{S} \subseteq P(X)$ nazywamy **ciałem podzbiorów** zbioru X jeśli $\mathcal{S} \neq \emptyset$ oraz $A \cup B \in \mathcal{S}$ i $A^c \in \mathcal{S}$ dla dowolnych $A, B \in \mathcal{S}$.*

Z praw de Morgana rachunku zbiorów wynika, że jeśli $\mathcal{S}$ jest ciałem, to jest ono zamknięte na operację mnożenia zbiorów, czyli z tego, że $A, B \in \mathcal{S}$ wynika, że $A \cap B \in \mathcal{S}$. A z tego zaś bezpośrednio wynika, że $\{\emptyset, X\} \subseteq \mathcal{S}$ dla dowolnego ciała podzbiorów zbioru X. Oczywiście $\{\emptyset, X\}$ jest najmniejszym w sensie inkluzji ciałem podzbiorów zbioru X, zaś $P(X)$ jest największym ciałem podzbiorów zbioru X.

Twierdzenie A.3 *Przekrój dowolnej rodziny ciał podzbiorów zbioru X jest ciałem podzbiorów zbioru X.*

Dowód. Niech $(S_t)_{t\in T}$ będzie rodziną ciał podzbiorów zbioru X. Dla każdego $t \in T$ zachodzi inkluzja $\{0, X\} \subseteq S_t$, zatem $\{0, X\} \subseteq \bigcap_{t\in T} S_t$, a więc $\bigcap_{t\in T} S_t$ jest zbiorem niepustym. Załóżmy teraz, że $A, B \in \bigcap_{t\in T} S_t$. Wtedy dla każdego $t \in T$ mamy $A, B \in S_t$. Zatem $A \cup B \in S_t$ oraz $A^c \in S_t$ dla każdego $t \in T$, co oznacza, że $A \cup B \in \bigcap_{t\in T} S_t$ oraz $A^c \in \bigcap_{t\in T} S_t$. Tak więc $\bigcap_{t\in T} S_t$ jest rodziną zbiorów zamknięta na operację sumy oraz dopełnienia do zbioru X. Zatem $\bigcap_{t\in T} S_t$ jest ciałem podzbiorów zbioru X. □

Z udowodnionego twierdzenia wynika, że dla dowolnej rodziny $\mathcal{A}$ podzbiorów ustalonego zbioru X istnieje najmniejsze ciało podzbiorów zbioru X które zawiera rodzinę $\mathcal{A}$. Jest nim bowiem ciało

$$c(\mathcal{A}, X) = \bigcap \{\mathcal{S} \subseteq P(X) : \mathcal{A} \subseteq \mathcal{S} \wedge \mathcal{S} \text{ jest ciałem podzbiorów } X\},$$

które nazywamy *ciałem generowanym* przez rodzinę $\mathcal{A}$.

Przykład A.8 *Niech $A \subset X$. Wtedy ciałem generowanym przez rodzinę $\{A\}$ jest $\{\emptyset, A, A^c, X\}$.*

Definicja A.6 *Niech $\mathcal{A} = (A_1, \ldots, A_n)$ będzie indeksowaną rodziną podzbiorów zbioru X. Dla $\sigma \in \{0, 1\}^n$ określamy*

$$A_\sigma = \bigcap_{i=1}^{n} A_i^{\sigma(i)},$$

gdzie $A_i^0 = X \setminus A_i$ oraz $A_i^1 = A_i$. Zbiory postaci A_σ nazywamy składowymi rodziny $\mathcal{A}$.

Niech $A = (A_1, \ldots, A_n)$ będzie rodziną podzbiorów zbioru X oraz załóżmy, że $\sigma, \eta \in \{0, 1\}^n$ oraz $\sigma \neq \eta$. Ustalmy $i \in \{1, \ldots, n\}$ takie, że $\sigma(i) \neq \eta(i)$. Wtedy

$$A_\sigma \cap A_\eta \subseteq A_i^{\sigma(i)} \cap A_i^{\eta(i)} = \emptyset.$$

Widzimy więc, że różne składowe są rozłączne. Ustalmy teraz $x \in X$. Dla każdego $i \in \{1, \ldots, n\}$ prawdziwa jest równość $A_i^0 \cup A_i^1 = X$. Zatem dla każdego $i \in \{1, \ldots, n\}$ istnieje $\sigma(i)$ takie, że $x \in A_i^{\sigma(i)}$. Wtedy $x \in A_\sigma$. Pokazaliśmy więc, że $\bigcup\{A_\sigma : \sigma \in \{0,1\}^n\} = X$. Rodzina wszystkich składowych $\{A_\sigma : \sigma \in \{0,1\}^n\}$ jest więc rozbiciem zbioru X. Pokażemy teraz, jak za pomocą składowych można podać opis ciała zbiorów generowanego przez skończone rodziny zbiorów.

Twierdzenie A.4 *Niech $\mathcal{A} = (A_1, \ldots, A_n)$ będzie indeksowaną rodziną podzbiorów zbioru X. Wtedy*

$$c(\{A_1, \ldots, A_n\}, X) = \{\bigcup_{\sigma \in S} A_\sigma : S \in P(\{0,1\}^n)\}$$

Dowód. Niech $\mathcal{C} = \{\bigcup_{\sigma \in S} A_\sigma : S \in P(\{0,1\}^n)\}$. Zauważmy, że jeśli $\mathcal{S}$ jest ciałem podzbiorów X takim, że $\{A_1, \ldots, A_n\} \subseteq \mathcal{S}$, to $\mathcal{C} \subseteq \mathcal{S}$. Wystarczy więc pokazać, że $\mathcal{C}$ jest ciałem zbiorów zawierającym rodzinę zbiorów $\{A_1, \ldots, A_n\}$.
Zauważmy najpierw, że

$$A_i = \bigcup\{A_\sigma : \sigma \in \{0,1\}^n \wedge \sigma(i) = 1\},$$

więc $\{A_1, \ldots, A_n\} \subseteq \mathcal{C}$. Niech $S, T \subseteq \{0,1\}^n$. Łatwo sprawdzić, że

$$\bigcup_{\sigma \in S} A_\sigma \cup \bigcup_{\sigma \in T} A_\sigma = \bigcup_{\sigma \in S \cup T} A_\sigma,$$

oraz

$$(\bigcup_{\sigma \in S} A_\sigma)^c = \bigcup_{\sigma \in \{0,1\}^n \setminus S} A_\sigma,$$

więc $\mathcal{C}$ jest ciałem podzbiorów zbioru X, co kończy dowód. □

Definicja A.7 *Rodzinę zbiorów $\mathcal{A} = (A_1, \ldots, A_n)$ nazywamy niezależną, jeśli każda jej składowa jest niepusta.*

Jeśli $\mathcal{A} = (A_1, \ldots, A_n)$ jest niezależną rodziną podzbiorów zbioru X, to wtedy ciało $s(\mathcal{A})$ ma 2^{2^n} elementów.

Opis ciał generowanych przez nieskończone rodziny zbiorów jest z reguły znacznie bardziej skomplikowany. W niektórych przypadkach można jednak podać pełen ich opis.

Przykład A.9 *Niech X będzie zbiorem nieskończonym oraz niech $\mathcal{A} = \{A \in P(X) : |A| < \aleph_0\}$. Wtedy $c(\mathcal{A}, X) = \{A \subseteq X : |A| < \aleph_0 \vee |X \setminus A| < \aleph_0\}$.*

Zauważmy, że jeśli $\mathcal{S}$ jest ciałem podzbiorów niepustego zbioru X, to struktura $(\mathcal{S}, \cup, \cap, ^c, \emptyset, X)$ jest algebrą Boole'a. W algebrach tej postaci nierówność $\leq$ pokrywa się, podobnie jak w algebrach postaci $\mathcal{P}(X)$, z inkluzją obciętą do rodziny zbiorów $\mathcal{S}$. W dalszej części tego wykładu pokażemy, że każda algebra Boole'a jest algebrą tej postaci.

W wielu dziedzinach matematyki ważną rolę odgrywają ciała zbiorów, które zamknięte są na przeliczalne sumy.

Definicja A.8 *Ciało $\mathcal{A}$ podzbiorów zbioru X nazywamy σ-**ciałem** jeśli dla dowolnego ciągu $(A_n)_{n \in \mathbb{N}}$ elementów ciała $\mathcal{A}$ mamy $\bigcup_{n \in \mathbb{N}} A_n \in \mathcal{A}$.*

Z twierdzenia de'Morgana wynika, że jeśli $\mathcal{A}$ jest σ-ciałem oraz $\{A_n : n \in \mathbb{N}\} \subseteq \mathcal{A}$, to $\bigcap_{n\in\mathbb{N}} A_n \in \mathcal{A}$. Rzeczywiście, jeśli $\{A_n : n \in \mathbb{N}\} \subseteq \mathcal{A} \subseteq P(X)$, to również $\{A_n^c : n \in \mathbb{N}\} \subseteq \mathcal{A}$ (dopełnienia bierzemy do przestrzeni X). Zatem $\bigcup_{n\in\mathbb{N}} A_n^c \in \mathcal{A}$, więc również

$$\bigcap_{n\in\mathbb{N}} A_n = \big(\bigcup_{n\in\mathbb{N}} A_n^c\big)^c \in \mathcal{A}.$$

Podobne rozumowanie do tego, które przeprowadziliśmy w dowodzie Twierdzenia A.3 pokazuje, że przekrój dowolnej rodziny σ ciał podzbiorów ustalonego zbioru X jest również σ-ciałem. A z tego wynika, że dla każdej rodziny zbiorów $\mathcal{A} \subseteq P(X)$ istnieje najmniejsze σ-ciało podzbiorów X, które zawiera rodzinę $\mathcal{A}$. Jest nim

$$\sigma(\mathcal{A}, X) = \bigcap\{\mathcal{S} \subseteq P(X) : \mathcal{A} \subseteq \mathcal{S} \wedge \mathcal{S} \text{ jest } \sigma - \text{ciałem podzbiorów } X\}.$$

Ciało to nazywamy *σ-ciałem generowanym* przez rodzinę zbiorów $\mathcal{A}$.

Rozważmy rodzinę $\mathcal{O} = \{(a, b) : a, b \in \mathbb{R}\}$ wszystkich odcinków otwartych liczb rzeczywistych. Niech $\mathbf{B}(\mathbb{R}) = \sigma(\mathcal{O}, \mathbb{R})$. Ciało $\mathbf{B}(\mathbb{R})$ nazywamy σ-ciałem podzbiorów borelowskich prostej rzeczywistej, zaś jego elementy nazywamy podzbiorami borelowskimi prostej rzeczywistej.

A.2 Ideały i filtry

Pojęcia ideału oraz filtru zastosowane do rodzin zbiorów precyzują pojęcie "małego zbioru" oraz "wielkiego zbioru". Wykorzystywane są one w wielu dziedzinach matematyki.

Definicja A.9 *Niech $(A, \vee, \wedge, -, 0, 1)$ będzie algebrą Boole'a. Zbiór $I \subseteq A$ nazywamy **ideałem** jeśli jest niepusty oraz*

1. $(\forall x \in I)(\forall y)(y \leq x \to y \in I)$,
2. $(\forall x, y \in I)((x \in I \wedge y \in I) \to x \vee y \in I)$.

Niech $(A, \vee, \wedge, -, 0, 1)$ będzie algebrą Boole'a. Oczywiście cały zbiór A jest ideałem w tej algebrze. Ten ideał nazywamy *ideałem niewłaściwym*. Łatwo zauważyć, że ideał I jest ideałem niewłaściwym wtedy i tylko wtedy, gdy $1 \in I$. Ideał nazywamy *właściwym* jeśli nie jest ideałem niewłaściwym. Niech teraz $a \in A$. Oznaczmy przez I_a zbiór $\{x \in A : x \leq a\}$. Wtedy $a \in I_a$. Jeśli $y \leq x \in I_a$ to $y \leq x \leq a$, więc $y \in I_a$. Jeśli zaś $x \in I_a$ oraz $y \in I_a$ to $x \leq a$ i $y \leq a$, więc $x \vee y \leq a$ czyli $x \vee y \in I_a$. Zbiór I_a jest więc ideałem. Nazywamy go *ideałem głównym* wyznaczonym przez element a. Ideał I_a jest właściwy wtedy i tylko wtedy, gdy $a \neq 1$. Nie każdy ideał jest ideałem głównym.

Przykład A.10 *Niech $[\mathbb{N}]^{<\aleph_0} = \{X \subseteq \mathbb{N} : |X| < \aleph_0\}$. Wtedy $[\mathbb{N}]^{<\aleph_0}$ jest ideałem w algebrze $\mathcal{P}(\mathbb{N})$. Nie jest on ideałem głównym. Warto zauważyć, że każde jego rozszerzenie do ideału właściwego jest ideałem niegłównym.*

Twierdzenie A.5 *Każdy ideał w skończonej algebrze Boole'a jest ideałem głównym.*

Dowód. Niech I będzie ideałem w skończonej algebrze Boole'a. Wtedy I jest zbiorem skończonym. Niech $I = \{a_1, \ldots, a_n\}$ oraz $a = a_1 \vee \ldots \vee a_n$. Wtedy $a \in I$ oraz $x \leq a$ dla dowolnego elementu $x \in I$. Zatem $I = I_a$.

□

Definicja A.10 *Niech $(A, \vee, \wedge, -, 0, 1)$ będzie algebrą Boole'a. Zbiór $F \subseteq A$ nazywamy **filtrem** jeśli jest niepusty oraz*

1. $(\forall x \in F)(\forall y)(x \leq y \rightarrow y \in F)$,
2. $(\forall x, y \in F)(x \wedge y \in F)$.

Pojęcie filtru jest dualne do pojęcia ideału w następującym sensie:

- jeśli I jest ideałem w danej algebrze Boole'a, to zbiór $F = \{-a : a \in I\}$ jest filtrem w tej algebrze
- jeśli F jest filtrem w danej algebrze Boole'a, to zbiór $I = \{-a : a \in F\}$ jest ideałem w tej algebrze

Pojęcia "ideal właściwy", "ideał główny" mają swoje dualne odpowiedniki dla filtrów. Filtr F jest właściwy jeśli $0 \notin F$. Filtr F jest filtrem głównym, jeśli istnieje taki element $a \in A$, że $F = \{x \in A : a \leq x\}$. Filtr ten oznaczamy symbolem F_a.

Definicja A.11 *Niech $\mathcal{A} = (A, \vee, \wedge, -, 0, 1)$ będzie algebrą Boole'a. Filtr F algebry $\mathcal{A}$ nazywamy **ultrafiltrem** jeśli jest filtrem właściwym oraz każdy filtr istotnie go rozszerzający nie jest właściwy.*

Alterantywną nazwą na ultrafiltr jest określenie "*filtr maksymalny*". Filtr główny F_a jest ultrafiltrem wtedy i tylko wtedy, co łatwo sprawdzić, gdy a jest atomem.

Twierdzenie A.6 *Każdy właściwy filtr można rozszerzyć do ultrafiltru.*

Dowód. Niech F będzie właściwym filtrem w algebrze Boole'a o nośniku A. Rozważmy rodzinę

$$\mathcal{H} = \{G \subset A : F \subseteq G \wedge G \text{ jest filtrem właściwym}\}.$$

Pokażemy, że $(\mathcal{H}, \subseteq)$ spełnia założenia Lematu Kuratowskiego-Zorna. Załóżmy bowiem, że $\mathcal{S} \subseteq \mathcal{H}$ jest liniowo uporządkowany przez inkluzję. Pokażemy, że $\bigcup \mathcal{S}$ jest elementem $\mathcal{H}$.
Jasne jest, że $F \subseteq \bigcup \mathcal{S}$ oraz, że $0 \notin \bigcup \mathcal{S}$. Załóżmy, że $x \in \bigcup \mathcal{S}$ oraz $x \leq y$. Istnieje wtedy $G \in \mathcal{S}$ taki, że $x \in G$. Lecz G jest filtrem, więc $y \in G$, a zatem $y \in \bigcup \mathcal{S}$.
Załóżmy teraz, że $x, y \in \bigcup \mathcal{S}$. Istnieją wtedy takie filtry $G_1, G_2 \in \mathcal{S}$, że $x \in G_1$ oraz $y \in G_2$. Rodzina $\mathcal{S}$ jest liniowo uporządkowana przez inkluzję, więc $G_1 \subseteq G_2$ lub $G_2 \subseteq G_1$. W pierwszym przypadku $x, y \in G_2$, więc $x \vee y \in G_2$, a więc $x \vee y \in \mathcal{S}$. W drugim przypadku $x \vee y \in G_1$, a więc również $x \vee y \in \mathcal{S}$. Pokazaliśmy więc, że $\bigcup \mathcal{S}$ jest elementem rodziny $\mathcal{H}$.
Na mocy Lematu Kuratowskiego-Zorna istnieje element maksymalny w rodzinie $\mathcal{H}$. Zatem istnieje ultrafiltr rozszerzający F. □

A.3 Twierdzenie o reprezentacji

Rozważania rozpoczniemy od pewnej prostej charakteryzacji ultrafiltrów.

Twierdzenie A.7 *Niech F będzie filtrem właściwym w algebrze Boole'a o uniwersum A. Wtedy następujące zdania są równoważne:*

1. *F jest ultrafiltrem,*
2. *$(\forall a \in A)(a \in F \vee -a \in F)$,*
3. *$(\forall a, b \in A)(a \vee b \in F \rightarrow (a \in F) \vee (b \in F))$.*

Dowód. Załóżmy najpierw, że prawdziwe jest zdanie (2). Załóżmy, że $G \supseteq F$ jest filtrem takim, że $G \neq F$. Niech $a \in G \setminus F$. Wtedy $a \notin F$, więc na mocy założenia mamy $-a \in F$. Lecz wtedy $a \in G$ oraz $-a \in G$, zatem i $0 = a \wedge (-a) \in G$, więc G nie jest filterm właściwym. Zatem F jest ultrafiltrem. Pokazaliśmy więc implikację (2) $\rightarrow$ (1).

Załóżmy teraz, że zdanie (2) jest fałszywe, czyli, że istnieje taki element $a \in A$, że $a \notin F$ oraz $-a \notin F$. Rozważmy następujący zbiór

$$G = \{x \in A : (\exists b \in F)(b \wedge a \leq x)\}.$$

Jest jasne, że jeśli $x \in G$ oraz $x \leq y$ to $y \in G$. Załóżmy, że $x_1 \in G$ oraz $x_2 \in G$. Istnieją wtedy takie elementy $b_1, b_2 \in F$, że $b_1 \wedge a \leq x_1$ oraz $b_2 \wedge a \leq x_2$. Niech $b = b_1 \wedge b_2$. Wtedy $b \in F$ oraz $b \wedge a \leq x_1 \wedge x_2$, więc $x_1 \wedge x_2 \in G$. Zatem G jest filtrem. Zauważmy, że jeśli $b \in F$ to $b \wedge a \neq 0$. Zatem G jest filtrem właściwym. Lecz $a \in G$. Zatem G jest właściwym istotnym rozszerzeniem filtru F. Zatem F nie jest ultrafiltrem. A więc zdanie (1) nie jest prawdziwe. Pokazaliśmy więc, że zdania (1) i (2) są równoważne.

Zdanie (3) zastosowane do pary elementów $\{a, -a\}$ implikuje zdanie(2). Załóżmy więc, że F jest ultrafiltrem oraz, że $a \vee b \in F$. Gdyby $a \notin F$ oraz $b \notin F$, to ze zdania (2) mamy $-a \in F$ i $-b \in F$, a więc $(-a) \wedge (-b) \in F$. Na mocy prawa de Morgana otrzymujemy więc $-(a \vee b) \in F$, co jest sprzeczne z tym, że filtr F jest właściwy. □

Definicja A.12 ***Zbiorem Stone'a*** *algebry Boole'a $\mathcal{A}$ o nośniku A nazywamy zbiór*

$$st(\mathcal{A}) = \{F \subseteq A : F \textit{ jest ultrafiltrem}\}.$$

Odwzorowaniem Stone'a *nazywamy funkcję $s : A \rightarrow P(st(\mathcal{A}))$ określoną wzorem*

$$s(a) = \{F \in st(\mathcal{A}) : a \in F\}.$$

Twierdzenie A.8 *Odwzorowanie Stone'a posiada następujące własności:*

1. *$s(-a) = st(\mathcal{A}) \setminus s(a)$,*
2. *$s(a \vee b) = s(a) \cup s(b)$,*
3. *$s(a \wedge b) = s(a) \cap s(b)$.*

Dowód. Niech A będzie nośnikiem algebry Boole'a $\mathcal{A}$. Rozważmy dowolny ultrafiltr $F \in st(\mathcal{A})$. Na mocy Twierdzenia A.7 mamy

$$F \in s(-a) \leftrightarrow -a \in F \leftrightarrow \neg(a \in F) \leftrightarrow F \in st(\mathcal{A}) \setminus s(a).$$

Własność (1) została więc pokazana. Własność (2) również wynika z Twierdzenia A.7:

$$F \in s(a \vee b) \leftrightarrow a \vee b \in F \leftrightarrow (a \in F) \vee (b \in F) \leftrightarrow$$
$$F \in s(a) \vee F \in s(b) \leftrightarrow F \in s(a) \cup s(b)$$

Własność (3) wynika z tylko tego, że F jest filtrem:

$$F \in s(a \wedge b) \leftrightarrow a \wedge b \in F \leftrightarrow (a \in F) \wedge (b \in F) \leftrightarrow$$
$$F \in s(a) \wedge F \in s(b) \leftrightarrow F \in s(a) \cap s(b).$$ □

Rozważania o algebrach Boole'a zakończymy słabą wersją twierdzenia Stone'a o reprezentacji.

Wniosek A.3 *Dla każdej algebry Boole'a $\mathcal{B}$ istnieje zbiór X oraz ciało S podzbiorów zbioru X takie, że algebry $\mathcal{B}$ oraz $(S, \cup, \cap, ^c, \emptyset, X)$ są izomorficzne.*

Dowód. Niech $X = st(\mathcal{B})$ oraz $S = \{s(b) : s(b) \in B\}$. Pokażemy, że odwzorowanie Stone'a s jest różnowartościowe. Załóżmy więc, że $a, b \in B$ oraz $a \neq b$. Wtedy $a - b \neq 0$ lub $b \neq a = 0$. W pierwszym przypadku niech F będzie ultrafiltream takim, że $a - b = a \wedge (-b) \in F$. Wtedy $F \in s(a)$ oraz $F \notin s(b)$, zatem $s(a) \neq s(b)$. W drugim przypadku należy wziąć ultrafiltr F taki, że $b - a \in F$. Pokazaliśmy więc, że s jest różnowartościowe. A więc s jest szukanym izomorfizmem. □

Uwaga. Na zbiorze $st(B)$ możemy określić naturalną topologię której bazą jest rodzina $\{s(b) : s(b) \in B\}$. Ta przestrzeń topologiczna nazywa się przestrzenią Stone'a algebry Boole'a $\mathcal{B}$. Posiada ona szereg interesujących własności i zastosowań. W szczególności jest ona zwartą przestrzenią Hausdorffa.

A.4 Ćwiczenia i zadania

Ćwiczenie A.1 *Narysuj diagramy Hassego algebr Boole'a $\mathcal{B}_1$, $\mathcal{B}_2$ oraz $\mathcal{B}_3$. Ile atomów mają te algebry?*

Ćwiczenie A.2 *Załóżmy, że $\emptyset \neq A \subset B \subset X$. Ile elementów ma ciało podzbiorów zbioru X generowane przez rodzinę $\{A, B\}$?*

Ćwiczenie A.3 *Pokaż, nie powołując się na twierdzenie a reprezentacji, że jedyną, z dokładnością do izomorfizmu, czteroelementową algebrą Boole'a jest $\mathcal{P}(\{0, 1\})$.*

Ćwiczenie A.4 *Pokaż, że jeśli $|X| = |Y|$ to algebry $P(X)$ oraz $P(Y)$ są izomorficzne.*

Ćwiczenie A.5 *Pokaż, że w dowolnej algebrze Boole'a, z nierówności $a \leq b$ oraz $c \leq d$ wynikają nierówności $a \vee c \leq b \vee d$ oraz $a \wedge c \leq b \wedge d$.*

Ćwiczenie A.6 *Ciało zbiorów $\mathcal{S}$ nazywamy σ-ciałem jeśli dla dowolnej rodziny $(A_n)_{n\in\mathbb{N}}$ zbiorów z ciała $\mathcal{S}$ ich suma $\bigcup_{n\in\mathbb{N}} A_n$ należy do $\mathcal{S}$. Pokaż, że przekrój dowolnej rodziny σ-ciał podzbiorów ustalonego zbioru X jest również σ-ciałem.*

Ćwiczenie A.7 *Opisz σ-ciało generowane przez rodzinę jednoelementowych podzbiorów zbioru $\mathbb{N}$. Opisz σ-ciało generowane przez rodzinę przeliczalnych podzbiorów zbioru $\mathbb{R}$.*

Ćwiczenie A.8 *Pokaż, że filtr główny F_a jest ultrafiltrem wtedy i tylko wtedy, gdy a jest atomem.*

Ćwiczenie A.9 *Pokaż, że jeśli $\mathcal{A} = (A_1, \ldots, A_n)$ jest niezależną rodziną podzbiorów zbioru X, to ciało $s(\mathcal{A})$ ma $2^{(2^n)}$ elementów.*

Ćwiczenie A.10 *Dla każdej liczby naturalnej n znajdź n- elementową rodzinę zbiorów niezależnych.*

Ćwiczenie A.11 *Pokaż,że następujące podzbiory prostej rzeczywistej $\mathbb{R}$ są zbiorami borelowskimi: $[0,1]$, $[0,1]\cup(1,2]$,$\{1\}$, dowolny podzbiór przeliczalny $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{R}\setminus\mathbb{Q}$.*

Zadanie A.1 *Pokaż, że jeśli algebry $\mathcal{P}(X)$ oraz $\mathcal{P}(Y)$ są izomorficzne, to $|X| = |Y|$.*

Zadanie A.2 *Pokaż, że metoda dowodzenia twierdzeń postaci $\Phi = \Psi$, gdzie Φ i Ψ są wyrażeniami zbudowanymi z operacji $\cup$,$\cap$,^{c} za pomocą diagramów Venna jest poprawna.*

Zadanie A.3 *Niech $\mathcal{B}$ będzie skończoną algebrą Boole'a.*

1. *Opisz wszystkie ultrafiltry w $\mathcal{B}$,*
2. *Wyznacz funkcję Stone'a algebry $\mathcal{B}$,*
3. *Wyznacz moc algebry $\mathcal{B}$.*

Zadanie A.4 *Wyznacz wszystkie ultrafiltry w ciele zbiorów*

$$\mathcal{S} = \{X \subseteq \mathbb{N} : |X| < \aleph_0 \vee |\mathbb{N}\setminus X| < \aleph_0\}.$$

Zadanie A.5 *Pokaż, że w każdej nieskończonej algebrze Boole'a istnieje ultrafiltr niegłówny.*

Zadanie A.6 *Pokaż, że istnieje rodzina zbiorów $\mathcal{A} \subseteq P(\mathbb{N})$ taka, że $|\mathcal{A}| = \mathfrak{c}$ oraz dla dowolnych $n, m \in \mathbb{N}$ oraz parami różnych $X_1, \ldots, X_n, Y_1, \ldots, Y_m \in \mathcal{A}$ mamy*

$$X_1 \cap \ldots \cap X_n \cap (\mathbb{N}\setminus Y_1) \cap \ldots \cap (\mathbb{N}\setminus Y_m) \neq \emptyset.$$

Zadanie A.7 *Wywnioskuj z poprzedniego zadania, że $|st(P(\mathbb{N})| = 2^{\mathfrak{c}}$.*

Zadanie A.8 *Zbiór $X \subseteq \mathbb{R}$ nazywamy zbiorem **miary Lebesgue'a zero**, jeśli dla każdego $\varepsilon > 0$ istnieje rodzina odcinków $((a_n, b_n))_{n\in\mathbb{N}}$ taka, że $X \subseteq \bigcup\{(a_n, b_n) : n \in \mathbb{N}\}$ oraz $\sum_{n\in\mathbb{N}} |b_n - a_n| < \varepsilon$. Pokaż, że każdy jednoelementowy podzbiór prostej rzeczywistej $\mathbb{R}$ jest miary Lebesgue'a zero. Pokaż, że suma przeliczalnej ilości zbiorów miary miary Lebesgue'a zero jest również zbiorem miary Lebesgue'a zero. Własność tą nazywamy σ-addytywnością zbiorów miary zero.*

B Kraty

W rozdziale tym omówimy dwie ważne klasy częściowych porządków: kraty oraz drzewa. Przypomnijmy (patrz Definicja 6.6), że kresem górnym podzbioru A częściowego porządku $(X, \leq)$ nazywamy najmniejsze ograniczenie górne zbioru A oraz, że kresem dolnym zbioru A nazywamy największe ograniczenie dolne zbioru A. Kres górny zbioru A, nazywany również supremum zbioru A, oznaczamy symbolem $\sup(A)$. Kres dolny zbioru A, nazywany również infimum zbioru A , oznaczamy symbolem $\inf(A)$.

Definicja B.1 *Częściowy porządek $(X, \leq)$ nazywamy **kratą** jeśli każdy niepusty i skończony podzbiór zbioru X posiada kres górny oraz kres dolny.*

W Rozdziale **??** podaliśmy przykład porządku który nie jest kratą. Jednakże wiele ważnych częściowych porządków jest kratami.

Przykład B.1 *Każdy liniowy porządek jest kratą, gdyż każdy skończony podzbior zbioru liniowo uporządkowanego posiada element największy i najmniejszy.*

Przykład B.2 *Każda algebra Boole'a jest kratą. W szczególności porządki postaci $(P(X), \subseteq)$ są kratami.*

Przykład B.3 *Struktura $(\mathbb{N} \setminus \{0\}, |)$ jest kratą. Kresem górnym niepustego zbioru $A \subseteq \mathbb{N} \setminus \{0\}$ jest najmniejsza wspólna wielokrotność elementów zbioru A, zaś kresem dolnym - największy wspólny dzielnik elementów A.*

Niech $(X, \leq)$ będzie ustaloną kratą. Na kracie X określamy dwie binarne operacje $\vee$ i $\wedge$:

- $a \vee b = \sup\{a, b\}$,
- $a \wedge b = \inf\{a, b\}$.

Bezpośrednio z definicji wynika, że $a \wedge b \leq a, b \leq a \vee b$. Następujące twierdzenie opisuje najważniejsze własności wprowadzonych operacji:

Twierdzenie B.1 *Niech $(X, \leq)$ będzie kratą oraz niech $a, b, c \in X$. Wtedy*

1. *$a \vee a = a$, $a \wedge a = a$ (idempotentność),*
2. *$a \vee b = b \vee a$, $a \wedge b = b \wedge a$ (przemienność),*
3. *$a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (łączność),*
4. *$a \vee (a \wedge b) = a$, $a \wedge (a \vee b) = a$ (prawo absorpcji).*

Dowód. Pierwsze trzy równości wynikają bezpośrednio z definicji operacji $\vee$ oraz $\wedge$. Pokażemy pierwszą część prawa absorpcji. Zauważmy najpierw, że $a \leq \max\{a, x\}$ dla dowolnego elementu $x \in X$, a więc $a \vee (a \wedge b) \geq a$. Z nierówności $\min\{x, b\} \leq x$ wynika, że

$$a \vee (a \wedge b) \leq a \vee a = a,$$

co kończy dowód. □

B.1 Kraty zupełne

Kraty stanowią stosunkowo obszerną klasę struktur. Zajmiemy się teraz specjalną podrodziną krat a mianowicie kratami zupełnymi.

Definicja B.2 *Częściowy porządek $(X, \leq)$ nazywamy **kratą zupełną** jeśli każdy niepusty podzbiór zbioru X posiada kres górny oraz kres dolny.*

Zauważmy, że w kracie zupełnej istnieje element największy (jest on kresem górnym wszystkich elementów), oznaczany z reguły przez 1 oraz element najmniejszy, oznaczany przez 0. Widzimy więc, że $(\mathbb{R}, \leq)$ i $(\mathbb{N}, \leq)$ są przykładami krat, które nie są zupełne.

Przykład B.4 *Następujące struktury są kratami zupełnymi:*

1. $(P(X), \subseteq)$
2. $([0, 1], \leq)$
3. *rodzina wszystkich wypukłych podzbiorów ustalonej przestrzeni wektorowej*
4. *rodzina wszystkich podgrup danej grupy*

Twierdzenie B.2 (Knaster-Tarski) *Niech $(L, \leq)$ będzie kratą zupełną oraz niech $f : L \to L$ będzie funkcją monotoniczną (czyli $(\forall x, y \in L)(x \leq y \to f(x) \leq f(y))$). Wtedy funkcja f ma najmniejszy **punkt stały**, czyli istnieje $a \in L$ takie, że $f(a) = a$ oraz $(\forall b \in L)(f(b) = b \to a \leq b)$.*

Dowód. Rozważmy zbiór

$$X = \{x \in L : f(x) \leq x\}.$$

Zbiór ten jest niepusty, gdyż $1 \in X$. Niech $a = \inf(X)$. Rozważmy dowolny element $x \in X$. Wtedy $a \leq x$, a więc z monotoniczności funkcji f wynika, że $f(a) \leq f(x)$. Z tego, że $x \in X$ wynika, że $f(x) \leq x$, więc widzimy, że

$$(\forall x \in X)(f(a) \leq x).$$

Zatem $f(a)$ jest ograniczeniem dolnym zbioru X, a więc

$$f(a) \leq a. \tag{B.1}$$

Ponownie nakładając funkcję f na powyższą nierówność otrzymujemy

$$f(f(a)) \leq f(a),$$

z czego wnioskujemy, że $f(a) \in X$. Zatem $a \leq f(a)$, co w połączeniu z nierównością B.1 daje nam równość $f(a) = a$. Pokazaliśmy więc, że a jest punktem stałym odwzorowania f.

Załóżmy teraz, że $b \in L$ jest innym punktem stałym odwzorowania f, czyli, że $f(b) = b$. Wtedy $f(b) \leq b$ zatem $b \in X$, a więc $a \leq b$. □

Uwaga. Twierdzenia o punkcie stałym odgrywają bardzo ważną rolę w wielu dziedzinach matematyki oraz w jej zastosowaniach. Najbardziej znanym tego typu wynikiem jest twierdzenie Brouwera o punkcie stałym, które orzeka, że „dowolna funkcja ciągła $f : [0,1]^n \to [0,1]^n$ ma punkt stały, gdzie n jest dowolną liczbą naturalną". Twierdzenie to dla $n = 1$ ma prosty dowód korzystający z własności Darboux funkcji ciągłych. Jednakże już dla $n = 2$ jest ono nietrywialnym wynikiem.

Podamy teraz kilka zastosowań Twierdzenie Knastera-Tarskiego.

Przykład B.5 (Podgrupy) *Niech $(G, \cdot)$ będzie grupą oraz $A \subseteq G$. Niech $F_A : P(G) \to P(G)$ będzie funkcją określoną wzorem*

$$F_A(X) = A \cup X \cup \{x \cdot y^{-1} : x, y \in X\}.$$

Najmniejszym punktem stałym odwzorowania F_A jest najmniejsza podgrupa grupy G zawierająca zbiór A. Rzeczywiście, jeśli $F_A(X) = X$ to $A \subseteq F_A(X) = X$ oraz jeśli $x, y \in X$, to $x \cdot y^{-1} \in F_A(X)$, a więc $x \cdot y^{-1} \in X$. Zatem jeśli $F_A(X) = X$ to X jest podgrupa zawierającą zbiór A. Zachodzi również odwrotna implikacja: jeśli X jest podgrupą zawierającą zbiór A, to $F_A(X) = X$. Zatem rodzina podgrup zawierających zbiór A pokrywa się z rodziną punktów stałych odwzorowania F_A. Najmniejszy punkt stały odwzorowanie F_A jest więc najmniejszą podgrupą grupy G zawierającą zbiór A.

Przykład B.6 (Podprzestrzenie) *Niech E będzie przestrzenią liniową nad ciałem algebraicznym K oraz $A \subseteq E$. Niech $F_A : P(E) \to P(E)$ będzie funkcją określoną wzorem*

$$F_A(X) = A \cup X \cup \{a \cdot x + b \cdot y : x, y \in X \wedge k, l \in K\}.$$

Najmniejszym punktem stałym odwzorowania F_A jest najmniejsza podprzestrzeń liniowa przestrzeni E zawierająca zbiór A.

Przykład B.7 (Dowód Twierdzenia Banacha) *Podamy teraz alternatywny dowód twierdzenia Banacha (patrz Twierdzenie 8.1). Niech $f : A \to B$ i $g : B \to A$ będą injekcjami. Definiujemy odwzorowanie $F : P(A) \to P(A)$ wzorem*

$$F(X) = A \setminus g[B \setminus f[X]].$$

Bez trudu sprawdzamy, że F jest odwzorowaniem monotonicznym. Istnieje więc punkt stały odwzorowania F. Z tego punktu, w podobny sposób jak w oryginalnym dowodzie twierdzenia Banacha, konstruujemy szukane rozbicia zbiorów A i B.

Przykład B.8 (Tranzytywne domknięcie) *Ustalmy zbiór Ω oraz relację $R \subseteq \Omega \times \Omega$. Niech $F_R : P(\Omega \times \Omega) \to P(\Omega \times \Omega)$ będzie funkcją zdefiniowaną wzorem*

$$F_R(X) = R \cup (X \circ X).$$

Jest jasne, że F_R jest odwzorowaniem monotonicznym. Najmniejszy punkt stały tego odwzorowania jest najmniejszą relacją przechodnią zawierającą relację R_R. Rzeczywiście, jeśli $F_R(X) = X$, to $X = R \cup (X \circ X)$, więc $R \subseteq X$ oraz $X \circ X \subseteq X$, a więc X jest relacją przechodnią. Relację tą nazywamy tranzytywnym domknięciem relacji R.

Punkty stałe pewnych odwzorowań istnieją dla szerszej klasy struktur niż kraty zupełne. Przypomnijmy, że podzbiór A częściowego porządku $(X, \leq)$ nazywamy łańcuchem, jeśli $(\forall x, y \in A)(x \leq y \vee y \leq x)$.

Definicja B.3 *Niech $(X, \leq)$ będzie częściowym porządkiem. Funkcję $f : X \to X$ nazywamy **ciągłą** jeśli dla każdego przeliczalnego łańcucha $\{c_n\}_{n\in\mathbb{N}}$ dla którego istnieje* $\sup\{c_n : n \in \mathbb{N}\}$ *zachodzi równość* $f(\sup\{c_n : n \in \mathbb{N}\}) = \sup\{f(c_n) : n \in \mathbb{N}\}$.

Zauważmy, że każda funkcja ciągła jest monotoniczna. Rzeczywiście, jeśli $x \leq y$ to $y = \sup\{x, y\}$, zatem $f(y) = \sup\{f(x), f(y)\}$, a więc $f(x) \leq f(y)$.

Twierdzenie B.3 (Kantorovitch-Tarski) *Niech $(X, \leq)$ będzie częściowym porządkiem w którym każdy przeliczalny łańcuch ma supremum. Niech $f : X \to X$ będzie funkcją ciągłą oraz niech $b \in X$ będzie takie, że $b \leq f(b)$. Wtedy* $\sup\{f^n(b) : n \in \mathbb{N}\}$ *jest najmniejszym punktem stałym większym lub równym b.*

Dowód. Z nierówności $b \leq f(b)$ wynika, że $f(b) \leq f(f(b)) = f^2(b)$. W podobny sposób, indukcją względem liczby naturalnej n, pokazujemy, że $(\forall n \in \mathbb{N})(f^n(b) \leq f^{n+1}(b))$. Zatem $\{f^n(b) : n \in \mathbb{N}\}$ jest przeliczalnym łańcuchem. Niech $a = \sup\{f^n(b) : n \in \mathbb{N}\}$. Z ciągłości odwzorowania f wynika, że

$$f(a) = \sup\{f(f^n(b)) : n \in \mathbb{N}\} = \sup\{f^{n+1}(b) : n \in \mathbb{N}\} = a,$$

więc a jest punktem stałym odwzorowania f. Pokazać musimy jeszcze, że a jest najmniejszym punktem stałym odwzorowania f większym lub równym b. Załóżmy zatem, że $b \geq c$ oraz $f(c) = c$. Lecz wtedy $(\forall n \in \mathbb{N})(f^n(b) \leq f^n(c) = c)$, więc $a = \sup\{f^n(b) : n \in \mathbb{N}\} \leq c$. □

B.2 Tablice semantyczne

Niech $\mathcal{L}$ będzie zbiorem wszystkich zdań języka Rachunku Zdań. Dowolny podzbiór $T \subseteq \mathcal{L}$ nazywamy teorią.

Definicja B.4 (Spełnianie) *Niech π będzie waluacją i niech T będzie dowolną teorią Wtedy*

$$(\pi \models T) \leftrightarrow (\forall \varphi \in T)(\pi(\varphi) = \mathbb{1}).$$

Relację $\models$ nazywamy spełnianiem.

Teorię T nazywamy niesprzeczną, jeśli istnieje waluacja π, która jest jej modelem, czyli taka, że $\pi \models T$. Łatwo jest podać przykłady teorii sprzecznych. Jest nią na przykład zbiór $\{p, \neg p\}$ lub $\{p, \neg q, p \to q\}$. Teoria $\{p, p \vee q, \neg q\}$ jest niesprzeczna, gdyż jej modelem jest dowolna waluacja π taka, że $\pi(p) = \mathbb{1}$.

Definicja B.5 *Niech T będzie teorią oraz niech $\varphi \in \mathcal{L}$. Wtedy*

$$(T \models \varphi) \leftrightarrow (\forall \pi)(\pi \models T \rightarrow \pi(\varphi) = \mathbb{1})$$

Zdanie „$(T \models \varphi)$" odczytujemy „T pociąga φ". Pokażemy teraz twierdzenie, które jest bardzo często wykorzystywane w algorytmach automatycznego dowodzenia twierdzeń:

Twierdzenie B.4 *Dla dowolnej teorii T oraz dowolnego zdania φ prawdziwa jest równoważność*

$$(T \models \varphi) \leftrightarrow (\textit{teoria } T \cup \{\neg\varphi\} \textit{ jest sprzeczna}).$$

Dowód. Załóżmy, że teoria $T \cup \{\neg\varphi\}$ jest niesprzeczna. Niech π będzie jej modelem. Wtedy $\pi \models T$ oraz $\pi(\neg\varphi) = \mathbb{1}$, więc $\pi \models T$ oraz $\pi(\varphi) = \mathbb{0}$. Zatem nie jest prawdą, że $T \models \varphi$.

Załóżmy teraz, że $T \models \varphi$ oraz, że $\pi \models T \cup \{\neg\varphi\}$. Wtedy również $\pi \models T$, a więc $\pi(\varphi) = \mathbb{1}$, co jest sprzeczne z tym, że $\pi(\neg\varphi) = \mathbb{1}$. □

Do zbadania tego, czy dany skończony zbiór zdań jest sprzeczny można zastosować metodę tablic zero - jedynkowych. Omówimy teraz inną technikę, zwaną techniką tablic semantycznych, często stosowaną w Sztucznej Inteligencji. Polega ona na zbudowaniu pewnego skończonego drzewa słów nad zbiorem $\{0, 1\}$, którego wierzchołkom w będą przyporządkowane skończone podzbiory $\Lambda(w)$ zbioru zdań $\mathcal{L}$.

Definicja B.6 ***Drzewem semantycznym*** *nazywamy trójkę $(T, \leq, \Lambda)$ taką, że $(T, \leq)$ jest skończonym drzewem słów nad zbiorem $\{0, 1\}$ oraz $\Lambda : T \rightarrow P(\mathcal{L})$. Element $w \in T$ nazywamy* ***zamkniętym*** *jeśli istnieje zdanie α takie, że $\{\alpha, \neg\alpha\} \subseteq \Lambda(t)$. Element który nie jest zamknięty nazywamy* ***otwartym***.

Elementarnym przekształceniem drzewa semantycznego będzie polegało na dopisaniu do jakiegoś otwartego liścia jednego lub dwóch potomków i rozszerzeniu nań funkcji Λ za pomocą jednej z przedstawionych niżej elementarnych transformacji. Załóżmy więc $(T, \leq, \Lambda)$ jest drzewem semantycznym. Niech w będzie liściem drzewa T. Oto lista reguł rozszerzania liścia w:

1. $\{w : \neg\neg\alpha\} \rightarrow \{w0 : \alpha\}$,
2. $\{w : \alpha \wedge \beta\} \rightarrow \{w0 : \alpha, \beta\}$
3. $\{w : \alpha \vee \beta\} \rightarrow \{w0 : \alpha\}, \{w1 : \beta\}$
4. $\{w : \neg(\alpha \vee \beta)\} \rightarrow \{w0 : \neg\alpha, \neg\beta\}$
5. $\{w : \alpha \rightarrow \beta\} \rightarrow \{w0 : \neg\alpha\}, \{w1 : \beta\}$
6. $\{w : \neg(\alpha \rightarrow \beta)\} \rightarrow \{w0 : \alpha, \neg\beta\}$
7. $\{w : \alpha \leftrightarrow \beta\} \rightarrow \{w0 : \alpha, \beta\}, \{w1 : \neg\alpha, \neg\beta\}$
8. $\{w : \neg(\alpha \leftrightarrow \beta)\} \rightarrow \{w0 : \neg\alpha, \beta\}, \{w1 : \alpha, \neg\beta\}$

Regułę pierwszą należy odczytywać następująco: jeśli w jest liściem drzewa i zdanie $\neg\neg\alpha \in \Lambda(w)$ to liść w możemy rozszerzyć o liść $w0$ i dla liścia $w0$ funkcję $\Lambda(w0)$ określamy następująco: $\big(\Lambda(w) \setminus \{\neg\neg\alpha\}\big) \cup \{\alpha\}$, czyli zdanie $\neg\neg\alpha$ zastępujemy zdaniem α.

Regułę trzecią interpretujemy następująco: jeśli w jest liściem drzewa i zdanie $\alpha \vee \beta \in \Lambda(w)$ to liść w można rozszerzyć o elementy 0 i 1; w liściu $w0$ element $\alpha \vee \beta$ zbioru $\Lambda(w0)$ zastępujemy przez α zaś w liściu $w1$ element $\alpha \vee \beta$ zbioru $\Lambda(w0)$ zastępujemy przez β.

Podobnie interpretujemy pozostałe reguły.

Łatwo można zauważyć następującą własność reguł rozszerzania liści: jeśli π jest waluacją, która jest modelem pewnego liścia drzewa T i liść ten został rozszerzony, to π będzie modelem przynajmniej jednego z tych rozszerzeń. Prawdziwa jest również implikacja odwrotna: jeśli po rozszerzeniu liścia któryś z jego potomków będzie niesprzeczny, to również i ów liść liść jest niesprzeczny.

Definicja B.7 ***Tablicą semantyczną*** *dla zbioru zdań G nazywamy drzewo semantyczne $(T, \leq, \Lambda)$ które może zostać zbudowane z drzewa $(\{\varepsilon\}, \leq \{(\varepsilon, G)\})$ za pomocą elementarnych transformacji.*

Definicja B.8 ***Maksymalną tablicą semantyczną*** *zbioru zdań G nazywamy taką tablicę semantyczną $(T, \leq, \Lambda)$ zbioru G, że dla dowolnego liścia $l \in T$ istnieje zdanie α takie, że $\{\alpha, \neg\alpha\} \subseteq \Lambda(l)$ lub l nie może być rozszerzone za pomocą żadnej elementarnej transformacji.*

Zauważmy, że każdą tablicę semantyczną dla zbioru skończonego G można rozszerzyć za pomocą elementarnych transformacji do tablicy maksymalnej - zastosowanie każdej z reguł „upraszcza” transformowane zdania. Pokazać można, że dla dowolnego skończonego zbioru zdań G następujące zdania są równoważne:

- zbiór zdań G jest sprzeczny,
- istnieje maksymalna tablica semantyczna zbioru G, której wszystkie liście są zamknięte,
- w każdej maksymalnej tablicy semantycznej zbioru G wszystkie liście są zamknięte.

Otwarty liść l maksymalnej tablicy semantycznej musi się składać z samych literałów, czyli zmiennych zdaniowych lub ich negacji. Ustalmy otwarty liść l maksymalnej tablicy semantycznej. Określmy waluację na zbiorze zmiennych zdaniowych występujących w G: $\pi(p) = \mathbb{1} \leftrightarrow p \in \Lambda(l)$. Wtedy $\pi \models \Lambda(l)$ i łatwo można pokazać, że również $\pi \models G$.

Przykład B.9 *Pokażemy za pomocą tablic semantycznych, że $\{p \to q, q \to r\} \models p \to r$. Niech $G = \{p \to q, q \to r, \neg(p \to r)\}$.*

$$
\begin{array}{ccccc}
\{p \to q, q \to r, \neg(p \to r)\} & & & & \\
\downarrow (6) & \searrow (6) & & & \\
\{\neg p, q \to r, \neg(p \to r)\} & & \{q, q \to r, \neg(p \to r)\} & & \\
\downarrow (7) & & \downarrow (7) & & \\
\{\neg p, q \to r, p, \neg r\} & & \{q, q \to r, p, \neg r\} & & \\
 & & \downarrow (6) & \searrow (6) & \\
 & & \{q, \neg q, p, \neg r\} & & \{q, r, p, \neg r\}
\end{array}
$$

Obok relacji w łączących wierzchołki z potomkami zaznaczone zostały numery zastosowanych elementarnych transformacji. Wszystkie liście tego drzewa są zamknięte. Oznacza to, że zbiór zdań $\{p \to q, q \to r, \neg(p \to r)\}$ *jest sprzeczny. Zatem* $\{p \to q, q \to r\} \models p \to r$.

Przykład B.10 *Sprawdzimy za pomocą tablic semantycznych, czy prawdziwe jest wynikanie* $\{p \to q, \neg p\} \models \neg r$. *Niech* $G = \{p \to q, \neg p, \neg\neg r\}$.

$$\begin{array}{ccc} \{p \to q, \neg p, \neg\neg r\} & & \\ \downarrow (1) & & \\ \{p \to q, \neg p, r\} & & \\ \downarrow (6) & \searrow (6) & \\ \{\neg p, \neg p, r\} & & \{q, \neg p, r\} \end{array}$$

Zbudowaliśmy więc drzewo maksymalne o otwartych liściach. Zbiór zdań G *jest więc niesprzeczny. Jedną z waluacji jest* π *taka, że* $\pi(p) = \mathbb{0}$ *oraz* $\pi(r) = \mathbb{1}$. *Widzimy, że rzeczywiście* $\pi \models \{p \to q, \neg p\}$ *oraz* $\neg(\pi \models r)$.

Metoda tablic semantyczne może być rozszerzona na rachunek kwantyfikatorów oraz na wiele innych logik.

B.3 Ćwiczenia i zadania

Ćwiczenie B.1 *Pokaż, że częściowy porządek* $(\mathbb{N} \setminus \{0\}, |)$ *jest kratą.*

Ćwiczenie B.2 *Niech* $(X, \leq)$ *będzie kratą oraz niech* $x, y, z \in X$. *Pokaż, że* $\min\{x, y, z\} = x \wedge (y \wedge z) = (x \wedge y) \wedge z$ *oraz* $\max\{x, y, z\} = x \vee (y \vee z) = (x \vee y) \vee z$.

Ćwiczenie B.3 *Pokaż, że*

$$\max(x, y) = \frac{x + y + |x - y|}{2},$$

$$\min(x, y) = \frac{x + y - |x - y|}{2}$$

dla dowolnych $x, y \in \mathbb{R}$.

Ćwiczenie B.4 *Załóżmy, że* $(L, \vee, \wedge)$ *jest strukturą w której prawdziwe są wszystkie własności z Twierdzenia B.1. W strukturze tej definiujemy nierówność* $a \leq b \leftrightarrow a \wedge b = a$.

1. *Pokaż, że* $a \leq b \leftrightarrow a \vee b = b$.
2. *Pokaż, że* $(L, \leq)$ *jest kratą.*

Ćwiczenie B.5 *Pokaż, że każda funkcja ciągła* $f : [0, 1] \to [0, 1]$ *(w sensie analizy matematycznej) ma punkt stały.*

Ćwiczenie B.6 *Niech*

$$R = \{((x, y), (x + 1, y)) : x, y \in \mathbb{Z}\} \cup \{((x, y), (x, y + 1)) : x, y \in \mathbb{Z}\}.$$

Wyznacz tranzytywne domknięcie relacji R.

Ćwiczenie B.7 *Rozstrzygnij za pomocą tablic semantycznych, czy zbiór*

$$\{\neg(p \wedge \neg q), q \to r, p \wedge \neg r\}$$

jest sprzeczny?

Zadanie B.1 *Kratę $(L, \leq)$ nazywamy dystrybutywną, jeśli $(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee z)$. Podaj przykład skończonej kraty, która nie jest dystrybutywna.*

Zadanie B.2 *Niech $R \subseteq X \times X$. Definiujemy odwzorowanie $F : P(X \times X) \to P(X \times X)$ wzorem $F(A) = R \cup Id_A \cup (A \circ A) \cup A^{-1}$. Wyznacz najmniejszy punkt stały odwzorowania F.*

Zadanie B.3 *Niech $\mathcal{A} \subseteq P(X)$. Definiujemy odwzorowanie $F : P(P(X)) \to P(P(X))$ wzorem*

$$F(\mathcal{R}) = \mathcal{A} \cup \{A \cup B : A, B \in \mathcal{R}\} \cup \{A^c : A \in \mathcal{R}\}$$

Wyznacz najmniejszy punkt stały odwzorowania F.

Zadanie B.4 *Pokaż, że złożenie funkcji ciągłych pomiędzy kratami jest również funkcją ciągłą pomiędzy kratami.*

Zadanie B.5 *Pokaż, że metoda tablic semantycznych jest zupełna, czyli że zbiór zdań jest sprzeczny, wtedy i tylko wtedy, gdy procedura budowy tablicy semantycznej prowadzi do drzewa o wszystkich liściach zamkniętych.*

C Aksjomaty teorii mnogości

> Set theory is the finest product of mathematical genius and one of the supreme achievements of purely intellectual human activity.
>
> D. Hilbert

W dodatku tym omówimy aksjomaty teorii mnogości Zermelo - Fraenkela którą oznaczać będziemy skrótem **ZF**. Język tej teorii jest zbudowany z symbolu $\in$, spójników logicznych, nawiasów, kwantyfikatorów $\exists$ oraz $\forall$ oraz symbolu równości.

C.1 Aksjomaty

Aksjomat 1 (Ekstensjonalności)

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

Aksjomat ten interpretujemy następująco: dwa zbiory są równe wtedy i tylko wtedy, gdy mają te same elementy. Po wprowadzeniu oznaczenia $x \subseteq y \leftrightarrow (\forall t)(t \in x \rightarrow t \in y)$ aksjomat ten można zapisać w postaci $(\forall x)(\forall y)((x \subseteq y) \wedge (y \subseteq x) \rightarrow x = y)$. Implikacja odwrotna, czyli zdanie $(\forall x)(\forall y)(x = y \rightarrow (\forall z)(z \in x \leftrightarrow z \in y)$ jest prawdziwa z powodów logicznych, gdyż jednym z aksjomatów logiki z równością jest postulat „*równe obiekty mają te same właściwości*" (jest to tak zwana „zasada Leibnitz'a").

Aksjomat 2 (Zbioru pustego)

$$(\exists x)(\forall y)(\neg(y \in x))$$

Aksjomat ten gwarantuje istnienie zbioru pustego. Z Aksjomatu Ekstensjonalności wynika, że istnieje tylko jeden zbiór pusty. Oznaczamy go, oczywiście, symbolem $\emptyset$.

Aksjomat 3 (Pary)

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

Aksjomat ten gwarantuje nam istnienie pary nieuporządkowanej dla dowolnych dwóch zbiorów. Z Aksjomatu Ekstensjonalności wynika jednoznaczość pary. Oznaczamy ją symbolem $\{x, y\}$. Wprowadzamy również oznaczenie $\{x\}$ na parę nieuporządkowaną $\{x, x\}$, czyli na zbiór który zawiera tylko element x.

Definicja C.1 (Kuratowski) $(x, y) = \{\{x\}, \{x, y\}\}$.

Aksjomat Pary implikuje istnienie pary uporządkowanej (x, y) dla dowolnych obiektów x i y.

Aksjomat 4 (Sumy)

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

Aksjomat ten gwarantuje istnienie sumy dowolnego zbioru. Z Aksjomatu Ekstensjonalności wynika jednoznaczność tej operacji. Sumę zbioru x oznaczamy symbolem $\bigcup x$. Dla danych zbiorów x i y definiujemy $x \cup y = \bigcup\{x, y\}$.

Aksjomat 5 (Zbioru potęgowego)

$$(\forall x)(\exists y)(\forall t)(t \in y \leftrightarrow t \subseteq x)$$

Aksjomat ten gwarantuje istnienie zbioru potęgowego dowolnego zbioru x, który oznaczmy symbolem $P(x)$. Zauważmy, że jeśli $x, y \in z$ to $\{x, y\} \in P(z)$ oraz $(x, y) \in P(P(z))$.

Aksjomat 6 (Wyróżniania) *Niech $\psi(x, y_1, \ldots, y_n)$ będzie dowolną formułą teorii mnogości. Wtedy następujące zdanie jest aksjomatem:*

$$(\forall t)(\forall y_1) \ldots (\forall y_n)(\exists s)(\forall x)(x \in s \leftrightarrow (x \in t \wedge \psi(x, y_1, \ldots, y_n))) \,.$$

Zbiór s którego istnienie postuluje Aksjomat Wyróżniania oznaczany jest przez $\{x \in s : \psi(x, y_1, \ldots, y_n))\}$. Zbiór aksjomatów $\{A1, A2, A3, A4, A5, A6\}$ umożliwia zdefiniowanie większości obiektów które są potrzebne do uprawiania matematyki. Możemy teraz zdefiniować podstawowe operacje mnogościowe:

Definicja C.2

1. $x \cap y = \{t \in x : t \in y\}$,
2. $x \setminus y = \{t \in x : t \notin y\}$,
3. $x \times y = \{t \in P(P(x \cup y)) : (\exists u)(\exists v)(u \in x \wedge v \in y \wedge t = (u, v))\}$,
4. $\bigcap x = \{t \in \bigcup x : (\forall y \in x)(t \in y)\}$.

Aksjomat Ekstensjonalności gwarantuje nam jednoznaczność wprowadzonych operacji. W definicji iloczynu kartezjańskiego skorzystaliśmy z uwagi sformułowanej po Aksjomacie zbioru potęgowego. Mając zdefiniowane pojęcie iloczynu kartezjańskiego możemy zdefiniować pojęcie relacji, funkcji, dziedziny i obrazu relacji.

Definicja C.3

1. $rel(x) = (\exists y)(\exists z)(x \subseteq y \times z)$,
2. $dom(x) = \{s \in \bigcup\bigcup x : (\exists t)((s, t) \in x)\}$,
3. $rng(x) = \{s \in \bigcup\bigcup x : (\exists t)((t, s) \in x)\}$,
4. $fnc(x) = rel(x) \wedge (\forall u)(\forall z)(\forall v)(((u, z) \in x \wedge (u, v) \in x) \rightarrow z = v)$.

W definicji dziedziny skorzystaliśmy z następującej obserwacji: jeśli $\{x, y\} \in a$ to $x, y \in \bigcup a$. Zatem jeśli $(x, y) \in a$ to $x, y \in \bigcup\bigcup a$.

Wprowadzimy teraz pewien skrót, który upraszcza niektóre z rozważanych w dalszej części formuł: $(\exists!x)\psi(x) = (\exists x)(\psi(x) \wedge (\forall y)(\psi(y) \rightarrow y = x))$.

Aksjomat 7 (Zastępowania) *Niech $\psi(x, y, z_1, \ldots, z_n)$ będzie dowolną formułą teorii mnogości. Wtedy następujące zdanie jest aksjomatem:*

$$(\forall s)(\forall \overrightarrow{z})((\forall x \in s)(\exists!y)\psi(x, y, \overrightarrow{z}) \rightarrow (\exists t)(\forall y)(y \in t \leftrightarrow (\exists x \in s)\psi(x, y, \overrightarrow{z}))) \; .$$

Zauważmy, że jeśli formuła $\psi(x, y)$ posiada własność $(\forall x)(\exists!y)\psi(x, y)$, to znaczy, że definiuje ona jednoznaczne przyporządkowanie: każdemu obiektowi x przyporządkowuje ona dokładnie jeden obiekt y taki, że $\psi(x, y)$. Nazwijmy formułę ψ o takiej własności przyporządkowaniem funkcyjnym. Aksjomat Zastępowania możemy wysłowić następująco: *obraz dowolnego zbioru przez przyporządkowanie funkcyjne jest zbiorem*. Aksjomat ten ogrywa rolę w dosyć subtelnych rozumowaniach. Posłużymy się w nim w następnym dodatku, do udowodnienia istnienia liczby $\aleph_1$.

Zbiór aksjomatów wprowadzonych do tej pory jest już stosunkowo silny. Jego siła odpowiada mniej więcej sile aksjomatów Peano arytmetyki liczb naturalnych. Nie można jednak z niego wywnioskować istnienia zbioru nieskończonego. Do jego istnienia potrzebny jest następny aksjomat.

Aksjomat 8 (Nieskończoności)

$$(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \rightarrow y \cup \{y\} \in x))$$

Niech x będzie zbiorem którego istnienie gwarantuje Aksjomat Nieskończoności. Definiujemy $\omega = \bigcap\{y \in P(x) : \emptyset \in y \wedge (\forall t)(t \in y \rightarrow t \cup \{t\} \in y)\}$. Pokazać można, że obiekt ten jest wyznaczony jednoznacznie (czyli, że nie zależy od wyboru zbioru x). Utożsamiamy go ze zbiorem liczb naturalnych.

Aksjomat 9 (Regularności)

$$(\forall x)(x \neq \emptyset \rightarrow (\exists t \in x)(t \cap x = \emptyset))$$

Z Aksjomatu Regularności wynika, między innymi, że nie istnieje ciąg elementów $x_1, \ldots, x_n$ takich, że $x_1 \in x_2 \in \ldots x_n \in x_1$. Rzeczywiście, gdyby taki ciąg istniał, to niech $a = \{x_1, \ldots, x_n\}$. Zbiór ten jest oczywiście niepusty. Zauważmy, że $x_n \in x_1 \cap a$ oraz jeśli $i > 1$ to $x_{i-1} \in x_i \cap a$. Nie istnieje więc zbiór $b \in a$ taki, że $b \cap a = \emptyset$. W szczególności widzimy, że Aksjomat Regularności implikuje, że $(\forall x)(\neg(x \in x))$.

Zbiór aksjomatów $\mathbf{A1}$, $\ldots$, $\mathbf{A9}$ nazywamy teorią mnogości Zermelo-Fraenkela i oznaczmy go przez $\mathbf{ZF}$. Jest to zbiór nieskończony, gdyż Aksjomaty Wyróżniania oraz Zastępowania nie są pojedynczymi zdaniami, lecz są schematami dotyczącymi wszystkich formuł teorii $\mathbf{ZF}$. Wiadomo, że nie można go zastąpić skończonym zbiorem zdań.

Ostatnim z aksjomatów omawianych w tym rozdziale jest Aksjomat Wyboru. W celu jego wyrażenia skorzystamy z pojęcia rozbicia:

Definicja C.4

$$part(x) = (\forall y \in x)(y \neq \emptyset) \wedge (\forall y, z \in x)(y \neq z \rightarrow y \cap z = \emptyset)$$

Aksjomat 10 (Wyboru)

$$(\forall x)(part(x) \rightarrow (\exists s)(\forall y \in x)(\exists t)(y \cap s = \{t\}))$$

W teorii mnogości **ZF** można udowodnić równoważność Aksjomatu Wyboru z wieloma innymi, łatwiejszymi do zastosowań, zdaniami. Przykładami takich zdań są:

1. produkt dowolnej rodziny zbiorów niepustych jest niepusty,
2. każdy zbiór można dobrze uporządkować,
3. Lemat Kuratowskiego-Zorna.

Aksjomat Wyboru oznaczany jest przez **AC**. Teorią mnogości **ZFC** nazywamy zbiór aksjomatów $\mathbf{ZF} \cup \{\mathbf{AC}\}$.

C.2 O niesprzeczności

Wszystkie formuły i zdania teorii mnogości **ZF** zbudowane są z symboli $\in$ oraz zmiennych, spójników, kwantyfikatorów, nawiasów i znaku równości. Znak $\in$ jest jedynym pozalogicznym symbolem tej teorii. Specjalną klasę formuł stanowią zdania. Są to formuły w których nie ma zmiennych wolnych, czyli takich zmiennych, które nie są w zasięgu działania żadnego kwantyfikatora.

Przykład C.1 *W formule $x_0 = x_3$ obie zmienne x_0 i x_3 są wolne. W formule $(\exists x)(x = y)$ zmienną wolną jest y. Formuła $(\exists x)(\forall y)(x = y)$ nie ma zmiennych wolnych, a więc jest zdaniem.*

Teorią nazywamy dowolny zbiór zdań. Aksjomaty teorii mnogości stanowią więc podzbiór zbioru zdań. Tak więc **ZF** oraz **ZFC** są przykładami teorii.

Niech T będzie teorią oraz ψ dowolnym zdaniem. Będziemy mówili, że ψ jest dowodliwe w teorii T ($T \vdash \psi$) jeśli zdanie ψ można wydedukować ze zbioru zdań T.

Uwaga. Zdanie ψ można wydedukować ze zbioru zdań T jeśli istnieje jego dowód ze zbioru zdań T, czyli skończony ciąg zadań $\varphi_0, \ldots, \varphi_n$ taki, że $\varphi_n = \psi$ oraz dla każdego $i \leq n$ zdanie φ_i jest tautologią, elementem zbioru T lub jest wnioskiem logicznym z pewnych zdań φ_k, φ_l takich, że $k, l < i$. Nie będziemy dalej precyzowali tego pojęcia. Czytelnik zaznajomi się z nim na wykładzie z logiki matematycznej.

Mówimy, że zbiór zdań T jest *niesprzeczny*, co zapisujemy jako $Con(T)$, jeśli nie istnieje zdanie ψ takie, że $T \vdash \psi$ oraz $T \vdash \neg\psi$. Zauważmy, że jeśli teoria jest sprzeczna, to można z niej wywnioskować dowolne zdanie, gdyż wyrażenie $\psi \wedge \neg\psi \rightarrow \varphi$ jest tautologią dla dowolnego zdania φ.

Do tej pory nie wiadomo, czy teoria mnogości **ZF** jest niesprzeczna. Jej badaczom wydaje się jednak, że jest ona niesprzeczna. Zbadano bowiem dosyć szczegółowo jej bardzo silne rozszerzenia i nawet w tych rozszerzeniach nie natrafiono na ślad sprzeczności. Niestety, w chwili obecnej nie widać żadnej rozsądnej metody, którą można by zastosować do udowodnienia jej niesprzeczności.

Definicja C.5 *Niech T będzie teorią oraz niech ψ będzie zdaniem. Mówimy, że zdanie ψ jest **niezależne** od teorii T jeśli $Con(T \cup \{\psi\})$ oraz $Con(T \cup \{\neg\psi\})$.*

Zauważmy, że jeśli zdanie ψ jest niezależne od teorii T, to $\neg(T \vdash \psi)$ oraz $\neg(T \vdash \neg\psi)$. Gdyby na przykład zdanie ψ było niezależne od teorii T oraz $T \vdash \psi$ to wtedy również $T \cup \{\neg\psi\} \vdash \psi$, a więc teoria $T \cup \{\neg\psi\}$ byłaby sprzeczna.

Aksjomat Wyboru jest przykładem zdania, które jest niezależne od teorii mnogości **ZF**. Prawdziwe są bowiem następujące twierdzenia:

Twierdzenie C.1 (Gödel) $Con(\mathbf{ZF}) \rightarrow Con(\mathbf{ZF} \cup \{\mathbf{AC}\})$

Twierdzenie C.2 (Cohen) $Con(\mathbf{ZF}) \rightarrow Con(\mathbf{ZF} \cup \{\neg\mathbf{AC}\})$

Innym słynnym przykładem zdania niezależnego od teorii mnogości **ZFC** jest tak zwana Hipoteza Continuum, którą omówimy w następnym rozdziale.

Aksjomat Regularności jest również aksjomatem niezależnym od pozostałych aksjomatów. Niesprzeczna jest teoria mnogości bez Aksjomatu Regularności ale za to zdaniem $(\exists x)(x \in x)$.

C.3 Zadania

Zadanie C.1 *Pokaż, że $(\forall x)(\forall y)(\exists! z)(z = x \cap y)$ oraz $(\forall x)(\forall y)(\exists! z)(z = x \times y)$.*

Zadanie C.2 *Pokaż, że jeśli $\{x, y\} \in a$ to $\{x, y\} \subseteq \bigcup a$ oraz, że jeśli $(x, y) \in a$ to $\{x, y\} \subseteq \bigcup\bigcup a$.*

Zadanie C.3 *Pokaż, że $(\forall x, y)(\exists z)(\forall f)(f \in z \leftrightarrow (fnc(f) \wedge dom(f) = x \wedge rng(f) \subseteq y))$*

Zadanie C.4 *Pokaż, że $\neg(\exists x)(\forall y)(y \subseteq x)$. Pokaż, że $\neg(\exists x)(\forall a)(\{a\} \in x)$.*

Zadanie C.5 *Z punktu widzenia teorii mnogości każda funkcja jest rodziną zbiorów, gdyż jedynymi obiektami tej teorii są zbiory. Zdefiniuj za pomocą Aksjomatu Wyróżniania produkt kartezjański dowolnej funkcji.*

Zadanie C.6 *Pokaż, że nie istnieje funkcja f taka, że*

$$dom(f) = \omega \wedge (\forall n)(f(n+1) \in f(n)).$$

Wywnioskuj z tego, że nie istnieje ciąg $x_1, \ldots, x_n$ taki, że

$$x_1 \in x_2 \in \ldots \in x_n \in x_1 \, .$$

Zadanie C.7 *Pokaż, że zbiór ω jest zdefiniowany jednoznacznie.*

Zadanie C.8 *Pokaż w teorii **ZF**, że jeśli $(X, \leq)$ jest liniowym porządkiem oraz $\mathcal{X} = (X_i)_{i \in I}$ jest dowolną rodziną parami rozłącznych, skończonych podzbiorów zbioru X, to istnieje selektor rodziny $\mathcal{X}$.*

Zadanie C.9 *Pokaż, że Aksjomat Pary można wyprowadzić z pozostałych aksjomatów teorii* **ZF**.

Zadanie C.10 *Pokaż, że dla każdego zbioru A istnieje zbiór $B \supseteq A$ taki, że $B \times B \subseteq B$. Czy istnieje niepusty zbiór A taki, że $A \times A = A$?*

Zadanie C.11 *Rozważmy język z jednym symbolem funkcyjnym $\cdot$ oraz z jedną stała e. Rozważmy następujący zbiór zdań:*

$$TG = \{(\forall x, y, x)(x \cdot (y \cdot z) = (x \cdot y) \cdot z), (\forall x)(x \cdot e = x \wedge e \cdot x = x), \\ (\forall x)(\exists y)(x \cdot y = e \wedge y \cdot x = e)\} .$$

Zbiór ten nazywamy, oczywiście, teorią grup. Pokaż, że zbiór ten jest niesprzeczny. Niech $AB = (\forall x, y)(x \cdot y = y \cdot x)$. Pokaż, że zdanie AB jest niezależne od teorii TG. Znajdź zdanie niezależne od teorii $TG \cup \{AB\}$.

Zadanie C.12 *Rozważmy język z jednym binarnym symbolem relacyjnym R. Rozważmy następujący zbiór zdań:*

$$PO = \{(\forall x, y, x)(R(x, y) \wedge R(y, z) \rightarrow R(x, z), (\forall x)R(x, x), \\ (\forall x, y)(R(x, y) \wedge R(y, x) \rightarrow x = y)\} .$$

Zbiór ten nazywamy, oczywiście, teorią częściowych porządków. Pokaż, że zbiór ten jest niesprzeczny. Niech $LIN = (\forall x, y)(R(x, y) \vee x = y \vee R(y, x))$. Pokaż, że zdanie LIN jest niezależne od teorii PO.

D Liczby Porządkowe i Kardynalne

W rozdziale rozważania będziemy prowadzili w teorii **ZFC**, a zajmować się będziemy zbiorami tranzytywnymi, liczbami porządkowymi oraz liczbami kardynalnymi. Rozważania rozpoczniemy od zdefiniowana tych obiektów.

Definicja D.1 $tran(x) = (\forall y \in x)(y \subseteq x)$

Definicja D.2 $ord(x) = tran(x) \wedge (\forall s, t \in x)(s \in t \vee s = t \vee t \in s)$

Definicja D.3 $card(x) = ord(x) \wedge (\forall y \in x)(|y| < |x|)$

Zbiór x nazywamy *tranzytywnym* jeśli prawdziwe jest zdanie $tran(x)$. Zbiór x nazywamy *liczbą porządkową* jeśli prawdziwe jest zdanie $ord(x)$. Zbiór x nazywamy *liczbą kardynalną* jeśli prawdziwe jest zdanie $card(x)$.

Zbiór pusty jest tranzytywny. Łatwo można pokazać, że jeśli x jest zbiorem tranzytywnym, to również zbiory $x \cup \{x\}$ oraz $P(x)$ są tranzytywne. Zbiór pusty jest również liczbą porządkową. Jeśli x jest liczbą porządkową to i zbiór $x \cup \{x\}$ jest również liczbą porządkową.

Przykład D.1 *Rozważmy ciąg zbiorów*

$$\emptyset, scf(\emptyset), scf(scf(\emptyset)), scf(scf(scf(\emptyset))), scf(scf(scf(scf(\emptyset)))), \ldots$$

Elementy tego ciągu są liczbami porządkowymi, gdyż $\emptyset$ jest liczbą porządkową i rodzina liczb porządkowych jest zamknięta na operację scf. Elementy tego ciągu utożsamiamy z liczbami naturalnymi. Zatem $0 = \emptyset$,$1 = \{\emptyset\}$, $2 = \emptyset \cup \{\emptyset\} = \{\emptyset\}$ itd. Zwróćmy uwagę na to, że dla dowolnego n prawdziwa jest równość $\mathbf{n} = \{\mathbf{0}, \ldots, \mathbf{n-1}\}$.

Przykład D.2 *W rozdziale C zdefiniowaliśmy zbiór ω. Był nim najmniejszy zbiór do którego należy $\emptyset$ i który jest zamknięty na operację $x \mapsto x \cup \{x\}$. Zbiór ten jest najmniejszą nieskończoną liczbą porządkową i utożsamiamy go ze zbiorem liczb naturalnych.*

Twierdzenie D.1 $(\forall \alpha)(\forall \beta)((ord(\alpha) \wedge \beta \in \alpha) \rightarrow ord(\beta))$

Dowód. Niech α będzie liczbą porządkową oraz niech $\beta \in \alpha$. Wtedy $\beta \subseteq \alpha$, więc relacja $\in$ liniowo porządkuje zbiór β. Musimy więc pokazać, że β jest zbiorem tranzytywnym. Załóżmy więc, że $x \in \beta$ oraz, że $t \in x$. Porównamy element t z elementem β. Zachodzi jedna z możliwości: $t \in \beta$, $t = \beta$, $\beta \in t$. Jeśli $t = \beta$ to $\beta = t \in x \in \beta$, co jest sprzeczne z Aksjomatem Regularności. Jeśli $\beta \in t$ to $t \in x \in \beta \in t$, co znowu jest niemożliwe. Zatem $t \in \beta$. Ponieważ t było dowolnym elementem obiektu x. więc $x \subseteq \beta$. Zatem β jest zbiorem tranzytywnym.

□

Dla każdej ustalonej liczbie porządkowej określamy relację

$$x \leq y \leftrightarrow (x \in y \vee x = y).$$

Relacja ta jest spójna, gdyż zdanie $s \in t \vee s = t \vee t \in s$ jest równoważne ze zdaniem $s \leq t \vee t \leq s$. Pokażemy, że tak określona relacja pokrywa się z zawieraniem.

Lemat D.1

$$(\forall\alpha)(\forall x)(\forall y)((ord(\alpha) \wedge x \in \alpha \wedge y \in \alpha) \rightarrow (x \subseteq y \leftrightarrow (x \in y \vee x = y)))$$

Dowód. Załóżmy, że α jest liczbą porządkową oraz $x, y \in \alpha$. Zaczniemy od pokazania, że $x \subseteq y \rightarrow (x \in y \vee x = y))$. Niech więc $x \subseteq y$. Z definicji liczby porządkowej wynika, że $x \in y$ lub $x = y$ lub $y \in x$. Trzecia możliwość, $y \in x$, jest sprzeczna z Aksjomatem Regularności. Zatem $x \in y$ lub $x = y$. Pokażemy teraz drugą implikację. Załóżmy więc, że $x \in y \vee x = y$. Jeśli $x = y$ to $x \subseteq y$. Załóżmy zatem, że $x \in y$. Z Twierdzenia D.1 wynika, że y jest zbiorem tranzytywnym, więc $x \subseteq y$. □

Udowodnimy teraz fundamentalne twierdzenie dla teorii mnogości.

Twierdzenie D.2 *Niech α będzie liczbą porządkową. Wtedy relacja $\leq$ dobrze porządkuje zbiór α.*

Dowód. Zwrotność, przechodniość oraz słaba-antysymetria wynika z odpowiednich własności inkluzji. Załóżmy więc, że A jest niepustym podzbiorem liczby porządkowej α. Z Aksjomatu regularności wynika, że istnieje $a \in A$ takie, że $a \cap A = \emptyset$. Pokażemy, że a jest $\leq$-najmniejszym elementem zbioru A. Niech $x \in A$. Gdyby x był elementem a, to wtedy przekrój $a \cap A$ byłby niepusty. Zatem $a = x$ lub $a \in x$, czyli $a \leq x$. □

Zajmiemy się teraz kolekcją wszystkich porządkowych. Rozważania rozpoczniemy od udowodnienia pewnej własności odcinków początkowych. Niech $(X, \leq)$ będzie porządkiem liniowym. Zbiór $A \subseteq X$ nazywamy odcinkiem początkowym, jeśli

$$(\forall x, y \in X)((x \in A \wedge (y \leq x)) \rightarrow y \in A).$$

Lemat D.2 *Niech α będzie liczbą porządkową oraz niech $X \subseteq \alpha$ będzie odcinkiem początkowym. Wtedy $X = \alpha$ lub $X = \beta$, gdzie β jest najmniejszym elementem zbioru $\alpha \setminus X$.*

Dowód. Niech α będzie liczbą porządkową oraz niech $X \subseteq \alpha$ będzie odcinkiem początkowym. Załóżmy, że $X \neq \alpha$. Niech a będzie $\leq$-minimalnym elementem zbioru $\alpha \setminus X$. Z minimalności elementu a wynika, że jeśli $t \in a$ to $t \in X$. Odwrotnie, jeśli $t \geq a$ oraz $t \in \alpha$ to $t \notin X$. Rzeczywiście, gdyby $t \in X$, to i $a \in X$, a to jest sprzeczne z tym, że $a \notin X$. □

Pokażemy teraz, że dowolne dwie liczby porządkowe są ze sobą porównywalne.

Twierdzenie D.3 $(\forall x)(\forall y)(ord(x) \wedge ord(y) \rightarrow (x \in y \vee x = y \vee y \in x))$

Dowód. Niech α i β będą liczbami porządkowymi oraz niech $X = \alpha \cap \beta$. Wtedy zbiór X jest odcinkiem początkowym α oraz β. Załóżmy, że $X \neq \alpha$ oraz $X \neq \beta$. Niech a będzie najmniejszym elementem $\alpha \setminus X$ oraz niech b będzie najmniejszym elementem $\beta \setminus X$. Z lematu D.2 wynika, że $X = a$ oraz $X = b$, co jest sprzeczne z definicjami liczb a i b.
Widzimy więc, że $\alpha \subseteq \beta$ lub $\beta \subseteq \alpha$. W pierwszym przypadku $\alpha = \beta$ lub $\alpha \in \beta$. W drugim przypadku $\beta = \alpha$ lub $\beta \in \alpha$. □

Definicja D.4 *1.* $scc(\alpha) = (\alpha = \emptyset) \vee (\exists\beta)(ord(\beta) \wedge \alpha = \beta \cup \{\beta\})$

2. $lim(\alpha) = ord(\alpha) \wedge \neg scc(\alpha)$

Jeśli prawdziwe jest zdanie $scc(\beta)$, to liczbę porządkową β nazywamy następnikiem. Jeśli prawdziwe jest zdanie $lim(\beta)$, to liczbę porządkową β nazywamy liczbą graniczną. Zbiór liczb naturalnych ω jest najmniejszą liczbą porządkową graniczną. Wszystkie jej elementy są następnikami. Następnikiem jest również liczba $\omega \cup \{\omega\}$.

Lemat D.3 *Załóżmy, że α jest liczbą porządkową. Wtedy liczba $\alpha \cup \{\alpha\}$ jest najmniejszą liczbą porządkową wiekszą od α.*

Dowód. Oczywiście α jest elementem zbioru $\alpha \cup \{\alpha\}$. Załóżmy, że $\gamma \in \alpha \cup \{\alpha\}$. Wtedy $\gamma \in \alpha$ lub $\gamma = \alpha$. □

Liczbą porządkową $\alpha \cup \{\alpha\}$ oznaczać będziemy od tej pory przez $\alpha + 1$.

D.1 Indukcja Pozaskończona

W rozdziale tym zajmiemy się rozumowaniami indukcyjnymi, których długość przekracza liczbę porządkową ω. Wprowadzimy najpierw dwa pomocnicze oznaczenia. Niech wyrażenie $(\forall x \in Ord)\psi(x)$ oznacza $(\forall x)(ord(x) \rightarrow \psi(x))$, oraz podobnie, niech $(\exists x \in Ord)\psi(x)$ oznacza $(\exists x)(ord(x) \wedge \psi(x))$. Wyrażenie $(\forall x \in Ord)\psi(x)$ traktujemy więc jako skrót, gdyż nie istnieje zbiór wszystkich liczb porządkowych.

Twierdzenie D.4 (O indukcji pozaskończonej) *Niech $\psi(x)$ będzie dowolną formułą. Wtedy*

$$(\forall\alpha \in Ord)((\forall\beta \in \alpha)\psi(\beta) \rightarrow \psi(\alpha)) \rightarrow (\forall\alpha \in Ord)\psi(\alpha)$$

Dowód. Załóżmy, że prawdziwe jest zdanie $(\forall\alpha \in Ord)((\forall\beta \in \alpha)\psi(\beta) \rightarrow \psi(\alpha))$ oraz, że istnieje liczba porządkowa α taka, że $\neg\psi(\alpha)$. Niech α_0 będzie taką liczbą. Wtedy $\neg((\forall\beta \in \alpha_0)\psi(\beta)$. Zatem zbiór

$$B = \{\beta \in \alpha_0 : \neg\psi(\beta)\}$$

jest niepusty. Niech β_0 będzie minimalnym elementem zbioru B. Wtedy $\neg\psi(\beta_0)$ oraz $(\forall\gamma \in \beta_0)\psi(\gamma)$, z czego wynika, że $\psi(\beta_0)$. Otrzymaliśmy więc sprzeczność, która kończy dowód. □

W rozdziale poświęconym indukcji udowodniliśmy twierdzenie o istnieniu funkcji definiowanych rekurencyjnie. Udowodnimy teraz wzmocnienie tego wyniku.

Twierdzenie D.5 (O rekursji pozaskończonej) *Załóżmy, że φ jest formułą taką, że $(\forall x)(\exists! y)\varphi(x,y)$. Wtedy*

$$(\forall \alpha \in Ord)\left((\exists! f)(fnc(f) \wedge dom(f) = \alpha \wedge (\forall \beta \in \alpha)\varphi(f \restriction \beta, f(\beta)))\right)$$

Dowód. Załóżmy, że φ jest formułą spełniającą założenia twierdzenia. Pokażemy najpierw, że jeśli istnieje co najwyżej jedna funkcja f która spełnia warunek

$$dom(f) = \alpha \wedge (\forall \beta \in \alpha)\varphi(f \restriction \beta, f(\beta)).$$

Załóżmy bowiem, że istnieją dwie różne funkcje f_1 i f_2 spełniające ten warunek. Niech γ będzie najmniejszą liczbą porządkową taką, że $f_1(\gamma) \neq f_2(\gamma)$. Wtedy $f_1 \restriction \gamma = f_2 \restriction \gamma$ więc prawdziwe jest zdanie $\varphi(f_1 \restriction \gamma, f_2(\gamma))$, z czego wynika, $f_1(\gamma) = f_2(\gamma)$.

Istnienie funkcji f udowodnimy indukcją pozaskończoną po parametrze α. Niech

$$GF(x,f) = ord(x) \wedge func(f) \wedge dom(f) = x \wedge (\forall y \in x)\varphi(f \restriction y, f(y)).$$

Załóżmy, że $(\forall \beta \in \alpha)(\exists f)GF(\beta, f)$.

Jeśli α jest następnikiem, to $\alpha = \beta + 1$ dla pewnej liczby porządkowej β. Niech f będzie taką funkcją, że $GF(\beta, f)$, niech y_0 będzie takim elementem, że zdanie $\varphi(f, y_0)$ jest prawdziwe oraz niech $g = f \cup \{(\beta, y_0)\}$. Wtedy $dom(g) = \alpha$ i zdanie $GF(\alpha, g)$ jest prawdziwe.

Załóżmy teraz, że α jest liczbą graniczną. Dla każdej liczby $\beta \in \alpha$ niech f_β będzie taką funkcją, że zdanie $GF(\beta, f_\beta)$ jest prawdziwe. Rozumowanie podobne do dowodu jednoznaczności funkcji f pokazuje, że jeśli $\beta_1 < \beta_2 < \alpha$ to $f_{\beta_1} \subseteq f_{\beta_2}$. Niech $f = \bigcup\{f_\beta : \beta < \alpha\}$. Wtedy zdanie $GF(\alpha, f)$ jest prawdziwe.

Pokazaliśmy więc, że

$$(\forall \beta \in \alpha)(\exists f)GF(\beta, f) \rightarrow (\exists f)GF(\alpha, f).$$

Zatem prawdziwe jest zdanie $(\forall \alpha \in Ord)(\exists f)(GF(\alpha, f)$, co kończy dowód twierdzenia. □

Rekursja pozaskończona pozwala na budowanie funkcji dowolnych długości porządkowych wtedy, gdy znamy jednoznaczny przepis na wyznaczenie wartości $f(\alpha)$ na podstawie wartości $(f(\beta))_{\beta<\alpha}$. W wielu przypadkach rekursję pozaskończoną wykorzystuje się w następujący sposób: definiuje się wartość funkcji dla liczby 0 i oddzielnie definiuje się wartości funkcji dla następników oraz liczb granicznych.

Przykład D.3 *Dodawanie liczb porządkowych definiujemy w następujący sposób:*

$$\begin{cases} \alpha + 0 & = & \alpha \\ \alpha + (\beta + 1) & = & (\alpha + \beta) + 1 \\ \alpha + \lambda & = & \bigcup\{\alpha + \beta : \beta < \lambda\}, \quad \textit{jeśli } lim(\lambda) \end{cases}$$

Łatwo sprawdzić, że $1 + \omega = \omega < \omega + 1$. Liczba porządkowa $\omega + \omega$ jest najmniejszą liczbą porządkową graniczną większą od ω.

Przykład D.4 *Mnożenie liczb porządkowych $\alpha \cdot \beta$ definiujemy w następujący sposób:*

$$\begin{cases} \alpha \cdot 0 & = & 0 \\ \alpha \cdot (\beta + 1) & = & (\alpha \cdot \beta) + \alpha \\ \alpha \cdot \lambda & = & \bigcup\{\alpha \cdot \beta : \beta < \lambda\} \textit{ jeśli } lim(\lambda) \end{cases}$$

Łatwo sprawdzić, że $2 \cdot \omega = \omega < \omega \cdot 2 = \omega + \omega < \omega \cdot \omega$.

Zdefiniujemy teraz ważną rodzinę zbiorów, za pomocą której można uzyskać pierwszy, co prawda mocno przybliżony mocno przybliżony, opis struktury całego uniwersum zbiorów:

$$\begin{cases} R_0 & = & \emptyset \\ R_{\alpha+1} & = & P(R_\alpha) \\ R_\lambda & = & \bigcup\{R_\beta : \alpha < \lambda\} \text{ jeśli } lim(\lambda) \end{cases}$$

Zbiory R_α są tranzytywne, gdyż $\emptyset$ jest zbiorem tranzytywnym i klasa zbiorów tranzytywnych jest zamknięta na operację potęgowania oraz sumy. Hierarchia ta jest rosnąca:

$$R_0 \subseteq R_1 \subseteq R_2 \subseteq \ldots \subseteq R_\omega \subseteq R_{\omega+1} \subseteq \ldots$$

Wszystkie inkluzje w powyższym ciągu są właściwe.

Twierdzenie D.6 (O strukturze uniwersum) $(\forall x)(\exists \alpha \in Ord)(x \in R_\alpha)$

Dowód. Załóżmy, że zdanie to nie jest prawdziwe. Istnieje więc zbiór a taki, że $(\forall \alpha \in Ord)(a \notin R_\alpha)$. Niech

$$a^* = \{a\} \cup a \cup (\bigcup a) \cup (\bigcup\bigcup a) \cup (\bigcup\bigcup\bigcup a) \cup \ldots$$

Zbiór a^* jest tranzytywny, gdyż jeśli $x \in y$ to $x \subseteq \bigcup y$. Niech $b = \{x \in a^* : (\forall \alpha \in Ord)(x \notin R_\alpha)\}$. Zbiór b jest niepusty, gdyż $a \in b$. Niech $c \in b$ będzie takim zbiorem, że $c \cap b = \emptyset$. Istnienie takiego elementu gwarantuje Aksjomat Regularności. Z tranzytywności zbioru a^* wynika, że $c \subseteq a^*$. Dla dowolnego elementu $t \in c$ istnieje więc α taka, że $t \in R_\alpha$. Rozważmy następującą formułę:

$$\psi(x, y) = (x \notin c \wedge y = 0) \vee (x \in c \wedge ord(y) \wedge x \in R_y \wedge (\forall z \in y)(x \notin R_z)).$$

Z definicji tej formuły wynika, że $(\forall x)(\exists! y)\psi(x, y)$. Z Aksjomatu Zastępowania wynika istnienie takiego zbioru d, że

$$(\forall u)(u \in d \leftrightarrow (\exists t \in c)\psi(t, u)).$$

Widzimy więc, że elementami zbioru d są liczby porządkowe. Niech $\alpha = \bigcup d + 1$. Wtedy $(\forall t \in c)(t \in R_\alpha)$. Zatem $c \subseteq R_\alpha$. A więc $c \in R_{\alpha+1}$. Otrzymaliśmy sprzeczność, która kończy dowód. □

Powyższe twierdzenie, w sposób nieco nieformalny, można zapisać następująco:

$$V = \bigcup_{\alpha \in \text{ Ord}} R_\alpha \ ,$$

gdzie V oznacza klasę wszystkich zbiorów, zaś Ord oznacza klasę wszystkich liczb porządkowych.

Przykład D.5 *Rozważmy strukturę $(R_\omega, \in)$. Elementy tej struktury możemy opisać jako zbiory dziedzicznie skończone, czyli takie zbiory x dla których zbiór x^* skonstruowany w dowodzie ostatniego twierdzenia jest skończony. Stosunkowo łatwo można pokazać, że w tej strukturze prawdziwe są wszystkie aksjomaty teorii ZFC z wyjątkiem Aksjomatu Nieskończoności. Wynika z tego, że Aksjomat Nieskończoności jest potrzebny, gdyż nie można go wyprowadzić z pozostałych aksjomatów.*

Pokażemy teraz, że liczby porządkowe opisują z dokładnością do izomorfizmu wszystkie dobre porządki.

Twierdzenie D.7 *Jeśli $(X, \leq)$ jest dobrym porządkiem, to istnieje dokładnie jedna liczba porządkowa α taka, że struktury $(X, \leq)$ oraz $(\alpha, \subseteq)$ są izomorficzne.*

Dowód. Ustalmy dobry porządek $(X, \leq)$. Niech

$$iso(\alpha, f, X) = ord(\alpha) \wedge f \in X^{\alpha+1} \wedge (\forall \beta \leq \alpha)(f(\beta) = min(X \setminus f[\beta])),$$

oraz

$$\psi(t, \alpha) = (t \in x) \wedge (\exists f)(iso(\alpha, f, X) \wedge f(\alpha) = t).$$

Bez trudu sprawdzić możemy, że $(\forall t \in X)(\exists! \alpha)\psi(t, \alpha)$. Niech A będzie takim zbiorem liczb porządkowych, że

$$(\forall y)(y \in A \leftrightarrow (\exists t \in X)\psi(t, y)).$$

Niech α będzie najmniejszą liczbą porządkową większą od wszystkich elementów zbioru A. Wtedy porządki $(X, \leq)$ oraz $(\alpha, \subseteq)$ są izomorficzne. Jednoznaczność liczby porządkowej α pozostawiamy czytelnikowi jako ćwiczenie. □

Jeśli liczba porządkowa α jest izomorficzna z dobrym porządkiem $(X, \leq)$, to mówimy, że $(X, \leq)$ ma typ porządkowy α i zapisujemy to $ot(X, \leq) = \alpha$.

Przykład D.6 *Niech $A = \{k - \frac{1}{n+1} : k, n \in \mathbb{N}\}$. Wtedy $ot(A, \leq) = \omega \times \omega$.*

D.2 Funkcja Hartogsa

W rozdziale tym wprowadzimy jedną funkcję, która każdemu zbiorowi przyporządkowuje najmniejszą liczbę porządkową, której nie można zanurzyć różnowartościowo w rozważany zbiór.

Twierdzenie D.8

$$(\forall x)(\exists \alpha \in Ord)(\neg(\exists f)(f : \alpha \to x \wedge f \textit{ jest injekcją}))$$

Dowód. Niech

$$WO(x) = \{r \in P(x^2) : r \text{ jest dobrym porządkiem na swojej dziedzinie}\}.$$

Każdemu elementowi $r \in WO(x)$ przyporządkowujemy jego typ porządkowy ot(r). Z Aksjomatu Zastępowania wynika, że istnieje zbiór A wszystkich typów porządkowych elementów zbioru $WO(x)$. Niech $\alpha = (\bigcup A) + 1$. Załóżmy, że istnieje injekcja $f : \alpha \to x$. Wtedy zbiór $r = \{(f(\beta), f(\gamma)) : \beta \leq \gamma < \alpha\}$ byłby dobrym porządkiem o polu zawartym w x o typie porządkowym α, co jest sprzeczne z tym, że $(\forall x \in A)(x < \alpha)$.

□

Definicja D.5 *Liczbą Hartogsa zbioru X nazywamy najmniejszą liczbę porządkową α taką, że nie istnieje injekcja $F : \alpha \to X$. Liczba ta oznaczana jest przez $\mathcal{H}(x)$.*

Z ostatniego twierdzenia wynika, że dla każdego zbioru X istnieje liczba porządkowa $\mathcal{H}(x)$.

Twierdzenie D.9 *Z Aksjomatu Wyboru wynika Zasada Dobrego Uporządkowania.*

Dowód. Niech X będzie dowolnym zbiorem. Niech $F : P(X)\setminus\{\emptyset\} \to X$ będzie taką funkcją, że $F(X) \in X$ dla wszystkich niepustych podzbiorów X. Niech następnie $\kappa = \mathcal{H}(X)$ oraz niech ∞ będzie dowolnym elementem nie należącym do zbioru X. Indukcją pozaskończoną dla liczb $\beta < \kappa$ definiujemy funkcję

$$f(\beta) = \begin{cases} F(X \setminus rng(f \restriction \beta)) & : \quad X \setminus rng(f \restriction \beta) \neq \emptyset \\ \infty & : \quad X \setminus rng(f \restriction \beta) = \emptyset \end{cases}$$

Zauważmy, że istnieje β taka, że $f(\beta) = \infty$, gdyż gdyby takiej liczby nie było, to funkcja f byłaby injekcją liczby $\mathcal{H}(X)$ w zbiór X, co jest sprzeczne z definicją funkcji Hartogsa. Niech β_0 będzie najmniejszą liczbą porządkową taką, że $f(\beta_0) = \infty$. Wtedy funkcja $h = f \restriction \beta_0$ jest bijekcją pomiędzy liczbą β_0 a zbiorem X. Na zbiorze X możemy więc zdefiniować dobry porządek wzorem $\{(h(x), h(y)) : x \leq y < \beta_0\}$. □

Przy okazji pokażemy, że z Aksjomatu Wyboru wynika Lemat Kuratowskiego - Zorna.

Twierdzenie D.10 (ZF) *Z Aksjomatu Wyboru wynika Lemat Kuratowskiego-Zorna.*

Dowód. Niech $(X, \leq)$ będzie częściowym porządkiem spełniającym założenia Lematu Kuratowskiego - Zorma. Niech $F : P(X) \setminus \{\emptyset\} \to X$ będzie taką funkcją, że $F(X) \in X$ dla wszystkich niepustych podzbiorów X. Niech następnie $\kappa = \mathcal{H}(X)$ oraz niech ∞ będzie dowolnym elementem nie należącym do zbioru X. Indukcją pozaskończoną dla liczb $\beta < \kappa$ definiujemy funkcję

$$f(\beta) = \begin{cases} F(\{x : (\forall \gamma < \beta)(x > f(\gamma))\} & : \quad (\exists x)(\forall \gamma < \beta)(x > f(\gamma)) \\ \infty & : \quad \neg(\exists x)(\forall \gamma < \beta)(x > f(\gamma)) \end{cases}$$

Zauważmy, że istnieje β taka, że $f(\beta) = \infty$, gdyż gdyby takiej liczby nie było, to funkcja f byłaby injekcją liczby $\mathcal{H}(X)$ w zbiór X, co jest sprzeczne z definicją funkcji Hartogsa. Niech β_0 będzie najmniejszą liczbą porządkową taką, że $f(\beta_0) = \infty$. Zauważmy, że β_0 nie może być liczbą graniczną, gdyż wtedy $\{f(\gamma) : \gamma < \beta_0\}$ byłby łańcuchem, a więc $\{x \in X : (\forall \gamma < \beta_0)(f(\gamma) < x)\}$ byłby zbiorem niepustym, a więc $f(\beta_0) \neq \infty$. Zatem jest γ taka, że $\gamma + 1 = \beta$. Wtedy $f(\gamma)$ jest elementem maksymalnym częściowego porządku $(X, \leq)$. □

Wniosek D.1 *Następujące zdania są równoważne w teorii ZF:*

1. *Aksjomat Wyboru*
2. *Lemat Kuratowskiego-Zorna*
3. *Zasada dobrego uporządkowania*

Uwaga. *Aksjomat Wyboru jest używany w wielu działach matematyki. Potrzebny jest on do udowodnienia równoważności definicji Heinego i Cauchy'ego ciągłości funkcji. Potrzebny jest do pokazania, że każda przestrzeń liniowa posiada bazę oraz, że każdy właściwy filtr rozszerza się do ultrafiltru.*

D.3 Liczby Kardynalne

Z definicji podanej na początku tego rozdziału wynika, że liczbami kardynalnymi są takie liczby porządkowe, które nie są równoliczne z żadnym swoim właściwym odcinkiem początkowym. Oczywiście wszystkie liczby naturalne oraz zbiór ω są liczbami kardynalnymi.

Definicja D.6

$$\begin{cases} \aleph_0 & = & \omega \\ \aleph_{\alpha+1} & = & H(\aleph_\alpha) \\ \aleph_\lambda & = & \bigcup\{\aleph_\beta : \beta < \lambda\} \textit{ jeśli } lim(\lambda) \end{cases}$$

Liczba $\aleph_0$ jest więc dobrze nam znaną liczbą porządkową ω. Liczba $\aleph_1$ jest najmniejszą liczbą kardynalną większą od liczby $\aleph_0$. Oznacza to, że liczba $\aleph_1$ jest nieprzeliczalna oraz, że dowolna liczba porządkowa $\beta < \aleph_1$ jest liczbą przeliczalną.

Bez trudu można pokazać, że każda nieskończona liczba kardynalną jest postaci $\aleph_\alpha$ dla pewnej liczby porządkowej α. Zatem ciąg

$$\aleph_0 < \aleph_1 < \aleph_2 < \ldots < \aleph_\omega < \ldots$$

zawiera wszystkie liczby kardynalne.

Zauważmy, że zdanie

$$(\forall x)(\exists\alpha)(ord(\alpha) \wedge |x| = |\alpha|)$$

implikuje Aksjomat Wyboru, gdyż za pomocą bijekcji $f : \alpha \to x$ bez trudu można zbudować dobry porządek na zbiorze x, a z istnienia dobrego porządku na dowolnym zbiorze x wynika (patrz Tw. 6.12) Aksjomat Wyboru. Prawdziwa jest również odwrotna implikacja.

Twierdzenie D.11 (ZF) $\mathbf{AC} \to (\forall x)(\exists\kappa)(card(\kappa) \wedge |x| = |\kappa|)$

Dowód. Niech x będzie dowolnym zbiorem. Z Aksjomatu Wyboru (Twierdzenie D.9) wynika, że istnieje dobry porządek $\preceq$ zbioru x. Niech $\alpha_0 = ot(X, \preceq)$. Niech $A = \{\alpha \leq \alpha_0 : ord(\alpha) \wedge |\alpha| = |\alpha_0|\}$. Niech w końcu κ będzie minimalnym elementem zbioru A. Wtedy κ jest liczbą kardynalną oraz $|x| = |\kappa|$. □

Od tej pory będziemy stosowali zapis $|x| = \kappa$ jeśli κ jest liczbą kardynalną oraz $|x| = |\kappa|$.

Definicja D.7 *Niech κ i λ będą liczbami kardynalnymi.*

1. $\kappa + \lambda = |(\kappa \times \{0\}) \cup (\lambda \times \{1\})|$,

2. $\kappa \cdot \lambda = |\kappa \times \lambda|$,

3. $\kappa^{\lambda} = |\kappa^{\lambda}|$.

Dodawanie oraz mnożenie nieskończonych liczb kardynalnych jest wyjątkowo proste, co pokazuje następujące twierdzenie:

Twierdzenie D.12 *Dla dowolnych dwóch nieskończonych liczb kardynalnych κ i λ prawdziwe są równości $\kappa + \lambda = \kappa \cdot \lambda = max\{\kappa, \lambda\}$.*

Dowód. Zauważmy, że wystarczy pokazać, że dla każdej liczby porządkowej α prawdziwy jest wzór $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$. Rzeczywiście, z ciągu oczywistych nierówności

$$|\aleph_{max\{\alpha,\beta\}}| \leq |\aleph_\alpha + \aleph_\beta| \leq |\aleph_\alpha \cdot \aleph_\beta| \leq |\aleph_{max\{\alpha,\beta\}} \cdot \aleph_{max\{\alpha,\beta\}}| = |\aleph_{max\{\alpha,\beta\}}|$$

oraz z twierdzenia Cantora-Bernsteina otrzymujemy równości

$$|\aleph_\alpha + \aleph_\beta| = |\aleph_\alpha \cdot \aleph_\beta| = |\aleph_{max\{\alpha,\beta\}}|$$

Dowód tego, że $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$ przeprowadzimy indukcją po α. Dla liczby $\alpha = 0$ dowodzone zdanie jest prawdziwe, gdyż $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Załóżmy więc, że dla wszystkich $\beta < \alpha$ zachodzi równość $\aleph_\beta \cdot \aleph_\beta = \aleph_\beta$. Rozważmy następujący porządek $\preceq$ na zbiorze $\aleph_\alpha \times \aleph_\alpha$:

$$(a,b) \preceq (c,d) \leftrightarrow (max\{a,b\} < max\{c,d\}) \vee (max\{a,b\} = max\{c,d\} \wedge a < c) \vee$$

$$(max\{a,b\} = max\{c,d\} \wedge a = c \wedge b \leq d).$$

Łatwo można sprawdzić, że relacja $\preceq$ jest dobrym porządkiem na iloczynie kartezjańskim $\aleph_\alpha \times \aleph_\alpha$. Rozważmy dowolny element $(a,b) \in \aleph_\alpha \times \aleph_\alpha$. Niech $c = max\{a,b\}$. Wtedy $(a,b) \preceq (c,c)$. Zauważmy, że

$$\{(x,y) \in \aleph_\alpha \times \aleph_\alpha : (x,y) \preceq (c,c)\} \subseteq (c+1) \times (c+1).$$

Niech $\beta < \alpha$ będzie taka, że $|c+1| \leq \aleph_\beta$. Wtedy, na mocy założenia indukcyjnego, mamy

$$|(c+1) \times (c+1)| \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta.$$

Pokazaliśmy więc, że $\preceq$ jest dobrym porządkiem na $\aleph_\alpha \times \aleph_\alpha$ takim, że dla dowolnego $(a,b) \in \aleph_\alpha \times \aleph_\alpha$ moc zbioru $\{(x,y) \in \aleph_\alpha \times \aleph_\alpha : (x,y) \preceq (a,b)\}$ jest ostro mniejsza od $\aleph_\alpha$. Zatem $ot((\aleph_\alpha \times \aleph_\alpha, \preceq)) \leq \aleph_\alpha$ A więc $|\aleph_\alpha \times \aleph_\alpha| \leq \aleph_\alpha$, co kończy dowód □

Wniosek D.2 $\mathbf{AC} \rightarrow (\forall x)(|x| \geq \aleph_0 \rightarrow |x \times x| = |x|)$

Dowód. Jeśli prawdziwy jest Aksjomat Wyboru, to każdy zbiór jest równoliczny z pewną liczbą kardynalną, a więc równość $|x \times x| = |x|$ wynika z poprzedniego twierdzenia. □

Uwaga. W powyższym wniosku założenie Aksjomatu Wyboru jest konieczne.

D.4 Potęgowanie Liczb Kardynalnych

Głównym celem tej części jest omówienie zagadnień związanych z mocą liczb rzeczywistych, czyli z wyznaczeniem wartości $2^{\aleph_0}$. W rozdziale tym zakładamy, że prawdziwy jest Aksjomat Wyboru, czego konsekwencją jest, między innymi to, że moc zbioru liczb rzeczywistych jest liczbą kardynalną.

Definicja D.8 (CH) *Hipotezą Continuum nazywamy zdanie* $2^{\aleph_0} = \aleph_1$.

Twierdzenie D.13 *Załóżmy, że* $2 \leq \lambda \leq \kappa$ *oraz, że* $\kappa \geq \omega$. *Wtedy* $\lambda^\kappa = 2^\kappa$.

Dowód. Zauważmy, że

$$2^\kappa \leq \lambda^\kappa \leq \kappa^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa} = 2^\kappa,$$

więc równość $\lambda^\kappa = 2^\kappa$ otrzymujemy z Twierdzenia Cantora-Bernsteina. □

Widzimy więc, że znajomość wartości 2^κ pozwala nam na wyliczenie wartości λ^κ dla wszystkich $\lambda \leq \kappa$. Szczególnym przypadkiem tego twierdzenia jest znana już nam równości $2^{\aleph_0} = (2^{\aleph_0})^{\aleph_0}$.

Definicja D.9 *Niech* $(\kappa_i)_{i \in I}$ *będzie dowolną rodziną liczb kardynalnych.*

1. $\sum_{i \in I} \kappa_i = |\bigcup_{i \in I} (\kappa_i \times \{i\})|$
2. $\prod_{i \in I} \kappa_i = |\prod_{i \in I} \kappa_i|$

Twierdzenie D.14 (König) *Załóżmy, że* $(\lambda_i)_{i \in I}$ *i* $(\kappa_i)_{i \in I}$ *będą takimi rodzinami liczb kardynalnych taką, że* $(\forall i \in I)(\lambda_i < \kappa_i)$. *Wtedy* $\sum_{i \in I} \lambda_i < \prod_{i \in I} \kappa_i$.

Dowód. Niech $P = \prod_{i \in I} \kappa_i$. Niech $(X_i)_{i \in I}$ będzie taką rodziną zbiorów, że $\bigcup_{i \in I} X_i = P$ oraz $|X_i| = \lambda_i$ dla wszystkich $i \in I$. Niech $f \in P$ będzie taką funkcją, że $f(i) \in \kappa_i \setminus \{x(i) : x \in X_i\}$ dla każdego $i \in I$. Wtedy $f \notin \sum_{i \in I} X_i$. □

Zauważmy, że z powyższego twierdzenia możemy w łatwy sposób wyprowadzić twierdzenie Cantora. Mianowicie, niech A będzie dowolnym zbiorem. Niech $\lambda_a = 1$ oraz $\kappa_a = 2$ dla wszystkich $a \in A$. Wtedy

$$|A| = \sum_{a \in A} \lambda_a < \prod_{a \in A} \kappa_a = 2^{|A|}.$$

Definicja D.10 *Kofinalnością nieskończonej liczby kardynalnej* κ *nazywamy liczbę*

$$cof(\kappa) = min\{\alpha \in Ord : (\exists f \in \kappa^\alpha)(\forall \beta < \kappa)(\exists \gamma < \alpha)(f(\gamma) > \beta)\}.$$

Kofinalność dowolnej nieskończonej liczby kardynalną jest liczbą kardynalną. Z równości $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$ również łatwo wynika, że $cof(\aleph_{\alpha+1}) = \aleph_{\alpha+1}$ dla dowolnej liczby porządkowej α. W szczególności $cof(\aleph_n) = \aleph_n$ dla każdej liczby naturalnej n. Jednak nie dla wszystkich liczb kardynalnych zachodzi równość $cf(\kappa) = \kappa$. Pierwszą liczbą kardynalną która nie ma tej własności jest liczba $\aleph_\omega$. Rozważmy bowiem funkcję $f(n) = \aleph_n$. Wtedy $f : \omega \to \aleph_\omega$ oraz $(\forall \beta \in \aleph_\omega)(\exists n \in \omega)(f(n) > \beta)$. Zatem $cof(\aleph_\omega) = \omega$. Liczbę kardynalną κ nazywamy *regularną*, jeśli $cof(\kappa) = \kappa$.

Twierdzenie D.15 (König) *Dla każdej nieskończonej liczby κ prawdziwa jest nierówność $cof(2^\kappa) > \kappa$.*

Dowód. Załóżmy, że $cof(2^\kappa) \leq \kappa$. Istnieje wtedy funkcja $f : \kappa \to 2^\kappa$ taka, że $\bigcup rng(f) = 2^\kappa$. Lecz wtedy

$$2^\kappa = \sum_{\alpha<\kappa} |f(\alpha)| < \prod_{\alpha<\kappa} 2^\kappa = (2^\kappa)^\kappa = 2^\kappa,$$

a więc otrzymaliśmy sprzeczność. □

Wniosek D.3 $cof(2^{\aleph_0}) > \aleph_0$

Wniosek ten można sformułować następująco: liczby rzeczywiste nie są przeliczalną sumą zbiorów mocy mniejszej od continuum. Otrzymany wynik jest jedynym praktycznym ograniczeniem na moc continuum.

Niech κ^+ oznacza najmniejszą liczbę kardynalną ostro większą od liczby κ. Oczywiście, jeśli $\kappa = \aleph_\alpha$ to $\kappa^+ = \aleph_{\alpha+1}$.

Twierdzenie D.16 (Hausdorff) *Załóżmy, że $2 \leq \lambda \leq \kappa$ oraz, że $\kappa \geq \omega$. Wtedy $(\kappa^+)^\lambda = \kappa^+ \cdot \kappa^\lambda$.*

Dowód. Z nierówności $\lambda \leq \kappa$ wynika, że $\lambda < cof(\kappa^+) = \kappa^+$. Zatem

$$(\kappa^+)^\lambda = |\bigcup_{\alpha<\kappa^+} \alpha^\lambda| \leq \sum_{\alpha<\kappa^+} |\alpha^\lambda| \leq \sum_{\alpha<\kappa^+} |\kappa^\lambda| \leq \kappa^+ \cdot \kappa^\lambda$$

Nierówność w drugą stronę jest zaś oczywista. □

Przykład D.7 *Ze wzoru Hausdorffa wynika, że*

$$\aleph_3{}^{\aleph_0} = \aleph_3 \cdot \aleph_2{}^{\aleph_0} = \aleph_3 \cdot \aleph_2 \cdot \aleph_1{}^{\aleph_0} = \aleph_3 \cdot \aleph_1 \cdot \aleph_0{}^{\aleph_0} = \aleph_3 \cdot 2^{\aleph_0}$$

Widzimy więc, że jeśli prawdziwa jest Hipoteza Continuum to wtedy $\aleph_3{}^{\aleph_0} = \aleph_3$.

Wróćmy do rozważań związanych z mocą zbioru liczb rzeczywistych, czyli z wyznaczeniem liczby $2^{\aleph_0}$.

Definicja D.11 (GCH) *Uogólnioną Hipotezą Continuum nazywamy zdanie*

$$(\forall \alpha \in Ord)(2^{\aleph_\alpha} = \aleph_{\alpha+1}).$$

Następujące dwa twierdzenia przyjmiemy bez dowodu:

Twierdzenie D.17 (Gödel) $Con(\mathbf{ZF}) \to Con(\mathbf{ZF} \cup \{\mathbf{GCH}\})$

Twierdzenie D.18 (Cohen) $Con(\mathbf{ZF}) \to Con(\mathbf{ZF} \cup \{\neg\mathbf{CH}\})$

Uwaga. Dowody obu twierdzeń są stosunkowo trudne. Pierwszy dowód polega na zbudowaniu uniwersum tak zwanych zbiorów konstruowalnych, pokazaniu, że jest ono modelem teorii **ZFC** oraz udowodnieniu, że w uniwersum zbiorów konstruowalnych prawdziwa jest **GCH**. Wymaga to znajomości logiki pierwszego rzędu oraz elementów teorii modeli. Dowód drugiego twierdzenia wymaga opanowania techniki forcingu. Polega ona na umiejętnym rozszerzaniu modeli teorii mnogości o specyficzne ultrafiltry w zupełnych algebrach Boolea'a z tych modeli.

Widzimy więc, że Hipoteza Continuum jest niezależna od teorii **ZFC**. Postaramy się teraz pokazać jak mocno niezdeterminowana jest wartość $2^{\aleph_0}$. Rozważmy funkcję $F(\kappa) = 2^\kappa$ określoną dla nieskończonych liczb kardynalnych κ. Funkcja ta posiada dwie własności:

- E1: jeśli $\kappa \leq \lambda$ to $F(\kappa) \leq F(\lambda)$,
- E2: $cf(F(\kappa)) > \kappa$ dla wszystkich regularnych liczb kardynalnych κ.

Okazuje się, że są to jedyne ograniczenia na wartości 2^κ dla regularnych liczb kardynalnych. Prawdziwe jest bowiem następujące twierdzenie

Twierdzenie D.19 (Easton) *Załóżmy, że F jest funkcją określoną dla nieskończonych, regularnych liczb kardynalnych spełniającą warunki E1 oraz E2. Wtedy teoria mnogości*

$$\mathbf{ZFC} \cup \{(\forall \kappa)(\kappa \textit{ jest regularna } \rightarrow 2^\kappa = F(\kappa))\}$$

jest relatywnie niesprzeczna.

Przez relatywną niesprzeczoność rozumiemy niesprzeczność pod warunkiem niesprzeczności teorii **ZF**. W szczególności, z Twierdzenia Eastona wynika, że jedynym ograniczeniem na wartość $2^{\aleph_0}$ jest to aby $cof(2^{\aleph_0}) > \aleph_0$. Niesprzeczne są więc teorie $\mathbf{ZFC} \cup \{2^{\aleph_0} = \aleph_1\}$, $\mathbf{ZFC} \cup \{2^{\aleph_0} = \aleph_2\}$, $\mathbf{ZFC} \cup \{2^{\aleph_0} = \aleph_3\}$ i.t.d. Zauważmy również, że wartość $2^{\aleph_0}$ nie ma większego wpływu na wartość liczby $2^{\aleph_1}$. Z twierdzenia Eastona wynika bowiem, niesprzeczne są teorie $\mathbf{ZFC} \cup \{2^{\aleph_0} = \aleph_2 + 2^{\aleph_1} = \aleph_2\}$ oraz $\mathbf{ZFC} \cup \{2^{\aleph_0} = \aleph_2 + 2^{\aleph_1} = \aleph_3\}$.

Twierdzenie Eastona pokazuje, że jedynymi ograniczeniami na wartości funkcji 2^κ dla liczb regularnych są własności [E1] oraz [E2]. Dla liczb nieregularnych sytuacja jest znacznie bardziej skomplikowana. Rozważania nasze zakończymy dwoma twierdzeniami, które ilustrują to zjawisko.

Twierdzenie D.20 (Silver) *Załóżmy, że $\aleph_1 \leq cof(\kappa) < \kappa$ oraz, że*

$$(\forall \lambda \in Card)(\lambda < \kappa \rightarrow 2^\lambda = \lambda^+).$$

Wtedy $2^\kappa = \kappa^+$.

Twierdzenie D.21 (Shelah)

$$(\forall n < \omega)(2^{\aleph_n} < \aleph_\omega) \rightarrow 2^{\aleph_\omega} < \aleph_{\aleph_4}$$

D.5 Zadania

Zadanie D.1 *Udowodnij prawdziwość następujących zdań:*

1. $(\forall x)(tran(x) \rightarrow tran(P(x)))$
2. $(\forall x)(tran(x) \rightarrow tran(scc(x))$
3. $(\forall x)(\forall y)((y \in x \rightarrow tran(z)) \rightarrow tran(\bigcup x))$

Zadanie D.2 *Udowodnij prawdziwość następujących zdań:*

1. $(\forall x)(ord(x) \rightarrow ord(scc(x)))$
2. $(\forall x)((\forall y)(y \in x \rightarrow ord(z)) \rightarrow ord(\bigcup x))$

Zadanie D.3 *Pokaż, że nie istnieje zbiór wszystkich liczb porządkowych. Pokaż, że nie istnieje zbiór wszystkich liczb kardynalnych.*

Zadanie D.4 *Pokaż, że dodawanie i mnożenie liczb porządkowych jest łączne.*

Zadanie D.5 *Pokaż, że jeśli $\alpha, \beta < \aleph_1$ to $\alpha \cdot \beta < \aleph_1$ (symbol $\cdot$ oznacza tutaj mnożenie liczb porządkowych). Pokaż, że istnieje nieskończona liczba porządkowa $\alpha < \aleph_1$ taka, że jeśli $\beta, \gamma < \alpha$ to $\beta \cdot \gamma < \alpha$.*

Zadanie D.6 *Dla danego zbioru a określamy $tc(a) = \{a\} \cup a \cup (\bigcup a) \cup (\bigcup\bigcup a) \cup (\bigcup\bigcup\bigcup a) \cup \ldots$. Pokaż, że $tc(a)$ jest najmniejszym zbiorem tranzytywnym do którego należy zbiór a.*

Zadanie D.7 *Pokaż, że dla każdej liczby porządkowej α zachodzi równość $\alpha = \{x \in R_\alpha : ord(x)\}$.*

Zadanie D.8 *Pokaż, że jeśli α, β są liczbami porządkowymi takim, że struktury $(\alpha, \subseteq)$ i $(\beta, \subseteq)$ są izomorficzne, to $\alpha = \beta$.*

Zadanie D.9 *Które aksjomaty teorii mnogości ZFC są prawdziwe w strukturze $(R_{\aleph_0}, \in)$? Które aksjomaty teorii mnogości ZFC są prawdziwe w strukturze $(R_{\aleph_1}, \in)$?*

Zadanie D.10 *Załóżmy, że $2^{\aleph_0} = 2^{\aleph_1} = 2^{\aleph_3} = \aleph_4$ oraz, że $(\forall \alpha \geq 4)(2^{\aleph_\alpha} = \aleph_{\alpha+1}$. Sprawdź, że założenie to spełnia warunki twierdzenia Eastona. Wyznacz wartości $\aleph_n^{\aleph_m}$ dla wszystkich par liczb naturalnych n oraz m.*

Zadanie D.11 *Pokaż, że $cof(\kappa)$ jest liczbą kardynalną oraz, że $cof(cof(\kappa)) = cof(\kappa)$ dla dowolnej nieskończonej liczby kardynalnej κ.*

Zadanie D.12 *Pokaż, przy pomocy Aksjomatu Wyboru, że $(\forall \alpha)(cf(\aleph_{\alpha+1}) = \aleph_{\alpha+1})$.*

Zadanie D.13 *Pokaż, że istnieje taki podzbiór A płaszczyzny $\mathbb{R}^2$ mocy continuum który z każdą prostą ma co najwyżej dwa wspólne punkty.*

Zadanie D.14 *Pokaż, że istnieje bijekcja $f : \mathbb{R} \rightarrow \mathbb{R}$, której wykres jest gęsty na płaszczyźnie.*

Zadanie D.15 *Pokaż, że jeśli prawdziwa jest Uogólniona Hipoteza Continuum, to*

$$\kappa^\lambda = \begin{cases} \kappa & : \quad \lambda < cof(\kappa) \\ \kappa^+ & : \quad cof(\kappa) \leq \lambda \leq \kappa \\ \lambda^+ & : \quad \kappa < \lambda \end{cases}$$

Zadanie D.16 (Sierpiński) *Niech κ będzie nieskończoną liczbą kardynalną i niech $(A_\alpha)_{\alpha<\kappa}$ będzie rodziną zbiorów mocy κ. Pokaż, że istnieje rodzina $(B_\alpha)_{\alpha<\kappa}$ parami rozłącznych zbiorów mocy κ taka, że $(\forall \alpha < \kappa)(B_\alpha \subseteq A_\alpha)$.*

Zadanie D.17 *Niech $\prec$ będzie taką relacją na zbiorze X, że*

$$(\forall A \subseteq X)(A \neq \emptyset \to (\exists a \in A)(\forall b)(b \prec a \to b \notin A)).$$

Pokaż, że istnieje wtedy taka liczba porządkowa α oraz funkcja $f : X \to \alpha$ taka, że $(\forall x, y \in X)(x \prec y \to f(x) \in f(y))$.

Zadanie D.18 *Każdą liczbę naturalną przedstawiamy w postaci $n = \sum_k \frac{b(n,k)}{2^k}$, gdzie $b(n,k) \in \{0,1\}$. Niech*

$$\pi(n) = \{\pi(k) : b(n,k) = 1\}.$$

Pokaż, że π jest bijekcją pomiędzy zbiorami ω oraz R_ω.

Zadanie D.19 *Pokaż, że rodzina wszystkich borelowskich podzbiorów prostej $\mathbb{R}$ jest mocy* $\mathfrak{c}$.

Zadanie D.20 *Pokaż, że nie istnieje podzbiór prostej $\mathbb{R}$ porządkowo izomorficzny z ω_1.*

Zadanie D.21 *Załóżmy, że $2^{\aleph_0} = 2^{\aleph_1} = 2^{\aleph_2} = \aleph_3$ oraz $2^{\aleph_3} = \aleph_4$. Wyznacz κ^λ dla wszystkich nieskończonych liczb kardynalnych $\kappa, \lambda \leq \aleph_3$.*

Zadanie D.22 *Niech E bedzie relacją ufundowaną na zbiorze X. Pokaż, że istnieje dobry porządek $(K, \preceq)$ oraz funkcja $f : X \to K$ taka, że $(\forall x, y \in X)(xEy \to f(x) \prec f(y))$.*

E Wskazówki do zadań

Zadanie 1.1. Rozważ rodzinę wszystkich napisów, które mają taką samą liczbę nawiasów otwierających co zamykających i pokaż, indukcją po stopniu złożoności, że każde zdanie należy do tej rodziny.

Zadanie 1.3. Zauważ, że $\pi(\varphi(\psi_0, \ldots, \psi_n)) = \omega(\varphi)$, gdzie ω jest waluacją określoną wzorem $(\pi(\psi_0), \ldots, \pi(\psi_n))$.

Zadanie 1.4. Indukcją względem n pokaż, że $\varphi_{2n} \equiv p$ oraz $\varphi_{2n+1} \equiv \mathbb{1}$.

Zadanie 1.5. Zauważ, ze każdy iloczyn X długości n można zapisać jako $(Y) \cdot (Z)$, gdzie Y jest pewnym iloczynem długości a, Z jest pewnym iloczynem długości b oraz $a + b = n$. Stąd łatwo wynika wzór (1.1). A z niego mamy $c_3 = c_0 \cdot c_3 + c_1 \cdot c_2 + c_2 \cdot c_1 + c_3 \cdot c_0 = 0 + 1 \cdot 1 + 1 \cdot 1 + 0 = 2$. Podobnie obliczamy, że $c_4 = 5$.

Zadanie 1.6. Można zbudować $2^{(2^2)}$, czyli 16 nierównoważnych zdań.

Zadanie 1.7. Pokaż, że jeśli φ jest zbudowane tylko za pomocą koniunkcji i alternatywy oraz π jest taką waluację, że $\pi(p_i) = \mathbb{1}$ dla każdego i, to $\pi(\varphi) = \mathbb{1}$.

Zadanie 1.8. Rozwinięcia dziesiętne liczb wymiernych są postaci

$$N.a_1 \ldots a_n b_1 \ldots b_k b_1 \ldots b_k b_1 \ldots b_k \ldots$$

dla pewnych ciągów cyfr $a_1 \ldots a_n$ oraz $b_1 \ldots b_k$. Rozważana liczba nie jest tej postaci.

Zadanie 1.9. Zbadaj pytanie „Którą drogę wskazał by twój współmieszkaniec?"

Zadanie 2.3. Pokaż, że $x_{n+1} = \{x_0, \ldots, x_n\}$ dla wszystkich n.

Zadanie 2.5. Załóż, że $A = P(A)$ i rozważ zbiór $D = \{x \in A : x \notin x\}$. Pokaż, że $D \in A$ i następnie, że $D \in D \leftrightarrow D \notin D$.

Zadanie 2.6. Załóż, że istnieje taki zbiór Ω. Pokaż, że wtedy zbiór $P(\Omega)$ byłby zbiorem wszystkich zbiorów.

Zadanie 3.1. Gracz pierwszy ma strategię zwycięską w tej grze. Opisać ją można następująco: *graj tak aby po każdym twoim ruchu liczba pozostałych zapałek była podzielna przez 4*.

Zadanie 3.2. Pokaż, że $A \times B = \{(x, y) \in P(P(A \cup B)) : x \in A \wedge y \in B\}$.

Zadanie 3.5. Na mocy twierdzenia Lagrange'a każdą liczbę naturalną można przedstawić jako sumę czterech kwadratów liczb naturalnych. Zatem

$$(x \geq 0) \leftrightarrow (\exists a, b, c, d)(x = a \cdot a + b \cdot b + c \cdot c + d \cdot d).$$

Zadanie 3.6. Pokaż najpierw, że za pomocą symbolu $|$ można zdefiniować własności $z = NWD(x, y)$ oraz $z = NWW(x, y)$. Pokaż następnie, że dla dowolnej dodatniej liczby naturalnej x mamy $NWD(x, x+1) = 1$ i wywnioskuj z tego, że $NWW(x, x+1) = x^2 + x$. Rozważ następnie formułę

$$k(x, y) = (x = 0 \wedge y = 0) \vee (x \neq 0 \wedge (x + y = NWW(x, x + 1)))$$

i sprawdź, że $k(x, y)$ jest prawdziwe dla liczb naturalnych x i y wtedy i tylko wtedy, gdy $y = x^2$. Rozważ w końcu formułę $\varphi(x, y, z)$ zdefiniowaną następująco

$$(\exists a)(\exists b)(\exists c)(k(x + y, a) \wedge k(x, b) \wedge k(y, c) \wedge a = b + z + z + c).$$

Pokaż, że $\varphi(x, y, z)$ jest prawdziwe wtedy i tylko wtedy, gdy $z = xy$.

Zadanie 4.2. Odpowiedź: $2^{(2^n)}$.

Zadanie 4.4. $\liminf_{n\in\mathbb{N}} A_n = A \cap B \cap C$, $\limsup_{n\in\mathbb{N}} A_n = A \cup B \cup C$.

Zadanie 4.5. Załóżmy, że $x \in \bigcap_{i\in I} \bigcup_{j\in J} A_{i,j}$, czyli, że $(\forall i \in I)(\exists j \in J)(x \in A_{i,j})$. Dla każdego $i \in I$ wybierzmy $j_i \in J$ takie, że $x \in A_{i,j_i}$ i połóżmy $f = \{(i, j_i) : i \in I\}$. Wtedy $x \in \bigcap_{i\in I} A_{i,f(i)}$, z czego wynika jedna inkluzja.

Zadanie 4.6. Chodzi o następujące uogólnienie: *jeśli $\mathcal{F}$ jest taką rodziną funkcji, że $(\forall f, g \in F)(f \cup g$ jest funkcją), to $\bigcup \mathcal{F}$ też jest funkcją.*

Zadanie 4.9. Rozważ alternatywę wszystkich koniunkcji postaci $\varphi = p_{i_1} \wedge \ldots \wedge p_{i_k}$ które mają następującą własność: dla każdego ciągu wartości logicznych $(t_1, \ldots, t_n)$ jeśli $(t_1, \ldots, t_n)(\varphi) = \mathbb{1}$, to $f(t_1, \ldots, t_n) = \mathbb{1}$.

Zadanie 4.10. Zauważ, że $|\{i > 1 : (1, i) \in R\}| \geq 3$ lub $|\{i > 1 : (1, i) \notin R\}| \geq 3$. Rozważ każdy z tych przypadków oddzielnie.

Zadanie 5.1. Zwrotność relacji $\sim_H$ wynika z tego, że $xx^{-1} = e \in H$. Do udowodnienia symetrii skorzystaj z tego, że równości $(xy)^{-1} = y^{-1}x^{-1}$ oraz $(x^{-1})^{-1} = x$ są prawdziwe w dowolnej dowolnej grupie.

Zadanie 6.1. Niech $p_1, \ldots, p_n$ będą różnymi liczbami pierwszymi. Rozważ zbiór $T = \{\prod_{i\in A} p_i : A \in P(\{1, \ldots, n\})\}$.

Zadanie 6.3. Niech $f(x) = \frac{w(x)}{v(x)}$, gdzie w jest wielomianem stopnia n oraz v jest wielomianem stopnia m. Pokaż, że $f(x) = \Theta(x^{n-m})$.

Zadanie 6.4. Pokaż, że jeśli $f \lhd g$, to $f \lhd \frac{f+g}{2} \lhd g$.

Zadanie 6.5. Zdefiniuj funkcję $f : \mathbb{N} \to X$ w następujący sposób: $f(0) = \min_{\leq}(X)$, $f(n+1) = \min_{\leq}(X \setminus \{f(0), \ldots, f(n)\})$. Pokaż, że $rng(f) = X$. Wskazówka: załóż, że $X \setminus rng(f) \neq \emptyset$ i przyjrzyj się $\leq$-najmniejszemu elementowi tego zbioru.

Zadanie 6.6. Niech S będzie selektorem rodziny $\{f^{-1}[\{b\}] : b \in B\}$. Rozważ taką funkcję $g : B \to A$, że $\{g(b)\} = S \cap f^{-1}[\{b\}]$.

Zadanie 6.7. Pokaż najpierw, że jeśli $(a_n)_{n\in\mathbb{N}}$ jest ciągiem liczb naturalnych, to istnieje ciąg $n_0 < n_1 < n_2 < \ldots$ taki, że $a_{n_0} \leq a_{n_1} \leq a_{n_2} \leq \ldots$.

Zadanie 6.8. Dla ciągu $x \in \{0,1\}^*$ przez $d(x)$ oznacz ciąg powstały z x przez podwojenie bitów, np. $d(0101) = 00110011$. Pokaż, że funkcja

$$f(x, y) = d(x)01y$$

jest injekcją.

Zadanie 7.3. Wypisując wszystkie ciągi bez dwóch kolejnych liter a długości 0, 1, 2, 3 stwierdzamy, że $s_0 = 1$, $s_1 = 2$, $s_2 = 3$ i $s_3 = 5$. Rozważ następnie ciągi długości $n+1$. Podziel je na dwa podzbiory: zaczynające się od b i zaczynające się od ab. Pokaż, że nie ma innych możliwości. Wywnioskuj z tego, że $s_{n+1} = s_n + s_{n-1}$. Następnie porównaj to równanie z definicją liczb Fibbonacciego (rodz. 7.1) i wywnioskuj, że $s_n = F_{n+1}$.

Zadanie 7.5. Pokaż indukcją matematyczną, że

$$(\forall n \in \mathbb{N})(\forall A \subseteq \{0, \ldots, n\})(A \neq \emptyset \to (\exists a \in A)(\forall x \in A)(a \leq x)).$$

Zadanie 7.5. Zauważ najpierw, że $n! = e^{\ln(n!)} = e^{\sum_{k=1}^{n} \ln(k)}$. Następnie, korzystając z monotoniczności funkcji $\ln(x)$ pokaż, że

$$\int_1^n \ln(x)dx < \sum_{k=1}^{n} \ln(k) < \int_2^{n+1} \ln(x)dx.$$

Skorzystaj teraz ze wzoru $\int \ln(x)dx = x(\ln(x) - 1) + C$.

Zadanie 7.6. Rozważ następujący porządek $\preceq$ na $\mathbb{N} \times \mathbb{N}$:

$$(n, m) \preceq (n', m') \leftrightarrow (n < n') \vee (n = n' \wedge m \leq m')$$

Z twierdzenia o produkcie dobrych porządków wynika, że jest to dobry porządek. Pokaż, że gdyby funkcja Ackermana nie była określona dla pewnej pary (n, m) to istniałby nieskończony malejący ciąg elementów $(\mathbb{N} \times \mathbb{N}, \preceq)$.

Zadanie 7.8. Rozważ zbiory $A_i = \{2^p(2i-1) : p \in \mathbb{N}\} \cap \{1, \ldots, 2n\}$ $(i = 1, \ldots, n)$. Wtedy $A_1 \cup \ldots \cup A_n = \{1, 2, ..., 2n\}$. Jest więc i (zasada Dirichletta) takie, że $|A \cap A_i| \geq 2$.

Zadanie 7.9. Załóż, że teza jest fałszywa. Każdej liczbie $i \in \{1, \ldots, mn+1\}$ przyporządkuj parę (r_i, m_i) taką, że r_i jest największą długością ciągu rosnącego zaczynającego się od x_i zaś m_i jest jest największą długością ciągu malejącego zaczynającego się od x_i. Z fałszywości tezy wynika, że dla każdego i mamy $1 \leq r_i \leq m$

oraz $1 \leq m_i \leq n$, czyli, że $(r_i, m_i) \in \{1, \ldots, m\} \times \{1, \ldots, n\}$. Z zasady Dirichletta wynika istnienie $i < j$ takiego, że $(r_i, m_i) = (r_j, m_j)$. Rozważ teraz dwa przypadki: $x_i < x_j$ oraz $x_i \geq x_j$.

Zadanie 7.10. Rozważ relację równważności $\approx$ na zbiorze $P(\{1, ..., n\}) \setminus \{\emptyset\}$ określoną formułą

$$A \approx B \leftrightarrow (A = B \vee A = B^c).$$

Wyznacz jej klasy abstrakcji, oblicz $|(P(\{1, ..., n\}) \setminus \{\emptyset\})/\approx|$ i skorzystaj z zasady Dirichletta.

Zadanie ??. Pokaż najpierw, że jeśli $(X, \leq)$ jest częściowym porządkiem, $a, b \in X$ są nieporównywalne (czyli $\neg(a \leq b)$ i $\neg(b \leq a)$), to relacja

$$\leq \cup \{(x, y) : x \leq a \wedge b \leq y\}$$

jest również częściowym porządkiem, który rozszerza istotnie porządek $\leq$.

Zadanie C.5. $\prod f = \{x \in P\big(dom(f) \times (\bigcup rng(f))\big) : func(x) \wedge dom(x) = dom(f) \wedge (\forall t \in dom(f))(x(t) \in f(t))\}$

Zadanie C.6. Załóż, że $dom(f) = \omega \wedge (\forall n)(f(n+1) \in f(n))$ i zastosuj Aksjomat Regularności do zbioru $rng(f)$.

Zadanie C.8. Zauważ, że w każdym skończonym i niepustym podzbiorze zbioru liniowo uporządkowanego można wyróżnić pewien element, a mianowicie element najmniejszy. Selektor rodziny $\mathcal{X}$ można więc otrzymać za pomocą Aksjomatu Wyróżniania. Przyjrzyj się bowiem zbiorowi

$$\{x \in X : (\exists A \in \mathcal{X})(x \in A \wedge (\forall y \in A)(x \leq y))\}.$$

Zadanie C.9. Pokaż najpierw, bez korzystania z Aksjomatu Pary, że istnieje zbiór c, który posiada dwa różne elementy a i b. Następnie dla ustalonych t_0 i t_1 rozważ formułę

$$\psi(x, y) = (x = a \wedge y = t_0) \vee (x \neq a \wedge y = t_1).$$

Zastosuj do formuły ψ oraz zbioru c Aksjomat Zastępowania.

Zadanie C.10. Zauważ, że $a \in \{a\} \in (a, b)$. Załóż, że istnieje $A \neq \emptyset$ taki, że $A \subseteq A \times A$. Wtedy dla każdego $a \in A$ istnieć musi $b \in A$ takie, że $b \in \{b\} \in a$. Skorzystaj teraz z Zadania C.6.

Zadanie D.12. Przypomnij sobie, że $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$. Przy pomocy Aksjomatu Wyboru pokaż, że jeśli $(X_\beta)_{\beta < \aleph_\alpha}$ jest rodziną zbiorów taką, że $(\forall \beta < \aleph_\alpha)(|X_\beta| \leq \aleph_\alpha)$, to $|\bigcup \{X_\beta : \beta < \aleph_\alpha\}| \leq \aleph_\alpha$.

Zadanie D.16. Wzoruj się na zadaniu 8.8, ale zamiast korzystać z równości $\aleph_0 \times \aleph_0 = \aleph_0$, skorzystaj z tego, że $\kappa \times \kappa = \kappa$, dla każdej nieskończonej liczby kardynalnej κ.

Zadanie D.17. Zdefiniuj funkcję f wzorem $f(x) = \{f(y) : y \prec x\}$. Oczywiście, musisz pokazać, że definicja ta jest poprawna.

Zadanie D.18. Zauważ, że jeśli $b(n,k) = 1$ to $k < n$. Wywnioskuj z tego, że funkcja π jest poprawnie określona. Następnie indukcją po n pokaż, że $(\forall m \geq n)(\pi(n) = \pi(m) \to m = n)$. Kolejnym indukcyjnym rozumowaniem pokaż, że $\pi : \mathbb{N} \xrightarrow{1-1} R_\omega$. Aby pokazać, że $\pi : \mathbb{N} \xrightarrow{na} R_\omega$ załóż, że to nie jest prawdą i zastosuj Aksjomat Regularności do zbioru $R_\omega \setminus rng(\pi)$.

Zadanie D.19. Niech $\sigma(\mathcal{A}) = \{\bigcup X : X \in \mathcal{A} \wedge |X| \leq \aleph_0\}$. Pokaż, że jeśli $|\mathcal{A}| \leq \mathfrak{c}$ to również $|\sigma(\mathcal{A})| \leq \mathfrak{c}$. Niech $\mathcal{A}_0$ będzie rodziną wszystkich odcinków. Załóżmy, że mamy zdefiniowane $\mathcal{A}_\beta$ dla wszystkich $\beta < \alpha$. Niech $\mathcal{S}_\alpha = \bigcup\{\mathcal{A}_\beta : \beta < \alpha\}$ oraz $\mathcal{B}_\alpha = \sigma(\mathcal{S}_\alpha)$. Kładziemy $\mathcal{A}_\alpha = \mathcal{B}_\alpha \cup \{\mathbb{R} \setminus X : X \in \mathcal{B}_\alpha\}$.

Pokaż, że dla każdej $\alpha < \omega_1$ mamy $|\mathcal{A}_\alpha| = \mathfrak{c}$ oraz, korzystając z regularności liczby ω_1, że $\mathbf{B}(\mathbb{R}) = \bigcup\{\mathcal{A}_\alpha : \alpha < \omega_1\}$.

Zadanie D.20. Jaka może być moc rodziny niepustych parami rozłącznych odcinków?

Zadanie D.21. Skorzystaj z twierdzenia Hausdorffa.

Bibliografia

[1] Z. Adamowicz, P. Zbierski. *Logika Matematyczna*. Polskie Wydawnictwo Naukowe, Warszawa, 1991.

[2] W. Guzicki, P. Zbierski. *Podstawy teorii mnogości*. Polskie Wydawnictwo Naukowe, Warszawa, 1978.

[3] T. Jech. *Set Theory*. Pure and Applied Mathematics. Academic Press, Inc., New York, 1978.

[4] K. Kuratowski. *Wstêp do teorii Mnogości i Topologii*. Polskie Wydawnictwo Naukowe, Warszawa, 1982.

[5] K Kuratowski, A. Mostowski. *Teoria mnogości*. Polskie Wydawnictwo Naukowe, Warszawa, 1978.

[6] W. Marek, J. Onyszkiewicz. *Zbiór zadañ z logiki i teorii mnogości*. Polskie Wydawnictwo Naukowe, Warszawa, 1982.

[7] K.A. Ross, C. R. B. Wright. *Matematyka dyskretna*. Wydawnictwa Naukowo-Techniczne, Warszawa, 2003.

Indeks