

Uniwersytet Wrocławski, Instytut Informatyki
Studia magisterskie na kierunku Informatyka
Przedmiot obowiązkowy w semestrze zimowym pierwszego roku studiów
30 godzin wykładu + 30 godzin repetytorium + 30 godzin ćwiczeń

Logika dla informatyków

Materiały do zajęć

Wrocław, 2009

2009/10

Właściciel tej kopii notatek

Rok akad.

Uwaga: W niniejszej książeczce zebrano listy zadań, notatki do wykładów oraz inne materiały przygotowywane do zajęć z *Logiki dla informatyków* w latach 1997–2009. Mimo iż materiały te posiadają bardziej dopracowaną formę, niż przygotowywane do innych zajęć kserograficzne kopie oraz zostały oddane do druku i oprawy, jednak nie były poddane — jak to ma miejsce w przypadku podręczników — solidnej korekcie i zawierają sporo błędów. Nie zamieszczono w nich także szczegółowych wyjaśnień i komentarzy. Dlatego notatki te *nie są podręcznikiem do wykładu*. Mają jedynie służyć jako wykaz zagadnień obowiązujących do egzaminu i lista zadań przerabianych na ćwiczeniach. Przegląd zalecanych do zajęć podręczników jest zamieszczony na stronie xi.

Podczas redagowania notatek wykorzystano:

- skrypt J. Tiurny *Wstęp do teorii mnogości i logiki*
- listy zadań M. Zakrzewskiego
- materiały A. Kościelskiego i T. Wierzbickiego
- podręczniki wymienione w bibliografii na stronie xi

Manuskrypt: L. Pacholski i W. Charatonik

Redakcja i skład: T. Wierzbicki

Konsultacja merytoryczna: A. Kościelski

Wydanie siódme, poprawione

Niniejsze notatki mogą być drukowane, powielane oraz rozpowszechniane w wersji elektronicznej i papierowej, w części bądź w całości — bez konieczności uzyskania zgody autora — pod warunkiem nieosiągania bezpośrednich korzyści finansowych z ich rozpowszechniania i z zachowaniem praw autorskich. W szczególności dodatkowe egzemplarze mogą być sprzedawane przez osoby trzecie jedynie po cenie uzyskania kopii (druku, wydruku, kserografowania itp.)

Data utworzenia dokumentu: 7 października 2009

Strona WWW zajęć: <http://www.ii.uni.wroc.pl/~wch/Dydaktyka/Logika/>

Szanowni Państwo,

Program wykładu logiki dla informatyków nie jest trudny — w następnych semestrach będziecie Państwo słuchali dużo trudniejszych wykładów. Mimo to co roku znaczna część studentów nie zdaje egzaminu z logiki.

Jednym z powodów niepowodzenia na egzaminie jest to, że jest to dla Was pierwszy w życiu wykład akademicki, w którym pojawia się duża liczba nowych pojęć. Pojęcia te, na ogół dosyć abstrakcyjne, pojawiają się licznie na każdych zajęciach. Trzeba się ich wszystkich nauczyć. Nauczyć — to mało, gdyż matematyka nie polega na wykonywaniu mniej lub bardziej skomplikowanych rachunków, lecz na przeprowadzaniu rozumowań. Dlatego jest bardzo ważne, byście nie tylko je znali, ale i dobrze rozumieli. Wykład ma Wam w tym pomóc, ale wielu z Was nie zdoła na samym wykładzie opanować całego materiału. Na wykładzie nie nauczycie się też sprawnie posługiwać wprowadzonymi pojęciami. Dlatego musicie systematycznie pracować w domu. Jeśli przed zajęciami przypomnicie sobie wcześniej wprowadzone definicje, zwiększycie swoje szanse na zrozumienie nowego materiału. Jeśli natomiast nie będziecie znać wcześniej wprowadzonych pojęć, będziecie z dużym prawdopodobieństwem siedzieć na wykładzie, jak na tureckim kazaniu. Jeżeli przyswojenie nowych pojęć sprawia Wam trudność, radzę także przed wykładem przejrzeć podane w przygotowanych przez nas notatkach definicje, które dopiero zostaną na zajęciach wprowadzone. Być może czytając je po raz pierwszy przed wykładem nie potraficie ich w pełni zrozumieć, ale gdy je wcześniej przeczytacie, wyniesiecie z wykładu znacznie więcej. Poza tym będziecie przed zajęciami wiedzieć, czego nie rozumiecie i o co na wykładzie zapytać.

Od wielu lat wszystkim studentom zaczynającym studia powtarzamy to, co napisaliśmy w poprzednim paragrafie. Niestety z marnym skutkiem. Co roku w drugiej połowie semestru okazuje się, że znaczna część studentów nie rozumie wykładu, bo nie pamięta wcześniej wprowadzonych definicji i nie zna treści udowodnionych wcześniej twierdzeń. Co roku mniej niż połowa studentów zdaje egzamin z logiki. Bardzo nas to martwi. Chcielibyśmy, aby znaczna większość z Was mogła ukończyć studia. Dlatego aby Was zdyscyplinować i zmusić do systematycznej pracy wprowadzamy opisane w regulaminie zajęć rygory (punktowy system zaliczania ćwiczeń, kartkówki, egzamin połówkowy itd.). Ich celem nie jest uprzykrzenie Wam życia, ale zwiększenie szansy na to, że zdacie egzamin.

Wykładowcy

Spis treści

A. Informacje ogólne	ix
A.1. Program wykładu	ix
A.2. Zapisy na zajęcia	ix
A.3. Obsada zajęć i konsultacje	x
B. Literatura	xi
C. Zasady prowadzenia i zaliczania ćwiczeń	xiii
C.1. Wstęp	xiii
C.2. Szczegółowe zasady prowadzenia zajęć	xiv
D. Egzaminy	xvii
D.1. Egzamin zasadniczy	xviii
D.1.1. Egzamin połówkowy	xix
D.1.2. Egzamin końcowy	xix
D.2. Egzamin poprawkowy	xix
0. Zadania na dobry początek	1
1. Rachunek zdań i rachunek kwantyfikatorów	5
1.1. Składnia rachunku zdań	5
1.2. Wartości logiczne i znaczenie formuł zdaniowych	5
1.2.1. Metoda zero-jedynkowa	7
1.2.2. Skrócona metoda zero-jedynkowa	7
1.2.3. Równoważność formuł	11
1.2.4. Lemat o podstawianiu	14
1.3. Formalizacja rozumowań w języku rachunku zdań	15
1.4. Własności formuł zdaniowych	16
1.5. Postaci normalne formuł zdaniowych	20
1.5.1. Usuwanie symbolu negacji	20

1.5.2.	Dysjunkcyjna postać normalna	21
1.5.3.	Koniunkcyjna postać normalna	22
1.6.	Funkcje boolowskie i zupełne zbiory spójników	24
1.7.	Składnia rachunku kwantyfikatorów	26
1.8.	Znaczenie formuł rachunku kwantyfikatorów	27
1.9.	Formalizacja wypowiedzi w języku rachunku kwantyfikatorów	30
2.	Zbiory	33
2.1.	Działania na zbiorach	34
2.2.	Operacje nieskończone na zbiorach	38
3.	Relacje	43
3.1.	Para uporządkowana i iloczyn (produkt) kartezjański	43
3.2.	Relacje	44
3.3.	Krotki (n -tki) uporządkowane i relacje n -argumentowe	46
3.4.	Złożenie relacji. Relacja odwrotna	46
4.	Funkcje	49
4.1.	Funkcje odwrotne i złożenie funkcji	50
4.2.	Obraz i przeciwobraz zbioru	50
5.	Relacje równoważności	53
6.	Teoria mocy	59
6.1.	Równoliczność zbiorów	59
6.2.	Własności pojęcia równoliczności zbiorów	61
6.3.	Zbiory skończone	62
6.3.1.	Wzór włączeń i wyłączeń	64
6.4.	Moce zbiorów nieskończonych	65
6.5.	Wyznaczanie mocy zbiorów	68
6.6.	Zbiory przeliczalne	70
7.	Relacje porządku	75
7.1.	Przykłady porządków	76
7.2.	Elementy wyróżnione	78
7.3.	Izomorfizm porządkowy	79
7.4.	Zawieranie zbiorów jako relacja porządku	82
7.5.	Liczba relacji porządku	82
8.	Języki formalne	85

9. Kresy zbiorów	87
9.1. Kraty	89
9.2. Porządki zupełne	89
9.3. Twierdzenia o punkcie stałym	92
9.4. Relacje w zbiorze formuł zdaniowych	93
10. Dobre porządki i indukcja	97
10.1. Porządki regularne	97
10.2. Indukcja	100
11. Elementy algebry uniwersalnej	107
11.1. Algebra termów	107
11.1.1. Inna definicja zbioru termów. Drzewa	108
11.1.2. Wartość termu	108
11.2. Homomorfizmy	109
11.3. Problem unifikacji	111
12. Elementy logiki formalnej	113
12.1. Rezolucja dla rachunku zdań	113
12.2. System Hilberta dla rachunku zdań ze spójnikami implikacji i fałszu	114
12.3. System naturalnej dedukcji	115
12.4. Składnia języka pierwszego rzędu	116
12.5. Semantyka języka pierwszego rzędu	117
12.6. Podstawienia	118
12.7. Rezolucja dla rachunku I rzędu	118
13. Zadania egzaminacyjne z rozwiązaniami	121



Informacje ogólne

A.1. Program wykładu

Ponieważ przedmiot *Logika dla Informatyków* jest obowiązkowy, jego program jest ustalony w *Programie Studiów Informatycznych na Uniwersytecie Wrocławskim* z 17 czerwca 1997 z późniejszymi zmianami, dostępnym m. in. w sekretariacie Instytutu Informatyki, pok. 234 i — w wersji elektronicznej — na stronach internetowych Instytutu Informatyki:

<http://www.ii.uni.wroc.pl/>

A.2. Zapisy na zajęcia

Na zajęcia należy się zapisać w internetowym systemie *Zapisy*, dostępnym pod adresem zapisy.ii.uni.wroc.pl. Zadeklarowanie przedmiotu w systemie *Zapisy* jest formą umowy pomiędzy studentem i uczelnią. Student zobowiązuje się uczęszczać na zajęcia, uczelnia zaś zobowiązuje się je prowadzić i ocenić studenta po ich zakończeniu. Dlatego do egzaminu będą mogły przystąpić jedynie osoby zapisane na wykład, a zaliczenie ćwiczeń będą mogły uzyskać jedynie osoby zapisane na ćwiczenia.

Chociaż w systemie *Zapisy* prowadzący są dla porządku przypisani do poszczególnych grup ćwiczeniowych, jednak w kolejnych tygodniach mają zajęcia z różnymi grupami. Dlatego przy wyborze grupy nie należy się kierować nazwiskiem prowadzącego, gdyż każdy student będzie miał przeciętnie trzy ćwiczenia z każdym z prowadzących.

Jedna z grup ćwiczeniowych jest oznaczona jako *grupa zaawansowana*. Do tej grupy powinni się zapisać studenci o większych zdolnościach i aspiracjach matematycznych. Rozwiązuje się w niej nieco trudniejsze (ale i ciekawsze) zadania i wymaga od studentów nieco większej samodzielności. Przytoczone na następnych stronach *Zasady prowadzenia i zaliczania ćwiczeń* dotyczą jedynie grup podstawowych. Sposób zaliczania ćwiczeń w grupie zaawansowanej jest ogłaszany przez prowadzącego

te ćwiczenia i nie jest opisany w niniejszych notatkach. Rotacja prowadzących nie obejmuje grupy zaawansowanej.

A.3. Obsada zajęć i konsultacje

Obsada zajęć dydaktycznych w danym roku akademickim jest dostępna w Systemie Zapisy.

Każdy student ma niepodważalne prawo do bezpośredniej rozmowy z prowadzącymi na temat zajęć, w których uczestniczy. Uważamy, że z takich spotkań, tj. *konsultacji*, studenci korzystają nawet zbyt mało. Serdecznie zapraszając na konsultacje mamy jednak prośbę, by przestrzegać ustalonych przez prowadzących zasad. Każdy pracownik dydaktyczny wyznacza dwie godziny w tygodniu, w czasie których jest do dyspozycji studentów. Poszczególne prowadzący ustalają także inne sposoby konsultacji. Pracownicy spędzają w Instytucie znacznie więcej czasu, niż podane dwie godziny, ale poza dydaktyką wykonują też wiele innych prac. Dlatego prosimy traktować ze zrozumieniem ogłoszenia typu „proszę studentów o nieprzychodzenie poza godzinami konsultacji”. Prośba o respektowanie podanych terminów dotyczy szczególnie spraw technicznych, takich jak reklamacje dotyczące rankingu, czy wpisy ocen do indeksów. Studentów zapisanych na przedmiot jest ponad stu, a prowadzący — jeden. Nie chcemy, żeby studenci odnieśli wrażenie, że prowadzący starają się od nich izolować. Chodzi tylko o to, by nasze kontakty z dużą liczbą studentów przebiegały sprawnie i nie dezorganizowały naszej pracy w Instytucie.

Godziny konsultacji można znaleźć m. in. na stronach domowych prowadzących.

Poza prowadzącymi wykład, repetytorium i ćwiczenia, zajęcia obsługuje także *sekretaarz dydaktyczny*. Do jego zadań należy m. in. przygotowywanie rankingów ćwiczeń i wyliczanie ocen końcowych. Wszelkie problemy techniczne dotyczące punktacji za zadania, zadania domowe i kartkówki proszę wyjaśniać nie z prowadzącymi ćwiczenia, lecz bezpośrednio u sekretarza dydaktycznego w podanych przez niego terminach.

B

Literatura

Podstawowym podręcznikiem do wykładu jest skrypt:

1. Jerzy Tiuryn, *Wstęp do teorii mnogości i logiki*, który można wypożyczyć w bibliotece Instytutu (10 egzemplarzy, sygnatury: S.3315, S.3316, S.3317, S.3318, S.3319, S.3320, S.3321, S.3322, S.3323, S.3324). Wersja elektroniczna jest dostępna pod adresem:

<http://www.mimuw.edu.pl/~tiuryn/>

Spośród licznych podręczników dostępnych w bibliotekach i księgarniach warto wymienić:

2. Wojciech Guzicki, Piotr Zakrzewski, *Wykłady ze wstępu do matematyki. Wprowadzenie do teorii mnogości oraz Wstęp do matematyki. Zbiór zadań*, PWN, Warszawa, 2005.
3. Kazimierz Kuratowski, *Wstęp do teorii mnogości i topologii*, PWN, Warszawa, 1982. Krótkie wprowadzenie do teorii mnogości. W bibliotece Instytutu jest 10 egzemplarzy, sygnatury: II 1310, II 1373, II 5874, II 4609, II 8355, S.3285, S.3382, S.3395, S.3410 oraz tłumaczenie angielskie: II 116.
4. Kazimierz Kuratowski, Andrzej Mostowski, *Teoria mnogości*, PWN, Warszawa, 1978. Obszerny wykład teorii mnogości. W bibliotece Instytutu są dwa egzemplarze, sygnatury: II 286, II 8358.
5. Wiktor Marek, Janusz Onyszkiewicz, *Elementy logiki i teorii mnogości w zadaniach*, PWN, Warszawa, 2000. Obszerny zbiór prostych, typowych zadań. W bibliotece Instytutu jest 12 egzemplarzy, sygnatury: II 2463, II 1180, II 6859, S.2752, II 8231, S.3156, S.3157, S.3158, S.3159, II 8334, S.3207, S.3208.
6. Helena Rasiowa, *Wstęp do matematyki współczesnej*, PWN, Warszawa, 1999. Klasyczny podręcznik podstaw logiki i teorii mnogości. W bibliotece Instytutu jest 14 egzemplarzy, sygnatury: S.2529, S.2687, I 7767, I 8144, S.3127, S.3128, S.3129, S.3164, S.3165, S.3166, S.3204, S.3205, S.3206, S.3242.

7. Kenneth A. Ross, Charles R. B. Wright, *Matematyka dyskretna*, PWN, Warszawa, 1986. Wbrew tytułowi książka zawiera sporo elementarnie wyłożonego materiału z logiki i teorii mnogości. W bibliotece Instytutu jest 16 egzemplarzy, sygnatury: S. 2936, S. 2937, S. 3301, S. 3302, S. 3303, S. 3304, S. 3305, S. 3338, S. 3339, II 7922, II 8535, II 8582, II 8890, II 8891, II 8954 i II 8955, oraz oryginał angielski (*Discrete Mathematics*, Prentice Hall, 1988): II 7074 i II 7133.
8. Jerzy Słupecki, Ludwik Borkowski, *Elementy logiki matematycznej i teorii mnogości*, PWN, Warszawa, 1963. W bibliotece Instytutu są trzy egzemplarze, sygnatury: S. 804, S. 3571 i S. 3572.

C

Zasady prowadzenia i zaliczania ćwiczeń

Poniższy regulamin dotyczy jedynie zajęć w grupach podstawowych i nie obejmuje grupy zaawansowanej.

C.1. Wstęp

Zasadniczym celem ćwiczeń z przedmiotu *Logika dla informatyków* jest ułatwienie studentom samodzielnej pracy nad opanowaniem materiału w czasie *całego semestru*. Ocena z ćwiczeń jest oceną jakości i intensywności pracy studenta w trakcie semestru, w odróżnieniu od egzaminu z przedmiotu *Logika dla informatyków*, który ocenia stan wiedzy studenta w chwili zakończenia semestru.

Wykładowca ogłasza z odpowiednim wyprzedzeniem numery zadań z niniejszego zbioru. Studenci rozwiązują podane zadania *samodzielnie w domu*. Jeżeli student ma wątpliwości i chciałby je skonsultować z prowadzącym, powinien to uczynić w czasie godzin konsultacji prowadzącego. Zakłada się przy tym, że studenci będą dążyć do pewnej samodzielności w pracy nad opanowaniem przedmiotu. Zachęca się także studentów do wspólnej nauki.

Podstawą do wystawienia oceny jest liczba zadań, które student rozwiązał w trakcie całego semestru i, pomijając wyjątkowe przypadki, ocena zależy w sposób liniowy od tej liczby. Prowadzący spotyka się ze studentami regularnie na ćwiczeniach, aby ustalić faktyczną liczbę zadań rozwiązanych przez każdego studenta. Dlatego pomimo iż na zajęciach powinna panować swobodna atmosfera, nie należy zapominać, że każde ćwiczenie są w istocie *sprawdzianem* wiedzy studentów. Prezentowanie rozwiązań na tablicy całej grupie studentów ma także walor dydaktyczny, pozwala bowiem osobom które nie poradziły sobie z zadaniem na poznanie jego wzorcowego rozwiązania (z określonych niżej zasad szczegółowych wynika, że rozwiązanie prezentują jedynie studenci dobrze przygotowani). Ocena studenta jest bezwzględna, tj. niezależna od osiągnięć innych uczestników zajęć.

Numery zadań obowiązujących na następny tydzień są ogłaszane w *Terminarzu zajęć* na dany rok. Podczas całego semestru jest prowadzony ranking ćwiczeń zawierający zestawienie aktualnie zdobytej liczby punktów przez każdego studenta i prognozę oceny końcowej. Po zakończeniu semestru ranking zawiera ostateczne wyniki ćwiczeń. We wszelkich sprawach dotyczących liczby zdobytych punktów i zadań domowych studenci winni zgłaszać się do sekretarza dydaktycznego w czasie jego godzin konsultacji.

Na każde z około 13 zajęć zadaje się przeciętnie 8 zadań. W semestrze zadaje się więc do rozwiązania około stu zadań. Niniejsze notatki zawierają 550 zadań, a więc spory nadmiar. Zachęca się studentów do rozwiązywania także pozostałych zadań.

Data ogłoszenia ocen z ćwiczeń jest podana w *Terminarzu zajęć*. Tego samego dnia w podanych godzinach studenci winni przyjść do sekretarza dydaktycznego celem uzyskania wpisów do indeksów. W tym terminie będzie też można wyjaśniać wszelkie problemy dotyczące liczby zdobytych punktów z ćwiczeń. Wpisy zaliczeń do indeksów w innych terminach nie będą dokonywane.

Pierwsze ćwiczenia w semestrze nie są punktowane. Na zajęciach są rozwiązywane zadania z rozdziału 0 niniejszych notatek.

C.2. Szczegółowe zasady prowadzenia zajęć

1. Co najmniej na trzy dni (zwykle na tydzień) przed zajęciami na stronie WWW wykładu jest ogłaszana lista numerów zadań z niniejszego zbioru. Na ćwiczeniach są rozwiązywane wybrane zadania z tej listy. Prowadzącemu pozostawia się decyzję odnośnie wyboru zadań do rozwiązania.
2. Przed rozpoczęciem zajęć student wypełnia kupon wpisując numery zadań z listy, które potrafi rozwiązać.¹ Kartka powinna być wypełniona czytelnie, zawierać datę, jednoznacznie wpisane numery zadań², sumę punktów oraz imię i nazwisko studenta. Bezpośrednio po wejściu do sali ćwiczeniowej prowadzący zajęcia zbiera kupony. *Gdy prowadzący przychodzi do sali ćwiczeniowej, kupony powinny być już wypełnione przez studentów tak, by mogły być natychmiast zebrane i by prowadzący nie musiał opóźniać rozpoczęcia zajęć oczekując na wypełnienie kuponów.*
3. Po rozpoczęciu zajęć dokonywanie jakichkolwiek zmian w treści złożonych deklaracji³ jest niemożliwe.
4. Na każdych zajęciach student zdobywa liczbę punktów równą sumie wartości zadań, które zgłosił do rozwiązania z listy przewidzianej na dane zajęcia, z wyjątkiem przypadków opisanych w punktach 9–11.

¹ Gotowe kupony można wyciąć z ostatnich stron niniejszej książeczki.

² Niedopuszczalne są sformułowania typu „pierwsza część zadania 7” itp. Zadanie jest niepodzielną całością a deklaracja studenta powinna być jednoznaczna: tak lub nie.

³ Np. prosby o wycofanie lub dopisanie jakiegoś zadania.

5. Student nieobecny na zajęciach nie otrzymuje punktów. Poza przypadkami długotrwałej (trwającej co najmniej trzy tygodnie) choroby poświadczonej zwolnieniem lekarskim nie można odzyskać utraconych w ten sposób punktów.
6. Rozwiązanie danego zadania na tablicy przedstawia jedna z osób, wybrana przez prowadzącego, która zgłosiła gotowość rozwiązania tego zadania.⁴ Prowadzący ma prawo przerwać osobie referującej w dowolnym momencie i poprosić inne osoby, które zgłosiły gotowość rozwiązania danego zadania, o kontynuowanie.⁵
7. W ciągu semestru student ma obowiązek dostarczyć rozwiązania dwóch zadań domowych. Na każdych zajęciach prowadzący wybierają po około trzy osoby w każdej grupie ćwiczeniowej. Te osoby mają obowiązek przynieść na następne ćwiczenia pracę pisemną, napisaną ręcznie i czytelnie na arkuszu papieru formatu A4. Zadania domowe mają rozwinać u studentów zdolność jasnego, precyzyjnego i czytelnego redagowania rozwiązań zadań. Za pracę można otrzymać od 0 do 3 punktów. Oceniona praca jest zwracana autorom w kolejnym tygodniu. Zadania sprawdza sekretarz dydaktyczny.
8. Student powinien znać definicje wprowadzanych na wykładzie pojęć i sformułowania podstawowych twierdzeń. Oczekujemy, że przed każdym wykładem i każdymi ćwiczeniami studenci będą przypominać sobie wcześniej poznany materiał. Aby ułatwić studentom systematyczne powtarzanie wcześniej poznanego materiału, ćwiczenia mogą rozpoczynać się od bardzo prostej kartkówki sprawdzającej znajomość pojęć wprowadzanych na wykładzie oraz podstawowych faktów (według niniejszych notatek do wykładu). Za znajomość definicji i podstawowych twierdzeń — czyli za poprawną odpowiedź na wszystkie pytania zadane w kartkówce — student otrzymuje 10 punktów. W semestrze odbędzie się około czterech kartkówek.
9. Jeżeli podczas przedstawiania rozwiązania na tablicy okaże się, że student popełnił błąd (np. przeoczył trudność lub źle zrozumiał treść zadania) i nie jest w stanie rozwiązać poprawnie tego zadania, nie otrzymuje punktów za to zadanie i dodatkowo traci dwa razy tyle punktów, ile można było zdobyć za jego poprawne rozwiązanie.
10. Student, który bez zbędnych dygresji przedstawia na tablicy eleganckie i zrozumiałe dla słuchaczy rozwiązanie zadania, otrzymuje za to zadanie dodatkowo jeden punkt.

⁴Niniejsze regulacje nie ustalają sposobu wyboru tej osoby. Może on być dokonany losowo. Prowadzący może też np. częściej wybierać osoby, które w przeszłości nie poradziły sobie, mimo zadeklarowanej chęci, z rozwiązaniem zadania na tablicy. Może również przedstawić rozwiązanie tego zadania samodzielnie albo pozostawić to rozwiązanie ochotnikom.

⁵Niniejsze regulacje nie precyzują postępowania w sytuacji, gdy następna osoba stwierdzi, że jej sposób rozumowania jest zupełnie inny. Może wówczas rozpocząć referowanie rozwiązania od początku. Decyzja należy do prowadzącego.

punkty	ocena
$-\infty \div 70$	ndst
$71 \div 83$	dst
$84 \div 101$	dst+
$102 \div 110$	db
$111 \div 124$	db+
$125 \div +\infty$	bdb

Tablica C.1. Sposób przeliczania liczby punktów na ocenę z ćwiczeń

11. Jeżeli okaże się, że student oświadczył nieprawdę i nie umie w ogóle rozwiązać zadania lub nawet nie rozumie jego treści, traci wszystkie punkty zdobyte danego dnia oraz dodatkowo 10 punktów.⁶
12. Liczba punktów uzyskana przez studenta w ciągu całego semestru jest sumą liczby punktów zadeklarowanych na ćwiczeniach (wraz z otrzymanymi punktami karnymi i punktami za przedstawianie rozwiązań przy tablicy), punktów za zadania domowe i punktów z kartkówek. Ocena końcowa z zajęć jest wystawiana na podstawie tej liczby, według tablicy C.1. W ciągu semestru do rozwiązania zostaną przedstawione zadania o łącznej liczbie punktów nie mniejszej niż 104. Oznacza to, że łącznie z punktami za zadania domowe (6) i za kartkówki (40) można uzyskać co najmniej 150 punktów oraz kilka do kilkunastu punktów za rozwiązywanie zadań przy tablicy.
13. Ocena końcowa nie podlega poprawianiu po zakończeniu semestru. Nie ma kolokwiiw poprawkowych.⁷
14. Studenci po zapisaniu się do grup ćwiczeniowych nie mogą ich zmieniać, mimo iż wszystkie zajęcia odbywają się w tym samym czasie.
15. Podczas referowania zadań przy tablicy student nie może mieć przy sobie notatek.

⁶Z punktu widzenia interesów studenta okazuje się krytyczne rozróżnienie między tym punktem i poprzednim. Niestety, mimo jasnego sformułowania, chodzi tu o kwestię merytoryczną co do której podanie ścisłego algorytmu postępowania jest niemożliwe. Rozróżnienie to pozostaje do decyzji prowadzącego.

⁷Student powinien mieć świadomość, że zajęć można nie zaliczyć. W szczególności utrata punktów zgodnie z paragrafem 11 może jednoznacznie i nieodwołalnie skazać studenta na niezaliczenie zajęć i konieczność powtarzania przedmiotu w następnym roku lub skreślenie z listy studentów.

D

Egzaminy

Oceną, jaką student otrzymuje z przedmiotu, jest wynik egzaminu zasadniczego. W razie otrzymania oceny niedostatecznej student ma prawo przystąpić do egzaminu poprawkowego. Egzamin zasadniczy składa się z trzech części: egzaminu połówkowego pisanego w połowie semestru oraz dwóch części egzaminu końcowego, zwanych umownie częścią licencjacką i maderską, pisanych w zimowej sesji egzaminacyjnej. Egzamin poprawkowy składa się z dwóch części tak jak egzamin końcowy.

W razie przyłapania na ściąganiu podczas którejkolwiek części egzaminu student otrzymuje ocenę niedostateczną. Ocena ta jest ostateczna i nie podlega poprawianiu, a sprawa tego studenta jest kierowana do Dziekana.

Na egzamin należy przynieść przybory do pisania (pióro, długopis) i dowolny dokument ze zdjęciem w celu potwierdzenia tożsamości (dowód osobisty, paszport, legitymacja studencka, indeks itp). W trakcie egzaminu indeksy nie będą zbierane. Używanie notatek i własnego papieru jest niedozwolone. Wnoszenie toreb, wierzchnich okryć i wszelkich innych ruchomości na salę egzaminacyjną jest niedopuszczalne. Studenci powinni pozostawić je np. w szafkach w szatni. Strój odświętny na egzaminie nie jest wymagany.

Zarówno za egzamin zasadniczy (trzyczęściowy), jak i poprawkowy (dwuczęściowy) można otrzymać od -100 do 100 punktów. Jeżeli punktacja za zadanie egzaminacyjne wynosi n , znaczy to, że za rozwiązanie tego zadania można otrzymać od $-n$ do n punktów. Punkty ujemne będą przyznawane za rozpoczęcie rozwiązywania zadania¹ oraz za umieszczenie w rozwiązaniu odpowiedzi kompromitująco fałszywych. Za brak rozwiązania zadania otrzymuje się 0 punktów. Liczba punktów możliwych do zdobycia na egzaminie może zostać zwiększona poprzez dodanie zadań bonusowych.

Do wyników egzaminu zasadniczego i poprawkowego dolicza się punkty bonusowe za zaliczenie ćwiczeń. Liczba punktów bonusowych jest częścią całkowitą ilorazu: $(C - 70)/10$, gdzie C oznacza całkowitą liczbę punktów uzyskanych na zalicze-

¹Ma to na celu eliminowanie odpowiedzi, w których nie ma w ogóle poprawnych rozumowań. Student oddając rozwiązanie zadania powinien być przekonany, że jest ono na tyle poprawne, że pozwoli mu przekroczyć próg 0 punktów.

punkty	ocena
$40 \div 54$	dst+
$55 \div 69$	db
$70 \div 84$	db+
$85 \div +\infty$	bdb

Tablica D.2. Sposób przeliczania liczby punktów na ocenę z egzaminu

nie ćwiczeń w semestrze bezpośrednio poprzedzającym egzamin. *Osobom, które zaliczyły ćwiczenia w poprzednich latach punktów bonusowych się nie dolicza. Studentom odbywającym ćwiczenia w grupie zaawansowanej punktów bonusowych się nie dolicza.* Punkty z egzaminu zasadniczego i poprawkowego przeliczają się na oceny zgodnie z tablicą D.2.

Terminy egzaminów, miejsca ich przeprowadzenia, przydział studentów do sal, terminy ogłoszenia wyników oraz miejsca i terminy konsultacji poegzaminacyjnych są podane w *Terminarzu zajęć*. Wszelkie wątpliwości dotyczące sposobu oceniania egzaminu i otrzymanych ocen studenci powinni wyjaśniać w trakcie konsultacji poegzaminacyjnych. W czasie konsultacji po egzaminie końcowym i poprawkowym studenci winni zgłosić się z indeksami i kartami zaliczeń celem otrzymania wpisu oceny do indeksu. Wpisy do indeksów i konsultacje dotyczące wyników egzaminów w innych terminach nie będą dokonywane.

Treść zadań egzaminacyjnych oraz wyniki egzaminów są ogłaszane w *Terminarzu zajęć* po zakończeniu egzaminu.

D.1. Egzamin zasadniczy

Ocena z egzaminu zasadniczego jest wystawiana na podstawie sumy punktów z dwóch egzaminów — połówkowego i końcowego — i punktów bonusowych. Egzamin połówkowy odbywa się w połowie semestru, egzamin końcowy zaś w sesji zimowej. Na egzaminie połówkowym można zdobyć do 40 punktów, na egzaminie zasadniczym zaś 60 punktów. Zakres materiału na egzaminie połówkowym obejmuje zajęcia poprzedzające egzamin. Zakres materiału na egzaminie końcowym obejmuje cały semestr.

Egzamin składa się z dwóch części zwanych dawniej częścią licencjacką i magisterską. Obie części odbywają się tego samego dnia i mogą być od siebie oddzielone krótką przerwą. Pierwsza część sprawdza podstawowe opanowanie materiału, natomiast druga sprawdza umiejętność twórczego posługiwania się nabytą wiedzą.

W razie nieobecności na egzaminie połówkowym lub końcowym spowodowanej chorobą student ma obowiązek dostarczyć egzaminatorowi (osobiście, pocztą lub przez osoby trzecie) zwolnienie lekarskie w ciągu trzech dni licząc od dnia egzaminu.

Nieusprawiedliwiona w ten sposób nieobecność studenta na którejkolwiek części egzaminu zasadniczego jest równoznaczna z uzyskaniem zerowej liczby punktów z tego egzaminu. W szczególnych przypadkach decyzję o usprawiedliwieniu nieobecności na egzaminie może podjąć Dziekan.

D.1.1. Egzamin połówkowy

Wszyscy studenci zapisani na przedmiot *Logika dla Informatyków* mają obowiązek stawić się na ten egzamin.

W razie usprawiedliwionej nieobecności na egzaminie połówkowym całkowitą liczbę punktów z egzaminu zasadniczego oblicza się na podstawie wyników egzaminu końcowego, mnożąc liczbę zdobytych na nim punktów przez 10/6.

D.1.2. Egzamin końcowy

Do egzaminu końcowego mogą przystąpić jedynie osoby, które uzyskały zaliczenie ćwiczeń. Wszyscy studenci zapisani na przedmiot *Logika dla Informatyków*, którzy uzyskali zaliczenie ćwiczeń, mają obowiązek stawić się na ten egzamin.

W razie usprawiedliwionej nieobecności na egzaminie końcowym egzaminator ustali dla danej osoby inny termin egzaminu w sesji zimowej (zwykle jest to pierwszy dzień roboczy po ustaniu przyczyny nieobecności).

Na pierwszej części egzaminu (licencjackiej) można zdobyć łącznie na egzaminie połówkowym i końcowym do 20 punktów. Osoby, które zdobędą co najmniej 10 punktów, będą mogły otrzymać (bez względu na wynik drugiej części) ocenę dostateczną z egzaminu końcowego. Ponadto osoby te będą mogły na pełnych prawach wziąć udział w drugiej części. Studenci, którzy w pierwszej części uzyskają mniej niż 10 punktów, otrzymają ocenę niedostateczną a ich prace z drugiej części egzaminu końcowego nie będą sprawdzane.

D.2. Egzamin poprawkowy

W razie otrzymania oceny niedostatecznej z egzaminu zasadniczego student przystępuje do egzaminu poprawkowego w sesji poprawkowej. Ocena z egzaminu poprawkowego nie podlega poprawianiu.

Notacja matematyczna

Matematycy używają liter pochodzących z różnych krojów pisma i różnych alfabetów. Poniżej są zebrane alfabety użyte w niniejszych notatkach.

Pismo łacińskie, gotyckie, blokowe i kaligraficzne

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z
ⱥ ⱦ Ⱨ ⱨ Ⱪ ⱪ Ⱬ ⱬ Ɑ Ɱ Ɐ Ɒ ⱱ Ⱳ ⱳ ⱴ Ⱶ ⱶ ⱷ ⱸ ⱹ ⱺ ⱻ
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Alfabet grecki

Niektóre małe litery greckie mają dwa warianty pisowni. Przeważnie używa się pierwszego z podanych.

<i>A</i>	<i>α</i>	alfa	<i>I</i>	<i>ι</i>	jota	<i>P</i>	<i>ρ, ϱ</i>	ro
<i>B</i>	<i>β</i>	beta	<i>K</i>	<i>κ</i>	kappa	<i>Σ</i>	<i>σ, ς</i>	sigma
<i>Γ</i>	<i>γ</i>	gamma	<i>Λ</i>	<i>λ</i>	lambda	<i>T</i>	<i>τ</i>	tau
<i>Δ</i>	<i>δ</i>	delta	<i>M</i>	<i>μ</i>	mi	<i>Υ</i>	<i>υ</i>	ypsilon
<i>E</i>	<i>ε, ⵈ</i>	epsilon	<i>N</i>	<i>ν</i>	ni	<i>Φ</i>	<i>φ, ϕ</i>	fi
<i>Z</i>	<i>ζ</i>	dzeta	<i>Ξ</i>	<i>ξ</i>	ksi	<i>X</i>	<i>χ</i>	chi
<i>H</i>	<i>η</i>	eta	<i>O</i>	<i>ο</i>	omikron	<i>Ψ</i>	<i>ψ</i>	psi
<i>Θ</i>	<i>θ, ϑ</i>	teta	<i>Π</i>	<i>π, ϖ</i>	pi	<i>Ω</i>	<i>ω</i>	omega

Alfabet hebrajski

Z alfabetu hebrajskiego używamy pierwszej litery א, która nazywa się *alef*.

0

Zadania na dobry początek

Zadania z bieżącego rozdziału są rozwiązywane na pierwszych ćwiczeniach w semestrze. Zadań tych nie deklaruje się i nie są one punktowane.

Przypomnijmy najpierw zasadę indukcji matematycznej.

Twierdzenie 1 (zasada indukcji). Niech X będzie takim podzbiorem zbioru liczb naturalnych $\mathbb{N}$, że

- $0 \in X$,
- dla wszystkich liczb naturalnych n spełniona jest implikacja

$$(\forall i \leq n \ i \in X) \Rightarrow n + 1 \in X.$$

Wtedy $X = \mathbb{N}$.

Zadanie 1. Być może w szkole usłyszałeś inną wersję zasady indukcji. Sformułuj tę zasadę.

Zadanie 2. Udowodnij indukcyjnie, że

1. $0 + 1 + \dots + n = \frac{n(n+1)}{2}$ dla wszystkich liczb naturalnych n ,
2. $1^3 + 2^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$, dla $n \geq 1$.

Zadanie 3. Liczby Fibonacciego $F_0, F_1, F_2, \dots$ definiuje się równaniami

- $F_0 = 1, F_1 = 1$,
- $F_n = F_{n-2} + F_{n-1}$ dla $n \geq 2$.

Udowodnij indukcyjnie, że dla każdego $n \in \mathbb{N}$ zachodzi $F_n \leq F_{n+1}$,

Zadanie 4. Oto przykłady trzech wnioskowań przez indukcję:

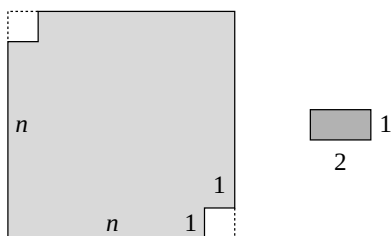
1. Pokaż, że wszystkie liczby naturalne są parzyste. Oczywiście 0 jest liczbą parzystą. Niech n będzie dowolną liczbą naturalną i założmy, że dla wszystkich $k < n$, k jest parzyste. Niech n_1 i n_2 będzie dowolnym rozbiem liczby n na sumę liczb mniejszych (tzn. $n = n_1 + n_2$). Ponieważ n_1 oraz n_2 są mniejsze od n , n_1 i n_2 są parzyste, a więc n jest parzyste jako suma dwóch liczb parzystych.
2. Pokaż, że wszystkie dodatnie liczby naturalne są nieparzyste. Oczywiście 1 jest liczbą nieparzystą. Niech n będzie dowolną liczbą naturalną i założmy, że dla wszystkich $k < n$, k jest nieparzyste. Niech $1, n_1$ i n_2 będzie dowolnym rozbiem liczby n na sumę trzech liczb mniejszych (tzn. $n = n_1 + n_2 + 1$). Ponieważ n_1 oraz n_2 są mniejsze od n , n_1 i n_2 są nieparzyste, a więc n jest nieparzyste jako suma dwóch liczb nieparzystych i liczby 1.
3. Pokaż, że wszystkie proste na płaszczyźnie są równoległe. Rozważmy jednoelementowy zbiór prostych na płaszczyźnie. Oczywiście wszystkie proste należące do tego zbioru są do siebie równoległe. Załóżmy, że w każdym n -elementowym zbiorze prostych wszystkie proste są do siebie równoległe. Rozważmy teraz $n + 1$ -elementowy zbiór prostych. Ustalmy w nim jedną prostą p . Na mocy założenia indukcyjnego wszystkie pozostałe n prostych jest do siebie równoległe. Ustalmy teraz inną prostą q . Na mocy założenia indukcyjnego wszystkie pozostałe n prostych jest również do siebie równoległe. Ponieważ relacja równoległości prostych jest przechodnia, wszystkie $n + 1$ prostych jest równoległe. Na mocy zasady indukcji matematycznej każdy zbiór prostych na płaszczyźnie zawiera wyłącznie proste równoległe. W szczególności dotyczy to zbioru wszystkich prostych na płaszczyźnie.

Które z tych rozumowań jest poprawne? Wskaż błędy popełnione w błędnych rozumowaniach.

Zadanie to zostało tu zamieszczone po to, by pokazać, że matematyka jest *nauką ścisłą*. Nie ma dowodów „prawie dobrych”. Nawet najdrobniejsza luka w rozumowaniu powoduje, że staje się ono bezwartościowe. Uprawiając matematykę musimy wypowiadać się bardzo jasno i precyzyjnie, i zwracać baczną uwagę, czy nasze rozumowania nie zawierają ukrytych błędów. Większość zadań w niniejszym zbiorze zawiera *prawdziwe* twierdzenia. Dlatego błędy w dowodach tych twierdzeń nie prowadzą do tak spektakularnych głupstw, jak w tym zadaniu. Nie oznacza to jednak, że możemy przedstawiać fałszywe dowody tych twierdzeń. Takie dowody są bowiem równie złe i bezużyteczne, jak fałszywe dowody fałszywych twierdzeń!

Celem kolejnych zadań jest zwrócenie uwagi na fakt, że matematyka jest sztuką przeprowadzania rozumowań a nie wykonywania rachunków. Wrażenie, że zadania te są mniej „matematyczne” niż np. ćwiczenia polegające na wyznaczeniu całki nieoznaczonej jest zupełnie błędne. Przeciwnie, sposób ich rozwiązywania ma więcej wspólnego z metodami pracy matematyków niż sposoby rozwiązywania zadań rachunkowych.

Zadanie 5. Rozważmy kwadrat o boku n , gdzie $n \geq 3$, z którego usunięto dwa naprzeciwległe narożniki o wymiarach 1×1 , jak na poniższym rysunku:



Dla jakich n można tak otrzymaną figurę pokryć prostokątami o wymiarach 1×2 ? (Prostokąty można obracać.)

Zadanie 6. Oto fragment raportu policji sporządzony przez młodego aspiranta:

Świadek nie był zastraszony lub też, jeśli Henry popełnił samobójstwo, to testament odnaleziono. Jeśli świadek był zastraszony, to Henry nie popełnił samobójstwa. Jeśli testament odnaleziono, to Henry popełnił samobójstwo. Jeśli Henry nie popełnił samobójstwa, to testament odnaleziono.

Co komendant policji może wywnioskować z powyższego raportu (poza oczywistym faktem, że należy zwolnić aspiranta)? Odpowiedz na pytania: *Czy świadek był zastraszony? Czy Henry popełnił samobójstwo? Czy testament odnaleziono?*

Rozumowania, które przeprowadzamy, są często tak subtelne i skomplikowane, że musimy używać sformalizowanego języka, by móc przedstawić nasze idee dostatecznie precyzyjnie. Symboliki matematycznej nie należy nadużywać, jednak sprawne posługiwanie się notacją matematyczną jest niezbędną umiejętnością. Trzy kolejne zadania dotyczą właśnie tego zagadnienia.

Zadanie 7. Następująca formuła mówi, że funkcja $f : \mathbb{R} \rightarrow \mathbb{R}$ jest ciągła.

$$\forall x_0 \in \mathbb{R} \forall \epsilon > 0 \exists \delta > 0 \forall x \in \mathbb{R} (|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon).$$

Nie używając znaku negacji zapisz formułę „funkcja f nie jest ciągła.”

Zadanie 8. Następująca formuła mówi, że liczba $g \in \mathbb{R}$ jest granicą (w sensie Cauchy’ego) funkcji $f : \mathbb{R} \rightarrow \mathbb{R}$ w punkcie x_0 .

$$\forall \epsilon > 0 \exists \delta > 0 \forall x \in \mathbb{R} (0 < |x - x_0| < \delta \Rightarrow |f(x) - g| < \epsilon).$$

Nie używając znaku negacji zapisz formułę „liczba g nie jest granicą funkcji f w punkcie x_0 .”

Zadanie 9. Następująca formuła mówi, że liczba $g \in \mathbb{R}$ jest *granicą* (w sensie Heinego) funkcji $f : \mathbb{R} \rightarrow \mathbb{R}$ w punkcie y .

$$\forall x \in \mathbb{R}^{\mathbb{N}} \left(\left(\lim_{n \rightarrow \infty} x_n = y \wedge \forall n \in \mathbb{N} \, x_n \neq y \right) \Rightarrow \lim_{n \rightarrow \infty} f(x_n) = g \right).$$

Nie używając znaku negacji zapisz formułę „liczba g nie jest granicą funkcji f w punkcie y .”

Rachunek zdań i rachunek kwantyfikatorów

1.1. Składnia rachunku zdań

Definicja 2. *Formuły rachunku zdań* budujemy ze *zmiennych zdaniowych* i *spójników logicznych* (*funktorów zdaniotwórczych*): fałszu $\perp$, prawdy $\top$, negacji $\neg$, koniunkcji $\wedge$, alternatywy $\vee$, implikacji $\Rightarrow$ i równoważności $\Leftrightarrow$ w następujący sposób:

1. Symbole $\perp$ i $\top$ są formułami rachunku zdań.
2. Każda zmienna zdaniowa jest formułą rachunku zdań.
3. Jeżeli ϕ , ϕ_1 i ϕ_2 są formułami rachunku zdań, to są nimi także: $(\neg\phi)$, $(\phi_1 \wedge \phi_2)$, $(\phi_1 \vee \phi_2)$, $(\phi_1 \Rightarrow \phi_2)$ i $(\phi_1 \Leftrightarrow \phi_2)$.
4. Wszystkie formuły rachunku zdań można zbudować przy pomocy reguł opisanych w punktach 1–3.

Zmienne zdaniowe będziemy oznaczać literami: p , q , r , s itd., często z indeksami: p_1 , p_2 itd. Formuły zdaniowe będziemy oznaczać literami: ϕ , ψ , ρ itd., często również z indeksami: ϕ_1 , ϕ_2 itd. Dla większej czytelności będziemy w formułach opuszczać nawiasy, zakładając następującą kolejność wiązania (od najsilniejszego do najsłabszego): $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ i przyjmując, że $\wedge$, $\vee$ i $\Leftrightarrow$ łączą w lewo, tj. np. $p \vee r \vee s$ znaczy $(p \vee r) \vee s$, zaś $\Rightarrow$ — w prawo, tj. np. $p \Rightarrow r \Rightarrow s$ znaczy $p \Rightarrow (r \Rightarrow s)$. Zatem np. $p \vee q \vee r \wedge s$ oznacza $(p \vee q) \vee (r \wedge s)$.

1.2. Wartości logiczne i znaczenie formuł zdaniowych

Definicja 3. Zbiór *wartości logicznych* $\mathcal{B} = \{\top, \text{F}\}$ zawiera dwa elementy: $\top$ (prawda) i F (fałsz).¹ Niech V oznacza zbiór zmiennych zdaniowych. *Wartościowanie*

¹Oznaczenia pochodzą od angielskich słów *true* i *false*.

$\frac{\perp}{F}$	$\frac{T}{T}$	$\frac{\phi}{F} \mid \frac{\neg\phi}{T}$ $\frac{\phi}{T} \mid \frac{\neg\phi}{F}$	$\frac{\phi}{F} \mid \frac{\psi}{F} \mid \frac{\phi \wedge \psi}{F}$ $\frac{\phi}{F} \mid \frac{\psi}{T} \mid \frac{\phi \wedge \psi}{F}$ $\frac{\phi}{T} \mid \frac{\psi}{F} \mid \frac{\phi \wedge \psi}{F}$ $\frac{\phi}{T} \mid \frac{\psi}{T} \mid \frac{\phi \wedge \psi}{T}$
$\frac{\phi}{F} \mid \frac{\psi}{F} \mid \frac{\phi \vee \psi}{F}$ $\frac{\phi}{F} \mid \frac{\psi}{T} \mid \frac{\phi \vee \psi}{T}$ $\frac{\phi}{T} \mid \frac{\psi}{F} \mid \frac{\phi \vee \psi}{T}$ $\frac{\phi}{T} \mid \frac{\psi}{T} \mid \frac{\phi \vee \psi}{T}$	$\frac{\phi}{F} \mid \frac{\psi}{F} \mid \frac{\phi \Rightarrow \psi}{T}$ $\frac{\phi}{F} \mid \frac{\psi}{T} \mid \frac{\phi \Rightarrow \psi}{T}$ $\frac{\phi}{T} \mid \frac{\psi}{F} \mid \frac{\phi \Rightarrow \psi}{F}$ $\frac{\phi}{T} \mid \frac{\psi}{T} \mid \frac{\phi \Rightarrow \psi}{T}$	$\frac{\phi}{F} \mid \frac{\psi}{F} \mid \frac{\phi \Leftrightarrow \psi}{T}$ $\frac{\phi}{F} \mid \frac{\psi}{T} \mid \frac{\phi \Leftrightarrow \psi}{F}$ $\frac{\phi}{T} \mid \frac{\psi}{F} \mid \frac{\phi \Leftrightarrow \psi}{F}$ $\frac{\phi}{T} \mid \frac{\psi}{T} \mid \frac{\phi \Leftrightarrow \psi}{T}$	

Rysunek 1. Znaczenie spójników logicznych

zmiennych, to odwzorowanie $\sigma : V \rightarrow \mathcal{B}$. Nadaje ono wartości logiczne zmiennym zdaniowym.

Wartość logiczna dowolnej formuły zdaniowej zależy jedynie od wartościowania występujących w niej zmiennych i można ją wyznaczyć korzystając z tabel z rysunku 1. Dlatego mówimy, że wartościowanie zmiennych nadaje wartość logiczną formułom. Formalnie, wartościowanie zmiennych σ wyznacza *wartościowanie formuł* $\hat{\sigma}$, które przypisuje wartości logiczne dowolnym formułom w następujący sposób:

$$\begin{aligned}
 \hat{\sigma}(\perp) &= F \\
 \hat{\sigma}(T) &= T \\
 \hat{\sigma}(p) &= \sigma(p) \\
 \hat{\sigma}(\neg\phi) &= \begin{cases} T, & \text{gdy } \hat{\sigma}(\phi) = F \\ F, & \text{gdy } \hat{\sigma}(\phi) = T \end{cases} \\
 \hat{\sigma}(\phi_1 \wedge \phi_2) &= \begin{cases} T, & \text{gdy } \hat{\sigma}(\phi_1) = T \text{ i } \hat{\sigma}(\phi_2) = T \\ F, & \text{w p.p.} \end{cases} \\
 \hat{\sigma}(\phi_1 \vee \phi_2) &= \begin{cases} T, & \text{gdy } \hat{\sigma}(\phi_1) = T \text{ lub } \hat{\sigma}(\phi_2) = T \\ F, & \text{w p.p.} \end{cases} \\
 \hat{\sigma}(\phi_1 \Rightarrow \phi_2) &= \begin{cases} F, & \text{gdy } \hat{\sigma}(\phi_1) = T \text{ i } \hat{\sigma}(\phi_2) = F \\ T, & \text{w p.p.} \end{cases} \\
 \hat{\sigma}(\phi_1 \Leftrightarrow \phi_2) &= \begin{cases} T, & \text{gdy } \hat{\sigma}(\phi_1) = \hat{\sigma}(\phi_2) \\ F, & \text{w p.p.} \end{cases}
 \end{aligned}$$

Wartość logiczną $\hat{\sigma}(\phi) \in \mathcal{B}$ nazywamy *wartością logiczną formuły ϕ przy wartościowaniu σ* . Ponieważ dla danego wartościowania zmiennych wartościowanie formuł

jest określone jednoznacznie, znak $\wedge$ będziemy opuszczać i zarówno wartościowanie zmiennych, jak i wartościowanie formuł będziemy oznaczać tym samym symbolem i nazywać po prostu *wartościowaniem*.

Definicja 4. Formuła jest:

- *spełniona* przy danym wartościowaniu zmiennych, jeżeli przy tym wartościowaniu ma ona wartość T;
- *spełnialna*, jeżeli istnieje wartościowanie zmiennych, dla którego ta formuła jest spełniona;
- *prawdziwa* (jest *tautologią*), jeśli jest spełniona dla każdego wartościowania zmiennych;
- *sprzeczna*, jeśli nie jest spełniona (ma wartość F) dla żadnego wartościowania zmiennych.

O formule spełnionej przy danym wartościowaniu zmiennych będziemy niekiedy mówić, że jest *prawdziwa* przy tym wartościowaniu. W analogicznej sytuacji, gdy formuła nie jest spełniona, będziemy ją nazywać *fałszywą* przy tym wartościowaniu.

Obecnie zajmiemy się sposobami sprawdzania, czy dana formuła jest tautologią.

1.2.1. Metoda zero-jedynkowa

Przykładami tautologii są formuły $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ oraz $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ zwane *prawami de Morgana*. Aby się o tym przekonać rysujemy tabelkę (rysunek 2) umieszczając w kolumnach 1 i 2 wartości zmiennych zdaniowych p i q . W kolumnie 3 umieszczamy wartości formuły $p \vee q$ wyliczone z użyciem tabelki dla alternatywy. W kolumnie 4 obliczamy, w oparciu o tabelkę negacji, wartości formuły $\neg(p \vee q)$. Kolumny 5 i 6 wyznaczamy również w oparciu o tabelkę negacji. Aby wyznaczyć wartości formuły $(\neg p) \wedge (\neg q)$ korzystamy z wartości zapisanych w kolumnach 5 i 6 i z tabelki koniunkcji. Ostatnią, ósmą kolumnę wyznaczamy przy użyciu tabelki dla równoważności z wartości logicznych zapisanych w kolumnach 4 i 7. Po skonstruowaniu tabelki zauważamy, że dla każdego z czterech możliwych wartościowań zmiennych p i q formuła $\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$ ma wartość logiczną T, jest więc tautologią.

1.2.2. Skrócona metoda zero-jedynkowa

Sprawdzenie czy formuła jest tautologią można znacznie przyspieszyć, jeśli zamiast bezmyślnie sprawdzać wartość formuły dla wszystkich możliwych wartościowań zmiennych, będziemy świadomie poszukiwać wartościowania, dla którego formuła nie jest spełniona. Ustalenie takiego wartościowania przekona nas, że formuła

$\phi = \neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$							
1	2	3	4	5	6	7	8
p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	ϕ
F	F	F	T	T	T	T	T
F	T	T	F	T	F	F	T
T	F	T	F	F	T	F	T
T	T	T	F	F	F	F	T

Rysunek 2. Tabelkowa metoda sprawdzenia, że formuła ϕ jest tautologią

$$\begin{array}{ccccccc} \phi = (\neg p \Rightarrow \neg q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow q) & & & & & & \\ | & & | & & | & | & | \\ \text{T} & & \text{F} & & \text{F} & \text{T} & \text{F} \\ & & & & | & & | \\ & & & & \text{T} & & \text{F} \end{array}$$

Rysunek 3. Wartościowanie, dla którego formuła ϕ nie jest spełniona

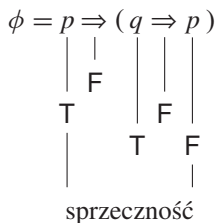
nie jest tautologią, dojście do sprzeczności zaś — że nią jest. Rozważmy dla ustalenia uwagi formułę $(\neg p \Rightarrow \neg q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow q)$. Formuła ta nie jest spełniona, jeśli poprzednik implikacji $\neg p \Rightarrow \neg q$ jest prawdziwy przy pewnym wartościowaniu, jej następnik $(\neg p \Rightarrow q) \Rightarrow q$ zaś fałszywy przy tym wartościowaniu. Formuła $(\neg p \Rightarrow q) \Rightarrow q$ jest fałszywa tylko wówczas, gdy $\neg p \Rightarrow q$ jest spełniona oraz $\sigma(q) = F$. Ale $\neg p \Rightarrow q$ jest spełniona dla $\sigma(q) = F$ tylko wówczas, gdy $\neg p$ nie jest spełniona, tj. gdy $\sigma(p) = T$. Zauważamy na koniec, że przy wartościowaniu $\sigma(p) = T$ i $\sigma(q) = F$ nasza wyjściowa formuła istotnie nie jest spełniona, nie jest więc tautologią (rysunek 3).

Rozważmy teraz formułę $\phi = p \Rightarrow (q \Rightarrow p)$. Aby ϕ nie była spełniona, musi być $\sigma(p) = \text{T}$ oraz powinna nie być spełniona formuła $q \Rightarrow p$. Formuła ostatnia nie jest spełniona tylko wówczas, gdy $\sigma(q) = \text{T}$ oraz $\sigma(p) = \text{F}$. Zatem aby ϕ nie była spełniona, musiałoby być jednocześnie $\sigma(p) = \text{T}$ i $\sigma(p) = \text{F}$, co jest niemożliwe. Formuła ϕ jest zatem tautologią (rysunek 4).

Przykład 5. Przykładami tautologii są

$$\begin{aligned} (p \Rightarrow (q \Rightarrow r)) &\Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r)) \\ (\neg p \Rightarrow \neg q) &\Rightarrow ((\neg p \Rightarrow q) \Rightarrow p) \end{aligned}$$

Zadanie 10. Udowodnij, że podane formuły są tautologiami.



Rysunek 4. Ilustracja dowodu nie wprost, iż formuła ϕ jest tautologią

1. (**modus ponens**) $(p \Rightarrow q) \wedge p \Rightarrow q$
2. (**modus tollens**) $(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$
3. (**prawo kompozycji**) $(p \vee q \Rightarrow r) \Rightarrow p \Rightarrow r$
4. (**prawo kompozycji**) $(p \vee q \Rightarrow r) \Rightarrow q \Rightarrow r$
5. (**prawo symplifikacji**) $p \wedge q \Rightarrow p$
6. (**prawo symplifikacji**) $q \Rightarrow p \vee q$
7. (**prawo symplifikacji**) $p \Rightarrow q \Rightarrow p$
8. (**prawo Dunsza Szkota**) $\neg p \Rightarrow p \Rightarrow q$
9. (**prawo dylematu konstrukcyjnego**) $(p \Rightarrow r) \wedge (q \Rightarrow r) \wedge (p \vee q) \Rightarrow r$
10. (**prawo eksportacji**) $(p \wedge q \Rightarrow r) \Rightarrow p \Rightarrow q \Rightarrow r$
11. (**prawo importacji**) $(p \Rightarrow q \Rightarrow r) \Rightarrow p \wedge q \Rightarrow r$
12. (**prawo redukcji do absurdu**) $(p \Rightarrow \neg p) \Rightarrow \neg p$
13. (**prawo sprzeczności**) $\neg(p \wedge \neg p)$
14. (**prawo wyłączonego środka**) $p \vee \neg p$
15. (**prawo sylogizmu hipotetycznego**) $(p \Rightarrow q) \Rightarrow (q \Rightarrow r) \Rightarrow p \Rightarrow r$
16. (**prawo Pierce’a**) $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$
17. (**Prawo Claviusa**) $(\neg p \Rightarrow p) \Rightarrow p$
18. (**prawo tożsamości**) $p \Leftrightarrow p$

Powyższe tautologie były od dawna badane przez logików, gdyż opisują typowe schematy przeprowadzania rozumowań. Ich zwyczajowe nazwy podano w nawiasach.

Zadanie 11. Sprawdź, które z podanych formuł są (a) tautologiami, (b) formułami spełnialnymi, (c) formułami sprzecznymi.

1. $p \vee q \vee r \Rightarrow \neg p \Rightarrow (q \vee r) \wedge \neg p$

2. $(p \Rightarrow q) \Leftrightarrow (p \wedge q \Leftrightarrow p)$
3. $(p \vee q \Rightarrow r) \Rightarrow (p \Rightarrow r) \vee (q \Rightarrow r)$
4. $(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow p \wedge s \Rightarrow q \vee r$
5. $p \vee q \vee r \Rightarrow ((p \vee q) \wedge \neg r) \vee (r \wedge p \wedge q)$
6. $((p \vee q) \wedge \neg r) \vee (r \wedge p \wedge q) \Rightarrow p \vee q \vee r$
7. $(p \vee q \Leftrightarrow r \vee s) \Rightarrow ((p \Leftrightarrow r) \vee (q \Leftrightarrow s))$
8. $(p \Leftrightarrow r) \vee (q \Leftrightarrow s) \Rightarrow (p \vee q \Leftrightarrow r \vee s)$
9. $(p \wedge q \Leftrightarrow r \wedge s) \Rightarrow ((p \Leftrightarrow r) \wedge (q \Leftrightarrow s))$
10. $(p \Rightarrow q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$
11. $(p \vee q) \wedge \neg p \Rightarrow q$
12. $(p \Rightarrow q) \Rightarrow p \wedge r \Rightarrow q$
13. $(p \Rightarrow q) \Rightarrow p \Rightarrow q \vee r$
14. $p \Rightarrow \neg p \vee q$
15. $(p \vee q) \wedge (p \Rightarrow q) \Rightarrow q \Rightarrow p$
16. $\neg(p \wedge (\neg p \wedge q))$
17. $p \Rightarrow \neg q \wedge q \Rightarrow r$
18. $(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow p \vee q$
19. $(p \vee q \Rightarrow p \vee \neg q) \Rightarrow \neg p \vee q$
20. $(p \wedge q) \vee (p \Rightarrow q) \Rightarrow p \Rightarrow q$
21. $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
22. $(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow p \vee r \Rightarrow q \vee s$
23. $(p \wedge q \Rightarrow r) \Rightarrow (p \Rightarrow r) \wedge (q \Rightarrow r)$
24. $(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow p \wedge r \Rightarrow q \wedge s$
25. $(p \wedge q \Rightarrow r) \wedge (p \vee q \Rightarrow \neg r) \Rightarrow p \wedge q \wedge r$
26. $\neg(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow p \wedge \neg q$
27. $((p \Rightarrow q) \Rightarrow q \Rightarrow r) \Rightarrow (r \Rightarrow p) \Rightarrow q \Rightarrow p$
28. $(p \Rightarrow q) \vee (p \Rightarrow r) \vee (p \Rightarrow s) \Rightarrow p \Rightarrow q \vee r \vee s$
29. $(p \Rightarrow q) \wedge (r \Rightarrow q) \wedge (s \Rightarrow q) \Rightarrow p \wedge r \wedge s \Rightarrow q$
30. $(p \Rightarrow q) \wedge (r \Rightarrow q) \wedge (s \Rightarrow q) \Rightarrow p \wedge r \wedge \neg s \Rightarrow q$
31. $(p \wedge q \Rightarrow r) \wedge (p \wedge q \Rightarrow \neg r) \Rightarrow \neg p \wedge \neg q \wedge \neg r$
32. $(\neg p \wedge q) \vee (p \vee \neg q) \Rightarrow (p \Rightarrow q \vee r) \Rightarrow p \Rightarrow r$

33. $(p \vee q) \wedge (r \vee s) \Rightarrow ((p \Rightarrow q) \vee (p \Rightarrow r)) \wedge ((q \Rightarrow s) \vee (q \Rightarrow p))$
34. $(p \Rightarrow q) \wedge (r \Rightarrow s) \wedge (t \Rightarrow u) \Rightarrow p \wedge r \wedge t \Rightarrow q \wedge s \wedge u$
35. $(p \Leftrightarrow q) \wedge p \Rightarrow q$
36. $(\neg p \Rightarrow \neg q) \Rightarrow (\neg p \Rightarrow q) \Rightarrow p$

Zadanie 12. Niech symbole ϕ i ψ oznaczają formuły zdaniowe. Udowodnij poniższe stwierdzenia lub podaj przykłady świadczące o ich fałszywości:

1. Jeśli $\phi \Rightarrow \psi$ jest tautologią i ϕ jest tautologią, to ψ jest tautologią.
2. Jeśli $\phi \Rightarrow \psi$ jest spełnialna i ϕ jest spełnialna, to ψ jest spełnialna.
3. Jeśli $\phi \Rightarrow \psi$ jest tautologią i ϕ jest spełnialna, to ψ jest spełnialna.
4. Jeśli $\phi \Rightarrow \psi$ jest spełnialna i ϕ jest tautologią, to ψ jest spełnialna.

Zadanie 13. Które z poniższych zdań są prawdziwe dla dowolnych formuł zdaniowych ϕ i ψ ?

1. Jeśli $\phi \Rightarrow \psi$ oraz $\neg\phi \Rightarrow \psi$ są tautologiami, to ψ jest tautologią.
2. Jeśli $\phi \Rightarrow \psi$ oraz $\neg\phi \Rightarrow \psi$ są spełnialne, to ψ jest spełnialna.
3. Jeśli $\phi \Rightarrow \psi$ jest tautologią oraz $\neg\phi \Rightarrow \psi$ jest spełnialna, to ψ jest spełnialna.
4. Jeśli $\phi \Rightarrow \psi$ jest tautologią oraz $\neg\phi \Rightarrow \psi$ jest spełnialna, to ϕ jest tautologią.

Podaj dowody ich prawdziwości. W pozostałych przypadkach wskaż kontrprzykłady.

1.2.3. Równoważność formuł

Definicja 6. Mówimy, że formuły ϕ i ψ są *równoważne*, jeśli dla każdego wartościowania przyjmują tę samą wartość logiczną (tj. gdy formuła $\phi \Leftrightarrow \psi$ jest tautologią).

Będziemy używać notacji $\phi \equiv \psi$ do oznaczenia, że formuły ϕ i ψ są równoważne.²

Przykład 7. Formuły $\neg(p \vee q)$ i $\neg p \wedge \neg q$ są równoważne.

Zadanie 14. Udowodnij, że a) dowolne dwie tautologie, b) dowolne dwie formuły sprzeczne są równoważne. Czy dowolne dwie formuły spełnialne są równoważne?

Zadanie 15. Udowodnij, że podane formuły są równoważne.

1. (**prawo transpozycji prostej**) $p \Rightarrow q$ oraz $\neg q \Rightarrow \neg p$

²Warto tu zauważyć, że $\phi \equiv \psi$ jest zdaniem *metajęzyka* (czyli języka, w którym mówimy o formułach) dotyczącym *dwoch* formuł, natomiast $\phi \Leftrightarrow \psi$ jest *jedną* formułą rachunku zdań.

2. (**prawo transpozycji złożonej**) $p \wedge q \Rightarrow r$ oraz $p \wedge \neg r \Rightarrow \neg q$
3. (**prawo pochłaniania**) p oraz $p \vee (p \wedge q)$
4. (**prawo pochłaniania**) p oraz $p \wedge (p \vee q)$
5. (**prawo podwójnego przeczenia**) $\neg\neg p$ oraz p
6. (**prawo negowania fałszu**) $\neg\perp$ oraz $\top$
7. (**prawo negowania prawdy**) $\neg\top$ oraz $\perp$
8. (**prawo de Morgana**) $\neg(p \wedge q)$ oraz $\neg p \vee \neg q$
9. (**prawo de Morgana**) $\neg(p \vee q)$ oraz $\neg p \wedge \neg q$
10. (**prawo negowania implikacji**) $\neg(p \Rightarrow q)$ oraz $p \wedge \neg q$
11. (**prawo negowania równoważności**) $\neg(p \Leftrightarrow q)$ oraz $\neg p \Leftrightarrow q$
12. (**prawo negowania równoważności**) $\neg(p \Leftrightarrow q)$ oraz $p \Leftrightarrow \neg q$
13. $p \Rightarrow q$ oraz $\neg p \vee q$
14. $p \Leftrightarrow q$ oraz $(p \Rightarrow q) \wedge (q \Rightarrow p)$
15. $p \Leftrightarrow q$ oraz $(p \wedge q) \vee (\neg p \wedge \neg q)$

Równoważność przedstawionych powyżej formuł jest od dawna znana logikom, wykorzystuje się ją bowiem przeprowadzając rozumowania. W nawiasach wymieniono zwyczajowe nazwy podanych praw.

Zadanie 16. Sprawdź, czy podane formuły są równoważne.

1. $p \vee q \Rightarrow r$ oraz $p \Rightarrow q \Rightarrow r$
2. $p \wedge q \Rightarrow r$ oraz $p \Rightarrow q \Rightarrow r$
3. $(p \Leftrightarrow q) \Rightarrow r$ oraz $p \Rightarrow q \Rightarrow r$

Zadanie 17. Sprawdź, czy podane formuły są równoważne.

1. $p \vee q$ oraz $q \vee p$
2. $p \wedge q$ oraz $q \wedge p$
3. $p \Rightarrow q$ oraz $q \Rightarrow p$
4. $p \Leftrightarrow q$ oraz $q \Leftrightarrow p$

Spójnik logiczny $\oplus$ jest *przemienny*, jeżeli formuły $p \oplus q$ i $q \oplus p$ są równoważne. W powyższym zadaniu sprawdza się więc, które spośród spójników logicznych są przemienne.

Zadanie 18. Sprawdź, czy podane formuły są równoważne.

1. $p \vee (q \vee r)$ oraz $(p \vee q) \vee r$
2. $p \wedge (q \wedge r)$ oraz $(p \wedge q) \wedge r$
3. $p \Rightarrow (q \Rightarrow r)$ oraz $(p \Rightarrow q) \Rightarrow r$
4. $p \Leftrightarrow (q \Leftrightarrow r)$ oraz $(p \Leftrightarrow q) \Leftrightarrow r$

Spójnik logiczny $\oplus$ jest *łączny*, jeżeli formuły $p \oplus (q \oplus r)$ i $(p \oplus q) \oplus r$ są równoważne. W powyższym zadaniu sprawdza się więc, które spośród spójników logicznych są łączne.

Zadanie 19. Sprawdź, czy podane formuły są równoważne.

1. $p \vee (q \vee r)$ oraz $q \vee (p \vee r)$
2. $p \wedge (q \wedge r)$ oraz $q \wedge (p \wedge r)$
3. $p \Rightarrow (q \Rightarrow r)$ oraz $q \Rightarrow (p \Rightarrow r)$
4. $p \Leftrightarrow (q \Leftrightarrow r)$ oraz $q \Leftrightarrow (p \Leftrightarrow r)$

Zadanie 20. Sprawdź, czy podane formuły są równoważne.

1. $p \wedge (q \vee r)$ oraz $(p \wedge q) \vee (p \wedge r)$
2. $p \wedge (q \wedge r)$ oraz $(p \wedge q) \wedge (p \wedge r)$
3. $p \wedge (q \Rightarrow r)$ oraz $(p \wedge q) \Rightarrow (p \wedge r)$
4. $p \wedge (q \Leftrightarrow r)$ oraz $(p \wedge q) \Leftrightarrow (p \wedge r)$
5. $p \vee (q \vee r)$ oraz $(p \vee q) \vee (p \vee r)$
6. $p \vee (q \wedge r)$ oraz $(p \vee q) \wedge (p \vee r)$
7. $p \vee (q \Rightarrow r)$ oraz $(p \vee q) \Rightarrow (p \vee r)$
8. $p \vee (q \Leftrightarrow r)$ oraz $(p \vee q) \Leftrightarrow (p \vee r)$
9. $p \Rightarrow (q \vee r)$ oraz $(p \Rightarrow q) \vee (p \Rightarrow r)$
10. $p \Rightarrow (q \wedge r)$ oraz $(p \Rightarrow q) \wedge (p \Rightarrow r)$
11. $p \Rightarrow (q \Rightarrow r)$ oraz $(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$
12. $p \Rightarrow (q \Leftrightarrow r)$ oraz $(p \Rightarrow q) \Leftrightarrow (p \Rightarrow r)$
13. $p \Leftrightarrow (q \vee r)$ oraz $(p \Leftrightarrow q) \vee (p \Leftrightarrow r)$
14. $p \Leftrightarrow (q \wedge r)$ oraz $(p \Leftrightarrow q) \wedge (p \Leftrightarrow r)$
15. $p \Leftrightarrow (q \Rightarrow r)$ oraz $(p \Leftrightarrow q) \Rightarrow (p \Leftrightarrow r)$
16. $p \Leftrightarrow (q \Leftrightarrow r)$ oraz $(p \Leftrightarrow q) \Leftrightarrow (p \Leftrightarrow r)$

Spójnik logiczny $\oplus$ jest *lewostronnie rozdzielny* względem spójnika $\otimes$, jeżeli formuły $p \oplus (q \otimes r)$ i $(p \oplus q) \otimes (p \oplus r)$ są równoważne. W powyższym zadaniu sprawdza się więc, które spośród spójników logicznych są rozdzielne względem których.

Zadanie 21. Spójnik logiczny $\oplus$ jest *prawostronnie rozdzielny* względem spójnika $\otimes$, jeżeli formuły $(p \otimes q) \oplus r$ i $(p \oplus r) \otimes (q \oplus r)$ są równoważne. Które spośród spójników logicznych $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$ są prawostronnie rozdzielne względem których?

1.2.4. Lemat o podstawianiu

Definicja 8. *Podstawieniem* formuły ψ w miejsce zmiennej zdaniowej p nazywamy przekształcenie, które formule ϕ przyporządkowuje formułę powstałą przez wstawienie formuły ψ w miejsce każdego wystąpienia zmiennej p w formule ϕ . Formalnie:

$$\begin{aligned} p[p/\psi] &= \psi \\ q[p/\psi] &= q, \quad \text{dla } q \neq p \\ (\neg\phi)[p/\psi] &= \neg(\phi[p/\psi]) \\ (\phi_1 \vee \phi_2)[p/\psi] &= (\phi_1[p/\psi]) \vee (\phi_2[p/\psi]) \\ (\phi_1 \wedge \phi_2)[p/\psi] &= (\phi_1[p/\psi]) \wedge (\phi_2[p/\psi]) \\ (\phi_1 \Rightarrow \phi_2)[p/\psi] &= (\phi_1[p/\psi]) \Rightarrow (\phi_2[p/\psi]) \\ (\phi_1 \Leftrightarrow \phi_2)[p/\psi] &= (\phi_1[p/\psi]) \Leftrightarrow (\phi_2[p/\psi]) \end{aligned}$$

Przykład 9. $(p \Rightarrow p \vee q)[p/q \Rightarrow p] = (q \Rightarrow p) \Rightarrow (q \Rightarrow p) \vee q$.

W podobny sposób definiujemy jednoczesne podstawienie formuł w miejsce kilku zmiennych zdaniowych $[p_1/\psi_1, \dots, p_n/\psi_n]$. Jest to odwzorowanie, które formule ϕ przyporządkowuje formułę powstałą przez wstawienie formuły ψ_i w miejsce każdego wystąpienia zmiennej p_i w formule ϕ , dla każdego $i = 1, \dots, n$.

Lemat 10 (o podstawianiu). Niech ϕ i ψ będą formułami, niech p będzie zmienną zdaniową i niech σ będzie wartościowaniem. Niech σ' będzie wartościowaniem zdefiniowanym wzorem

$$\sigma'(q) = \begin{cases} \sigma(q), & \text{gdy } p \neq q, \\ \hat{\sigma}(\psi), & \text{gdy } p = q. \end{cases}$$

Wtedy $\hat{\sigma}(\phi[p/\psi]) = \hat{\sigma}'(\phi)$.

Wniosek. Jeżeli formuła ϕ jest tautologią, to dla dowolnej zmiennej p i dowolnej formuły ψ formuła $\phi[p/\psi]$ jest tautologią.

Wniosek ten pozwala dowodzić, że skomplikowane formuły są tautologiami. Dla przykładu formuła $(q \Rightarrow p) \Rightarrow (q \Rightarrow p) \vee q$ z przykładu 9 jest tautologią, gdyż jest wynikiem podstawienia formuły $q \Rightarrow p$ w miejsce zmiennej p w tautologii $p \Rightarrow p \vee q$.

Wniosek. Jeżeli formuły ψ i ψ' są równoważne, to dla dowolnej zmiennej p i dowolnej formuły ϕ formuły $\phi[p/\psi]$ i $\phi[p/\psi']$ są równoważne.

Powyższy wniosek ma bardzo duże znaczenie praktyczne, pozwala bowiem w dowolnie skomplikowanych formułach zamieniać dowolne podformuły na formuły im równoważne, co w szczególności umożliwia upraszczanie formuł. Dla przykładu formuły $\neg(p \Rightarrow q) \vee (p \wedge q)$ i $(p \wedge \neg q) \vee (p \wedge q)$ są równoważne, co wynika z równoważności formuł $\neg(p \Rightarrow q)$ i $(p \wedge \neg q)$ po podstawieniu ich w miejsce zmiennej r w formule $r \vee (p \wedge q)$.

W zadaniach 22–25 zbadaj, czy podane formuły są tautologiami.

Zadanie 22. $(s \wedge u \wedge t \wedge (p \vee q \vee r)) \Rightarrow (x \Rightarrow y \wedge \neg z) \Leftrightarrow ((p \vee q \vee r) \Rightarrow (s \wedge u \wedge t) \Rightarrow (x \Rightarrow y \wedge \neg z))$

Zadanie 23. $((p \Rightarrow q \wedge (r \vee s \Leftrightarrow \neg p)) \wedge \neg((p \Rightarrow q \wedge (r \vee s \Leftrightarrow \neg p))))$

Zadanie 24. $(p \wedge \neg q) \wedge ((r \Rightarrow s) \vee (p \Rightarrow q \Rightarrow r \vee \neg s)) \Rightarrow \neg(q \vee \neg p)$

Zadanie 25. $((p \Rightarrow q \vee r) \vee s \vee t) \wedge \neg(p \Rightarrow q \vee r) \Rightarrow s \vee t$

Zadanie 26. Wskaż podstawienie $[p/\phi_1, q/\phi_2, r/\phi_3]$, dla którego formuła

$$(p \vee (q \wedge r)) [p/\phi_1, q/\phi_2, r/\phi_3]$$

jest a) tautologią, b) formułą spełnialną, c) formułą sprzeczną.

1.3. Formalizacja rozumowań w języku rachunku zdań

Zadanie 27. Sformalizuj zadanie 6, tj. pokaż, jak znaleźć odpowiedzi na postawione w nim pytania korzystając z rachunku zdań.

Zadanie 28. Podczas pewnej kampanii wyborczej Olek, Józek i Kazik wygłosili następujące oświadczenia:

Olek: *Józek zawsze kłamie.*

Józek: *Kazik zawsze kłamie.*

Kazik: *Olek zawsze kłamie.*

Pokaż, że co najmniej dwóch spośród nich nie miało racji.

Zadanie 29. Podczas tej samej kampanii wyborczej Basia, Hania, Kasia i Ola stwierdziły, że:

Basia: *Hania zawsze kłamie.*

Hania: *Kasia czasem mówi prawdę.*

Kasia: *Ola czasem kłamie.*

Ola: *Basia zawsze mówi prawdę.*

Ile pań powiedziało prawdę?

Zadanie 30. Zbadaj zasadność poniższych rozumowań:

1. Jeśli stopa procentowa nie ulegnie zmianie, to wzrosną wydatki rządowe lub pojawi się bezrobocie. Jeśli wydatki rządowe nie wzrosną, to podatki zostaną obniżone. Jeśli podatki zostaną obniżone i stopa procentowa nie ulegnie zmianie, to bezrobocie się nie pojawi. Zatem wydatki rządowe wzrosną.
2. Jeśli ceny wzrosną, to spadnie popyt. Jeśli popyt spadnie, to spadną ceny. Zatem jeśli ceny wzrosną, to spadną. Zatem ceny spadną!

1.4. Własności formuł zdaniowych

Definicja 11. Napis $\bigwedge_{i=1}^n \phi_i$ oznacza $\phi_1 \wedge \dots \wedge \phi_n$, zaś $\bigvee_{i=1}^n \phi_i$ oznacza $\phi_1 \vee \dots \vee \phi_n$.

Przyjmujemy przy tym, że $\bigwedge_{i=1}^0 \phi_i$ oznacza $\top$, zaś $\bigvee_{i=1}^0 \phi_i$ oznacza $\perp$.

Definicja 12. Niech V będzie zbiorem zmiennych zdaniowych. V -literałem nazywamy formułę postaci p lub $\neg p$, gdzie $p \in V$. Jeżeli zbiór zmiennych zdaniowych jest ustalony, to formułę takiej postaci nazywamy po prostu *literałem*. Niekiedy do zbioru literałów zaliczamy też stałe logiczne $\top$ i $\perp$.

Zadanie 31. Dane są formuły $\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_n$. Wykaż, że dla każdego n poniższa formuła zdaniowa jest tautologią:

$$\left(\bigwedge_{i=1}^n (\phi_i \Rightarrow \psi_i) \right) \Rightarrow \left(\left(\bigvee_{i=1}^n \phi_i \right) \Rightarrow \left(\bigvee_{i=1}^n \psi_i \right) \right).$$

Zadanie 32. Dane są formuły $\phi_1, \dots, \phi_n, \psi$. Wykaż, że dla każdego n poniższa formuła zdaniowa jest tautologią:

$$\left(\bigvee_{i=1}^n (\phi_i \Rightarrow \psi) \right) \Rightarrow \left(\left(\bigwedge_{i=1}^n \phi_i \right) \Rightarrow \psi \right).$$

Zadanie 33. Czy istnieje taki nieskończony ciąg formuł $\{\phi_i\}_{i=1}^{\infty}$ rachunku zdań, że wszystkie formuły $\phi_{i+1} \Rightarrow \phi_i$ są tautologiami rachunku zdań, zaś żadna z formuł $\phi_i \Rightarrow \phi_{i+1}$ nie jest tautologią?

Zadanie 34. Czy istnieje taki nieskończony ciąg formuł $\{\phi_i\}_{i=1}^{\infty}$ rachunku zdań, że wszystkie formuły $\phi_i \Rightarrow \phi_{i+1}$ są tautologiami rachunku zdań, zaś żadna z formuł $\phi_{i+1} \Rightarrow \phi_i$ nie jest tautologią?

Zadanie 35. Udowodnij, że formuła rachunku zdań zbudowana wyłącznie ze zmiennych i spójnika równoważności „ $\Leftrightarrow$ ” (oczywiście do jej zapisania można też używać nawiasów) jest tautologią wtedy i tylko wtedy, gdy każda zmienna występuje w niej parzystą liczbę razy.

Zadanie 36. Udowodnij, że jeśli p jest zmienną zdaniową, a ϕ taką formułą rachunku zdań, że $p \Rightarrow \phi$ i $\neg\phi \Rightarrow p$ są tautologiami, to ϕ jest tautologią.

Zadanie 37. Niech $\phi_1, \dots, \phi_n$ będą formułami zdaniowymi, w których nie występują zmienne zdaniowe $p_1, \dots, p_{n+1}$. Udowodnij, że formuła

$$\bigwedge_{i=1}^n \phi_i$$

jest tautologią wtedy i tylko wtedy, gdy tautologią jest formuła

$$\neg p_1 \vee \bigvee_{i=1}^n (\phi_i \wedge p_i \wedge \neg p_{i+1}) \vee p_{n+1}.$$

Zadanie 38. Udowodnij, że jeżeli formuła ϕ jest tautologią, to dla dowolnych formuł $\psi_1, \dots, \psi_n$ formuła

$$\psi_1 \Rightarrow \dots \Rightarrow \psi_n \Rightarrow \phi$$

jest tautologią.

Zadanie 39. Udowodnij, że jeżeli ϕ jest formułą sprzeczną, to dla dowolnych formuł $\psi_1, \dots, \psi_n$ formuła

$$\phi \Rightarrow \psi_1 \Rightarrow \dots \Rightarrow \psi_n$$

jest tautologią.

Zadanie 40. Dla jakich $n \geq 1$ formuła

$$(\dots((p \Rightarrow p) \Rightarrow p) \Rightarrow \dots) \Rightarrow p,$$

w której zmienna p występuje n razy jest tautologią?

Zadanie 41. Niech p^0 oznacza $\neg p$ oraz niech p^1 oznacza p . Dla jakich ciągów $(i_1, \dots, i_n) \in \{0, 1\}^n$ formuła

$$(\dots((p^{i_1} \Rightarrow p^{i_2}) \Rightarrow p^{i_3}) \Rightarrow \dots) \Rightarrow p^{i_n})$$

jest tautologią?

Zadanie 42. Niech $p_1, \dots, p_n$ będą wszystkimi zmiennymi zdaniowymi występującymi w formule ϕ . Udowodnij, że formuła ϕ jest spełnialna wtedy i tylko wtedy, gdy istnieje podstawienie $[p_1/\phi_1, \dots, p_n/\phi_n]$ takie, że formuła $\phi[p_1/\phi_1, \dots, p_n/\phi_n]$ jest tautologią. Udowodnij, że formuła ϕ nie jest tautologią wtedy i tylko wtedy, gdy istnieje podstawienie $[p_1/\phi_1, \dots, p_n/\phi_n]$ takie, że formuła $\phi[p_1/\phi_1, \dots, p_n/\phi_n]$ jest sprzeczna.

Zadanie 43. Dane są formuły $\phi_1, \dots, \phi_n, \psi$. Czy formuły

$$(\dots((\psi \Rightarrow \phi_1) \Rightarrow \phi_2) \Rightarrow \dots) \Rightarrow \phi_n$$

oraz

$$\psi \Rightarrow (\phi_1 \vee \phi_2 \vee \dots \vee \phi_n)$$

są równoważne?

Zadanie 44. Dane są formuły $\phi_1, \dots, \phi_n, \psi$. Czy formuły

$$\phi_1 \Rightarrow (\phi_2 \Rightarrow (\dots \Rightarrow (\phi_n \Rightarrow \psi) \dots))$$

oraz

$$(\phi_1 \wedge \phi_2 \wedge \dots \wedge \phi_n) \Rightarrow \psi$$

są równoważne?

Zadanie 45. Pokaż przez indukcję, że każda formuła ϕ zbudowana ze zmiennych p i q oraz spójnika $\Rightarrow$ jest równoważna dokładnie jednej z formuł z poniższego zbioru:

$$\{\top, p, q, (p \Rightarrow q), (q \Rightarrow p), (p \vee q)\}.$$

W poniższych zadaniach przyjmujemy następujące oznaczenia. Niech ϕ będzie formułą rachunku zdań zbudowaną wyłącznie ze zmiennych zdaniowych oraz spójników $\vee$ oraz $\wedge$ (oczywiście można używać nawiasów). Niech ϕ^d oznacza formułę powstałą z ϕ przez zastąpienie każdego wystąpienia spójnika $\vee$ spójnikiem $\wedge$, zaś każdego wystąpienia spójnika $\wedge$ spójnikiem $\vee$. Niech ϕ^n oznacza formułę powstałą przez zastąpienie każdego wystąpienia zmiennej zdaniowej negacją tej zmiennej.

Zadanie 46. Udowodnij, że jeżeli formuły ϕ_1 i ϕ_2 są równoważne, to równoważne są także formuły ϕ_1^d i ϕ_2^d .

Zadanie 47. Udowodnij, że jeżeli formuły ϕ_1 i ϕ_2 są równoważne, to równoważne są także formuły ϕ_1^n i ϕ_2^n .

Zadanie 48. Udowodnij, że dla dowolnej formuły ϕ formuły $\neg\phi^d$ oraz ϕ^n są równoważne.

Zadanie 49. Wykaż, że dla każdej formuły spełnialnej ϕ ze zmiennymi ze zbioru $V = \{p, q, r\}$ istnieje formuła ψ postaci $\phi_1 \wedge \phi_2 \wedge \phi_3$ taka, że każde ϕ_i jest V -literałem, ϕ_i są parami różne oraz $\psi \Rightarrow \phi$ jest tautologią.

Zadanie 50 (lemat interpolacyjny Craiga dla rachunku zdań). Niech $V(\phi)$ oznacza zbiór zmiennych zdaniowych występujących w formule ϕ . Przypuśćmy, że ϕ i ψ są takimi formułami rachunku zdań, że $\phi \Rightarrow \psi$ jest tautologią. Udowodnij, że istnieje taka formuła ρ , że $\phi \Rightarrow \rho$ oraz $\rho \Rightarrow \psi$ są tautologiami i $V(\rho) \subseteq V(\phi) \cap V(\psi)$.

Zadanie 51 (o zamkniętym układzie twierdzeń). Niech n będzie ustaloną liczbą naturalną. Przypuśćmy, że dla pewnego wartościowania są spełnione formuły:

$$\begin{aligned} p_1 \vee \dots \vee p_n, \\ p_i \Rightarrow q_i, \quad \text{dla } i = 1, \dots, n, \\ \neg(q_i \wedge q_j), \quad \text{dla } 1 \leq i < j \leq n. \end{aligned}$$

Udowodnij, że wartościowanie to spełnia także formuły

$$q_i \Rightarrow p_i, \quad \text{dla } i = 1, \dots, n.$$

Przez *wartościowanie formuły ϕ* będziemy w poniższych zadaniach rozumieć odwzorowanie przyporządkowujące zmiennym występującym w tej formule wartości logiczne T i F. Formuła zawierająca n różnych zmiennych ma więc 2^n wartościowań.

Zadanie 52. Wykaż, że formuła $(\dots((p_1 \Rightarrow p_2) \Rightarrow p_3) \Rightarrow \dots \Rightarrow p_{n-1}) \Rightarrow p_n$ jest fałszywa dla dokładnie

$$\frac{2^n - (-1)^n}{3}$$

wartościowań tej formuły. Dla ilu wartościowań jest fałszywa formuła

$$p_n \Rightarrow (p_{n-1} \Rightarrow (p_{n-2} \Rightarrow \dots \Rightarrow (p_2 \Rightarrow p_1) \dots) ?$$

Zadanie 53. Niech ϕ oraz ψ będą formułami rachunku zdań zbudowanymi wyłącznie ze zmiennych zdaniowych oraz spójników $\vee$ oraz $\wedge$ (oczywiście można używać nawiasów). Pokaż, że formuła $\phi \Leftrightarrow \psi$ jest spełniona przez co najmniej dwa wartościowania. Podaj przykład formuł ϕ i ψ takich, że formuła $\phi \Leftrightarrow \psi$ jest spełniona przez dokładnie dwa wartościowania.

Zadanie 54. Niech n będzie dodatnią liczbą naturalną i niech $V_n = \{p_0, \dots, p_{n-1}\}$ będzie zbiorem zmiennych zdaniowych. Przyjmijmy, że dla formuły ϕ nie zawierającej zmiennych spoza zbioru V_n napis $nv_n(\phi)$ oznacza liczbę wartościowań $\sigma : V_n \rightarrow \{T, F\}$ spełniających tę formułę. Pokaż, że dla dowolnych formuł zdaniowych ϕ oraz ψ , które nie zawierają zmiennych spoza zbioru V_n , równość

$$nv_n(\phi \vee \psi) = nv_n(\phi) + nv_n(\psi)$$

zachodzi wtedy i tylko wtedy, gdy $\phi \wedge \psi$ jest formułą sprzeczną.

Zadanie 55. Niech V będzie niepustym i skończonym zbiorem zmiennych zdaniowych. Znajdź zbiór wszystkich wartościowań spełniających formułę

$$\neg \bigwedge_{p,q \in V} (p \Rightarrow q).$$

1.5. Postaci normalne formuł zdaniowych

1.5.1. Usuwanie symbolu negacji

Formuły w których symbol negacji występuje przed formułą złożoną są często trudne do zrozumienia (wyrażenie „nie prawda, że liczba n dzieli się przez 2 lub przez 3” jest bardziej skomplikowane, niż równoważne mu wyrażenie „liczba n nie dzieli się przez 2 i nie dzieli się przez 3”). *Prawa negowania formuł zdaniowych* (punkty 5–12 z zadania 15) pozwalają znaleźć dla danej formuły formułę jej równoważną, w której negacja występuje jedynie przed zmiennymi zdaniowymi. Istotnie, dla dowolnej formuły ϕ na mocy lematu o podstawianiu i prawa podwójnego przeczenia formuły $\neg\neg\phi$ oraz ϕ są równoważne. Na mocy lematu o podstawianiu i prawa de Morgana dla dowolnych formuł ϕ_1 i ϕ_2 formuły $\neg(\phi_1 \wedge \phi_2)$ oraz $\neg\phi_1 \vee \neg\phi_2$ są równoważne. Podobnie postępujemy dla formuł dowolnej innej postaci. Możemy zatem zdefiniować odwzorowanie T przyporządkowujące dowolnym formułom formuły, w których negacja występuje jedynie przed zmiennymi zdaniowymi:

$$\begin{aligned} T(p) &= p, & \text{dla } p \in V \\ T(\perp) &= \perp \\ T(\top) &= \top \\ T(\phi_1 \vee \phi_2) &= T(\phi_1) \vee T(\phi_2) \\ T(\phi_1 \wedge \phi_2) &= T(\phi_1) \wedge T(\phi_2) \\ T(\phi_1 \Rightarrow \phi_2) &= T(\phi_1) \Rightarrow T(\phi_2) \\ T(\phi_1 \Leftrightarrow \phi_2) &= T(\phi_1) \Leftrightarrow T(\phi_2) \\ T(\neg p) &= \neg p, & \text{dla } p \in V \end{aligned}$$

$$\begin{aligned}
\mathcal{T}(\neg \perp) &= \top \\
\mathcal{T}(\neg \top) &= \perp \\
\mathcal{T}(\neg(\phi_1 \vee \phi_2)) &= \mathcal{T}(\neg\phi_1) \wedge \mathcal{T}(\neg\phi_2) \\
\mathcal{T}(\neg(\phi_1 \wedge \phi_2)) &= \mathcal{T}(\neg\phi_1) \vee \mathcal{T}(\neg\phi_2) \\
\mathcal{T}(\neg(\phi_1 \Rightarrow \phi_2)) &= \mathcal{T}(\phi_1) \wedge \mathcal{T}(\neg\phi_2) \\
\mathcal{T}(\neg(\phi_1 \Leftrightarrow \phi_2)) &= \mathcal{T}(\neg\phi_1) \Leftrightarrow \mathcal{T}(\phi_2) \\
\mathcal{T}(\neg\neg\phi) &= \mathcal{T}(\phi)
\end{aligned}$$

Fakt 13. Dla dowolnej formuły ϕ , formuły ϕ oraz $\mathcal{T}(\phi)$ są równoważne i w formule $\mathcal{T}(\phi)$ negacja występuje jedynie przed zmiennymi zdaniowymi.

Zadanie 56. Zaneguj formuły z zadania 10 i — korzystając z praw negowania formuł logicznych — znajdź formuły im równoważne, w których negacja występuje jedynie przed zmiennymi zdaniowymi.

Zadanie 57. Zaneguj formuły z zadania 11 i — korzystając z praw negowania formuł logicznych — znajdź formuły im równoważne, w których negacja występuje jedynie przed zmiennymi zdaniowymi.

Formuły, w których negacja występuje jedynie przed zmiennymi zdaniowymi możemy określić jako formuły zbudowane z literalów przy pomocy spójników logicznych alternatywy, koniunkcji, implikacji i równoważności. Zauważmy, że na mocy lematu o podstawianiu i punktów 13–15 zadania 15 każda formuła jest równoważna pewnej formule nie zawierającej spójników implikacji i równoważności. Możemy więc rozpatrywać formuły zbudowane z literalów jedynie przy pomocy spójników alternatywy i koniunkcji. Jeszcze węższe klasy formuł rozważamy w następnych paragrafach.

1.5.2. Dysjunkcyjna postać normalna

Definicja 14. Formuła ma *dysjunkcyjną postać normalną* (DNF, ang. *Disjunctive Normal Form*), jeśli ma postać

$$\bigvee_{i=1}^n \left(\bigwedge_{j=1}^{m_i} l_{ij} \right),$$

gdzie l_{ij} są literalami, dla $i = 1, \dots, n$ oraz $j = 1, \dots, m_i$. Mówiąc skrótowo, dysjunkcyjna postać normalna, to alternatywa koniunkcji literalów.

Zadanie 58. Udowodnij, że dla każdej formuły zdaniowej ϕ istnieje formuła ψ równoważna z ϕ i mająca dysjunkcyjną postać normalną.

Zadanie 59. Znajdź formuły zdaniowe ϕ_1, ϕ_2, ϕ_3 mające dysjunkcyjną postać normalną, zawierające zmienne p, q i r i spełnione dla podanych niżej wartościowań:

p	q	r	ϕ_1	ϕ_2	ϕ_3
T	T	T	T	F	F
T	T	F	F	F	F
T	F	T	T	T	F
T	F	F	F	T	T
F	T	T	T	F	T
F	T	F	F	F	T
F	F	T	F	F	T
F	F	F	F	F	F

Zadanie 60. Znajdź formuły mające dysjunkcyjną postać normalną równoważne formułom z zadania 10.

Zadanie 61. Znajdź formuły mające dysjunkcyjną postać normalną równoważne formułom z zadania 11.

1.5.3. Koniunkcyjna postać normalna

Definicja 15. *Klauzulą* nazywamy formułę postaci

$$\bigvee_{j=1}^m l_j,$$

gdzie l_j są literałami, dla $j = 1, \dots, m$. Innymi słowy klauzula to alternatywa literałów.

Definicja 16. Formuła ma *koniunkcyjną postać normalną* (CNF, ang. *Conjunctive Normal Form*), jeśli ma postać

$$\bigwedge_{i=1}^n \left(\bigvee_{j=1}^{m_i} l_{ij} \right),$$

gdzie l_{ij} są literałami, dla $i = 1, \dots, n$ oraz $j = 1, \dots, m_i$, tj. gdy jest koniunkcją klauzul.

Zadanie 62. Udowodnij, że dla każdej formuły zdaniowej ϕ istnieje formuła ψ równoważna z ϕ i mająca koniunkcyjną postać normalną.

Zadanie 63. Znajdź formuły mające koniunkcyjną postać normalną równoważne formułom z zadania 10.

Zadanie 64. Znajdź formuły mające koniunkcyjną postać normalną równoważne formułom z zadania 11.

Definicja 17. Formuła ma postać k -CNF, gdzie k jest liczbą naturalną, jeżeli ma postać

$$\bigwedge_{i=1}^n \left(\bigvee_{j=1}^k l_{ij} \right),$$

gdzie l_{ij} są literałami, dla $i = 1, \dots, n$ oraz $j = 1, \dots, k$, tj. gdy jest koniunkcją klauzul zawierających po k literałów.

Zadanie 65. Wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci 1-CNF.

Zadanie 66. Dla każdego $k \geq 1$ wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci k -CNF.

Definicja 18. Formuła ma postać CNF_j , gdzie j jest liczbą naturalną, jeżeli ma postać CNF i każda zmienna występuje w niej co najwyżej j razy. Formuła ma postać k -CNF $_j$, gdzie k i j są liczbami naturalnymi, jeżeli ma postać k -CNF i każda zmienna występuje w niej co najwyżej j razy.

Zadanie 67. Wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci CNF_1 .

Zadanie 68. Dla każdego $k \geq 1$ wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci CNF_k .

Definicja 19. Literał l jest *pozytywny*, jeżeli $l = p$ dla pewnej zmiennej $p \in V$. Literał l jest *negatywny*, jeżeli $l = \neg p$ dla pewnej zmiennej $p \in V$.

Definicja 20. Operację negowania literału definiujemy następująco:

$$\begin{aligned} \overline{\overline{p}} &= \neg p, \\ \overline{\neg p} &= p, \end{aligned}$$

dla dowolnego $p \in V$.

Zadanie 69. Niech $C = \bigvee_{j=1}^m l_j$ będzie dowolną klauzulą i niech

$$\begin{aligned} P &= \{j \in \{1, \dots, m\} \mid \text{litera } l_j \text{ jest pozytywny}\}, \\ N &= \{j \in \{1, \dots, m\} \mid \text{litera } l_j \text{ jest negatywny}\} \end{aligned}$$

oraz

$$C' = \bigwedge_{j \in N} \bar{l}_j \Rightarrow \bigvee_{j \in P} l_j.$$

Udowodnij, że formuły C oraz C' są równoważne.

Na mocy powyższego zadania klauzule można zapisywać w postaci

$$\bigwedge_{j=1}^m p_j \Rightarrow \bigvee_{j=1}^n q_j,$$

gdzie p_j i q_j są zmiennymi zdaniowymi.

Definicja 21. Klauzula $\bigvee_{j=1}^m l_j$ jest *klauzulą hornowską*, jeżeli co najwyżej jeden spośród literałów $l_1, \dots, l_m$ jest pozytywny. Formuła ma *postać hornowską*, jeżeli jest koniunkcją klauzul hornowskich.

Klauzule hornowskie można więc zapisać w postaci

$$\bigwedge_{j=1}^m p_j \Rightarrow q \quad \text{lub} \quad \bigwedge_{j=1}^m p_j \Rightarrow \perp,$$

gdzie p_j oraz q są zmiennymi zdaniowymi.

Zadanie 70. Wskaż przykład formuły, która nie jest równoważna z żadną formułą w postaci hornowskiej.

Zadanie 71. Które spośród formuł z zadania 10 można przedstawić w postaci hornowskiej? Tam, gdzie to możliwe, podaj tę postać.

Zadanie 72. Które spośród formuł z zadania 11 można przedstawić w postaci hornowskiej? Tam, gdzie to możliwe, podaj tę postać.

1.6. Funkcje boolowskie i zupełne zbiory spójników

Definicja 22. Funkcje $f : \mathcal{B}^n \rightarrow \mathcal{B}$, gdzie $\mathcal{B} = \{T, F\}$ i $n \geq 0$, nazywamy n -argumentowymi *funkcjami boolowskimi* lub *funkcjami logicznymi*.

Do tej pory zbiór spójników logicznych był ustalony ($\perp$, $\top$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$). Nic jednak nie stoi na przeszkodzie, by rozważać różne zestawy spójników i wprowadzać nowe spójniki. Z każdym spójnikiem wiążemy jego *znaczenie* — funkcję boolowską określającą prawdziwość formuł zbudowanych przy użyciu tego spójnika. Tabelki funkcji boolowskich określających prawdziwość spójników $\perp$, $\top$, $\neg$, $\vee$, $\wedge$, $\Rightarrow$ i $\Leftrightarrow$ zostały przedstawione na rysunku 1.

Definicja 23. Formuła ϕ zbudowana ze zmiennych $p_1, \dots, p_n$ opisuje n -argumentową funkcję boolowską f , jeżeli dla każdego wartościowania σ zmiennych $p_1, \dots, p_n$ zachodzi:

$$f(\sigma(p_1), \dots, \sigma(p_n)) = \sigma(\phi).$$

Jeżeli formuła ϕ zbudowana ze zmiennych $p_1, \dots, p_n$ opisuje funkcję f , to piszemy

$$f(p_1, \dots, p_n) \equiv \phi.$$

Definicja 24. Zbiór spójników logicznych jest *zupełny*, jeżeli dowolną funkcję boolowską można opisać za pomocą formuły zdaniowej zawierającej jedynie spójniki z tego zbioru i zmienne. Zbiór spójników jest *k-zupełny*, jeżeli każdą *co najwyżej k-argumentową* funkcję boolowską można opisać za pomocą formuły zdaniowej zawierającej jedynie spójniki z tego zbioru i zmienne.

Innymi słowy zbiór spójników jest *zupełny* (*k-zupełny*), jeśli każdą funkcję boolowską (każdą funkcję boolowską co najwyżej *k*-argumentową) można przedstawić jako złożenie funkcji boolowskich określających znaczenie spójników z podanego zbioru.

Zadanie 73. Ile jest funkcji boolowskich n -argumentowych?

Zadanie 74. Pokaż, że $\{\vee, \wedge\}$ nie jest zupełny.

Zadanie 75. Pokaż, że $\{\vee, \wedge, \Leftrightarrow, \Rightarrow\}$ nie jest zupełny.

Zadanie 76. Pokaż, że $\{\Leftrightarrow, \perp\}$ nie jest zupełny oraz że jest 1-zupełny.

Zadanie 77. Pokaż, że $\{\wedge, \vee, \neg\}$ jest zupełny.

Zadanie 78. Pokaż, że $\{\wedge, \neg\}$ jest zupełny.

Zadanie 79. Pokaż, że $\{\vee, \neg\}$ jest zupełny.

Zadanie 80. Pokaż, że $\{\Rightarrow, \perp\}$ jest zupełny.

Zadanie 81. Pokaż, że $\{\Rightarrow, \neg\}$ jest zupełny.

Zadanie 82. Pokaż, że $\{\vee, \Leftrightarrow, \perp\}$ jest zupełny.

Zadanie 83. Udowodnij, że każdy 2-zupełny zbiór spójników jest zupełny.

Zadanie 84. Udowodnij, że zbiór $\{\vee, \wedge, \Rightarrow, \neg\}$ jest 2-zupełny.

Zadanie 85. Czy system spójników $\{\oplus, \top\}$ jest zupełny, gdzie $p \oplus q$ jest prawdziwe wtedy i tylko wtedy, gdy $p \wedge \neg q$ jest prawdą, zaś $\top$ oznacza prawdę?

Zadanie 86. Pokaż, że istnieje taki dwuargumentowy spójnik $\uparrow$, że $\{\uparrow\}$ jest zupełny.

Zadanie 87. Ile jest takich dwuargumentowych spójników logicznych $\oplus$, że $\{\oplus\}$ jest zupełny?

Zadanie 88. Niech s będzie takim spójnikiem logicznym, że $s(\top, \top) = F$. Udowodnij, że zbiór $\{s, \Rightarrow\}$ jest zupełny.

1.7. Składnia rachunku kwantyfikatorów

Definicja 25. W rachunku kwantyfikatorów używamy tzw. *zmiennych indywidualnych* pochodzących z nieskończonego zbioru $X = \{x, y, z, x_1, x_2, \dots\}$, *symboli funkcyjnych* $f, g, f_1, f_2, \dots$ i *symboli relacyjnych* $p, q, p_1, p_2, \dots$. Z każdym symbolem funkcyjnym i z każdym symbolem relacyjnym związujemy liczbę naturalną, która określa liczbę jego argumentów (*arność*). Symbole funkcyjne 0-argumentowe nazywamy *symbolami stałych*. Symbole relacyjne można uważać za uogólnienie zmiennych zdaniowych z rachunku zdań (zmienne zdaniowe, to 0-argumentowe symbole relacyjne).

Termy są napisami postaci $x, f(x), g(f_1(x), f_2(x))$ itp. Formalnie:

1. Każda zmienna indywidualna jest termem.
2. Każdy symbol stałej jest termem.
3. Jeśli $t_1, \dots, t_n$ są termami, a f jest n -argumentowym ($n > 0$) symbolem funkcyjnym, to $f(t_1, \dots, t_n)$ jest termem.
4. Każdy term można zbudować przy pomocy reguł 1–3.

Formuły atomowe są napisami postaci $p(t_1), q(t_1, t_2)$ itp., gdzie t_1 i t_2 są termami. Formalnie:

1. Symbole $\perp$ i $\top$ są formułami atomowymi.
2. Każdy 0-argumentowy symbol relacyjny jest formułą atomową.
3. Jeśli $t_1, \dots, t_n$ są termami, a p jest n -argumentowym ($n > 0$) symbolem relacyjnym, to $p(t_1, \dots, t_n)$ jest formułą atomową.
4. Każdą formułę atomową można otrzymać przy pomocy reguł 1–3.

Formuły rachunku kwantyfikatorów (które będziemy oznaczać $\phi, \psi, \dots$) budujemy z formuł atomowych za pomocą spójników logicznych w sposób podobny, jak w rachunku zdań. Ponadto możemy używać kwantyfikatorów $\forall$ i $\exists$. Formalnie:

1. Każda formuła atomowa jest formułą rachunku kwantyfikatorów.
2. Jeżeli ϕ_1 i ϕ_2 są formułami rachunku kwantyfikatorów, to są nimi także: $(\neg\phi_1)$, $(\phi_1 \wedge \phi_2)$, $(\phi_1 \vee \phi_2)$, $(\phi_1 \Rightarrow \phi_2)$ i $(\phi_1 \Leftrightarrow \phi_2)$.
3. Jeżeli x jest zmienną indywiduową, a ϕ — formułą rachunku kwantyfikatorów, to formułami rachunku kwantyfikatorów są też $(\forall x \phi)$ i $(\exists x \phi)$.
4. Każdą formułę rachunku kwantyfikatorów można otrzymać przy pomocy reguł 1–3.

Dla zwiększenia czytelności opuszczamy niektóre nawiasy w podobny sposób, jak w rachunku zdań. Niektóre symbole funkcyjne lub relacyjne piszemy infiksowo.

Definicja 26. Mówimy, że w formule $\forall x \phi$ (lub $\exists x \phi$) kwantyfikator $\forall$ (lub $\exists$) *wiąże* wystąpienia zmiennej x w formule ϕ , oraz że wystąpienia zmiennej x w formule ϕ są *związane* przez ten kwantyfikator. Wystąpienia zmiennych, które nie są związane w danej formule, są w niej *wolne*. Formalnie zbiór $FV(\phi)$ zmiennych, które występują jako wolne w formule ϕ definiujemy następująco:

$$\begin{aligned}
 FV(x) &= \{x\} \\
 FV(f(t_1, \dots, t_n)) &= FV(t_1) \cup \dots \cup FV(t_n) \\
 FV(\perp) &= \emptyset \\
 FV(\top) &= \emptyset \\
 FV(p(t_1, \dots, t_n)) &= FV(t_1) \cup \dots \cup FV(t_n) \\
 FV(\neg\phi) &= FV(\phi) \\
 FV(\phi \circ \psi) &= FV(\phi) \cup FV(\psi), \quad \text{gdzie } \circ \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\} \\
 FV(Qx \phi) &= FV(\phi) \setminus \{x\}, \quad \text{gdzie } Q \in \{\forall, \exists\}
 \end{aligned}$$

Podobnie definiujemy zbiór zmiennych występujących w formule jako związane.

Przyjmujemy konwencję, że $(\forall\phi(x))\psi$ oznacza $\forall x(\phi(x) \Rightarrow \psi)$ oraz $(\exists\phi(x))\psi$ oznacza $\exists x(\phi(x) \wedge \psi)$.

1.8. Znaczenie formuł rachunku kwantyfikatorów

Formalna definicja *tautologii* (formuły prawdziwej, prawa rachunku kwantyfikatorów) jest nieco bardziej skomplikowana, niż w przypadku rachunku zdań. Z tego powodu podamy ją dopiero w rozdziale 12. Tutaj powiemy jedynie, że formuła ϕ jest tautologią, jeżeli jest spełniona przy każdej interpretacji symboli funkcyjnych i relacyjnych. Przy danej interpretacji symboli funkcyjnych i relacyjnych formuła $\forall x \phi$ jest spełniona, gdy jest spełniona formuła ϕ dla każdej wartości zmiennej x , zaś formuła $\exists x \phi$ jest spełniona, gdy istnieje pewna wartość zmiennej x , dla której formuła ϕ jest spełniona.

Przykład 27. Prawami rachunku kwantyfikatorów są np. *prawa negowania kwantyfikatorów*:

$$\begin{aligned}\neg(\forall x \phi) &\Leftrightarrow \exists x \neg\phi \\ \neg(\exists x \phi) &\Leftrightarrow \forall x \neg\phi\end{aligned}$$

Ich intuicyjny sens jest jasny: „nieprawda, że dla każdego x formuła ϕ jest prawdziwa” oznacza, że „istnieje x , dla którego formuła ϕ nie jest prawdziwa.” Podobnie „nieprawda, że istnieje x , dla którego formuła ϕ jest prawdziwa” oznacza, że „dla każdego x formuła ϕ nie jest prawdziwa.”

Przykład 28. Niech ϕ i ψ oznaczają formuły rachunku kwantyfikatorów być może zawierające wolne wystąpienia zmiennej x . Wtedy

$$\begin{aligned}\forall x (\phi \wedge \psi) &\Leftrightarrow \forall x \phi \wedge \forall x \psi \\ \exists x (\phi \vee \psi) &\Leftrightarrow \exists x \phi \vee \exists x \psi\end{aligned}$$

są prawami rachunku kwantyfikatorów.

Przykład 29. Niech ϕ i ψ oznaczają takie formuły rachunku kwantyfikatorów, że zmienna x nie ma wolnych wystąpień w formule ϕ (lecz może mieć w ψ). Wtedy

$$\begin{aligned}\forall x (\phi \vee \psi) &\Leftrightarrow \phi \vee (\forall x \psi) \\ \forall x (\phi \wedge \psi) &\Leftrightarrow \phi \wedge (\forall x \psi) \\ \exists x (\phi \vee \psi) &\Leftrightarrow \phi \vee (\exists x \psi) \\ \exists x (\phi \wedge \psi) &\Leftrightarrow \phi \wedge (\exists x \psi)\end{aligned}$$

są prawami rachunku kwantyfikatorów.

Niech ϕ i ψ oznaczają formuły rachunku kwantyfikatorów być może zawierające wolne wystąpienia zmiennej x . W poniższych zadaniach sprawdź, które z podanych formuł są prawami rachunku kwantyfikatorów.

Zadanie 89. $(\forall x (\phi \vee \psi)) \Rightarrow (\forall x \phi) \vee (\forall x \psi)$

Zadanie 90. $(\forall x \phi) \vee (\forall x \psi) \Rightarrow (\forall x (\phi \vee \psi))$

Zadanie 91. $(\forall x (\phi \wedge \psi)) \Rightarrow (\forall x \phi) \wedge (\forall x \psi)$

Zadanie 92. $((\forall x \phi) \Rightarrow (\forall x \psi)) \Rightarrow (\forall x (\phi \Rightarrow \psi))$

Zadanie 93. $(\forall x (\phi \Rightarrow \psi)) \Rightarrow (\exists x \phi) \Rightarrow (\forall x \psi)$

Zadanie 94. $((\exists x \phi) \Rightarrow (\forall x \psi)) \Rightarrow (\forall x (\phi \Rightarrow \psi))$

Zadanie 95. $(\exists x \phi) \wedge (\exists x \psi) \Rightarrow (\exists x (\phi \wedge \psi))$

Zadanie 96. $(\exists x (\phi \wedge \psi)) \Rightarrow (\exists x \phi) \wedge (\exists x \psi)$

Zadanie 97. $((\exists x \phi) \Rightarrow (\exists x \psi)) \Rightarrow (\exists x (\phi \Rightarrow \psi))$

Zadanie 98. $(\exists x (\phi \Rightarrow \psi)) \Rightarrow (\exists x \phi) \Rightarrow (\exists x \psi)$

Zadanie 99. $((\forall x \phi) \Rightarrow (\exists x \psi)) \Rightarrow (\exists x (\phi \Rightarrow \psi))$

Zadanie 100. $(\exists x (\phi \Rightarrow \psi)) \Rightarrow (\forall x \phi) \Rightarrow (\exists x \psi)$

Zadanie 101. $((\forall x \phi) \Leftrightarrow \neg(\forall x \psi)) \Rightarrow \exists x (\phi \Leftrightarrow \neg\psi)$

Zadanie 102. $\exists x (\phi \Leftrightarrow \neg\psi) \Rightarrow ((\forall x \phi) \Leftrightarrow \neg(\forall x \psi))$

Zadanie 103. $\forall x \phi \Rightarrow \exists x \phi$

Zadanie 104. $\exists x \phi \Rightarrow \forall x \phi$

Niech ϕ oznacza formułę rachunku kwantyfikatorów zawierającą być może wolne wystąpienia zmiennych x i y . W poniższych zadaniach sprawdź, które z podanych formuł są prawami rachunku kwantyfikatorów.

Zadanie 105. $(\forall x \exists y \phi) \Rightarrow (\exists y \forall x \phi)$

Zadanie 106. $(\exists y \forall x \phi) \Rightarrow (\forall x \exists y \phi)$

Niech ϕ i ψ oznaczać formuły rachunku kwantyfikatorów, przy czym zmienna x nie ma wolnych wystąpień w formule ϕ (lecz może mieć w ψ). W poniższych zadaniach sprawdź, czy podane formuły są równoważne.

Zadanie 107. $\forall x (\phi \Rightarrow \psi)$ oraz $\phi \Rightarrow (\forall x \psi)$

Zadanie 108. $\forall x (\phi \Rightarrow \psi)$ oraz $\phi \Rightarrow (\exists x \psi)$

Zadanie 109. $\forall x (\psi \Rightarrow \phi)$ oraz $(\forall x \psi) \Rightarrow \phi$

Zadanie 110. $\forall x (\psi \Rightarrow \phi)$ oraz $(\exists x \psi) \Rightarrow \phi$

Zadanie 111. $\forall x (\phi \Leftrightarrow \psi)$ oraz $\phi \Leftrightarrow (\forall x \psi)$

Zadanie 112. $\forall x (\phi \Leftrightarrow \psi)$ oraz $\phi \Leftrightarrow (\exists x \psi)$

Zadanie 113. $\exists x (\phi \Rightarrow \psi)$ oraz $\phi \Rightarrow (\exists x \psi)$

Zadanie 114. $\exists x (\phi \Rightarrow \psi)$ oraz $\phi \Rightarrow (\forall x \psi)$

Zadanie 115. $\exists x (\psi \Rightarrow \phi)$ oraz $(\exists x \psi) \Rightarrow \phi$

Zadanie 116. $\exists x (\psi \Rightarrow \phi)$ oraz $(\forall x \psi) \Rightarrow \phi$

Zadanie 117. $\exists x (\phi \Leftrightarrow \psi)$ oraz $\phi \Leftrightarrow (\exists x \psi)$

Zadanie 118. $\exists x (\phi \Leftrightarrow \psi)$ oraz $\phi \Leftrightarrow (\forall x \psi)$

1.9. Formalizacja wypowiedzi w języku rachunku kwantyfikatorów

Formuła ϕ jest w *postaci normalnej*, jeśli jest postaci $Q_1x_1 \dots Q_nx_n\psi$, gdzie x_i są pewnymi zmiennymi, Q_i są kwantyfikatorami ($Q_i \in \{\forall, \exists\}$ dla $i = 1, \dots, n$), a formuła ψ nie zawiera kwantyfikatorów i symbol negacji występuje w niej jedynie przed formułami atomowymi. Przykładem formuły w postaci normalnej jest $\forall x \exists y (x \neq y \vee \neg x \leq y)$. Formuła $\forall x \exists y \exists z \neg (z = y \vee y = z)$ nie jest w postaci normalnej.

Zadanie 119. Dla każdej z formuł poniżej podaj równoważną formułę w postaci normalnej

$$1. \forall x_0 \in \mathbb{R} \forall \epsilon > 0 \exists \delta > 0 \forall x \in \mathbb{R} (|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon)$$

$$2. \forall \epsilon > 0 \exists \delta > 0 \forall x \in \mathbb{R} (0 < |x - x_0| < \delta \Rightarrow |f(x) - g| < \epsilon)$$

Zadanie 120. Funkcja $f : \mathbb{N} \rightarrow \mathbb{N}$ jest *słabo rosnąca*, jeśli prawdziwa jest formuła

$$\forall x \forall y (x \leq y \Rightarrow f(x) \leq f(y)).$$

Funkcja $f : \mathbb{N} \rightarrow \mathbb{N}$ jest *słabo malejąca*, jeśli prawdziwa jest formuła

$$\forall x \forall y (x \leq y \Rightarrow f(y) \leq f(x)).$$

Zapisz poniższe zdania jako formuły w postaci normalnej:

1. funkcja f jest słabo rosnąca i słabo malejąca,
2. funkcja f nie jest słabo rosnąca i nie jest słabo malejąca.

Zadanie 121. Przy pomocy symboli $=, \leq, +, \times$, spójników logicznych i kwantyfikatorów zapisz następujące formuły dotyczące liczb naturalnych:

1. liczba x jest najmniejszą wspólną wielokrotnością y i z ,
2. każda liczba nieparzysta większa od 3 jest sumą dwóch liczb pierwszych,
3. nie istnieje największa liczba pierwsza,
4. liczby x i y mają takie same dzielniki pierwsze.

Przykład: formułę „ x jest sumą dwóch kwadratów liczb naturalnych” zapiszemy jako $\exists y \exists z (x = y \times y + z \times z)$.

Zadanie 122. Niech funkcja g będzie dla $n \in \mathbb{N}$ określona następująco:

$$g(n) = \begin{cases} n/2, & \text{gdy } n \text{ jest parzyste,} \\ 3n + 1, & \text{gdy } n \text{ jest nieparzyste.} \end{cases}$$

Używając symboli z zadania 121 oraz dodatkowo symbolu potęgowania $\uparrow$, zapisz zdanie równoważne zdaniu „dla każdej liczby naturalnej m istnieje taka liczba n , że $g^n(m) = 1$ ”, gdzie g^n oznacza funkcję g złożoną ze sobą n razy, na przykład $g^2(3) = 5$. *Wskazówka:* ciąg skończony liczb naturalnych $a_1, a_2, \dots, a_m$ możemy zakodować jako jedną liczbę $2^{a_1} 3^{a_2} \dots p_m^{a_m}$, gdzie p_i jest i -tą liczbą pierwszą.

Zadanie 123. Używając tylko kwantyfikatorów, zmiennych, nawiasów, spójników logicznych oraz symboli $\in, \mathbb{N}, +, \times, =, i \leq$ napisz formułę mówiącą, że wśród każdych trzech liczb naturalnych zawsze znajdują się dwie, których różnica jest nieujemna i parzysta. Czy taką formułę można zapisać używając wyłącznie kwantyfikatorów, zmiennych, nawiasów, spójników logicznych oraz symboli $\in, \mathbb{N}, +, i =$?

Używając tylko kwantyfikatorów, zmiennych, nawiasów, spójników logicznych oraz symboli $\in, \mathbb{N}, +, \times, =, <$ i symbolu f napisz formułę mówiącą, że jeśli funkcja $f: \mathbb{N} \rightarrow \mathbb{N}$ jest silnie rosnąca (dla większych argumentów ma większe wartości), to jej wartości są nieograniczone.

Zadanie 124. Liczbę naturalną q nazywamy *liczbą bliźniaczą*, jeżeli liczby q oraz $q+2$ są pierwsze. Używając symboli $+, \times, 0, 1, 2$ oraz nawiasów, zmiennych, kwantyfikatorów i spójników logicznych zapisz formalnie zdanie: „Istnieje największa liczba bliźniacza taka, że pomiędzy nią a poprzednią liczbą bliźniaczą jest co najwyżej jedna liczba pierwsza.”

Zadanie 125. Niech na pewnym skończonym zbiorze X będzie określona binarna relacja R . Mówimy, że zbiór X z relacją R jest *hamiltonowski*, jeśli istnieje taki ciąg elementów zbioru X , że każdy element zbioru X występuje w tym ciągu dokładnie raz, każde dwa kolejne elementy ciągu są ze sobą w relacji R , oraz ostatni element ciągu jest w relacji z pierwszym elementem ciągu. Używając jedynie poniższych słów i zwrotów (z odpowiednią odmianą) wyraż słownie, co to znaczy, że zbiór X wraz z relacją R nie jest hamiltonowski:

R	istnieje	pierwszy
X	każdy	raz
ciąg	kolejny	taki, że
dla	który	ten
dokładnie	lub	truskawka
dwa	moc	w
element	nie jest w relacji	występować
i	ostatni	zbiór

Zadanie 126. Po egzaminie z logiki studenci wybrali się na dyskotekę, w której bawi się pewna liczba pań i dżentelmenów. Niech

ϕ_1 oznacza, że każdy dżentelmen zna co najwyżej dwie panie,
 ϕ_2 oznacza, że każda pani zna co najwyżej dwóch dżentelmenów,
 ϕ_3 oznacza, że każdy dżentelmen zna co najmniej dwie panie,
 ϕ_4 oznacza, że żadne dwie panie nie znają dokładnie tych samych dżentelmenów.

Zapisz zdania ϕ_1 , ϕ_2 , ϕ_3 i ϕ_4 używając symboli zbiorów P i D oraz symbolu relacji $Z \subseteq (P \cup D)^2$, takich, że

$x \in P$	oznacza, że x jest panią,
$x \in D$	oznacza, że x jest dżentelmenem,
$Z(x, y)$	oznacza, że x zna y ,

oraz równości $=$ i spójników logicznych oraz kwantyfikatorów.

2

Zbiory

W teorii mnogości *zbiór* i *relację* $\in$ należenia do zbioru przyjmujemy za pojęcia pierwotne. Własności zbiorów i relacji $\in$ są zadane przez *aksjomaty*, tj. zdania, które przyjmujemy za prawdziwe bez dowodu.

Aksjomat 30 (zasada ekstensjonalności). Dwa zbiory są *równe*, jeżeli zawierają dokładnie te same elementy, tj. $A = B$ wtedy i tylko wtedy, gdy prawdziwa jest formuła

$$\forall x (x \in A \Leftrightarrow x \in B).$$

Definicja 31. *Zbiór pusty* $\emptyset$ jest zbiorem nie zawierającym żadnego elementu. Prawdziwa jest formuła

$$\forall x (x \notin \emptyset).$$

Aksjomat 32 (zbioru pustego). Zbiór pusty istnieje.

Zauważmy, że na mocy zasady ekstensjonalności istnieje dokładnie jeden zbiór pusty.

Definicja 33. Zbiór A jest *podzbiorem* zbioru B , co będziemy zapisywać $A \subseteq B$, jeżeli B zawiera wszystkie elementy zbioru A , tj. zachodzi

$$\forall x (x \in A \Rightarrow x \in B).$$

Zauważmy, że na mocy zasady ekstensjonalności dwa zbiory są równe wtedy i tylko wtedy, gdy są nawzajem swoimi podzbiarami, tj. $A = B$ wtedy i tylko wtedy, gdy $A \subseteq B$ oraz $B \subseteq A$.

Definicja 34. Napisy $\{x \mid \phi\}$ i $\{x : \phi\}$ oznaczają zbiór tych elementów x , które spełniają formułę ϕ . Będziemy również pisać $x \in A \stackrel{\text{df}}{\Leftrightarrow} \phi$ zamiast $A = \{x \mid \phi\}$.

Przykład 35. Napis $\{n \mid \exists m \in \mathbb{N} (n = 3m)\}$ oznacza zbiór liczb naturalnych podzielnych przez 3.

Definicja 36. Rodzinę wszystkich podzbiorów zbioru A nazywamy *zbiorem potęgowym* zbioru A i oznaczamy $\mathcal{P}(A)$. Możemy napisać:

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

2.1. Działania na zbiorach

Definicja 37. Na zbiorach wprowadzamy operacje *sumy* $\cup$, *przekroju* $\cap$ i *różnicy* $\setminus$:

$$\begin{aligned} x \in A \cup B & \stackrel{\text{df}}{\Leftrightarrow} x \in A \vee x \in B \\ x \in A \cap B & \stackrel{\text{df}}{\Leftrightarrow} x \in A \wedge x \in B \\ x \in A \setminus B & \stackrel{\text{df}}{\Leftrightarrow} x \in A \wedge x \notin B \end{aligned}$$

Powyższe operacje mają wiele ciekawych własności. Dla przykładu:

Fakt 38 (prawa rozdzielności).

$$\begin{aligned} A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \end{aligned}$$

Dowód. Udowodnimy pierwsze z nich. Na mocy prawa ekstensjonalności wystarczy pokazać, że dla każdego x zachodzi

$$x \in A \setminus (B \cup C) \Leftrightarrow x \in (A \setminus B) \cap (A \setminus C).$$

Równoważność tę pokażemy rozpoczynając od formuły $x \in A \setminus (B \cup C)$, przechodząc przez szereg formuł równoważnych i kończąc na $x \in (A \setminus B) \cap (A \setminus C)$. Z definicji różnicy zbiorów wiemy, że formuła

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

jest równoważna formule

$$x \in A \wedge \neg(x \in B \cup C).$$

Następnie korzystając z definicji sumy zbiorów otrzymujemy równoważną formułę

$$x \in A \wedge \neg(x \in B \vee x \in C).$$

Korzystając z prawa de Morgana $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ otrzymujemy

$$x \in A \wedge (x \notin B \wedge x \notin C).$$

Na mocy tautologii $p \Leftrightarrow (p \wedge p)$ możemy do formuły dopisać jeszcze jedno wystąpienie $x \in A$.

$$x \in A \wedge x \in A \wedge (x \notin B \wedge x \notin C).$$

Ponadto koniunkcja jest łączna i przemienna, możemy zatem dowolnie pogrupować jej czynniki:

$$(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C).$$

Korzystając dwukrotnie z definicji różnicy zbiorów dostajemy

$$(x \in A \setminus B) \wedge (x \in A \setminus C).$$

Na mocy definicji przekroju zbiorów mamy ostatecznie

$$x \in (A \setminus B) \cap (A \setminus C).$$

Twierdzenie jest zatem udowodnione. ■

Zadanie 127. Pokaż, że dla dowolnych zbiorów A , B i C zachodzą podane równości.

$$\begin{aligned} A \cup B &= B \cup A \\ A \cap B &= B \cap A \\ (A \cup B) \cup C &= A \cup (B \cup C) \\ (A \cap B) \cap C &= A \cap (B \cap C) \\ (A \cup B) \cap C &= (A \cap C) \cup (B \cap C) \\ (A \cap B) \cup C &= (A \cup C) \cap (B \cup C) \\ (A \cup B) \setminus C &= (A \setminus C) \cup (B \setminus C) \\ A \setminus (B \cup C) &= (A \setminus B) \setminus C \\ (A \cap B) \setminus C &= (A \setminus C) \cap (B \setminus C) \\ A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C) \end{aligned}$$

Zadanie 128. Pokaż, że dla dowolnych zbiorów A , B , C i D zachodzą podane równości.

$$\begin{aligned} (A \setminus B) \cup C &= (A \cup C) \setminus (B \setminus C) \\ (A \setminus B) \cap C &= (A \cap C) \setminus B \\ A \setminus (B \setminus C) &= (A \setminus B) \cup (A \cap C) \\ A \cup (B \setminus C) &= ((A \cup B) \setminus C) \cup (A \cap C) \\ A \setminus (B \setminus (C \setminus D)) &= (A \setminus B) \cup ((A \cap C) \setminus D) \\ (A \setminus B) \cap (C \setminus D) &= (A \cap C) \setminus (B \cup D) \\ \emptyset \cap A &= \emptyset \\ \emptyset \cup A &= A \\ \emptyset \setminus A &= \emptyset \\ A \setminus \emptyset &= A \end{aligned}$$

Zadanie 129. Czy dla dowolnych zbiorów A , B i C zachodzą podane równości?

$$\begin{aligned}
 (A \cup B) \setminus B &= A \\
 A \cup (A \cap B) &= A \\
 A \cap (A \cup B) &= A \\
 (A \setminus B) \setminus (B \setminus A) &= A \\
 A \setminus (B \cap A) &= A \\
 A \setminus (B \setminus A) &= A \\
 A \cup (B \setminus C) &= (A \cup B) \setminus C \\
 A \cap (B \setminus C) &= (A \cap B) \setminus C \\
 A \setminus (B \setminus C) &= (A \setminus B) \setminus C \\
 A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C)
 \end{aligned}$$

Zadanie 130. Pokaż, że dla dowolnych takich zbiorów A , B , C i D , że $A \subseteq B$ i $C \subseteq D$ zachodzą podane inkluzje.

$$\begin{aligned}
 A \cup C &\subseteq B \cup D \\
 A \cap C &\subseteq B \cap D \\
 A \setminus D &\subseteq B \setminus C
 \end{aligned}$$

Zadanie 131. Wykaż, że dla dowolnych zbiorów A , B , C i D zachodzi:

$$A \cap B \cap C \cap D \subseteq ((A \cap B) \cup C) \cap D.$$

Zadanie 132. Czy dla dowolnych zbiorów A , B i C zachodzą poniższe inkluzje?

$$\begin{aligned}
 A \cap (B \cup C) &\subseteq B \cap (A \cup C) \\
 A \cap (B \setminus C) &\subseteq B \cap (A \setminus C)
 \end{aligned}$$

W poniższych zadaniach przyjmij, że zbiory A , B i C spełniają podaną równość. Wymień wszystkie inkluzje między zbiorami A , B i C , które wynikają z podanej zależności (oprócz oczywistych inkluzji postaci $X \subseteq X$), i udowodnij, że wymienileś wszystkie takie inkluzje.

Zadanie 133. $(A \cup B) \setminus C = (A \setminus C) \cup B$

Zadanie 134. $(A \cup B) \setminus (B \cap C) = A \cap C$

Zadanie 135. $((A \cap B) \cup C) \setminus A = (A \cap B) \setminus C$

Zadanie 136. $(A \setminus C) \cup B = A \cup B$

Zadanie 137. $(A \cap B) \cup (C \cap B) = B$

Zadanie 138. $(A \cup B) \cap (C \cup B) = B$

Zadanie 139. Pokaż, że jeżeli dla pewnych zbiorów A i B jest $A \setminus B = B \setminus A$, to $A = B$.

Zadanie 140. Udowodnij, że dla dowolnych zbiorów A i B następujące formuły są równoważne

$$A \subseteq B, \quad A \cup B = B, \quad A \cap B = A, \quad A \setminus B = \emptyset.$$

Zadanie 141. Niech A , B i C będą dowolnymi zbiorami. Udowodnij, że $A \subseteq A \cup B$ i $B \subseteq A \cup B$. Udowodnij, że jeśli $A \subseteq C$ oraz $B \subseteq C$, to $A \cup B \subseteq C$. Innymi słowy suma zbiorów A i B jest najmniejszym (w sensie inkluzji) zbiorem zawierającym zbiory A i B .

Zadanie 142. Niech A , B i C będą dowolnymi zbiorami. Udowodnij, że $A \cap B \subseteq A$ i $A \cap B \subseteq B$. Udowodnij, że jeśli $C \subseteq A$ oraz $C \subseteq B$, to $C \subseteq A \cap B$. Innymi słowy przekrój zbiorów A i B jest największym (w sensie inkluzji) zbiorem zawartym w zbiorach A i B .

Zadanie 143. Niech A , B i C będą dowolnymi zbiorami. Udowodnij, że $A \setminus B \subseteq A$ i $(A \setminus B) \cap B = \emptyset$. Udowodnij, że jeśli $C \subseteq A$ oraz $C \cap B = \emptyset$, to $C \subseteq A \setminus B$. Innymi słowy różnica zbiorów A i B jest największym (w sensie inkluzji) zbiorem zawartym w A i rozłącznym z B .

Definicja 39. *Różnicę symetryczną* $\dot{-}$ zbiorów A i B definiujemy następująco:

$$x \in A \dot{-} B \stackrel{\text{df}}{\Leftrightarrow} x \in A \Leftrightarrow x \notin B.$$

Zadanie 144. Pokaż, że różnica symetryczna jest operacją *łączną* i *przemenną*, tj. że

$$(A \dot{-} B) \dot{-} C = A \dot{-} (B \dot{-} C) \quad \text{oraz} \quad A \dot{-} B = B \dot{-} A$$

dla dowolnych zbiorów A , B i C . Pokaż także następujące tożsamości:

$$A \dot{-} \emptyset = A, \quad A \dot{-} A = \emptyset \quad \text{oraz} \quad A \cap (B \dot{-} C) = (A \cap B) \dot{-} (A \cap C).$$

Zadanie 145. Udowodnij, że

$$A \dot{-} B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Zadanie 146. Wśród poniższych zdań wskaż zdania prawdziwe i udowodnij je. Dla pozostałych zdań podaj kontrprzykłady dowodzące, że zdania te nie są prawdziwe.

1. Równość $A \cap B = A \cap C$ implikuje równość $B = C$.
2. Równości $A \cap B = A \cap C$ oraz $A \cup B = A \cup C$ implikują równość $B = C$.
3. Inkluzja $A \cup B \subseteq A \cap B$ implikuje równość $A = B$.
4. Równość $A \div B = A \div C$ implikuje równość $B = C$.
5. Równość $A \div B = \emptyset$ implikuje równość $A = B$.

Zadanie 147. Czy istnieją niepuste zbiory A i B takie, że

$$A \subseteq A \div B \subseteq A \setminus B?$$

Zadanie 148. Czy dla dowolnych zbiorów A i B zachodzą równości:

$$\begin{aligned} A \cup (B \div C) &= (A \cup B) \div (A \cup C), \\ A \cup B &= (A \div B) \div (A \cap B)? \end{aligned}$$

2.2. Operacje nieskończone na zbiorach

Definicja 40. Rodziną zbiorów indeksowaną elementami zbioru S nazywamy odwzorowanie, które każdemu elementowi $s \in S$ przyporządkowuje pewien zbiór A_s . Rodzinę zbiorów oznaczamy $\{A_s\}_{s \in S}$. Rodziną zbiorów $\{A_{s,t}\}_{s \in S, t \in T}$ indeksowaną elementami dwóch zbiorów S i T nazywamy odwzorowanie, które każdej parze $\langle s, t \rangle$, gdzie $s \in S$ oraz $t \in T$ przyporządkowuje pewien zbiór $A_{s,t}$. Jeżeli $S = \{i \in \mathbb{N} \mid i \geq n\}$, to zamiast $\{A_i\}_{i \in S}$ piszemy też $\{A_i\}_{i=n}^\infty$. Jeżeli $S = \{n, \dots, m\}$, to zamiast $\{A_i\}_{i \in S}$ piszemy też $\{A_i\}_{i=n}^m$.

Definicja 41. Dwuargumentowe operacje sumy i przekroju zbiorów można rozszerzyć na dowolne rodziny zbiorów. Suma wszystkich zbiorów z rodziny $\{A_s\}_{s \in S}$ jest zbiorem zawierającym elementy występujące w którymkolwiek ze zbiorów A_s . Podobnie przekrój tej rodziny jest zbiorem zawierającym elementy występujące w każdym ze zbiorów A_s . Formalnie:

$$\begin{aligned} x \in \bigcup_{s \in S} A_s &\stackrel{\text{df}}{\Leftrightarrow} \exists s \in S (x \in A_s), \\ x \in \bigcap_{s \in S} A_s &\stackrel{\text{df}}{\Leftrightarrow} \forall s \in S (x \in A_s). \end{aligned}$$

Czasem zbiór indeksów nie jest istotny dla naszych rozważań i wtedy piszemy po prostu $\bigcup \mathcal{A}$ oraz $\bigcap \mathcal{A}$ dla oznaczenia odpowiednio sumy i przekroju rodziny zbiorów $\mathcal{A}$. Notację tę można sformalizować przyjmując konwencję, że rodzina $\mathcal{A}$ jest indeksowana swoimi elementami, czyli zamiast $\{X\}_{X \in \mathcal{A}}$ piszemy $\mathcal{A}$. Wtedy $\bigcup \mathcal{A} = \bigcup_{X \in \mathcal{A}} X$ oraz $\bigcap \mathcal{A} = \bigcap_{X \in \mathcal{A}} X$.

W poniższych zadaniach udowodnij, że dla dowolnych rodzin zbiorów $\{A_t\}_{t \in T}$, $\{B_t\}_{t \in T}$, gdzie T jest niepustym zbiorem indeksów, zachodzą podane relacje. W których przypadkach zachodzi inkluzja odwrotna?

$$\text{Zadanie 149. } \bigcup_{t \in T} (A_t \cup B_t) = \bigcup_{t \in T} A_t \cup \bigcup_{t \in T} B_t$$

$$\text{Zadanie 150. } \bigcap_{t \in T} (A_t \cap B_t) = \bigcap_{t \in T} A_t \cap \bigcap_{t \in T} B_t$$

$$\text{Zadanie 151. } \bigcup_{t \in T} (A_t \cap B_t) \subseteq \bigcup_{t \in T} A_t \cap \bigcup_{t \in T} B_t$$

$$\text{Zadanie 152. } \bigcap_{t \in T} A_t \cup \bigcap_{t \in T} B_t \subseteq \bigcap_{t \in T} (A_t \cup B_t)$$

$$\text{Zadanie 153. } \bigcap_{t \in T} A_t \cup \bigcap_{t \in T} B_t \subseteq \bigcup_{t \in T} (A_t \cup B_t)$$

$$\text{Zadanie 154. } \bigcap_{t \in T} (A_t \cup B_t) \subseteq \bigcup_{t \in T} A_t \cup \bigcup_{t \in T} B_t$$

$$\text{Zadanie 155. } \bigcap_{t,s \in T} (A_t \cup B_s) \subseteq \bigcap_{t \in T} (A_t \cup B_t)$$

$$\text{Zadanie 156. } \bigcup_{t \in T} (A_t \cap B_t) \subseteq \bigcup_{t,s \in T} (A_t \cap B_s)$$

$$\text{Zadanie 157. } \bigcup_{t \in T} (A_t \setminus B_t) \subseteq \bigcup_{t \in T} A_t \setminus \bigcap_{t \in T} B_t$$

$$\text{Zadanie 158. } \bigcap_{t \in T} (A_t \setminus B_t) = \bigcap_{t \in T} A_t \setminus \bigcup_{t \in T} B_t$$

W poniższych zadaniach udowodnij, że dla dowolnego zbioru A i dowolnej rodziny zbiorów $\{B_t\}_{t \in T}$, gdzie T jest niepustym zbiorem indeksów, zachodzą podane równości.

$$\text{Zadanie 159. } \bigcup_{t \in T} (A \cup B_t) = A \cup \bigcup_{t \in T} B_t$$

$$\text{Zadanie 160. } \bigcap_{t \in T} (A \cup B_t) = A \cup \bigcap_{t \in T} B_t$$

$$\text{Zadanie 161. } \bigcup_{t \in T} (A \cap B_t) = A \cap \bigcup_{t \in T} B_t$$

$$\text{Zadanie 162. } \bigcap_{t \in T} (A \cap B_t) = A \cap \bigcap_{t \in T} B_t$$

W poniższych zadaniach udowodnij, że dla dowolnej rodziny zbiorów $\{A_{t,s}\}_{t \in T, s \in S}$, gdzie T i S są niepustymi zbiorami indeksów, zachodzą podane relacje. Czy zachodzą inkluzje odwrotne?

Zadanie 163. $\bigcup_{t \in T} \bigcup_{s \in S} A_{t,s} = \bigcup_{s \in S} \bigcup_{t \in T} A_{t,s}$

Zadanie 164. $\bigcap_{t \in T} \bigcap_{s \in S} A_{t,s} = \bigcap_{s \in S} \bigcap_{t \in T} A_{t,s}$

Zadanie 165. $\bigcup_{t \in T} \bigcap_{s \in S} A_{t,s} \subseteq \bigcap_{s \in S} \bigcup_{t \in T} A_{t,s}$

W poniższych zadaniach udowodnij, że dla dowolnej rodziny zbiorów $\{A_{t,s}\}_{t,s \in T}$, gdzie T jest niepustym zbiorem indeksów, zachodzą podane relacje. Czy zachodzą inkluzje odwrotne?

Zadanie 166. $\bigcup_{t \in T} A_{t,t} \subseteq \bigcup_{t \in T} \bigcup_{s \in T} A_{t,s}$

Zadanie 167. $\bigcap_{t \in T} \bigcap_{s \in T} A_{t,s} \subseteq \bigcap_{t \in T} A_{t,t}$

W poniższych zadaniach udowodnij, że dla dowolnych rodzin zbiorów $\{A_t\}_{t \in T}$, $\{B_s\}_{s \in S}$, gdzie T i S są niepustymi zbiorami indeksów, zachodzą podane równości.

Zadanie 168. $\bigcup_{t \in T} A_t \cup \bigcup_{s \in S} B_s = \bigcup_{t \in T} \bigcup_{s \in S} (A_t \cup B_s)$

Zadanie 169. $\bigcup_{t \in T} A_t \cap \bigcup_{s \in S} B_s = \bigcup_{t \in T} \bigcup_{s \in S} (A_t \cap B_s)$

Zadanie 170. $\bigcap_{t \in T} A_t \cup \bigcap_{s \in S} B_s = \bigcap_{t \in T} \bigcap_{s \in S} (A_t \cup B_s)$

Zadanie 171. $\bigcap_{t \in T} A_t \cap \bigcap_{s \in S} B_s = \bigcap_{t \in T} \bigcap_{s \in S} (A_t \cap B_s)$

W poniższych zadaniach udowodnij, że dla dowolnej rodziny zbiorów $\{A_n\}_{n=0}^{\infty}$ zachodzą podane relacje. W których przypadkach zachodzi inkluzja odwrotna?

Zadanie 172. $\bigcap_{n=0}^{\infty} A_n \subseteq \bigcup_{n=0}^{\infty} \bigcap_{k=n}^{\infty} A_k$

Zadanie 173. $\bigcup_{n=0}^{\infty} \bigcap_{k=n}^{\infty} A_k \subseteq \bigcap_{n=0}^{\infty} \bigcup_{k=n}^{\infty} A_k$

Zadanie 174. $\bigcap_{n=0}^{\infty} \bigcup_{k=n}^{\infty} A_k \subseteq \bigcup_{n=0}^{\infty} A_n$

Zadanie 175. $\bigcup_{n=0}^{\infty} A_{n+1} \subseteq \bigcup_{n=0}^{\infty} (A_{n+1} \setminus \bigcup_{m=1}^n A_m)$

Zadanie 176. $\bigcup_{n=0}^m A_n = \left(\bigcup_{n=0}^{m-1} (A_n \setminus A_{n+1}) \right) \cup (A_m \setminus A_0) \cup \bigcap_{n=0}^m A_n$

Zadanie 177. $\bigcup_{n=0}^{\infty} A_n = \left(\left(\bigcup_{n=0}^{\infty} A_n \right) \setminus A_0 \right) \cup \left(\bigcup_{n=1}^{\infty} (A_n \setminus A_{n+1}) \right) \cup \bigcap_{n=0}^{\infty} A_n$

Definicja 42. Rodzina zbiorów $\{A_n\}_{n \in \mathbb{N}}$ jest *zstępująca*, jeżeli $A_{n+1} \subseteq A_n$ dla każdego $n \in \mathbb{N}$ i *wstępująca*, jeżeli $A_n \subseteq A_{n+1}$ dla każdego $n \in \mathbb{N}$.

Zadanie 178. Udowodnij, że jeśli $\{A_n\}_{n \in \mathbb{N}}$ i $\{B_n\}_{n \in \mathbb{N}}$ są zstępującymi rodzinami zbiorów, to

$$\bigcap_{i \in \mathbb{N}} (A_i \cup B_i) = \left(\bigcap_{i \in \mathbb{N}} A_i \right) \cup \left(\bigcap_{i \in \mathbb{N}} B_i \right).$$

Wskaż przykład rodzin $\{A_n\}_{n \in \mathbb{N}}$ i $\{B_n\}_{n \in \mathbb{N}}$ dla których równość powyższa nie zachodzi. Czy równość powyższa zachodzi dla rodzin wstępujących?

Zadanie 179. Udowodnij, że jeśli $\{A_n\}_{n \in \mathbb{N}}$ i $\{B_n\}_{n \in \mathbb{N}}$ są wstępującymi rodzinami zbiorów, to

$$\bigcup_{i \in \mathbb{N}} (A_i \cap B_i) = \left(\bigcup_{i \in \mathbb{N}} A_i \right) \cap \left(\bigcup_{i \in \mathbb{N}} B_i \right).$$

Wskaż przykład rodzin $\{A_n\}_{n \in \mathbb{N}}$ i $\{B_n\}_{n \in \mathbb{N}}$ dla których równość powyższa nie zachodzi. Czy równość powyższa zachodzi dla rodzin zstępujących?

Zadanie 180. Udowodnij, że jeśli $\{A_n\}_{n \in \mathbb{N}}$ jest zstępującą rodziną zbiorów, to

$$\bigcup_{n \in \mathbb{N}} (A_{2n+1} \setminus A_{2n+2}) \cup \bigcap_{n \in \mathbb{N}} A_n = A_0 \setminus \bigcup_{n \in \mathbb{N}} (A_{2n} \setminus A_{2n+1}).$$

Zadanie 181. Udowodnij, że jeśli $\{A_n\}_{n \in \mathbb{N}}$ jest zstępującą rodziną zbiorów, to

$$\bigcup_{n=0}^{\infty} \bigcap_{i=0}^n A_i = \bigcap_{n=0}^{\infty} \bigcup_{i=0}^n A_i.$$

Zadanie 182. Udowodnij, że jeśli $\{A_n\}_{n \in \mathbb{N}}$ jest wstępującą rodziną zbiorów, to

$$\bigcup_{n=0}^{\infty} \bigcap_{i=0}^n A_i = \bigcap_{n=0}^{\infty} \bigcup_{i=0}^n A_i.$$

Zadanie 183. Udowodnij, że jeśli $\{A_n\}_{n \in \mathbb{N}}$ jest zstępującą rodziną zbiorów, to

$$\bigcup_{n=0}^{\infty} \bigcap_{i=n}^{\infty} A_i = \bigcap_{n=0}^{\infty} \bigcup_{i=n}^{\infty} A_i = \bigcap_{n=0}^{\infty} A_n.$$

Zadanie 184. Udowodnij, że jeśli $\{A_n\}_{n \in \mathbb{N}}$ jest wstępującą rodziną zbiorów, to

$$\bigcup_{n=0}^{\infty} \bigcap_{i=n}^{\infty} A_i = \bigcap_{n=0}^{\infty} \bigcup_{i=n}^{\infty} A_i = \bigcup_{n=0}^{\infty} A_n.$$

Zadanie 185. Niech $\{A_{n,m}\}_{n,m=0}^{\infty}$ będzie rodziną zbiorów indeksowaną parami liczb naturalnych. Pokaż, że jeśli

$$A_{n,m} \subseteq A_{n+1,m} \cap A_{n,m+1}$$

dla wszelkich n i m , to

$$\bigcup_{n=0}^{\infty} \bigcup_{m=0}^{\infty} A_{n,m} = \bigcup_{n=0}^{\infty} A_{n,n}.$$

Zadanie 186. Dane są rodziny zbiorów $\{A_i\}_{i \in \mathbb{N}}$ i $\{B_i\}_{i \in \mathbb{N}}$. Wiadomo, że dla każdego i istnieje k takie, że $A_i \subseteq \bigcup_{j=0}^k B_j$. Udowodnij, że:

1. dla każdego i istnieje takie k , że $\bigcup_{j=0}^i A_j \subseteq \bigcup_{j=0}^k B_j$,
2. $\bigcup_{i=0}^{\infty} A_i \subseteq \bigcup_{i=0}^{\infty} B_i$.

Zadanie 187. Rozważmy dowolną rodzinę zbiorów $\mathcal{A}$.

1. Udowodnij, że $\mathcal{A} \subseteq \mathcal{P}(\bigcup \mathcal{A})$.
2. Udowodnij, że $\mathcal{P}(\bigcup \mathcal{A}) \subseteq \mathcal{A}$ wtedy i tylko wtedy, gdy istnieje taki zbiór B , że $\mathcal{A} = \mathcal{P}(B)$.

3

Relacje

3.1. Para uporządkowana i iloczyn (produkt) kartezjański

Parę uporządkowaną (w skrócie *parę*) elementów a i b będziemy zapisywać w postaci $\langle a, b \rangle$. Para będzie dla nas pojęciem pierwotnym. Przyjmujemy, że spełnia ona następujący aksjomat.

Aksjomat 43. $\langle a, b \rangle = \langle c, d \rangle$ wtedy i tylko wtedy, gdy $a = c$ oraz $b = d$.

Aby określić parę uporządkowaną wystarczy podać dwuelementowy zbiór jej elementów i wskazać, który z nich jest pierwszy. Specjaliści od podstaw matematyki pragną za pojęcia pierwotne uważać jedynie zbiór i relację należenia do zbioru i dlatego wolą *zdefiniować* parę następująco:

$$\langle a, b \rangle = \{\{a\}, \{a, b\}\}.$$

Zadanie 188. Udowodnij, że zdefiniowana wyżej para $\langle a, b \rangle$ spełnia aksjomat 43.

Definicja 44. *Iloczynem kartezjańskim* dwóch zbiorów nazywamy zbiór wszystkich par uporządkowanych złożonych z elementów tych zbiorów:

$$A \times B = \{\langle a, b \rangle \mid a \in A \wedge b \in B\}.$$

Zadanie 189. Uzupełnij i udowodnij podane wzory.

$$(A \cap B) \times C = (A \times C) \cap (B \times C)$$

$$(A \cup B) \times C = ?$$

$$(A \cup B) \times (C \cup D) = ?$$

Zadanie 190. Udowodnij, że dla dowolnych zbiorów A i B równość $A \times B = B \times A$ zachodzi wtedy i tylko wtedy, gdy

$$A = \emptyset \text{ lub } B = \emptyset \text{ lub } A = B.$$

Zadanie 191. Udowodnij, że jeżeli $A \times B = C \times D$, to

$$(A = C \text{ i } B = D) \text{ lub } ((A = \emptyset \text{ lub } B = \emptyset) \text{ i } (C = \emptyset \text{ lub } D = \emptyset)).$$

Zadanie 192. Załóżmy, że $B \subseteq Y$. Czy dla dowolnych zbiorów A i X zachodzi równość

$$(X \times Y) \setminus (A \times B) = (X \times (Y \setminus B)) \cup ((X \setminus A) \times B)?$$

3.2. Relacje

Definicja 45. Dowolny podzbiór $R \subseteq A \times B$ produktu kartezjańskiego zbiorów A i B nazywamy *relacją dwuargumentową (binarną)*. Jeśli $\langle a, b \rangle \in R$, to mówimy, że elementy $a \in A$ i $b \in B$ są ze sobą w relacji R . Zamiast pisać $\langle a, b \rangle \in R$, piszemy też niekiedy aRb lub $R(a, b)$. Podzbiory $A \times A$ są *binarnymi relacjami na zbiorze A* .

Przykład 46. Relacjami binarnymi są:

- identyczność (równość, przekątna) na zbiorze $\mathbb{N}$: $\{\langle x, x \rangle \in \mathbb{N}^2 \mid x \in \mathbb{N}\}$,
- relacja mniejszości $\leq$ na zbiorze $\mathbb{N}$: $\{\langle x, y \rangle \in \mathbb{N}^2 \mid x \leq y\}$,
- taka $R \subseteq \mathbb{Z} \times \mathbb{N}$, że xRy gdy $y = x^2$.

Zadanie 193. Podaj intuicyjny sens poniższych relacji dwuargumentowych na zbiorze $\{1, 2, 3, 4, 5, 6\}$:

a)	$y \setminus x$	1	2	3	4	5	6
	1	1	0	0	1	0	0
	2	1	0	0	1	0	0
	3	1	0	0	1	0	0
	4	1	0	0	1	0	0
	5	1	0	0	1	0	0
	6	1	0	0	1	0	0

b)	$y \setminus x$	1	2	3	4	5	6
	1	0	0	1	0	0	1
	2	0	1	0	0	1	0
	3	1	0	0	1	0	0
	4	0	0	1	0	0	1
	5	0	1	0	0	1	0
	6	1	0	0	1	0	0

c)

$y \setminus x$	1	2	3	4	5	6
1	0	0	0	0	0	1
2	1	0	0	0	0	0
3	0	1	0	0	0	0
4	0	0	1	0	0	0
5	0	0	0	1	0	0
6	0	0	0	0	1	0

(Liczba 1 w tabelce oznacza, że dana para elementów należy do relacji, 0 zaś, że nie.)

Definicja 47. Relacja $R \subseteq A \times A$ jest

- *zwrotna*, jeśli dla wszystkich $a \in A$ zachodzi aRa ,
- *symetryczna*, jeśli dla wszystkich $a, b \in A$ zachodzi implikacja $aRb \Rightarrow bRa$,
- *przechodnia*, jeśli dla wszystkich $a, b, c \in A$ zachodzi $aRb \wedge bRc \Rightarrow aRc$.
- *antyzwrotna*, jeśli dla wszystkich $a \in A$ zachodzi $\neg aRa$,
- *antysymetryczna*, jeśli dla wszystkich $a, b \in A$ zachodzi implikacja $aRb \Rightarrow \neg bRa$,
- *słabo antisymetryczna*, jeśli dla wszystkich $a, b \in A$ zachodzi implikacja $aRb \wedge bRa \Rightarrow a = b$,

Relację zwrotną, symetryczną i przechodnią nazywamy *relacją równoważności*. Relację zwrotną, przechodnią i słabo antisymetryczną nazywamy *relacją częściowego porządku*.

Zadanie 194. Niech dla relacji R

- $Z(R)$ oznacza, że R jest zwrotna,
- $S(R)$ oznacza, że R jest symetryczna,
- $P(R)$ oznacza, że R jest przechodnia,
- $A(R)$ oznacza, że R jest słabo antisymetryczna.

Podaj przykłady relacji R_1, R_2, R_3 i R_4 takich, że zachodzi

1. $Z(R_1) \wedge S(R_1) \wedge P(R_1)$,
2. $Z(R_2) \wedge P(R_2) \wedge \neg S(R_2)$,
3. $Z(R_3) \wedge S(R_3) \wedge P(R_3) \wedge A(R_3)$,
4. $\neg Z(R_4) \wedge \neg A(R_4) \wedge P(R_4)$.

3.3. Krotki (n -tki) uporządkowane i relacje n -argumentowe

Pojęcie pary łatwo uogólnić na ciągi uporządkowane dowolnej, skończonej długości, które będziemy nazywać *krotkami* (n -tkami). Zakładamy, że $\langle a_1, \dots, a_n \rangle$ jest pojęciem pierwotnym i przyjmujemy:

Aksjomat 48. $\langle a_1, \dots, a_n \rangle = \langle b_1, \dots, b_n \rangle \Leftrightarrow a_1 = b_1 \wedge \dots \wedge a_n = b_n$.

Krotki można również zdefiniować za pomocą pojęcia pary: krotka dwuelementowa jest parą, krotka $n + 1$ -elementowa jest parą złożoną z pierwszego elementu i krotki n -elementowej:

$$\langle a_0, a_1, \dots, a_n \rangle = \langle a_0, \langle a_1, \dots, a_n \rangle \rangle$$

Definicja 49. W oczywisty sposób uogólniamy pojęcie *produktu* na n zbiorów:

$$A_1 \times \dots \times A_n = \{ \langle a_1, \dots, a_n \rangle \mid a_1 \in A_1, \dots, a_n \in A_n \}.$$

Dla $n \geq 2$ zamiast

$$\underbrace{A \times \dots \times A}_{n \text{ razy}}$$

piszemy w skrócie A^n . Przyjmujemy dodatkowo, że $A^1 = A$.

Definicja 50. Relacją n -argumentową nazywamy dowolny podzbiór produktu n zbiorów.

Dla przykładu

$$\{ \langle a, b, c \rangle \in \mathbb{N}^3 \mid a \cdot b = c \} \quad \text{oraz} \quad \{ \langle a, b, c \rangle \in \mathbb{N}^3 \mid a \cdot b < c \}$$

są relacjami trójargumentowymi na zbiorze $\mathbb{N}$.

Zadanie 195. Ile jest relacji n -argumentowych na zbiorze 5-elementowym?

3.4. Złożenie relacji. Relacja odwrotna

Definicja 51. Dane są relacje $P \subseteq A \times B$ i $Q \subseteq B \times C$. Relacja

$$QP = \{ \langle a, c \rangle \mid \exists b (aPb \wedge bQc) \} \subseteq A \times C$$

nazywa się *złożeniem* relacji P i Q . Relacja

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

nazywa się *relacją odwrotną* do P .

Zadanie 196. Niech A będzie ustalonym niepustym zbiorem. Czy prawdą jest, że dla dowolnej relacji $R \subseteq A^2$ zachodzi

$$\phi(R) \Rightarrow \phi(RR),$$

gdzie RR oznacza złożenie relacji R ze sobą, a $\phi(R)$ oznacza, że relacja R jest

1. zwrotna na zbiorze A ,
2. symetryczna na zbiorze A ,
3. przechodnia na zbiorze A ,
4. antysymetryczna na zbiorze A .

Zadanie 197. Niech R będzie relacją binarną. Które z poniższych stwierdzeń są prawdziwe:

1. $RR \subseteq R$,
2. $RR = R$,
3. $RR \supseteq R$,

jeżeli relacja R jest

1. zwrotna?
2. symetryczna?
3. przechodnia?

Twierdzenie 52. Dla dowolnych relacji $R \subseteq A \times B$, $S \subseteq B \times C$ i $T \subseteq C \times D$:

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

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

Zadanie 198. Oblicz $R^2 = RR$, R^3 i R^4 dla relacji z zadania 193.

Zadanie 199. Uzupełnij i udowodnij wzory:

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

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

$$(R \cup S)^{-1} = R^{-1} \cup S^{-1}$$

$$(R \cap S)^{-1} = R^{-1} \cap S^{-1}$$

$$(R^{-1})^{-1} = R$$

$$T(R \cup S) = TR \cup TS$$

$$T(R \cap S) \subseteq TR \cap TS$$

$$(T(R \cup S))^{-1} = R^{-1}T^{-1} \cup S^{-1}T^{-1}$$

$$(A \times B)^{-1} = B \times A$$

$$(A \times B)(C \times D) = ?$$

Dla relacji $R \subseteq A^2$ definiujemy $R^1 = R$ oraz $R^{n+1} = R^n R$ dla $n \geq 1$.

Zadanie 200. Wykaż, że jeśli R jest relacją zwrotną i przechodnią, to $R^n = R$ dla każdego $n \geq 1$.

Zadanie 201. Niech $R \subseteq A^2$ będzie dowolną relacją i niech R^0 będzie relacją równości na A (to znaczy $\langle x, y \rangle \in R^0$ wtedy i tylko wtedy, gdy $x = y$). Wykaż, że $R \cup R^0 \cup R^{-1}$ jest relacją zwrotną i symetryczną.

Zadanie 202. Niech $R \subseteq A^2$ będzie pewną relacją binarną na zbiorze A oraz

$$\begin{aligned}\mathcal{T} &= \{S \subseteq A^2 \mid S \text{ jest przechodnia} \wedge R \subseteq S\}, \\ R^+ &= \bigcap \mathcal{T}.\end{aligned}$$

Pokaż, że

1. $R \subseteq R^+$,
2. jeśli S jest relacją przechodnią taką, że $R \subseteq S$, to $R^+ \subseteq S$,
3. R^+ jest relacją przechodnią.

Relacja R^+ jest zatem najmniejszą (w sensie zawierania zbiorów) relacją przechodnią zawierającą relację R .

Definicja 53. Relację R^+ nazywamy *przechodnim (tranzytywnym) domknięciem* R .

Zadanie 203. Niech $Q \subseteq A^2$ będzie dowolną relacją. Kładziemy $\bar{Q} = \bigcup_{n=1}^{\infty} Q^n$. Wykaż, że $\bar{Q}$ jest relacją przechodnią.

Zadanie 204. Wykaż, że relacja $\bar{Q}$ z poprzedniego zadania jest przechodnim domknięciem relacji Q .

4

Funkcje

Definicja 54. Relację $f \subseteq A \times B$ nazywamy *funkcją o dziedzinie A i zbiorze wartości (przeciwdziedzinie) B* , jeżeli spełnia ona dwa warunki

1. dla każdego $a \in A$ istnieje taki $b \in B$, że $\langle a, b \rangle \in f$,
2. dla dowolnych $a \in A$ oraz $b_1, b_2 \in B$, jeśli $\langle a, b_1 \rangle \in f$ oraz $\langle a, b_2 \rangle \in f$, to $b_1 = b_2$.

Zbiór wszystkich funkcji o dziedzinie A i przeciwdziedzinie B oznaczamy B^A .

Relację spełniającą jedynie warunek 2 nazywamy *funkcją częściową*. Dziedziną funkcji częściowej f nazywamy zbiór

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

Zamiast $f \in B^A$ piszemy zwykle $f : A \rightarrow B$. Napis $f(a)$ oznacza taki element b , że $\langle a, b \rangle \in f$ (jeśli relacja f jest funkcją, to dla każdego a taki element b istnieje i jest dokładnie jeden, oznaczenie $f(a)$ jest więc jednoznaczne).

Pytanie 55. Ile jest funkcji $f : A \rightarrow B$? Ile jest funkcji $f : \emptyset \rightarrow B$, a ile $f : A \rightarrow \emptyset$?

Z pomocą pojęcia funkcji możemy jeszcze inaczej zdefiniować n -tki uporządkowane: $\langle a_1, \dots, a_n \rangle$ jest funkcją $f : \{1, \dots, n\} \rightarrow A$. Wówczas $f(i)$ jest i -tym elementem krotki.

Definicja 56. Funkcja $f : A \rightarrow B$ jest *różnowartościowa* (jest *injekcją*), jeżeli

$$\text{dla dowolnych } a_1, a_2 \in A, \text{ jeśli } a_1 \neq a_2, \text{ to } f(a_1) \neq f(a_2).$$

Funkcja $f : A \rightarrow B$ jest „na” (jest *surjekcją*), jeżeli

$$\text{dla dowolnego } b \in B \text{ istnieje taki } a \in A, \text{ że } f(a) = b.$$

Funkcja f jest *odwzorowaniem wzajemnie jednoznacznym* (*bijekcją*), jeśli jest różnowartościowa i „na”.

Zadanie 205. Które spośród relacji z zadania 193 są funkcjami?

4.1. Funkcje odwrotne i złożenie funkcji

Twierdzenie 57. Niech dane będą funkcje $f : A \rightarrow B$ i $g : B \rightarrow C$. Wówczas relacja $gf \subseteq A \times C$ jest funkcją z A w C oraz $(gf)(a) = g(f(a))$ dla każdego $a \in A$. Jeżeli ponadto obie funkcje f i g są różnowartościowe, to gf też jest różnowartościowa. Jeżeli obie funkcje f i g są „na”, to gf też jest „na”.

Definicja 58. Niech $f : A \rightarrow B$ będzie funkcją. Wtedy funkcja $g : B \rightarrow A$ jest *funkcją odwrotną* do f , jeśli $gf = I_A$ oraz $fg = I_B$ (gdzie I_A, I_B oznaczają funkcje identycznościowe odpowiednio na zbiorach A i B).

Twierdzenie 59. Niech $f : A \rightarrow B$ będzie funkcją. Wtedy następujące warunki są równoważne:

1. f ma funkcję odwrotną,
2. f jest bijekcją,
3. relacja odwrotna f^{-1} jest funkcją określoną na zbiorze B .

Funkcję odwrotną do f oznaczamy f^{-1} .

Zadanie 206. Niech $f : A \rightarrow B$ i $g : B \rightarrow C$. Które z poniższych implikacji są prawdziwe?

1. Jeżeli gf jest „na”, to f jest „na”.
2. Jeżeli gf jest „na”, to g jest „na”.
3. Jeżeli gf jest różnowartościowa, to f jest różnowartościowa.
4. Jeżeli gf jest różnowartościowa, to g jest różnowartościowa.

4.2. Obraz i przeciwobraz zbioru

Definicja 60. Niech $f : A \rightarrow B$ będzie funkcją i niech $X \subseteq A$. *Obrazem zbioru X w odwzorowaniu f* nazywamy zbiór

$$f(X) = \{b \in B \mid \exists a \in X \ f(a) = b\}.$$

Przeciwobrazem zbioru $Y \subseteq B$ w odwzorowaniu f nazywamy zbiór

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

Definicja 61. Niech $\mathcal{X}$ będzie rodziną podzbiorów zbioru A . Wtedy

$$\begin{aligned} \bigcup \mathcal{X} &= \bigcup_{X \in \mathcal{X}} X \\ \bigcap \mathcal{X} &= \bigcap_{X \in \mathcal{X}} X \end{aligned}$$

Twierdzenie 62. Niech $f : A \rightarrow B$ będzie funkcją, $\mathcal{X}$ rodziną podzbiorów zbioru A , zaś $\mathcal{Y}$ rodziną podzbiorów zbioru B . Wtedy

$$f\left(\bigcup \mathcal{X}\right) = \bigcup \{f(X) \mid X \in \mathcal{X}\} \quad (1)$$

$$\text{Jeśli } \mathcal{X} \neq \emptyset, \text{ to } f\left(\bigcap \mathcal{X}\right) \subseteq \bigcap \{f(X) \mid X \in \mathcal{X}\} \quad (2)$$

$$f^{-1}\left(\bigcup \mathcal{Y}\right) = \bigcup \{f^{-1}(Y) \mid Y \in \mathcal{Y}\} \quad (3)$$

$$\text{Jeśli } \mathcal{Y} \neq \emptyset, \text{ to } f^{-1}\left(\bigcap \mathcal{Y}\right) = \bigcap \{f^{-1}(Y) \mid Y \in \mathcal{Y}\} \quad (4)$$

Pytanie 63. Czy symbol „ $\subseteq$ ” we wzorze (2) można zastąpić symbolem „ $=$ ”?

Zadanie 207. Niech $f : X \rightarrow Y$ oraz $A, B \subseteq X$. Uzupełnij i udowodnij wzory:

$$f(A \cup B) = f(A) \cup f(B)$$

$$f(A \cap B) \quad ? \quad f(A) \cap f(B)$$

$$f^{-1}(f(A)) \quad ? \quad A$$

Zadanie 208. Niech $f : X \rightarrow Y$ oraz $C, D \subseteq Y$. Uzupełnij i udowodnij wzory:

$$f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$$

$$f^{-1}(C \cup D) = ?$$

$$f(f^{-1}(C)) \quad ? \quad C$$

$$f(f^{-1}(C)) = ?$$

Zadanie 209. Niech $f : X \rightarrow Y$ będzie bijekcją, a $g : Y \rightarrow X$ funkcją odwrotną do f . Udowodnij, że $f^{-1}(C) = g(C)$ dla dowolnego $C \subseteq Y$.

Zadanie 210. Rozważmy funkcję $f : A \rightarrow B$ i zdefiniujmy funkcję $g : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$ wzorem

$$g(Y) = f^{-1}(Y).$$

Udowodnij, że g jest różnowartościowa wtedy i tylko wtedy, gdy f jest „na”.

Zadanie 211. Udowodnij, że istnieje dokładnie jedna monotoniczna bijekcja $f : \mathbb{N} \rightarrow \mathbb{N}$.

Zadanie 212. Udowodnij, że jeśli $f : A \rightarrow B$ i $g : B \rightarrow A$ są takimi funkcjami, że $gf = I_A$ to f jest różnowartościowa a g jest „na”.

Zadanie 213. Udowodnij, że jeśli $f : A \rightarrow B$ jest różnowartościowa to $f^{-1}(f(X)) = X$ dla wszystkich zbiorów $X \subseteq A$. Czy $f(f^{-1}(Y)) = Y$ dla wszystkich zbiorów $Y \subseteq B$?

Zadanie 214. Udowodnij, że jeśli $f : A \rightarrow B$ jest „na” to $f(f^{-1}(Y)) = Y$ dla wszystkich zbiorów $Y \subseteq B$. Czy $f^{-1}(f(X)) = X$ dla wszystkich zbiorów $X \subseteq A$?

5

Relacje równoważności

Definicja 64. Klasą abstrakcji elementu $a \in A$ względem relacji równoważności $\sim \subseteq A \times A$ nazywamy zbiór

$$[a]_{\sim} = \{b \in A \mid a \sim b\}.$$

Rodzinę zbiorów $A/\sim = \{[a]_{\sim} \mid a \in A\}$ nazywamy zbiorem ilorazowym relacji $\sim$.

Definicja 65. Mówimy, że rodzina zbiorów $\{X_i\}_{i \in I}$ jest *podziałem* zbioru A , jeśli

1. zbiory X_i są niepuste:

$$X_i \neq \emptyset \text{ dla każdego } i \in I,$$

2. zbiory X_i pokrywają zbiór A :

$$\bigcup_{i \in I} X_i = A, \quad \text{oraz}$$

3. zbiory X_i są parami rozłączne:

$$X_i \cap X_j = \emptyset,$$

dla wszelkich takich $i, j \in I$, że $X_i \neq X_j$.

Definicja 66. Niech dane będą dwa podziały $\mathcal{P}_1$ i $\mathcal{P}_2$ zbioru A . Mówimy, że podział $\mathcal{P}_1$ jest *drobniejszy* od podziału $\mathcal{P}_2$, jeśli dla każdego $X \in \mathcal{P}_1$ istnieje taki $Y \in \mathcal{P}_2$, że $X \subseteq Y$.

Lemat 67. Dla dowolnej relacji równoważności $\sim \subseteq A \times A$ i elementów $a, b \in A$

$$a \sim b \quad \text{wtedy i tylko wtedy, gdy} \quad [a]_{\sim} = [b]_{\sim}.$$

Twierdzenie 68 (Zasada Abstrakcji).

1. Klasy abstrakcji dowolnej relacji równoważności na zbiorze A tworzą podział zbioru A .
2. Dla każdego podziału zbioru A istnieje dokładnie jedna relacja równoważności, której klasy abstrakcji tworzą ten podział.

Przykład 69. Niech $a, b, c, d \in \mathbb{Z}$, $c, d \neq 0$. Definiujemy relację $\sim \subseteq \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})^2$ wzorem

$$\langle a, b \rangle \sim \langle c, d \rangle \stackrel{\text{df}}{\Leftrightarrow} a \cdot d = b \cdot c.$$

Relacja $\sim$ jest relacją równoważności na $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Dowód polega na sprawdzeniu wprost z definicji, że $\sim$ jest zwrotna, symetryczna i przechodnia.

Zadanie 215. Używając kwantyfikatorów, spójników logicznych $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, oraz wyrażeń postaci $x \in A$, $x \notin A$, $R(x, y)$ i $\neg R(x, y)$ zapisz, że relacja R nie jest relacją równoważności na zbiorze A .

Zadanie 216. Napisz bez używania znaku negacji formuły mówiące, że

1. Rodzina $\{X_i\}_{i \in I}$ nie jest podziałem zbioru A . Wolno używać symbolu $\neq$.
2. Podział $\mathcal{P}_1$ nie jest drobniejszy od podziału $\mathcal{P}_2$. Wolno używać symbolu $\not\subseteq$.

Zadanie 217. Wykaż, że jeśli podział $\mathcal{P}_1$ jest drobniejszy od podziału $\mathcal{P}_2$, to dla każdego $X \in \mathcal{P}_2$ istnieje rodzina $\mathcal{R} \subseteq \mathcal{P}_1$, taka, że $X = \bigcup \mathcal{R}$.

Zadanie 218. Relacje R i S są relacjami równoważności na tym samym zbiorze. Czy $R \cup S$, $R \cap S$, $R \setminus S$, $R \div S$ też są relacjami równoważności?

Zadanie 219. Czy dla dowolnych relacji równoważności R i S na tym samym zbiorze, relacja SR jest relacją równoważności?

Zadanie 220. Niech R i S będą relacjami równoważności na tym samym zbiorze. Udowodnij, że $R \cup S$ jest relacją równoważności wtedy i tylko wtedy, gdy $R \cup S = RS$.

Zadanie 221. Niech $\mathcal{R}$ będzie pewną rodziną relacji równoważności określonych na pewnym zbiorze X . Czy $\bigcup \mathcal{R}$ i $\bigcap \mathcal{R}$ są relacjami równoważności na X ?

Zadanie 222. Niech $R \subseteq A^2$ będzie pewną relacją binarną na zbiorze A oraz

$$\begin{aligned} \mathcal{T} &= \{S \subseteq A^2 \mid S \text{ jest zwrotna i przechodnia} \wedge R \subseteq S\}, \\ R^* &= \bigcap \mathcal{T}. \end{aligned}$$

Pokaż, że

1. $R \subseteq R^*$,
2. jeśli S jest relacją zwrotną i przechodnią taką, że $R \subseteq S$, to $R^* \subseteq S$,
3. R^* jest relacją zwrotną i przechodnią.

Relacja R^* jest zatem najmniejszą (w sensie zawierania zbiorów) relacją zwrotną i przechodnią zawierającą relację R .

Definicja 70. Relację R^* nazywamy *zwrotnym i przechodnim domknięciem* R .

Zadanie 223. Niech $Q \subseteq A^2$ będzie dowolną relacją, $Q^0 = I$, gdzie I jest relacją równości na A i niech $Q^{n+1} = Q^n Q$ dla $n \geq 0$. Kładziemy $\hat{Q} = \bigcup_{n=0}^{\infty} Q^n$. Wykaż, że $\hat{Q}$ jest relacją zwrotną i przechodnią.

Zadanie 224. Wykaż, że relacja $\hat{Q}$ z poprzedniego zadania jest zwrotnym i przechodnim domknięciem relacji Q .

Zadanie 225. Korzystając z zadań poprzednich wykaż, że jeśli R jest dowolną relacją oraz $Q = R \cup R^{-1}$, to Q^* jest relacją równoważności.

Zadanie 226. Udowodnij, że jeśli R jest dowolną relacją oraz $Q = R \cup R^{-1}$, to Q^* jest najmniejszą (w sensie relacji inkluzji) relacją równoważności zawierającą relację R .

Zadanie 227. Udowodnij, że jeżeli R jest relacją taką, że R^* zawiera R^{-1} , to R^* jest relacją równoważności.

Zadanie 228. Dane jest przekształcenie $f : A \rightarrow B$. W zbiorze A definiujemy relację $\sim$ wzorem

$$x \sim y \stackrel{\text{df}}{\Leftrightarrow} f(x) = f(y).$$

Udowodnij, że $\sim$ jest relacją równoważności. Podaj warunek konieczny i dostateczny na to, by $\sim$ była identycznością na A .

Zadanie 229. Dane jest przekształcenie $f : A \rightarrow B$ oraz relacja równoważności R na B . W zbiorze A definiujemy relację $\sim$ wzorem

$$x \sim y \stackrel{\text{df}}{\Leftrightarrow} \langle f(x), f(y) \rangle \in R.$$

Udowodnij, że $\sim$ jest relacją równoważności.

Zadanie 230. Ile jest różnych relacji równoważności na zbiorze czteroelementowym? Ile jest różnych relacji równoważności na zbiorze sześcioelementowym?

Zadanie 231. W zbiorze $\mathbb{N}^{\mathbb{N}}$ definiujemy relacje R_1 , R_2 , R_3 i R_4 w następujący sposób:

- $f R_1 g$ wtedy i tylko wtedy, gdy $f(57) = g(57)$,
 $f R_2 g$ wtedy i tylko wtedy, gdy $f(57) - g(57)$ jest podzielne przez 57,
 $f R_3 g$ wtedy i tylko wtedy, gdy $f(n) = g(n)$ dla nieskończenie wielu $n \in \mathbb{N}$,
 $f R_4 g$ wtedy i tylko wtedy, gdy $f(n) \neq g(n)$ dla skończenie wielu $n \in \mathbb{N}$.

Która z relacji R_1 , R_2 , R_3 i R_4 jest relacją równoważności?

Zadanie 232. Sprawdź, dla jakich dodatnich liczb naturalnych k podane relacje na zbiorze $\mathbb{N}$ są relacjami równoważności. Opisz ich klasy abstrakcji. Napisz $k \mid m$ oznacza, że m jest podzielne przez k .

1. $x R_1 y \stackrel{\text{df}}{\Leftrightarrow} k \mid (x + y)$
2. $x R_2 y \stackrel{\text{df}}{\Leftrightarrow} k \mid (x - y)$
3. $x R_3 y \stackrel{\text{df}}{\Leftrightarrow} x - y = k$

Zadanie 233. Czy relacja R określona na zbiorze wielomianów jednej zmiennej o współczynnikach naturalnych wzorem

$$p R q \stackrel{\text{df}}{\Leftrightarrow} \text{wielomian } p - q \text{ ma wszystkie współczynniki parzyste}$$

jest relacją równoważności?

Zadanie 234. Dany jest zbiór X i jego podzbiór $C \subseteq X$. Czy relacja R określona na $\mathcal{P}(X)$ wzorem

$$A R B \stackrel{\text{df}}{\Leftrightarrow} A \div B \subseteq C$$

jest relacją równoważności? Jeśli tak, opisz jej klasy abstrakcji.

Zadanie 235. W zbiorze wszystkich zbieżnych ciągów nieskończonych o wyrazach wymiernych wprowadzamy relację

$$\bar{a} R \bar{b} \stackrel{\text{df}}{\Leftrightarrow} \lim_{n \rightarrow \infty} (a_n - b_n) = 0$$

Pokaż, że R jest relacją równoważności. Opisz jej klasy abstrakcji.

W poniższych zadaniach udowodnij, że podane relacje $R \subseteq X \times X$ są relacjami równoważności. Opisz ich klasy abstrakcji.

Zadanie 236. $X = \mathcal{P}(\mathbb{N})$,

$$ARB \stackrel{\text{df}}{\Leftrightarrow} A \dot{-} B \text{ jest zbiorem skończonym.}$$

Zadanie 237. $X = \mathbb{N} \times \mathbb{N}$,

$$\langle x_1, y_1 \rangle R \langle x_2, y_2 \rangle \stackrel{\text{df}}{\Leftrightarrow} x_1 - y_1 = x_2 - y_2.$$

Zadanie 238. $X = \mathbb{R} \times \mathbb{R}$,

$$\langle x_1, y_1 \rangle R \langle x_2, y_2 \rangle \stackrel{\text{df}}{\Leftrightarrow} x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Zadanie 239. $X = \mathbb{R} \times \mathbb{R}$,

$$\langle x_1, y_1 \rangle R \langle x_2, y_2 \rangle \stackrel{\text{df}}{\Leftrightarrow} |x_1| + |y_1| = |x_2| + |y_2|.$$

Zadanie 240. $X = \mathcal{P}(\mathbb{N})$,

$$R = \{ \langle A, B \rangle \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \mid A = B \vee 0 \notin A \cup B \}.$$

Zadanie 241. Na zbiorze $\mathcal{P}(\mathbb{N})$ określamy relację równoważności $\sim$ wzorem

$$X \sim Y \quad \text{wtw} \quad X \dot{-} Y \text{ jest zbiorem skończonym}$$

(patrz zadanie 236). W zbiorze $\mathcal{P}(\mathbb{N})/\sim$ definiujemy działania

$$[X]_{\sim} \sqcup [Y]_{\sim} = [X \cup Y]_{\sim}$$

$$[X]_{\sim} \cap [Y]_{\sim} = [X \cap Y]_{\sim}$$

$$[X]_{\sim} - [Y]_{\sim} = [X \setminus Y]_{\sim}$$

Czy powyższe definicje są poprawne?

Zadanie 242. W zbiorze liczb rzeczywistych $\mathbb{R}$ wprowadzamy taką relację $\sim$, że $x \sim y \stackrel{\text{df}}{\Leftrightarrow} \lfloor x \rfloor = \lfloor y \rfloor$. Udowodnij, że $\sim$ jest relacją równoważności. Opisz jej klasy abstrakcji.

Zadanie 243. W zbiorze $\mathbb{R}/\sim$, gdzie $\sim$ jest relacją z zadania 242, definiujemy działania arytmetyczne: $[x]_{\sim} + [y]_{\sim} = [x + y]_{\sim}$ oraz $[x]_{\sim} \cdot [y]_{\sim} = [x \cdot y]_{\sim}$. Czy powyższe definicje są poprawne?

6

Teoria mocy

6.1. Równoliczność zbiorów

Definicja 71. Zbiory A i B są równoliczne, jeżeli istnieje bijekcja $f : A \rightarrow B$. Piszemy wówczas $A \sim B$.

Przykład 72. Następujące zbiory są równoliczne:

- zbiór par liczb naturalnych i zbiór liczb naturalnych: $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$;
- zbiór liczb naturalnych i zbiór liczb naturalnych parzystych: $\mathbb{N} \sim \mathbb{P}$;
- dowolny niepusty przedział $(a, b) \subseteq \mathbb{R}$ i odcinek $(0, 1)$: $(a, b) \sim (0, 1)$.

Niech $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ i $\mathbb{R}$ oznaczają zbiory, odpowiednio, liczb naturalnych, całkowitych, wymiernych i rzeczywistych, $m \perp n$ oznacza, że m i n są względnie pierwsze oraz

(a, b)	oznacza zbiór	$\{x \in \mathbb{R} \mid a < x < b\}$,
$[a, b)$	oznacza zbiór	$\{x \in \mathbb{R} \mid a \leq x < b\}$,
$(a, b]$	oznacza zbiór	$\{x \in \mathbb{R} \mid a < x \leq b\}$,
$[a, b]$	oznacza zbiór	$\{x \in \mathbb{R} \mid a \leq x \leq b\}$,
(a, ∞)	oznacza zbiór	$\{x \in \mathbb{R} \mid a < x\}$,
$O((a, b), r)$	oznacza zbiór	$\{(x, y) \in \mathbb{R}^2 \mid (x - a)^2 + (y - b)^2 = r^2\}$,
$\mathbb{N}^+$	oznacza zbiór	$\{n \in \mathbb{N} \mid n > 0\}$,
$\mathbb{Q}^+$	oznacza zbiór	$\{q \in \mathbb{Q} \mid q > 0\}$.

Konstruując odpowiednie bijekcje udowodnij, że zbiory podane w poniższych zadaniach są równoliczne.

Zadanie 244. $[0, 1)$ oraz $O((0, 0), 1)$

Zadanie 245. $(0, 1)$ oraz $\mathbb{R}$

Zadanie 246. $[0, 1)$ oraz $[0, \infty)$

Zadanie 247. $(0, 1)$ oraz $[0, 1)$

Zadanie 248. $[0, 1)$ oraz $\mathbb{R}$

Zadanie 249. $[0, 1)$ oraz $(0, \infty)$

Zadanie 250. $\mathbb{R}$ oraz $\mathbb{R} \setminus \mathbb{N}$

Zadanie 251. $\mathbb{Q}$ oraz $\mathbb{Q} \setminus [0, 1]$

Zadanie 252. $\mathbb{N}$ oraz $\mathbb{Z}$

Zadanie 253. $\mathbb{N}$ oraz $\mathbb{N}^2$

Zadanie 254. $\mathbb{N}$ oraz $\mathbb{N}^3$

Zadanie 255. $\mathbb{N}$ oraz $\{(n, m) \in \mathbb{N}^+ \times \mathbb{N}^+ \mid m \perp n\}$

Zadanie 256. $\{(n, m) \in \mathbb{N}^+ \times \mathbb{N}^+ \mid m \perp n\}$ oraz $\mathbb{Q}^+$

Zadanie 257. $\mathbb{N}$ oraz $\mathbb{Q}$

Zadanie 258. $\mathbb{Z} \times ((0, 1] \cap \mathbb{Q})$ oraz $\mathbb{Q}$

Zadanie 259. $\mathbb{R}$ oraz $\mathbb{R} \setminus \mathbb{Q}$

Zadanie 260. $(0, 1] \times \mathbb{Z}$ oraz $\mathbb{R}$

Zadanie 261. $(0, 1) \times (0, 1)$ oraz $\mathbb{R} \times \mathbb{R}$

Zadanie 262. $\mathcal{P}(\mathbb{N})$ oraz $\mathbb{Z}^{\mathbb{N}}$

Zadanie 263. $\{0, 1\}^{\mathbb{N}}$ oraz $\mathbb{N}^{\mathbb{N}}$

Zadanie 264. $\mathbb{N}$ oraz $\{f : \mathbb{N} \rightarrow \{0, 1\} \mid f \text{ jest nierosnąca}\}$

Zadanie 265. $\mathbb{N}$ oraz $\{f : \mathbb{N} \rightarrow \{1, 2, 3, 4\} \mid f \text{ jest niemalejąca}\}$

Zadanie 266. $\{x \in \mathbb{R} \mid \sin(x) = 0\}$ oraz $\mathbb{Z}$

Zadanie 267. $\mathbb{Q}$ oraz $\mathbb{Q} \times \mathbb{Q}$

Zadanie 268. $(0, 1)$ oraz $(0, 1) \times (0, 1)$

Zadanie 269. $\mathbb{R}$ oraz $\mathbb{R} \times \mathbb{R}$

Zadanie 270. $\mathbb{R}$ oraz $\mathbb{R}^{\mathbb{N}}$

6.2. Własności pojęcia równoliczności zbiorów

Twierdzenie 73. Dla dowolnych zbiorów A, B, C

1. $A \sim A$,
2. Jeśli $A \sim B$ to $B \sim A$,
3. Jeśli $A \sim B$ oraz $B \sim C$ to $A \sim C$.

Zadanie 271. Wykaż, że jeśli $A_1 \sim A_2$, to

$$\mathcal{P}(A_1) \sim \mathcal{P}(A_2), \quad (1)$$

$$B^{A_1} \sim B^{A_2}, \quad (2)$$

$$A_1^B \sim A_2^B, \quad (3)$$

$$A_1 \times B \sim A_2 \times B. \quad (4)$$

Zadanie 272. Wykaż, że

$$(A^B)^C \sim A^{(B \times C)}, \quad (1)$$

$$(A \times B)^C \sim A^C \times B^C, \quad (2)$$

$$A \times \{a\} \sim A, \quad (3)$$

$$A^{\{a\}} \sim A, \quad (4)$$

dla dowolnych zbiorów A, B, C i jednoelementowego zbioru $\{a\}$.

Zadanie 273. Wykaż, że jeśli $A_1 \cap B_1 = A_2 \cap B_2 = \emptyset$ oraz $A_1 \sim A_2$ i $B_1 \sim B_2$, to

$$A_1 \cup B_1 \sim A_2 \cup B_2, \quad (1)$$

$$C^{A_1 \cup B_1} \sim C^{A_2} \times C^{B_2}. \quad (2)$$

Powyższe własności uwalniają nas od konieczności żmudnego konstruowania odpowiednich bijekcji, pozwalając w łatwy sposób wyprowadzać nowe fakty na temat równoliczności zbiorów z już poznanych. Dla przykładu skoro $\mathbb{N} \sim \mathbb{Q}$ (zadanie 257), to na mocy własności (2) z zadania 271 wnioskujemy, że $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}^{\mathbb{Q}}$.

Zadanie 274. Przyjmując za wiadome, że $\mathbb{N} \sim \mathbb{N} \times \mathbb{N}$ oraz $\mathbb{R} \sim \{0, 1\}^{\mathbb{N}}$ udowodnij, że $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$.

Zadanie 275. Dla jakich zbiorów A, B i C :

1. $A^B \sim B^A$?
2. $A^{B \cup C} \sim A^B \cup A^C$?

Zadanie 276. Czy istnieją takie zbiory A, B, C, D , że $A \not\sim B$ oraz $C \not\sim D$, ale $A^C \sim B^D$?

6.3. Zbiory skończone

Definicja 74. Napis $\underline{n}$ oznacza zbiór liczb naturalnych mniejszych od n , tj. zbiór = $\{0, 1, \dots, n-1\}$.

Definicja 75. Zbiór A jest *zbiorem skończonym*, jeśli istnieje taka liczba naturalna $n \in \mathbb{N}$, że $A \sim \underline{n}$. Zbiór, który nie jest skończony nazywamy *nieskończonym*.

Twierdzenie 76.

1. Dla żadnego $n \in \mathbb{N}$ nie istnieje funkcja różnowartościowa z $\underline{n+1}$ w $\underline{n}$.
2. Jeżeli istnieje funkcja różnowartościowa z $\underline{m}$ w $\underline{n}$, to $\underline{m} \subseteq \underline{n}$.
3. Jeżeli $\underline{m} \sim \underline{n}$, to $m = n$.
4. Dla każdego $m \in \mathbb{N}$ zachodzi $\underline{m} \not\sim \mathbb{N}$.

Jeśli więc zbiór A jest skończony, to istnieje dokładnie jedna taka liczba naturalna n , że $A \sim \underline{n}$.

Definicja 77. Niech A będzie zbiorem skończonym. Liczbę n taką, że $A \sim \underline{n}$ nazywamy *liczbą elementów* zbioru A i oznaczamy $|A|$. Liczbę elementów zbioru $|A|$ nazywamy też *mocą* zbioru A zwłaszcza gdy jednocześnie zajmujemy się zbiorami skończonymi i nieskończonymi.

Zbiór pusty ma zatem 0 elementów. Zbiór ma n elementów, jeżeli jego elementy można ponumerować bez powtórzeń liczbami $0, \dots, n-1$.

Zadanie 277. Udowodnij, że suma dwóch skończonych zbiorów jest zbiorem skończonym.

Zadanie 278. Udowodnij, że dla dowolnych liczb naturalnych $m, n \in \mathbb{N}$ jest

$$(\underline{m} \times \{0\}) \cup (\underline{n} \times \{1\}) \sim \underline{m+n}.$$

Wyprowadź stąd wniosek, że dla dowolnych skończonych rozłącznych zbiorów A i B zachodzi równość $|A \cup B| = |A| + |B|$.

Zadanie 279. Wykaż, że jeśli zbiory A i B są skończone, to $|A \times B| = |A| \cdot |B|$.

Zadanie 280. Wykaż, że jeśli zbiory A i B są skończone, to $|A^B| = |A|^{|B|}$.

Zadanie 281. Niech $A^1 = A$ oraz $A^{n+1} = A^n \times A$. Wykaż, że $A^n \sim \mathbb{N}^n$.

Zadanie 282. Niech $\{A_i\}_{i \in \mathbb{N}}$ będzie rodziną podzbiorów zbioru X . Niech (1) oznacza, że A_0 jest zbiorem skończonym, oraz (2) oznacza, że dla każdego n zachodzi $\bigcap_{i=0}^n A_i \neq \emptyset$. Pokaż, że: a) jeśli zachodzi (1) i (2), to $\bigcap_{i=0}^{\infty} A_i \neq \emptyset$, b) istnieje taka rodzina zbiorów $\{A_i\}_{i \in \mathbb{N}}$ spełniająca warunek (2), że $\bigcap_{i=0}^{\infty} A_i = \emptyset$.

Zadanie 283. Niech $\{A_i\}_{i \in \mathbb{N}}$ będzie rodziną skończonych podzbiorów zbioru X , taką, że $A_{n_1} \cap \dots \cap A_{n_k} \neq \emptyset$ dla dowolnych $n_1, \dots, n_k \in \mathbb{N}$. Pokaż, że $\bigcap_{i=1}^{\infty} A_i \neq \emptyset$.

Zadanie 284. Dane są dwie funkcje $f : A \rightarrow B$ i $g : B \rightarrow A$, obie typu „na”.

1. Czy z powyższych założeń wynika, że f i g są bijekcjami?
2. Jeśli dodatkowo A i B są zbiorami skończonymi, to czy wówczas f i g są bijekcjami?

Zadanie 285. Dane są zbiory $A_1, \dots, A_n$. Przypuśćmy, że $\mathcal{R}$ jest najmniejszą rodziną zbiorów o tej własności, że $A_i \in \mathcal{R}$ dla $i = 1, \dots, n$ oraz jeśli $X, Y \in \mathcal{R}$, to $X \cup Y \in \mathcal{R}$. Wyznacz maksymalną moc rodziny $\mathcal{R}$.

Zadanie 286. Dane są zbiory $A_1, \dots, A_n$. Przypuśćmy, że $\mathcal{R}$ jest najmniejszą rodziną zbiorów o tej własności, że $A_i \in \mathcal{R}$ dla $i = 1, \dots, n$ oraz jeśli $X, Y \in \mathcal{R}$, to $X \cup Y \in \mathcal{R}$ i $X \cap Y \in \mathcal{R}$. Wyznacz maksymalną moc rodziny $\mathcal{R}$. Dla jakich zbiorów $A_1, \dots, A_n$ wartość $|\mathcal{R}|$ jest największa?

Zadanie 287. Dane są zbiory $A_1, \dots, A_n$. Przypuśćmy, że $\mathcal{R}$ jest najmniejszą rodziną zbiorów o tej własności, że $A_i \in \mathcal{R}$ dla $i = 1, \dots, n$ oraz jeśli $X, Y \in \mathcal{R}$, to $X \cup Y \in \mathcal{R}$ i $X \setminus Y \in \mathcal{R}$. Wyznacz maksymalną moc rodziny $\mathcal{R}$. Dla jakich zbiorów $A_1, \dots, A_n$ wartość $|\mathcal{R}|$ jest największa?

Definicja 78. Przyjmujemy następujące oznaczenia: dla dowolnego zbioru $X \subseteq A$ napis X^1 oznacza zbiór X , zaś napis X^0 oznacza dopełnienie zbioru X do zbioru A , tj. zbiór $A \setminus X$.

Zadanie 288. Dany jest zbiór A i dodatnia liczba naturalna k oraz takie zbiory $X_i \subseteq A$ dla $i = 1, \dots, k$, że dla każdej funkcji $f : \{1, \dots, k\} \rightarrow \{0, 1\}$ zbiór $\bigcap_{i=1}^k X_i^{f(i)}$ ma co najwyżej 1 element. Wyznacz maksymalną moc zbioru A .

Definicja 79. Mówimy, że funkcja dwuargumentowa $f : A \times B \rightarrow C$ istotnie zależy od każdego z argumentów, jeśli istnieją takie elementy $a \in A$ i $b_1, b_2 \in B$, że $f(a, b_1) \neq f(a, b_2)$ oraz istnieją takie elementy $a_1, a_2 \in A$ i $b \in B$, że $f(a_1, b) \neq f(a_2, b)$.

Zadanie 289. Ile jest dwuargumentowych funkcji logicznych istotnie zależnych od każdego z argumentów? Ile jest funkcji $f : A \times B \rightarrow C$ istotnie zależnych od każdego z argumentów, gdy każdy ze zbiorów A, B, C ma 3 elementy?

Zadanie 290. Ile jest funkcji $f : A \times B \rightarrow C$ istotnie zależnych od każdego z argumentów, gdy każdy ze zbiorów A, B ma 4 elementy, a C ma n elementów?

Zadanie 291. a) Na prywatce u Jurka jest co najmniej jedna osoba znająca co najmniej jeden z sześciu języków: polski, angielski, francuski, niemiecki, rosyjski i hiszpański. Ponadto nie ma dwóch osób, które znałyby dokładnie te same języki. Oczywiście każdy gość Jurka zna co najmniej dwa języki. Oszacuj z góry i z dołu liczbę osób na prywatce u Jurka.

b) Na prywatce u Agaty jest co najmniej jedna osoba znająca co najmniej jeden z n języków. Ponadto nie ma dwóch osób, które znałyby dokładnie te same języki. Oczywiście każdy gość Agaty zna co najmniej jeden język. Oszacuj z góry i z dołu liczbę osób na prywatce u Agaty.

Zadanie 292. Funkcję f określoną w pewnej dziedzinie $\text{dom}(f) \subseteq \mathcal{P}(A)$ i przyjmującą wartości ze zbioru $\{0, 1\}$ nazywamy *funkcją parzystości w zbiorze $\mathcal{P}(A)$* , jeżeli

1. dla dowolnych $X \in \text{dom}(f)$ i $x \in A$ także $X \cup \{x\} \in \text{dom}(f)$ oraz $X \setminus \{x\} \in \text{dom}(f)$,
2. $\emptyset \in \text{dom}(f)$ oraz $f(\emptyset) = 0$,
3. dla dowolnego $X \in \text{dom}(f)$ i dowolnego $x \in A \setminus X$ zachodzi równość

$$f(X \cup \{x\}) = 1 - f(X).$$

Wykaż, że na zbiorze $\mathcal{P}(A)$ istnieje dokładnie jedna funkcja parzystości wtedy i tylko wtedy, gdy A jest zbiorem skończonym.

Zadanie 293. Pokaż, że zbiór wartości dowolnej nierosnącej funkcji

$$f : \mathbb{N} \rightarrow \left\{ n + \frac{m}{m+1} \mid n, m \in \mathbb{N} \right\}$$

jest skończony.

6.3.1. Wzór włączeń i wyłączeń

Zadanie 294. Pośród członków pewnego klubu lingwistycznego każdy uczy się francuskiego, niemieckiego lub hiszpańskiego. Wiadomo, że 20 uczy się francuskiego, 12 francuskiego i hiszpańskiego, 16 niemieckiego, 16 hiszpańskiego, 4 francuskiego i niemieckiego, 7 niemieckiego i hiszpańskiego, 3 wszystkich trzech języków. Ilu członków liczy klub? Ilu z nich uczy się dokładnie dwóch języków?

Zadanie 295. Korzystając z tego, iż jeżeli zbiory skończone A i B są rozłączne, to $|A \cup B| = |A| + |B|$ udowodnij, że dla dowolnych zbiorów A , B i C (niekoniecznie rozłącznych):

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Zadanie 296. Udowodnij indukcyjnie, że dla dowolnej rodziny zbiorów skończonych $\{A_i\}_{i=1}^n$ jest prawdziwy tzw. *wzór włączeń i wyłączeń*:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{j=1}^n \sum_{\substack{I \subseteq \{1, \dots, n\} \\ |I|=j}} (-1)^{j+1} \left| \bigcap_{i \in I} A_i \right|.$$

Zadanie 297. Rodzina $\{A_i\}_{i=1}^n$ jest rodziną zbiorów *k-rozłącznych*, jeśli dla każdego rosnącego ciągu liczb naturalnych $\langle i_1, i_2, \dots, i_k \rangle$ takiego, że $i_k \leq n$, mamy

$$\bigcap_{j=1}^k A_{i_j} = \emptyset.$$

Udowodnij, że dla dowolnej rodziny zbiorów skończonych *k-rozłącznych* $\{A_i\}_{i=1}^n$ jest prawdziwy wzór:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{j=1}^{k-1} \sum_{\substack{I \subseteq \{1, \dots, n\} \\ |I|=j}} (-1)^{j+1} \left| \bigcap_{i \in I} A_i \right|.$$

6.4. Moce zbiorów nieskończonych

Symbol $|A|$ zdefiniowaliśmy jedynie dla zbiorów skończonych. W teorii mocy definiuje się obiekty oznaczające „liczbę elementów” zbiorów nieskończonych, zwane *liczbami kardynalnymi*. Pozwala to rozszerzyć odwzorowanie $|\cdot|$ na zbiory nieskończone. Robimy to w ten sposób, że dwóm zbiorom przypisujemy tę samą liczbę kardynalną wtedy i tylko wtedy, gdy zbiory te są równoliczne. Wartość $|A|$ nazywamy wówczas *mocą* zbioru A . Moc zbioru liczb naturalnych (a więc i dowolnego zbioru równolicznego ze zbiorem liczb naturalnych) oznaczamy $\aleph_0$ (czytamy „alef zero”). Poniżej pokazujemy, że $\mathbb{N} \not\sim \mathbb{R}$. Moc zbioru liczb rzeczywistych nazywamy continuum i oznaczamy przez c . Mamy zatem $|\mathbb{N}| = \aleph_0$, $|\mathbb{R}| = c$ oraz $\aleph_0 \neq c$.

Definicja 80. Zbiór jest *przeliczalny*, jeśli jest skończony lub jest równoliczny ze zbiorem liczb naturalnych.

Definicja 81. Zbiór równoliczny ze zbiorem liczb rzeczywistych nazywamy *zbiorem mocy continuum*.

Nierównolicznych zbiorów nieskończonych jest nieskończenie wiele. Jest więc nieskończenie wiele różnych nieskończonych liczb kardynalnych. Można na nich określić operacje dodawania, mnożenia i potęgowania oraz relację porządku mające podobne własności, jak odpowiadające im operacje na liczbach naturalnych. Teoria

takich liczb nazywa się *arytmetyką liczb kardynalnych*. Tak subtelne teorie mają jednak niewiele zastosowań w informatyce, dlatego nam wystarczą jedynie pojęcia równoliczności, przeliczalności i mocy continuum. Tam, gdzie nie jest to niezbędne, nie należy więc używać pojęcia mocy $|A|$ zbioru A (formalnie nie zdefiniowaliśmy przecież tego obiektu!). W szczególności zamiast pisać $|A| = |B|$ lepiej napisać $A \sim B$. Oba wyrażenia oznaczają bowiem, że zbiory A i B są równoliczne, drugie jednak nie odwołuje się do (dosyć skomplikowanego) pojęcia liczby kardynalnej.

Definicja 82. Mówimy, że moc zbioru A jest nie większa niż moc zbioru B i piszemy $|A| \leq |B|$, jeśli istnieje funkcja różnowartościowa $f : A \rightarrow B$.

Definicja 83. Mówimy, że moc zbioru A jest mniejsza niż moc zbioru B i piszemy $|A| < |B|$, jeśli $|A| \leq |B|$ oraz $A \not\sim B$.

Uwagi na temat oznaczenia mocy $|A|$ zbioru A dotyczą też porównywania mocy zbiorów. Symbolu $\leq$ nie traktujemy jako binarnej relacji zachodzącej pomiędzy tajemniczymi obiektami $|A|$ i $|B|$, same napisy $|A|$ i $|B|$ nie oznaczają niczego, zaś napis $|A| \leq |B|$ oznacza jedynie, że zachodzi określona wyżej binarna relacja między zbiorami A i B (tj. że istnieje funkcja różnowartościowa $f : A \rightarrow B$). Tak dziwny sposób zapisu tej relacji wynika z konwencji przyjętych w teorii mocy, w której napisy $|A|$ i $|B|$ faktycznie oznaczają pewne obiekty, zaś $\leq$ oznacza obiekt „podobny” do relacji binarnej. Teorii tej nie będziemy tu jednak rozwijać.

Twierdzenie 84.

1. Dla dowolnego zbioru A zachodzi $|A| \leq |A|$.
2. Jeśli $|A| \leq |B|$ i $|B| \leq |C|$, to $|A| \leq |C|$.
3. Jeśli $n < m$, to $|\underline{n}| < |\underline{m}|$.
4. Dla dowolnej liczby naturalnej n zachodzi $|\underline{n}| < |\mathbb{N}|$.

Twierdzenie 85 (Cantor-Bernstein). Jeśli $|A| \leq |B|$ oraz $|B| \leq |A|$, to $|A| = |B|$.

Twierdzenie 86. Zbiór liczb rzeczywistych jest równoliczny ze zbiorem $\{0, 1\}^{\mathbb{N}}$. Zatem zbiór $\{0, 1\}^{\mathbb{N}}$ ma moc continuum.

Definicja 87. Jeśli $X \subseteq A$, to $f : A \rightarrow \{0, 1\}$ jest *funkcją charakterystyczną* zbioru X , jeśli

$$f(a) = \begin{cases} 0, & \text{gdy } a \notin X, \\ 1, & \text{gdy } a \in X, \end{cases}$$

dla dowolnego $a \in A$.

Fakt 88. Dla dowolnego zbioru A zachodzi $\underline{2}^A \sim \mathcal{P}(A)$.

Twierdzenie 89. Niech A i B będą zbiorami, przy czym $|B| \geq 2$. Wtedy

$$|\mathcal{P}(A)| \leq |B^A|.$$

Twierdzenie 90 (Cantor). Dla żadnego zbioru A nie istnieje funkcja z A na zbiór potęgowy $\mathcal{P}(A)$.

Dowód. Przypuśćmy przeciwnie, że pewna funkcja $f : A \rightarrow \mathcal{P}(A)$ przekształca A na $\mathcal{P}(A)$. Niech

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

Ponieważ $A_0 \subseteq A$ i f odwzorowuje A na $\mathcal{P}(A)$, więc istnieje takie $a_0 \in A$, że $f(a_0) = A_0$. Mamy wtedy

$$a_0 \in A_0 \Leftrightarrow a_0 \in f(a_0) \Leftrightarrow a_0 \notin A_0.$$

Założenie istnienia funkcji f doprowadziło do sprzeczności. ■

Dowód (twierdzenia Cantora dla przypadku $A = \mathbb{N}$). Przypuśćmy przeciwnie, że pewna funkcja $f : \mathbb{N} \rightarrow \underline{2}^{\mathbb{N}}$ przekształca $\mathbb{N}$ na $\underline{2}^{\mathbb{N}}$. Tworzymy nieskończoną tablicę

$(f(0))(0)$	$(f(0))(1)$	$(f(0))(2)$	$(f(0))(3)$	$(f(0))(4)$	$\dots$
$(f(1))(0)$	$(f(1))(1)$	$(f(1))(2)$	$(f(1))(3)$	$(f(1))(4)$	$\dots$
$(f(2))(0)$	$(f(2))(1)$	$(f(2))(2)$	$(f(2))(3)$	$(f(2))(4)$	$\dots$
$(f(3))(0)$	$(f(3))(1)$	$(f(3))(2)$	$(f(3))(3)$	$(f(3))(4)$	$\dots$
$(f(4))(0)$	$(f(4))(1)$	$(f(4))(2)$	$(f(4))(3)$	$(f(4))(4)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Tworzymy nową funkcję charakterystyczną

$$g(i) = 1 - (f(i))(i)$$

dla każdego $i \in \mathbb{N}$. Wtedy $g \neq f(i)$ dla dowolnego $i \in \mathbb{N}$, gdyż $g(i) = 1 - (f(i))(i) \neq (f(i))(i)$. Otrzymaliśmy sprzeczność z założeniem, że f jest na. ■

Twierdzenie 91. Dla każdego A jest $|\mathcal{P}(A)| > |A|$. Jeśli $|B| \geq 2$, to $|B^A| > |A|$.

Zadanie 298. Udowodnij, że $1 \leq |A| \leq |B|$ wtedy i tylko wtedy, gdy istnieje funkcja $f : B \rightarrow A$, która jest „na”. (Zadanie wymaga pewnika wyboru.)

Zadanie 299. Udowodnij, że jeżeli $A \subseteq B$, to $|A| \leq |B|$.

Zadanie 300. Czy $A_1 \sim A_2$, $B_1 \sim B_2$ i $|A_1| \leq |B_1|$, implikuje, że $|A_2| \leq |B_2|$?

Zadanie 301. Udowodnij, że A jest zbiorem nieskończonym wtedy i tylko wtedy, gdy zawiera podzbiór równoliczny ze zbiorem liczb naturalnych, tj. gdy istnieje taki zbiór $B \subseteq A$, że $B \sim \mathbb{N}$. (Uwaga: zadanie jest trudne, a dowód wymaga skorzystania z pewnika wyboru).

Zadanie 302. Udowodnij, że A jest zbiorem nieskończonym wtedy i tylko wtedy, gdy jest równoliczny ze swoim właściwym podzbiorem, tj. gdy istnieje taki zbiór $B \subseteq A$, że $B \neq A$ i $A \sim B$. (Uwaga: zadanie jest trudne, a dowód wymaga skorzystania z pewnika wyboru).

Zadanie 303. Udowodnij, że A jest zbiorem nieskończonym wtedy i tylko wtedy, gdy istnieją zbiory B i C takie, że $B \cap C = \emptyset$, $B \cup C = A$ i $A \sim B \sim C$. (Uwaga: zadanie jest trudne, a dowód wymaga skorzystania z pewnika wyboru).

Zadanie 304. Wykaż, że istnieje nieskończona rodzina zbiorów nieskończonych o tej własności, że żadne dwa spośród jej elementów nie są równoliczne.

Twierdzenie Cantora-Bernsteina pozwala ustalać równoliczność zbiorów A i B za pomocą konstrukcji dwóch funkcji różnowartościowych $f : A \rightarrow B$ i $g : B \rightarrow A$. Zbudowanie takich funkcji jest często znacznie łatwiejsze niż skonstruowanie bijekcji przekształcającej zbiór A na B .

W poniższych zadaniach konstruując dwie funkcje różnowartościowe udowodnij równoliczność podanych zbiorów.

Zadanie 305. $(0, 1]$ oraz $(0, 1]^2$

Zadanie 306. $(0, 1]$ oraz $\mathbb{Z}^{\mathbb{N}}$

Zadanie 307. $\mathbb{N}$ oraz $\mathbb{N} \times \mathbb{N}$

Zadanie 308. $\mathbb{Z} \times \mathbb{N}^+$ oraz $\mathbb{Q}$

Zadanie 309. $\{0, 1\}^{\mathbb{N}}$ oraz $\mathbb{N}^{\mathbb{N}}$

6.5. Wyznaczanie mocy zbiorów

Zadanie 310. Udowodnij, że dla każdej dodatniej liczby naturalnej n zbiór $\mathbb{R}^n$, gdzie $\mathbb{R}$ jest zbiorem liczb rzeczywistych, ma moc continuum.

Zadanie 311. Niech $R_I(x, y)$ oznacza relację zdefiniowaną formułą

$$\exists p \in I ((\phi(p, x) \wedge \neg \phi(p, y)) \vee (\phi(p, y) \wedge \neg \phi(p, x)))$$

na $\mathbb{N}^+ \times \mathbb{N}^+$, gdzie $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$, I jest skończonym niepustym zbiorem liczb pierwszych, a $\phi(x, y)$ jest formułą $\exists z (x \cdot z = y)$. Niech $Q_I = (\mathbb{N}^+ \times \mathbb{N}^+) \setminus R_I$.

- a) Czy R_I jest relacją równoważności? Jeśli tak, podaj liczbę klas równoważności relacji R_I .
- b) Czy Q_I jest relacją równoważności? Jeśli tak, podaj liczbę klas równoważności relacji Q_I .

Zadanie 312. Dla danej funkcji $f : \mathbb{N} \rightarrow \mathbb{N}$ definiujemy zbiór

$$A_f = \{n \in \mathbb{N} \mid f(n) > 1\}.$$

Niech $\mathcal{A} = \{A_f \mid f \in \mathbb{N}^{\mathbb{N}}\}$. Znajdź moc zbiorów $\mathcal{A}$ oraz $\bigcup_{f \in \mathbb{N}^{\mathbb{N}}} A_f$.

Zadanie 313. Dla ciągu nieskończonego $a = \langle a_1, a_2, a_3, \dots \rangle$ o wyrazach naturalnych określamy relację R_a w taki sposób, że dla dwóch ciągów nieskończonych o wyrazach naturalnych $b = \langle b_1, b_2, b_3, \dots \rangle$ i $c = \langle c_1, c_2, c_3, \dots \rangle$ zachodzi $b R_a c$, wtedy i tylko wtedy, gdy

$$\forall n \in \mathbb{N} (a_n = 0 \Rightarrow b_n = c_n).$$

1. Pokaż, że niezależnie od wyboru ciągu a relacja R_a jest relacją równoważności.
2. Jaka jest moc zbioru takich ciągów a , dla których wszystkie klasy abstrakcji R_a są przeliczalne?
3. Jaka jest moc zbioru takich ciągów a , dla których relacja R_a ma przeliczalnie wiele klas abstrakcji?
4. Jaka jest moc zbioru takich ciągów a , dla których relacja R_a ma continuum klas abstrakcji i każda z tych klas jest mocy continuum?
5. Jaka jest moc zbioru takich ciągów a , dla których relacja R_a ma przeliczalnie wiele klas abstrakcji i każda z tych klas jest przeliczalna?
6. Jaka jest moc zbioru takich ciągów a , dla których relacja R_a ma zarówno przeliczalne, jak i nieprzeliczalne klasy abstrakcji?

Zadanie 314. Niech $P \subseteq \mathbb{R} \times \mathbb{R}$ oznacza relację taką, że

$$P(x, y) \Leftrightarrow \exists q \in \mathbb{Q} (x = y + q),$$

gdzie $\mathbb{Q}$ jest zbiorem liczb wymiernych.

- a) Czy P jest relacją równoważności?
- b) Jakie są moce klas równoważności $[r]_P$ dla liczb $r \in \mathbb{R}$? Jaka jest moc klasy równoważności $[\pi]_P$? Jak jest moc klasy równoważności $[\frac{23}{7}]_P$? Czy wszystkie klasy równoważności mają tę samą moc?
- c) Czy rodzina klas równoważności relacji P jest przeliczalna?

Zadanie 315. Czy istnieje nieprzeliczalna rodzina $\mathcal{R}$ podzbiorów $\mathbb{N}$ taka, że dla dowolnych różnych $X, Y \in \mathcal{R}$ przekrój $X \cap Y$ jest skończony?

Zadanie 316. Niech $\{X_n\}_{n \in \mathbb{N}}$ będzie dowolną rodziną podzbiorów zbioru $\mathbb{N}$.

1. Czy istnieje taki nieskończony ciąg zerojedynkowy $(i_n)_{n \in \mathbb{N}}$, że

$$\bigcap_{n=0}^{\infty} X_n^{i_n} \neq \emptyset?$$

2. Jaka jest maksymalna moc zbioru wszystkich ciągów $(i_n)_{n \in \mathbb{N}}$ spełniających powyższy wzór?

Zadanie 317. Rozważamy relację $\sim$ określoną na funkcjach ze zbioru $\mathbb{N}^{\mathbb{N}}$ w następujący sposób:

$$f \sim g \stackrel{\text{df}}{\iff} \exists c > 0 \exists k > 0 \forall n > k (f(n) \leq cg(n) \wedge g(n) \leq cf(n)).$$

1. Pokaż, że $\sim$ jest relacją równoważności.
2. Jaka jest moc klasy abstrakcji funkcji f takiej, że $f(n) = 0$ dla każdego $n \in \mathbb{N}$?
3. Jaka jest moc klasy abstrakcji funkcji g takiej, że $g(n) = 1$ dla każdego $n \in \mathbb{N}$?

Zadanie 318. Dla każdej spośród relacji opisanych w zadaniu 231, która jest relacją równoważności wyznacz moc zbioru jej klas abstrakcji oraz moc każdej z jej klas.

6.6. Zbiory przeliczalne

Twierdzenie 92. Zbiór A jest przeliczalny wtedy i tylko wtedy, gdy $A = \emptyset$ lub istnieje funkcja z $\mathbb{N}$ na A .

Definicja 93. Ciągami elementów zbioru A nazywamy funkcję $f : \mathbb{N} \rightarrow A$.

Fakt 94. Zbiór niepusty jest przeliczalny, gdy wszystkie jego elementy można ustawić w ciąg.

Twierdzenie 95.

1. Podzbiór zbioru przeliczalnego jest przeliczalny.
2. Jeśli $f : A \rightarrow B$ oraz $X \subseteq A$ jest zbiorem przeliczalnym, to $f(X)$ też jest zbiorem przeliczalnym.
3. Jeśli A i B są przeliczalne, to $A \times B$ jest przeliczalny.

4. Jeśli $\{A_i\}_{i \in I}$ jest przeliczalną rodziną zbiorów przeliczalnych (tzn. I jest przeliczalny i każdy ze zbiorów A_i jest przeliczalny), to $\bigcup_{i \in I} A_i$ jest zbiorem przeliczalnym.

Zadanie 319. Niech $\mathcal{A}$ będzie przeliczalną rodziną zbiorów przeliczalnych. Pokaż, że $\bigcup \mathcal{A}$ i $\bigcap \mathcal{A}$ są zbiorami przeliczalnymi.

Zadanie 320. Niech $A \subseteq \mathbb{N}$ będzie zbiorem nieskończonym. Zdefiniuj bijekcje $f : A \rightarrow \mathbb{N}$ i $g : \mathbb{N} \rightarrow A$.

Zadanie 321. Niech A będzie nieskończonym zbiorem przeliczalnym i niech $f : A \rightarrow B$ będzie surjekcją (odwzorowaniem “na”). Zbuduj injekcję (funkcję różnowartościową) $g : B \rightarrow A$.

Zadanie 322. Udowodnij, że jeśli $f : \mathbb{R} \rightarrow \mathbb{R}$ jest monotoniczna, to zbiór jej punktów nieciągłości jest przeliczalny.

Zadanie 323. Czy istnieje taki zbiór A , że $\mathcal{P}(A) \sim \mathbb{N}$?

Zadanie 324. Niech $A_1 \sim B_1$ i $A_2 \sim B_2$. Czy:

1. $A_1 \times A_2 \sim B_1 \times B_2$,
2. $A_1 \cap A_2 \sim B_1 \cap B_2$,
3. $A_1 \cup A_2 \sim B_1 \cup B_2$?

W punkcie 3. możesz założyć, że zbiory A_1 , A_2 , B_1 i B_2 są przeliczalne (zadanie bez tego założenia jest trudne i wymaga użycia pewnika wyboru). Czy odpowiedzi na powyższe pytania ulegną zmianie, jeśli założymy, że jeden ze zbiorów A_1 lub A_2 jest nieskończony? Czy ulegną one zmianie jeśli założymy, że oba zbiory są nieskończone?

Zadanie 325. Zbiory A i B są przeliczalne oraz zbiór $A \times B$ jest nieskończony. Co można powiedzieć o mocach zbiorów A i B ?

Zadanie 326. Udowodnij, że zbiór wszystkich skończonych ciągów o elementach ze skończonego zbioru A jest przeliczalny.

Zadanie 327. Udowodnij, że zbiór wszystkich skończonych ciągów o elementach ze przeliczalnego zbioru A jest przeliczalny.

Zadanie 328. Udowodnij, że zbiór wielomianów jednej zmiennej o współczynnikach wymiernych jest przeliczalny.

Zadanie 329. Wykaż, że zbiór słabo rosnących funkcji $f : \mathbb{N} \rightarrow \mathbb{N}$ jest nieprzeliczalny (funkcja $f : \mathbb{N} \rightarrow \mathbb{N}$ jest *słabo rosnąca*, jeśli implikacja $x > y \Rightarrow f(x) \geq f(y)$ zachodzi dla wszelkich $x, y \in \mathbb{N}$).

Zadanie 330. Jaka jest moc zbioru nieskończonych ciągów o wyrazach wymiernych?

Zadanie 331. Jaka jest moc zbioru nieskończonych ciągów o wyrazach wymiernych, stałych od pewnego miejsca?

Zadanie 332. Ile jest ciągów liczb wymiernych zbieżnych do 1?

Zadanie 333. Ile jest rosnących ciągów liczb wymiernych zbieżnych do 1?

Zadanie 334. Czy zbiór nieskończonych nierosnących ciągów o wyrazach naturalnych jest przeliczalny? (Ciąg $(a_i)_{i \in \mathbb{N}}$ jest nierosnący, jeśli $a_i \geq a_{i+1}$ dla każdego $i \in \mathbb{N}$).

Zadanie 335. Wykaż, że zbiór słabo malejących funkcji $f : \mathbb{N} \rightarrow \mathbb{N}$ jest przeliczalny (funkcja $f : \mathbb{N} \rightarrow \mathbb{N}$ jest *słabo malejąca*, jeśli $x > y \Rightarrow f(x) \leq f(y)$ dla wszelkich $x, y \in \mathbb{N}$).

Zadanie 336. Liczba a jest punktem skupienia ciągu $(x_i)_{i=1}^{\infty}$ liczb rzeczywistych, jeśli istnieje podciąg (x_{j_i}) ciągu (x_i) zbieżny do a . Ile ciąg może mieć punktów skupienia?

Zadanie 337. Ile jest bijekcji $f : A \rightarrow A$, gdy zbiór A jest przeliczalny?

Zadanie 338. Liczba rzeczywista x jest *algebraiczna*, jeśli istnieje taki wielomian jednej zmiennej o współczynnikach wymiernych, że x jest jego pierwiastkiem. Udowodnij, że zbiór liczb algebraicznych jest przeliczalny.

Zadanie 339. Jaka jest moc zbioru wszystkich nieskończonych niemalejących ciągów o wyrazach naturalnych? Jaka jest, dla danego n , moc zbioru wszystkich nieskończonych niemalejących ciągów o wyrazach ze zbioru $\{0, \dots, n-1\}$?

Zadanie 340. Wykaż, że jeśli $\sim$ jest relacją równoważności w zbiorze przeliczalnym A , to zbiór klas równoważności $A/\sim = \{[a]_{\sim} : a \in A\}$ jest przeliczalny.

Zadanie 341. Wiadomo, że $\sim$ jest relacją równoważności na zbiorze A , zbiór klas równoważności $A/\sim$ jest przeliczalny oraz dla każdego $a \in A$, klasa równoważności $[a]_{\sim}$ elementu a jest przeliczalna. Wykaż, że zbiór A jest przeliczalny.

Zadanie 342. Czy zbiór relacji równoważności na zbiorze przeliczalnym jest zbiorem przeliczalnym?

Zadanie 343. Dany jest nieskończony przeliczalny zbiór A i liczba $n \in \mathbb{N}$. Ile jest takich relacji równoważności $\sim$ na zbiorze A , że dla każdego $a \in A$ klasa abstrakcji $[a]_{\sim}$ ma dokładnie n elementów?

Zadanie 344. Ile jest relacji równoważności na przeliczalnym zbiorze A takich, że wszystkie ich klasy abstrakcji są skończone?

Zadanie 345. Niech zbiory $A \cup B$ i $C \cup D$ będą przeliczalne nieskończone. Która z poniższych formuł wynika z tego założenia? Uzasadnij swoje odpowiedzi.

$$\begin{aligned} A &\sim C \vee B \sim D \\ A &\sim C \vee A \sim D \vee B \sim C \vee B \sim D \\ (A &\sim C \wedge B \sim D) \vee (A \sim D \wedge B \sim C) \\ A &\sim C \vee A \sim D \end{aligned}$$

Zadanie 346. Mówimy, że ciąg liczb rzeczywistych $(y_n)_{n \in \mathbb{N}}$ *rośnie szybciej* niż ciąg $(x_n)_{n \in \mathbb{N}}$, gdy

$$\lim_{n \rightarrow \infty} \frac{x_n}{y_n} = 0.$$

Pokaż, że dla każdego ciągu $(x_n)_{n \in \mathbb{N}}$ istnieje ciąg rosnący od niego szybciej. Niech $\mathfrak{S}$ będzie zbiorem ciągów liczb rzeczywistych o tej własności, że dla każdego ciągu liczb rzeczywistych $(x_n)_{n \in \mathbb{N}}$ istnieje w zbiorze $\mathfrak{S}$ ciąg $(y_n)_{n \in \mathbb{N}} \in \mathfrak{S}$ rosnący od niego szybciej. Wykorzystując metodę przekątniową udowodnij, że $\mathfrak{S}$ nie jest zbiorem przeliczalnym.

Zadanie 347. Udowodnij, że każdy zbiór rozłącznych odcinków na prostej jest przeliczalny. Pokaż, że istnieje nieprzeliczalny zbiór rozłącznych odcinków na płaszczyźnie.

Zadanie 348. Udowodnij, że każdy zbiór rozłącznych kół na płaszczyźnie jest przeliczalny. Pokaż, że istnieje nieprzeliczalny zbiór rozłącznych okręgów na płaszczyźnie. Koło to zbiór punktów $\langle x, y \rangle$ spełniających warunek

$$(x - x_0)^2 + (y - y_0)^2 \leq r^2$$

dla pewnego punktu $\langle x_0, y_0 \rangle$ i dodatniej liczby rzeczywistej r , a okrąg to zbiór punktów $\langle x, y \rangle$ spełniających warunek

$$(x - x_0)^2 + (y - y_0)^2 = r^2.$$

Zadanie 349. Ósemka, to dwa zewnętrznie styczne okręgi. Udowodnij, że każdy zbiór rozłącznych ósemek na płaszczyźnie jest przeliczalny. Czy można ułożyć na płaszczyźnie więcej niż przeliczalnie wiele rozłącznych okręgów?

Zadanie 350. T-kształt, to figura na płaszczyźnie, złożona z pary prostopadłych odcinków o niezerowej długości, z których jeden końcem styka się z drugim w miejscu różnym od końca tego drugiego (dlatego ta figura przypomina literę T). Krzyż, to figura złożona z pary nierównoległych, przecinających się odcinków niezerowej długości, które nie mają wspólnych końców. Jak wiele rozłącznych T-kształtów można ułożyć na płaszczyźnie? Jak wiele krzyży można ułożyć na płaszczyźnie?

Zadanie 351. Parasol, to bryła złożona z koła o niezerowej średnicy i prostopadłego do niego odcinka o niezerowej długości, który styka się swym końcem ze środkiem koła. Pokaż, że każdy zbiór rozłącznych parasoli w przestrzeni trójwymiarowej jest co najwyżej przeliczalny.

Zadanie 352. Ile jest wszystkich funkcji $f : \mathbb{N} \rightarrow \mathbb{N}$? A ile jest funkcji $f : \mathbb{N} \rightarrow \mathbb{N}$ których wartość możemy obliczać przy pomocy komputera (tj. takich, dla których istnieje program komputerowy, który wczytuje liczbę naturalną n i wypisuje liczbę $f(n)$ dla dowolnego $n \in \mathbb{N}$)?

7

Relacje porządku

Definicja 96. *Częściowym porządkiem w zbiorze A nazywamy relację $\leq$ (będącą podzbiorem A^2), która jest zwrotna, przechodnia i słabo antysymetryczna, tzn. prawdziwe są formuły*

- $\forall a \in A (a \leq a)$,
- $\forall a, b \in A (a \leq b \wedge b \leq a \Rightarrow a = b)$,
- $\forall a, b, c \in A (a \leq b \wedge b \leq c \Rightarrow a \leq c)$.

Definicja 97. Jeśli $\leq$ jest częściowym porządkiem na A , to $a < b$ oznacza

$$a \leq b \wedge a \neq b.$$

Definicja 98. *Zbiór częściowo uporządkowany, to zbiór A z relacją częściowego porządku $\leq$. Zbiór częściowo uporządkowany oznaczamy $\langle A, \leq \rangle$.*

Przykład 99. Oto przykłady zbiorów uporządkowanych:

1. $\langle \mathcal{P}(A), \subseteq \rangle$ (rodzina podzbiorów zbioru A z relacją inkluzji);
2. $\langle \mathbb{N}, \leq \rangle$ (zbiór liczb naturalnych ze zwykłym porządkiem);
3. $\langle \mathcal{B}, \subseteq \rangle$, gdzie $\mathcal{B} \subseteq \mathcal{P}(A)$;
4. $\langle \mathbb{N}, | \rangle$, gdzie $a|b \stackrel{\text{df}}{\Leftrightarrow} \exists x (ax = b)$.

Definicja 100. Porządek częściowy $\leq$ w zbiorze A jest *liniowy*, jeśli

$$\text{dla dowolnych } a, b \in A \text{ zachodzi } a \leq b \text{ lub } b \leq a.$$

Przykład 101. Porządkiem liniowym jest relacja $\leq$ na zbiorze liczb rzeczywistych. Relacja inkluzji $\subseteq$ na zbiorze $\mathcal{P}(\mathbb{N})$ nie jest porządkiem liniowym.

Definicja 102. Łańcuchem w zbiorze uporządkowanym $\langle A, \leq \rangle$ nazywamy taki podzbiór L zbioru A , że dla wszystkich $a, b \in L$ zachodzi $a \leq b$ lub $b \leq a$. Antylańcuchem w $\langle A, \leq \rangle$ nazywamy taki podzbiór L zbioru A , że dla wszystkich $a, b \in L$ jeśli zachodzi $a \leq b$ lub $b \leq a$, to $a = b$.

Innymi słowy, łańcuch to dowolny liniowo uporządkowany podzbiór A , natomiast antylańcuch to dowolny podzbiór składający się z elementów wzajemnie nieporównywalnych.

7.1. Przykłady porządków

Zadanie 353. Niech A będzie zbiorem niepustym oraz niech $\langle B, \leq_B \rangle$ będzie porządkiem częściowym. Na zbiorze funkcji B^A określamy relację $\leq$ przyjmując, że dla $f, g \in B^A$ jest $f \leq g$, wtedy i tylko wtedy, gdy $f(a) \leq_B g(a)$ dla każdego $a \in A$. Wykaż, że $\langle B^A, \leq \rangle$ jest porządkiem częściowym.

Zadanie 354. Podaj przykład przeliczalnego zbioru uporządkowanego, zawierającego zarówno nieskończony łańcuch jak i nieskończony antylańcuch.

Zadanie 355. Pokaż, że na zbiorze liczb zespolonych $\mathbb{C}$ nie można wprowadzić takiego porządku $\leq$, że jednocześnie:

- zero jest porównywalne z każdą liczbą zespoloną, tj. $z = 0$ lub $z > 0$ lub $z < 0$ dla każdej liczby $z \in \mathbb{C}$;
- porządek $\leq$ jest zgodny z działaniami arytmetycznymi, dokładniej $-z < 0$ i $wz > 0$ dla dowolnych $w, z > 0$ oraz $-z > 0$ dla dowolnego $z < 0$.

Zadanie 356. Czy dla danego zbioru $X \neq \emptyset$ można tak określić relację R , by równocześnie:

1. zbiór $\langle X, R \rangle$ był zbiorem częściowo uporządkowanym,
2. R była relacją równoważności w X ?

Zadanie 357. Czy dla danego takiego zbioru X , że $|X| \geq 2$ można określić taką relację R , by równocześnie:

1. zbiór $\langle X, R \rangle$ był zbiorem liniowo uporządkowanym,
2. R była relacją równoważności w X ?

Zadanie 358. Na zbiorze $\mathbb{N}^{\mathbb{N}}$ określamy relacje:

1. $f R_1 g$ jeśli $|\{n \in \mathbb{N} \mid f(n) \neq g(n)\}| < \infty$,
2. $f R_2 g$ jeśli $|\{n \in \mathbb{N} \mid f(n) \neq g(n)\}| < 5$,

3. $f R_3 g$ jeśli $|\{n \in \mathbb{N} \mid f(n) < g(n)\}| < \infty$,
4. $f R_4 g$ jeśli $|\{n \in \mathbb{N} \mid f(n) < g(n)\}| < 5$,
5. $f R_5 g$ jeśli $f(n) \leq g(n)$ dla każdego $n \in \mathbb{N}$.

Które z nich są relacjami a) równoważności, b) częściowego porządku, c) liniowego porządku?

Definicja 103. Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Na zbiorze A^* skończonych ciągów elementów zbioru A określamy relację $\leq_{lex}$ przyjmując, że dla dowolnych $u, w \in A^*$ zachodzi $u \leq_{lex} w$ wtedy i tylko wtedy, gdy u jest przedrostkiem w lub istnieje $i \leq \min(|u|, |w|)$ takie, że dla $j < i$ zachodzi $u(j) = w(j)$ oraz $u(i) < w(i)$. Relację $\leq_{lex}$ nazywamy *porządkiem leksykograficznym* na A^* generowanym przez porządek $\leq$.

Zadanie 359. Wykaż, że relacja $\leq_{lex}$ jest porządkiem częściowym.

Zadanie 360. Wykaż, że jeśli $\langle A, \leq \rangle$ jest porządkiem liniowym, to $\langle A^*, \leq_{lex} \rangle$ też jest porządkiem liniowym (udowodnij tylko liniowość). Czy zachodzi implikacja w drugą stronę?

Zadanie 361. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą porządkami liniowymi. Relację $\leq$ na $A \times B$ określamy wzorem

$$\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle \stackrel{\text{df}}{\Leftrightarrow} a_1 \leq_A a_2 \wedge b_1 \leq_B b_2$$

Wykaż, że: a) $\leq$ jest porządkiem częściowym na $A \times B$, b) $\leq$ jest porządkiem liniowym wtedy i tylko wtedy, gdy zbiór A lub zbiór B jest co najwyżej jednoelementowy.

Zadanie 362. Kandydaci do objęcia pewnego stanowiska oceniani są w $k \in \mathbb{N}$ różnych kategoriach. W każdej z tych kategorii otrzymują ocenę będącą liczbą naturalną nie mniejszą niż 1 i nie większą niż 6. Kandydat k_1 uważany jest za lepszego niż k_2 (co zapisujemy jako $k_1 L k_2$) jeśli k_1 ma wyższe oceny niż k_2 we wszystkich kategoriach oprócz co najwyżej dwóch. Niech R będzie najmniejszą zwrotną relacją taką, że $RR \subseteq R$ i $L \subseteq R$. Czy R jest częściowym porządkiem, jeśli:

- a) $k = 12$,
- b) $k = 13$?

Zadanie 363. Niech R będzie relacją zwrotną i przechodnią. Łańcuchem względem R nazywamy ciąg $\langle a_1, \dots, a_n \rangle$ taki, że $\langle a_i, a_{i+1} \rangle \in R$ dla $i \in \{1, \dots, n-1\}$ oraz $a_i \neq a_j$ dla $i \neq j$. Łańcuch $\langle a_1, \dots, a_n \rangle$ jest *cyklem* względem R , jeśli $n > 1$ i $\langle a_n, a_1 \rangle \in R$. Udowodnij, że jeśli nie istnieje cykl względem R , to R jest porządkiem częściowym.

Definicja 104. Porządek $\leq$ na zbiorze A jest *gęsty*, gdy dla dowolnych takich $a, b \in A$, że $a < b$, istnieje taki $c \in A$, że $a < c < b$.

Zadanie 364. Niech symbol $\leq$ oznacza liniowy porządek w niepustym, skończonym zbiorze A . Udowodnij, że porządek $\leq$ jest gęsty wtedy i tylko wtedy, gdy zbiór A jest jednoelementowy.

Zadanie 365. *Wielomianem jednej zmiennej* nad zbiorem liczb rzeczywistych $\mathbb{R}$ nazywamy funkcję daną wzorem

$$P(x) = \sum_{i=0}^n a_i x^i,$$

gdzie $a_i \in \mathbb{R}$ dla $i = 0, \dots, n$. Niech $\mathbb{R}[x]$ oznacza zbiór wielomianów jednej zmiennej nad $\mathbb{R}$. a) Wyznacz moc zbioru $\mathbb{R}[x]$. Na zbiorze $\mathbb{R}[x]$ definiujemy relację $\preceq$ w następujący sposób:

$$P \preceq Q \stackrel{\text{df}}{\Leftrightarrow} \exists x \in \mathbb{R} \forall y \in \mathbb{R} (x \leq y \Rightarrow P(y) \leq Q(y)),$$

dla $P, Q \in \mathbb{R}[x]$. Udowodnij, że relacja $\preceq$ jest porządkiem na $\mathbb{R}[x]$. Czy jest to porządek a) liniowy, b) gęsty?

7.2. Elementy wyróżnione

Definicja 105. Niech $\langle P, \leq \rangle$ będzie porządkiem częściowym i niech $X \subseteq P$. Element $x \in X$ jest *elementem największym* (odpowiednio *najmniejszym*) w X , jeśli dla każdego $y \in X$ zachodzi $y \leq x$ (odpowiednio $x \leq y$). Element najmniejszy zbioru P oznacza się $\perp$, zaś największy $\top$.

Definicja 106. Element $x \in X$ jest elementem *maksymalnym* (odpowiednio *minimalnym*) w X , jeśli dla każdego $y \in X$ z warunku $x \leq y$ (odpowiednio $y \leq x$) wynika $x = y$.

Elementy minimalne, maksymalne, najmniejsze i największe w zbiorze uporządkowanym, podobnie jak zdefiniowane w rozdziale 9 kresy i ograniczenia, nazywamy *elementami wyróżnionymi*.

Definicja 107. Niech $\langle P, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Porządek $\langle P, \leq^{-1} \rangle$ nazywamy porządkiem *dualnym* do $\langle P, \leq \rangle$. Jeśli dane jest pojęcie Q dotyczące porządków, to pojęcie Q^{-1} dualne do niego otrzymujemy przez zastąpienie w definicji Q symbolu $\leq$ przez symbol $\leq^{-1}$. Zauważmy, że pojęcia minimalny i maksymalny oraz najmniejszy i największy są dualne.

Twierdzenie 108. Niech $\langle P, \leq \rangle$ będzie częściowym porządkiem i niech $X \subseteq P$. Wtedy element największy w X jest elementem maksymalnym w X .

Twierdzenie 109. Niech $\langle P, \leq \rangle$ będzie zbiorem uporządkowanym. Dla dowolnego zbioru $X \subseteq P$ istnieje co najwyżej jeden element największy tego zbioru.

Zatem każdy zbiór posiada też co najwyżej jeden element najmniejszy. Elementów maksymalnych i minimalnych może być natomiast wiele.

Przykład 110. Niech X będzie zbiorem niepustym i niech $P = \mathcal{P}(X) \setminus \{\emptyset\}$. Wtedy w zbiorze uporządkowanym $\langle P, \subseteq \rangle$ jest $|X|$ elementów minimalnych.

Zadanie 366. Rozważmy relację $|$ na zbiorze $\mathbb{N} \setminus \{0\}$.

1. Znajdź zbiór elementów minimalnych w zbiorze $\langle \mathbb{N} \setminus \{0\}, | \rangle$.
2. Udowodnij, że w zbiorze $\langle \mathbb{N} \setminus \{0\}, | \rangle$ nie ma elementów maksymalnych.

Zadanie 367.

1. Znajdź ogólną postać łańcucha w zbiorze $\langle \mathbb{N} \setminus \{0\}, | \rangle$,
2. Udowodnij, że relacja inkluzji w zbiorze łańcuchów zbioru $\langle \mathbb{N} \setminus \{0\}, | \rangle$ jest częściowym porządkiem. Znajdź postać łańcuchów minimalnych i maksymalnych względem relacji inkluzji.

Zadanie 368. Znajdź przykład zbioru częściowo uporządkowanego $\langle X, R \rangle$ takiego, że w zbiorze $\langle X, R \rangle$ jest dokładnie jeden element maksymalny i nie ma elementu największego. Znajdź przykład zbioru częściowo uporządkowanego $\langle X, R \rangle$, takiego, że w zbiorze $\langle X, R \rangle$ jest dokładnie jeden element minimalny i nie ma elementu najmniejszego.

Zadanie 369. Znajdź elementy minimalne, maksymalne, największy i najmniejszy w zbiorze $\langle \mathbb{N}^{\mathbb{N}}, R \rangle$ z zadania 377.

7.3. Izomorfizm porządkowy

Definicja 111. Zbiory uporządkowane $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ są *izomorficzne*, jeżeli istnieje bijekcja $\phi : A \rightarrow B$ zachowująca porządek, tzn. taka, że $\phi(a_1) \leq_B \phi(a_2)$ wtedy i tylko wtedy, gdy $a_1 \leq_A a_2$, dla wszelkich $a_1, a_2 \in A$.

Definicja 112. Niech $\langle P, \leq_P \rangle$ oraz $\langle Q, \leq_Q \rangle$ będą zbiorami częściowo uporządkowanymi. Funkcja $f : P \rightarrow Q$ jest *monotoniczna*, jeśli

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

Fakt 113. Funkcja ϕ jest izomorfizmem porządkowym, jeśli jest bijekcją oraz ϕ i ϕ^{-1} są monotoniczne.

Twierdzenie poniżej mówi, że izomorfizmy porządkowe zachowują elementy wyróżnione.

Twierdzenie 114. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą zbiorami uporządkowanymi, $\phi : A \rightarrow B$ izomorfizmem porządkowym i niech $X \subseteq A$. Wtedy a jest elementem najmniejszym (odpowiednio, minimalnym, największym, maksymalnym) w X wtedy i tylko wtedy, gdy $\phi(a)$ jest elementem najmniejszym (odpowiednio, minimalnym, największym, maksymalnym) w $\phi(X)$.

W poniższych zadaniach $\mathbb{Q}$ oznacza zbiór liczb wymiernych, $\mathbb{R}$ — zbiór liczb rzeczywistych, (a, b) — przedział otwarty o końcach a i b , $[a, b]$ zaś — przedział domknięty.

Zadanie 370. Udowodnij, że funkcja $f : \mathbb{R} \rightarrow (-1, 1)$ (gdzie oba zbiory są uporządkowane zwykłą relacją porządku) dana wzorem $f(x) = \frac{x}{1+|x|}$ jest izomorfizmem porządkowym.

Zadanie 371. Udowodnij, że zbiory $\mathbb{Q}$, $\mathbb{Q} \cap (0, 1)$ i $\mathbb{Q} \setminus [0, 1)$ uporządkowane zwykłą relacją porządku są izomorficzne.

Zadanie 372. Udowodnij, że zbiory $\mathbb{Q}$, $\mathbb{Q} \setminus \{0\}$ i $\mathbb{Q} \setminus [0, 1]$ uporządkowane zwykłą relacją porządku są izomorficzne.

Definicja 115. Porządek $\leq$ na zbiorze A jest:

- *gęsty*, jeśli pomiędzy każdą parą elementów zbioru A znajduje się trzeci element, tj. gdy dla dowolnych takich $a, b \in A$, że $a < b$, istnieje taki $c \in A$, że $a < c < b$;
- *bez końców*, jeśli dla dowolnego elementu zbioru A istnieje element od niego większy i element od niego mniejszy, tj. gdy dla każdego $a \in A$ istnieją takie $b, c \in A$, że $b < a < c$.

Dla przykładu zwykły porządek na wszystkich pięciu zbiorach z zadań 371 i 372 jest gęsty i bez końców. Zbiory te są izomorficzne nie przez przypadek, o czym przekonasz się rozwiązując kolejne zadanie. Zauważ ponadto, że zwykły porządek na zbiorze $\mathbb{Q} \setminus (0, 1)$ nie jest gęsty, a na zbiorze $\mathbb{Q} \cap [0, 1]$ nie jest bez końców.

Zadanie 373. Pokaż, że dowolne dwa zbiory przeliczalne uporządkowane liniowymi, gęstymi relacjami porządku bez końców są izomorficzne.

Zadanie 374. Uzasadnij, że twierdzenie z poprzedniego zadania jest fałszywe dla zbiorów nieprzeliczalnych, tj. podaj przykład dwóch nieprzeliczalnych zbiorów tej samej mocy, uporządkowanych liniowymi, gęstymi relacjami porządku bez końców, które nie są izomorficzne.

Zadanie 375. Pokaż, że zbiory: liczb naturalnych ze zwykłym porządkiem i skończonych ciągów liczb naturalnych z porządkiem leksykograficznym generowanym przez zwykły porządek na liczbach naturalnych *nie są* izomorficzne.

Zadanie 376. Pokaż, że zbiory: liczb rzeczywistych ze zwykłym porządkiem i skończonych ciągów liczb rzeczywistych z porządkiem leksykograficznym generowanym przez zwykły porządek na liczbach rzeczywistych *nie są* izomorficzne.

Zadanie 377. W zbiorze $\mathbb{N}^{\mathbb{N}}$ wprowadzamy relację R wzorem

$$\bar{a} R \bar{b} \stackrel{\text{df}}{\Leftrightarrow} \forall n (a_n \leq b_n),$$

dla $\bar{a} = (a_k)_{k \in \mathbb{N}}$ i $\bar{b} = (b_k)_{k \in \mathbb{N}}$. Udowodnij, że zbiór $\langle \mathbb{N}^{\mathbb{N}}, R \rangle$ jest częściowo uporządkowany. Czy R jest liniowym porządkiem? Czy jest gęstym porządkiem? Czy ten porządek jest izomorficzny z $\langle \mathbb{R}, \leq \rangle$?

Zadanie 378. W zbiorze $\mathbb{C}$ liczb zespolonych wprowadzamy porządek

$$x R y \stackrel{\text{df}}{\Leftrightarrow} \operatorname{Re} x < \operatorname{Re} y \vee (\operatorname{Re} x = \operatorname{Re} y \wedge \operatorname{Im} x \leq \operatorname{Im} y).$$

Udowodnij, że R jest liniowym gęstym porządkiem bez końców. Czy $\langle \mathbb{C}, R \rangle$ jest izomorficzny z $\langle \mathbb{R}, \leq \rangle$?

Definicja 116. Niech $\langle X, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. *Następnikiem* $x \in X$ nazywamy taki element $y \in X$, że $x < y$ i dla każdego takiego $z \in X$, że $z < y$ zachodzi $z \leq x$. Podobnie *poprzednikiem* $x \in X$ nazywamy taki element $y \in X$, że $y < x$ i dla każdego takiego $z \in X$, że $y < z$ zachodzi $x \leq z$.

Zadanie 379. Udowodnij, że każdy taki niepusty zbiór liniowo uporządkowany $\langle X, \preceq \rangle$, że każdy jego element posiada poprzednik i następnik, oraz że jeśli $x \preceq y$, to zbiór $\{z \mid x \preceq z \wedge z \preceq y\}$ jest skończony, jest izomorficzny ze zbiorem $\langle \mathbb{Z}, \leq \rangle$ liczb całkowitych uporządkowanym standardową relacją mniejszości $\leq$.

Zadanie 380. Podaj przykład przeliczalnego liniowego porządku takiego, że każdy element posiada następnik, istnieje element najmniejszy, każdy element prócz najmniejszego posiada poprzednik, ale nie izomorficznego z $\langle \mathbb{N}, \leq \rangle$.

Zadanie 381. W zbiorze $\mathbb{R}/\sim$, gdzie $\sim$ jest relacją z zadania 242, definiujemy taką relację $\preceq$, że

$$[x]_{\sim} \preceq [y]_{\sim} \stackrel{\text{df}}{\iff} x \sim y \vee x < y,$$

gdzie $\leq$ jest standardowym porządkiem na liczbach rzeczywistych. Uzasadnij, że definicja $\preceq$ jest poprawna. Udowodnij, że $\langle \mathbb{R}/\sim, \preceq \rangle$ jest zbiorem liniowo uporządkowanym. Pokaż, że $\langle \mathbb{R}/\sim, \preceq \rangle$ i $\langle \mathbb{Z}, \leq \rangle$ są izomorficzne porządkowo, gdzie $\langle \mathbb{Z}, \leq \rangle$ jest zbiorem liczb całkowitych ze standardowym porządkiem.

7.4. Zawieranie zbiorów jako relacja porządku

Definicja 117. Rodzina zbiorów $\{A_t\}_{t \in T}$ jest *prawie rozłączna*, jeśli dla wszelkich różnych $s, t \in T$ zbiór $A_t \cap A_s$ jest skończony.

Zadanie 382 (Sierpiński). Pokaż, że w $\mathcal{P}(\mathbb{N})$ istnieje rodzina mocy continuum zbiorów prawie rozłącznych.

Zadanie 383. Pokaż, że w $\langle \mathcal{P}(\mathbb{N}), \subseteq \rangle$ istnieje antyłańcuch mocy continuum.

Zadanie 384. Pokaż, że w $\langle \mathcal{P}(\mathbb{N}), \subseteq \rangle$ istnieje łańcuch mocy continuum.

Definicja 118. Dla danego zbioru X , filtrem w zbiorze $\mathcal{P}(X)$ nazywamy taki zbiór $\mathcal{F} \subset \mathcal{P}(X)$, że jeśli $A \in \mathcal{F}$ i $A \subseteq B \subseteq X$, to również $B \in \mathcal{F}$, oraz jeśli $A, B \in \mathcal{F}$, to również $A \cap B \in \mathcal{F}$.

Zadanie 385. Udowodnij, że jeśli $A \subseteq X$ to $\{B \subseteq X \mid A \subseteq B\}$ jest filtrem. Nazywamy go *filtrem głównym wyznaczonym przez A* .

Zadanie 386. Pokaż, że jeśli X jest zbiorem skończonym, to każdy filtr na $\mathcal{P}(X)$ jest główny.

Zadanie 387. Pokaż, że jeśli X jest zbiorem nieskończonym, to istnieje filtr na $\mathcal{P}(X)$, który nie jest główny.

Zadanie 388. Niech $\mathcal{F}$ będzie filtrem na $\mathcal{P}(\mathbb{N})$. Dla ciągów o wyrazach naturalnych określamy relację R jak następuje: $\bar{a}R\bar{b}$ wtedy i tylko wtedy, gdy $\{n \mid a_n = b_n\} \in \mathcal{F}$. Udowodnij, że R jest relacją równoważności.

7.5. Liczba relacji porządku

Zadanie 389. Ile jest relacji częściowego porządku w zbiorze n -elementowym?

Zadanie 390. Ile jest relacji porządku liniowego w zbiorze n elementowym?

Zadanie 391. Niech $\preceq$ oznacza porządek częściowy na liczbach naturalnych. Mówimy, że $\preceq$ jest *zgodny* ze zwykłym porządkiem, gdy

$$\forall n_1, n_2 \in \mathbb{N} \quad (n_1 \preceq n_2 \Rightarrow n_1 \leq n_2).$$

Ile jest porządków częściowych $\preceq \subseteq \mathbb{N} \times \mathbb{N}$ zgodnych ze zwykłym porządkiem i takich, że

1. w każdym antyłańcuchu są co najwyżej dwa elementy?
2. co najwyżej skończona liczba elementów należy do jakiegoś łańcucha o liczbie elementów większej niż 1?
3. zbiór

$$\{x \mid \exists y (x \neq y \wedge (y \preceq x \vee x \preceq y))\}$$

jest skończony?

4. w zbiorze $\langle \mathbb{N}, \preceq \rangle$ istnieje element największy?
5. w każdym łańcuchu są co najwyżej dwa elementy?

8

Języki formalne

Definicja 119. Niech A będzie dowolnym zbiorem. Będziemy nazywać go *alfabetem*. Słowem nad alfabetem A nazywamy dowolny skończony ciąg elementów zbioru A . Słowo puste (ciąg długości zero) oznaczamy ϵ . Przez A^* oznaczamy zbiór wszystkich słów nad alfabetem A . Jeżeli $u = u_1u_2 \dots u_n$ i $w = w_1w_2 \dots w_m$, to uw oznacza złożenie (konkatenację) słów u i w , tj. słowo $u_1u_2 \dots u_nw_1w_2 \dots w_m$. Słowo u jest przedrostkiem (prefiksem) słowa w , jeśli istnieje takie słowo v , że $uv = w$. Podobnie, słowo u jest przyrostkiem (sufiksem) słowa w , jeśli istnieje takie słowo v , że $vu = w$.

Fakt 120. Niech A będzie dowolnym zbiorem i niech $u \leq w$ oznacza, że u jest przedrostkiem w . Wtedy $\langle A, \leq \rangle$ jest zbiorem częściowo uporządkowanym.

Definicja 121. Niech L będzie zbiorem słów (językiem) nad alfabetem $\{0, 1\}$. Mówimy, że słowa $u, v \in \{0, 1\}^*$ są równoważne względem języka L , jeżeli prawdziwa jest formuła

$$\forall x \in \{0, 1\}^* (ux \in L \Leftrightarrow vx \in L).$$

Zapis $u \sim_L v$ oznacza, że słowa u i v są równoważne względem języka L .

Dla danego słowa w nad ustalonym alfabetem przez w^n oznaczamy słowo $\underbrace{ww \dots w}_n$.

Formalnie

$$\begin{aligned} w^0 &= \epsilon, \\ w^{n+1} &= ww^n, \end{aligned}$$

gdzie ϵ jest słowem pustym. Przez w^* oznaczamy zbiór słów postaci w^n dla wszystkich naturalnych n , tj. $w^* = \{w^n \mid n \in \mathbb{N}\}$.

Zadanie 392. Wykaż, że $\sim_L$ jest relacją równoważności.

Zbiór klas równoważności relacji $\sim_L$ oznaczamy $\mathcal{Q}(L)$.

Zadanie 393. Pokaż, że jeśli dla pewnych słów $w \in L$ i $v \in \{0, 1\}^*$ zachodzi $wv \in [w]_{\sim}$, to $ww^n \in L$ dla każdego $n \in \mathbb{N}$.

Zadanie 394. Opisz klasy abstrakcji relacji $\sim_L$ równoważności słów względem następujących języków:

$$L_1 = \{1^n \mid 1 \leq n \leq 6\}$$

$$L_2 = (0011)^*$$

$$L_3 = \{0^n 1^n \mid n \in \mathbb{N}\}$$

Zadanie 395. Dla języka L nad alfabetem $\{0, 1\}$ określamy funkcje

$$f : \mathcal{Q}(L) \times \mathcal{Q}(L) \rightarrow \mathcal{Q}(L),$$

$$g : \mathcal{Q}(L) \times \{0, 1\} \rightarrow \mathcal{Q}(L),$$

gdzie $\mathcal{Q}(L)$ jest rodziną klas abstrakcji relacji $\sim_L$ równoważności względem języka L , wzorami:

$$f([u]_{\sim_L}, [w]_{\sim_L}) = [uw]_{\sim_L},$$

$$g([u]_{\sim_L}, a) = [ua]_{\sim_L},$$

gdzie $u, w \in \{0, 1\}^*$ oraz $a \in \{0, 1\}$. Które z powyższych definicji są poprawne?

Zadanie 396. Niech g będzie funkcją zdefiniowaną w poprzednim zadaniu. Kładziemy

$$g^*(\epsilon) = g([\epsilon]_{\sim_L}, \epsilon),$$

$$g^*(wa) = g(g^*(w), a),$$

dla $w \in \{0, 1\}^*$ i $a \in \{0, 1\}$. Wykaż, że słowo $w \in \{0, 1\}^*$ należy do języka L wtedy i tylko wtedy, gdy $g^*(w) \subseteq L$.

Zadanie 397. Niech Ω oznacza zbiór wszystkich — zarówno skończonych, jak i nieskończonych — ciągów zero-jedynkowych, symbol $[\alpha]$ — zbiór wszystkich ciągów o długości przynajmniej takiej, jak α , których początkowe wyrazy są równe kolejnym wyrazom ciągu α , a symbol ϵ — pusty ciąg zero-jedynkowy. Udowodnij, że dopełnienie $\Omega \setminus [0]$ zbioru $[0]$ jest równe $[1] \cup \{\epsilon\}$. Podaj podobny wzór na dopełnienie zbioru $[0101]$ i udowodnij jego poprawność. Podaj i udowodnij wzór na dopełnienie zbioru $[\alpha]$ dla dowolnego skończonego ciągu α .

9

Kresy zbiorów

Definicja 122. Niech $\langle P, \leq \rangle$ będzie częściowym porządkiem i niech $X \subseteq P$. Element $a \in P$ jest *ograniczeniem górnym* zbioru X , jeśli dla każdego $x \in X$ zachodzi $x \leq a$. *Kresem górnym* zbioru X nazywamy najmniejszy element zbioru $\{a \mid a \text{ jest ograniczeniem górnym } X\}$. Kres górny zbioru X oznaczamy $\bigvee X$ lub $\sup X$. Dualnie można zdefiniować pojęcia *ograniczenia dolnego* i *kresu dolnego* (kres dolny zbioru X oznaczamy $\bigwedge X$ lub $\inf X$).

Zadanie 398. Rodzinę $\mathcal{P}(A)$ podzbiorów niepustego zbioru A porządkujemy relacją inkluzji $\subseteq$. Wykaż, że kres górny dowolnego podzbioru $\mathcal{X} \subseteq \mathcal{P}(A)$ jest równy sumie teoriomnogościowej zbiorów do niego należących, a kres dolny — przekrojowi. Formalnie: $\sup\{X_s\}_{s \in S} = \bigcup_{s \in S} X_s$ oraz $\inf\{X_s\}_{s \in S} = \bigcap_{s \in S} X_s$ dla dowolnej rodziny $\{X_s\}_{s \in S} \subseteq \mathcal{P}(A)$.

Definicja 123. Relacja podzielności liczb naturalnych $\mid \subset \mathbb{N}^2$ jest określona następująco:

$$x \mid y \stackrel{\text{df}}{\iff} \exists z \in \mathbb{N} (xz = y).$$

Zadanie 399. Pokaż, że relacja $\mid$ jest porządkiem częściowym. Udowodnij, że każdy niepusty podzbiór $\langle \mathbb{N}, \mid \rangle$ posiada kres dolny. Pokaż też, że $\inf\{m, n\} = \gcd(m, n)$ i $\sup\{m, n\} = \text{lcm}(m, n)$, gdzie $\gcd$ jest największym wspólnym dzielnikiem dwu liczb, a lcm — najmniejszą wspólną wielokrotnością.

Zadanie 400. Czy w $\langle \mathbb{N}, \mid \rangle$ istnieje element a) najmniejszy, b) największy?

Definicja 124. Funkcje $f : \mathbb{N} \rightarrow \mathbb{N}$ i $g : \mathbb{N} \rightarrow \mathbb{N}$ są *równe prawie wszędzie*, jeśli zbiór

$$\{n \in \mathbb{N} \mid f(n) \neq g(n)\}$$

jest skończony. Zapis $f \approx g$ oznacza, że funkcje f i g są równe prawie wszędzie.

Zadanie 401. Pokaż, że $\approx$ jest relacją równoważności.

Zadanie 402. Ile jest klas abstrakcji relacji $\approx$? Jaka jest moc każdej z nich?

Definicja 125. Funkcja $f : \mathbb{N} \rightarrow \mathbb{N}$ *majoryzuje* funkcję $g : \mathbb{N} \rightarrow \mathbb{N}$, jeśli zbiór

$$\{n \in \mathbb{N} \mid f(n) < g(n)\}$$

jest skończony. Zapis $g \preceq f$ oznacza, że funkcja f majoryzuje funkcję g .

Na zbiorze $\mathcal{F} = \{[f]_{\approx} \mid f : \mathbb{N} \rightarrow \mathbb{N}\}$ klas abstrakcji relacji $\approx$ wprowadzamy relację $\preceq$ przyjmując, że

$$[f]_{\approx} \preceq [g]_{\approx} \stackrel{\text{df}}{\iff} f \preceq g.$$

Zadanie 403. Wykaż, że definicja relacji $\preceq$ na zbiorze $\mathcal{F}$ jest poprawna (nie zależy od wyboru reprezentantów klas abstrakcji) i że relacja $\preceq$ jest częściowym porządkiem na $\mathcal{F}$.

Zadanie 404. Niech dana będzie funkcja $e(n) = 2^n$ i rodzina funkcji $f_k(n) = n^k$ dla $k \in \mathbb{N}$. Wykaż, że dla żadnego k funkcja f_k nie majoryzuje funkcji e .

Zadanie 405. Czy istnieje taki ciąg funkcji $\langle f_i : i \in \mathbb{N} \rangle$, że $f_i \preceq f_{i+1}$ dla $i \in \mathbb{N}$, oraz dla każdej funkcji $g : \mathbb{N} \rightarrow \mathbb{N}$ istnieje i takie, że $g \preceq f_i$?

Zadanie 406. Wykaż, że każdy przeliczalny podzbiór $X \subseteq \mathcal{F}$ posiada w zbiorze $\mathcal{F}$ ograniczenie górne.

Zadanie 407. Niech $\{A_i \mid i \in \mathbb{N}\}$ będzie podziałem zbioru $\mathbb{N}$ na zbiory nieskończone. Definiujemy ciąg funkcji $\langle f_j : j \in \mathbb{N} \rangle$ kładąc

$$f_j(n) = \begin{cases} 1, & \text{jeżeli } n \in \bigcup_{i=1}^j A_i, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Wykaż, że zbiór $\{[f_j]_{\approx} \mid j \in \mathbb{N}\}$ nie ma kresu górnego w $\langle \mathcal{F}, \preceq \rangle$.

Definicja 126. *Nieskończonym łańcuchem wstępującym* w zbiorze uporządkowanym $\langle A, \leq \rangle$ nazywamy ciąg $\langle a_i : i \in \mathbb{N} \rangle$ taki, że $a_i < a_{i+1}$ dla każdego $i \in \mathbb{N}$, gdzie $a < b$ oznacza, że $a \leq b$ i $a \neq b$. Podobnie ciąg $\langle a_i : i \in \mathbb{N} \rangle$ jest *łańcuchem zstępującym*, jeśli $a_{i+1} < a_i$ dla każdego $i \in \mathbb{N}$.

Zadanie 408. Wykaż, że żaden przeliczalny nieskończony ściśle wstępujący łańcuch nie posiada w zbiorze $\mathcal{F}$ kresu górnego.

Zadanie 409. Jak jest największa moc ściśle a) wstępującego, b) zstępującego łańcucha w zbiorze $\mathcal{F}$?

Zadanie 410. Na zbiorze $\{0, 1\}$ wprowadzamy porządek $\leq$ kładąc $0 \leq 1$. Niech $\preceq$ będzie porządkiem leksykograficznym na zbiorze $\{0, 1\}^*$ wyznaczonym przez porządek $\leq$. Wykaż, że w zbiorze $(\{0, 1\}^*, \preceq)$ istnieje nieskończony łańcuch wstępujący i nieskończony łańcuch zstępujący. Czy zbiór $(\{0, 1\}^*, \preceq)$ posiada element najmniejszy lub największy?

9.1. Kraty

Definicja 127. Porządek $\langle P, \leq \rangle$ jest *kratą zupełną*, jeśli każdy podzbiór zbioru P ma kres górny i kres dolny. Porządek $\langle P, \leq \rangle$ jest *kratą*, jeśli posiada elementy najmniejszy i największy oraz gdy każdy *skończony* podzbiór zbioru P ma kres górny i kres dolny.

Przykład 128. Dla dowolnego zbioru A rodzina $\mathcal{P}(A)$ uporządkowana relacją inkluzji $\subseteq$ jest kratą zupełną.

Twierdzenie 129. Niech $\langle P, \leq \rangle$ będzie porządkiem. Wtedy następujące warunki są równoważne:

1. $\langle P, \leq \rangle$ jest kratą zupełną.
2. Każdy podzbiór P ma kres górny w $\langle P, \leq \rangle$.
3. Każdy podzbiór P ma kres dolny w $\langle P, \leq \rangle$.

Zadanie 411. Niech A będzie dowolnym zbiorem niepustym. Czy $\langle \mathcal{K}, \subseteq \rangle$ jest kratą zupełną, jeżeli $\mathcal{K}$ jest rodziną wszystkich

1. relacji binarnych,
2. relacji równoważności,
3. relacji częściowego porządku

na zbiorze A ?

Zadanie 412. Niech $\mathcal{X}$ będzie przeliczalną rodziną podzbiorów $\mathbb{N}$. Udowodnij, że istnieje przeliczalna rodzina $\mathcal{K}$, taka, że $\mathcal{X} \subseteq \mathcal{K}$ i $\langle \mathcal{K}, \subseteq \rangle$ jest kratą.

Zadanie 413. Czy porządek z zadania 365 jest a) kratą, b) kratą zupełną?

9.2. Porządki zupełne

Definicja 130. Niech $\langle P, \leq_P \rangle$ będzie zbiorem częściowo uporządkowanym. Wtedy zbiór $\emptyset \neq X \subseteq P$ jest zbiorem *skierowanym*, jeśli każda para $x, y \in X$ elementów zbioru X ma w X ograniczenie górne, tj. prawdziwa jest formuła

$$\forall x, y \in X \exists z \in X (x \leq z \wedge y \leq z).$$

Zbiór $\langle P, \leq_P \rangle$ jest *porządkiem zupełnym*, jeśli P ma element najmniejszy oraz każdy skierowany podzbiór X zbioru P ma kres górny.

Definicja 131. Na zbiorze $\mathcal{P}(\mathbb{N})$ określamy relację równoważności $\sim$ wzorem

$$X \sim Y \quad \text{wtw} \quad |X \dot{-} Y| < \aleph_0$$

(patrz zadanie 236). W zbiorze klas abstrakcji $\mathcal{P}(\mathbb{N})/\sim$ wprowadzamy taką relację $\leq$, że

$$[X]_{\sim} \leq [Y]_{\sim} \quad \text{wtw} \quad |X \setminus Y| < \aleph_0.$$

Zadanie 414. Sprawdź, czy definicja $\leq$ jest poprawna.

Zadanie 415. Sprawdź, czy $\leq$ jest porządkiem częściowym.

Zadanie 416. Znajdź w $\langle \mathcal{P}(\mathbb{N})/\sim, \leq \rangle$ nieskończony podzbiór liniowo uporządkowany.

Zadanie 417. Znajdź w $\langle \mathcal{P}(\mathbb{N})/\sim, \leq \rangle$ nieskończony antyłańcuch.

Zadanie 418. Wykaż, że $\langle \mathcal{P}(\mathbb{N})/\sim, \leq \rangle$ nie jest zupełny.

Zadanie 419. Niech Z oznacza zbiór wszystkich nieskończonych podzbiorów zbioru liczb naturalnych. Wykaż, że każdy ściśle malejący ciąg $x_1 > x_2 > x_3 > \dots$ elementów $\langle Z/\sim, \leq \rangle$ (gdzie $x > y$ gdy $y \leq x$ i $y \neq x$) ma w $Z/\sim$ ograniczenie dolne, tj. istnieje $y \in Z/\sim$, taki że $y \leq x_i$ dla każdego i .

Zadanie 420. Czy $\langle \mathcal{P}(\mathbb{N})/\sim, \leq \rangle$ jest kratą?

Definicja 132. W zbiorze $\mathcal{P}(\mathbb{N})/\sim$ definiujemy porządek $\preceq$ kładąc $[X]_{\sim} \preceq [Y]_{\sim}$, jeśli $X \cup Y \in [Y]_{\sim}$.

Zadanie 421. Sprawdź, czy powyższa definicja jest poprawna. Czy $\langle \mathcal{P}(\mathbb{N})/\sim, \preceq \rangle$ jest kratą?

Zadanie 422. Czy zbiór $\{[X_n]_{\sim} \mid n \in \mathbb{N}\}$, gdzie $X_n = \{2^k k \mid k \in \mathbb{N}\}$ ma kres dolny w $\langle \mathcal{P}(\mathbb{N})/\sim, \preceq \rangle$?

Zadanie 423. Czy w $\langle \mathcal{P}(\mathbb{N})/\sim, \preceq \rangle$ istnieje nieskończony antyłańcuch?

Definicja 133. Niech $\langle P, \leq_P \rangle$ oraz $\langle Q, \leq_Q \rangle$ będą porządkami zupełnymi. Funkcja $f : P \rightarrow Q$ jest *ciągła*, jeśli zachowuje kresy górne, to znaczy, gdy dla dowolnego zbioru skierowanego $X \subseteq P$ zbiór $f(X)$ ma kres górny oraz $f(\bigvee X) = \bigvee f(X)$.

Twierdzenie 134.

1. Każda funkcja ciągła jest monotoniczna.
2. Złożenie funkcji ciągłych jest funkcją ciągłą.

Zadanie 424. Udowodnij, że jeśli $\langle P, \leq_P \rangle$ jest skończoną kratą to każda monotoniczna funkcja $f : P \rightarrow P$ jest ciągła.

Zadanie 425. Pokaż, że relacja inkluzji na rodzinie skończonych podzbiorów zbioru liczb naturalnych nie jest porządkiem zupełnym.

Zadanie 426. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą porządkami zupełnymi. W produkcie $A \times B$ definiujemy relację $\leq$ w następujący sposób: $\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle$ wtedy i tylko wtedy, gdy $a_1 \leq_A a_2$ oraz $b_1 \leq_B b_2$. Udowodnij, że $\langle A \times B, \leq \rangle$ jest porządkiem zupełnym.

Zadanie 427. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą porządkami zupełnymi. W produkcie $A \times B$ definiujemy relację $\leq$ jako rozszerzenie leksykograficzne obu porządków, czyli $\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle$ wtedy i tylko wtedy, gdy $a_1 <_A a_2$ lub gdy $a_1 = a_2$ i $b_1 \leq_B b_2$. Udowodnij, że $\langle A \times B, \leq \rangle$ jest porządkiem zupełnym.

Zadanie 428. Podaj przykład takiego porządku zupełnego $\langle A, \leq \rangle$, że porządek leksykograficzny na A^* generowany przez $\leq$ nie jest zupełny.

Zadanie 429. Niech A będzie zbiorem niepustym oraz niech $\langle B, \leq_B \rangle$ będzie porządkiem częściowym zupełnym. Wykaż, że $\langle B^A, \leq \rangle$ jest porządkiem zupełnym, gdzie $f \leq g$ dla $f, g \in B^A$, wtedy i tylko wtedy, gdy $f(a) \leq_B g(a)$ dla każdego $a \in A$.

Zadanie 430. Niech $\langle A, \leq_A \rangle$ oraz $\langle B, \leq_B \rangle$ będą porządkami częściowymi zupełnymi. Wykaż, że $\langle [A, B], \leq \rangle$ jest porządkiem zupełnym, gdzie $[A, B]$ oznacza zbiór funkcji ciągłych z A w B oraz $f \leq g$, dla $f, g \in B^A$, wtedy i tylko wtedy, gdy $f(a) \leq_B g(a)$ dla każdego $a \in A$.

Zadanie 431. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą porządkami zupełnymi. Pokaż, że funkcja $\phi : [A, B] \times A \rightarrow B$, gdzie $[A, B]$ jest zbiorem funkcji ciągłych z A w B , zdefiniowana wzorem $\phi(f, a) = f(a)$ jest ciągła.

Zadanie 432. Wykaż, że dla dowolnych zbiorów A i B relacja inkluzji na zbiorze $B^{\subseteq A}$ funkcji częściowych z A w B jest porządkiem zupełnym. Czy $\langle B^{\subseteq A}, \subseteq \rangle$ jest kratą zupełną?

Zadanie 433. Zbiór W na płaszczyźnie jest wypukły, jeśli wraz z każdymi dwoma punktami zawiera cały łączący je odcinek, tj. gdy $\overline{ab} \subseteq W$ dla dowolnych punktów $a, b \in W$. Pokaż, że relacja inkluzji na rodzinie wypukłych podzbiorów płaszczyzny jest porządkiem zupełnym.

Zadanie 434. Czy porządek z zadania 365 jest zupełny?

9.3. Twierdzenia o punkcie stałym

Twierdzenie 135 (Knaster, Tarski). Niech $\langle P, \leq \rangle$ będzie krata zupełną i niech funkcja $f : P \rightarrow P$ będzie monotoniczna. Wtedy istnieje $a \in P$ taki, że

1. $f(a) = a$
2. dla każdego $b \in P$, jeśli $f(b) = b$, to $a \leq b$.

Element a z twierdzenia Knastera-Tarskiego nazywamy *najmniejszym punktem stałym* funkcji f . Element spełniający tylko warunek 1 nazywamy *punktem stałym*.

Twierdzenie 136 (Kleene). Niech $\langle P, \leq_P \rangle$ będzie porządkiem zupełnym oraz niech funkcja $f : P \rightarrow P$ będzie ciągła. Wtedy element $a = \bigvee \{f^n(\perp) \mid n \in \mathbb{N}\}$ jest najmniejszym punktem stałym funkcji f .

Zadanie 435. Niech $A \neq \emptyset$ i niech $f : A \rightarrow A$. Udowodnij, że dla dowolnego $a \in A$ istnieje najmniejszy zbiór $X \subseteq A$ taki, że $a \in X$ oraz $f^{-1}(X) \subseteq X$.

Zadanie 436. Niech $\mathcal{K} = \mathcal{P}(A^2)$ będzie zbiorem uporządkowanym relacją inkluzji $\subseteq$, $R \in \mathcal{K}$ i niech funkcja $\phi_R : \mathcal{K} \rightarrow \mathcal{K}$ będzie zdefiniowana wzorem

$$\phi_R(X) = X \cup X^{-1} \cup XX \cup E_A \cup R,$$

gdzie $E_A = \{\langle x, x \rangle \mid x \in A\}$. Wykaż, że dla każdej relacji $R \subseteq A^2$ istnieje najmniejszy punkt stały funkcji ϕ_R .

Zadanie 437. Niech R^+ będzie najmniejszym punktem stałym funkcji ϕ_R . Wykaż, że R^+ jest najmniejszą (względem relacji inkluzji $\subseteq$) relacją równoważności zawierającą relację R .

Zadanie 438. Na rodzinie $\mathcal{L} = \mathcal{P}(\{0, 1\}^*)$ wszystkich języków nad alfabetem $\{0, 1\}$ określamy funkcję

$$f(X) = X \cup \{w01 \mid w \in X\} \cup \{\epsilon\}.$$

Znajdź najmniejszy punkt stały funkcji f w zbiorze $\mathcal{L}$ uporządkowanym relacją inkluzji. Czy istnieje największy punkt stały tej funkcji? Ile punktów stałych ma funkcja $g(X) = \{w01 \mid w \in X\} \cup \{\epsilon\}$?

Zadanie 439. Grafem skierowanym o wierzchołkach V i krawędziach E nazywamy taką parę $\langle V, E \rangle$, że V jest skończonym zbiorem oraz $E \subseteq V \times V$. Ścieżką (długości n , o początku w v_0 i końcu w v_n) w grafie $\langle V, E \rangle$ nazywamy taki ciąg wierzchołków $\langle v_0, \dots, v_n \rangle$, że dla wszystkich $0 \leq i \leq n-1$ zachodzi $\langle v_i, v_{i+1} \rangle \in E$ (w szczególności dla dowolnego wierzchołka v ciąg $\langle v \rangle$ jest ścieżką długości 0). Mówimy,

że wierzchołek v jest osiągalny z wierzchołka v_0 jeśli w grafie istnieje ścieżka o początku w v_0 i końcu w v . Udowodnij, że zbiór wierzchołków osiągalnych z v_0 w grafie $\langle V, E \rangle$ jest najmniejszym punktem stałym funkcji $f : \mathcal{P}(V) \rightarrow \mathcal{P}(V)$ zadanej wzorem

$$f(X) = \{v_0\} \cup \{v \in V \mid \exists x \in X \langle x, v \rangle \in E\}.$$

Zadanie 440. Niech $R \subseteq A^2$ będzie relacją binarną na zbiorze A . Udowodnij, że przechodnie domknięcie relacji R jest najmniejszym punktem stałym funkcji $f : A^2 \rightarrow A^2$ danej wzorem $f(X) = R \cup XX$.

9.4. Relacje w zbiorze formuł zdaniowych

Definicja 137. Niech V będzie zbiorem zmiennych zdaniowych. W zbiorze $\mathcal{F}(V)$ formuł zdaniowych, zbudowanych ze zmiennych ze zbioru V , spójnika negacji $\neg$ i spójników koniunkcji $\wedge$, alternatywy $\vee$, implikacji $\Rightarrow$ i równoważności $\Leftrightarrow$ wprowadzamy binarną relację $\sim$ przyjmując, że:

$\alpha \sim \beta$ wtedy i tylko wtedy, gdy formuła $(\alpha \Leftrightarrow \beta)$ jest tautologią.

Zadanie 441. Wykaż, że $\sim$ jest relacją równoważności.

Zadanie 442. W zbiorze $\mathcal{F}(V)$ wprowadzamy relacje $\sim_1, \sim_2$ i $\sim_3$ przyjmując, że

- $\alpha \sim_1 \beta$ wtedy i tylko wtedy, gdy formuła $(\alpha \Leftrightarrow \beta)$ jest spełnialna;
- $\alpha \sim_2 \beta$ wtedy i tylko wtedy, gdy formuła $(\alpha \Leftrightarrow \beta)$ jest sprzeczna;
- $\alpha \sim_3 \beta$ wtedy i tylko wtedy, gdy formuła $(\alpha \Leftrightarrow \beta)$ jest prawdziwa dla dokładnie połowy wartościowań zmiennych występujących w formułach α i β .

Które z tych relacji są relacjami równoważności?

Definicja 138. Niech $\phi_a \in \mathcal{F}(V)$ będzie ustaloną formułą. W zbiorze formuł zdaniowych $\mathcal{F}(V)$ wprowadzamy binarną relację $\sim_{\phi_a}$, przyjmując, że

$\phi_1 \sim_{\phi_a} \phi_2$ wtedy i tylko wtedy, gdy formuła $(\phi_a \Rightarrow (\phi_1 \Leftrightarrow \phi_2))$ jest tautologią.

Zadanie 443. Udowodnij, że $\sim_{\phi_a}$ jest relacją równoważności. Opisz klasy równoważności formuł $p \vee \neg p$ i $p \wedge \neg p$.

Definicja 139. W zbiorze klas abstrakcji $\mathcal{F}(V)/\sim$ wyżej opisanej relacji $\sim$ wprowadzamy relację $\leq$ taką, że $[\phi_1]_{\sim} \leq [\phi_2]_{\sim}$ wtedy i tylko wtedy, gdy $\phi_1 \Rightarrow \phi_2$ jest tautologią.

Zadanie 444. Sprawdź, że powyższa definicja relacji $\leq$ jest poprawna (nie zależy od wyboru reprezentanta klasy abstrakcji) i że definiuje porządek częściowy.

Zadanie 445. Czy $\langle \mathcal{F}(V)/\sim, \leq \rangle$ jest kratą?

Zadanie 446. Czy $\langle \mathcal{F}(V)/\sim, \leq \rangle$ jest kratą zupełną?

Zadanie 447. Przyjmijmy, że zbiór zmiennych V jest przeliczalny nieskończony. Znajdź w zbiorze $\langle \mathcal{F}(V)/\sim, \leq \rangle$ nieskończony podzbiór liniowo uporządkowany (łańcuch).

Zadanie 448. Przyjmijmy, że zbiór zmiennych V jest przeliczalny nieskończony. Czy można w zbiorze $\langle \mathcal{F}(V)/\sim, \leq \rangle$ znaleźć nieskończony antyłańcuch?

Zadanie 449. Ile jest klas abstrakcji relacji $\sim$ gdy a) $|V| = 2$, b) $|V| = 3$, c) $|V| = 5$, d) $|V| = n \in \mathbb{N}$, e) $|V| = \aleph_0$?

Zadanie 450. Wypisz najkrótszych reprezentantów wszystkich klas abstrakcji relacji $\sim$ gdy zbiór V ma dwa elementy. Narysuj diagram porządku $\leq$ dla tego przypadku.

Zadanie 451. Wyznacz zbiór elementów minimalnych i kres dolny zbioru $F_1 = \mathcal{F}(V)/\sim \setminus \{[\perp]_\sim\}$, gdy zbiór zmiennych V jest (a) skończony i (b) nieskończony.

Zadanie 452. Niech $V = \{p_n\}_{n=0}^\infty$ będzie zbiorem zmiennych. Wyznacz kresy (dolny i górny) zbiorów $F_2 = \{[a_n]_\sim\}_{n=0}^\infty$ i $F_3 = \{[\beta_n]_\sim\}_{n=0}^\infty$, gdzie $a_n = \bigwedge_{i=1}^n p_i = p_1 \wedge \dots \wedge p_n$ i $\beta_n = \bigvee_{i=1}^n p_i = p_1 \vee \dots \vee p_n$.

Zadanie 453. Niech $V = \{p_n\}_{n=0}^\infty$ będzie zbiorem zmiennych. Wyznacz kresy (dolny i górny) zbioru $F_4 = \{[\gamma_n]_\sim\}_{n=0}^\infty$, gdzie $\gamma_n = \bigvee_{i=0}^n (p_{2i} \vee \neg p_{2i+1})$.

Zadanie 454. W zbiorze $\mathcal{F}(V)$, gdzie $V = \{p_1, \dots, p_5\}$, definiujemy relacje R_1 , R_2 oraz R_3 w następujący sposób:

$$\begin{aligned} \phi R_1 \psi &\Leftrightarrow \phi \text{ i } \psi \text{ mają tyle samo wystąpień spójników logicznych} \\ \phi R_2 \psi &\Leftrightarrow (\phi \Leftrightarrow \psi) \text{ jest tautologią} \\ \phi R_3 \psi &\Leftrightarrow (\phi \Leftrightarrow \psi) \text{ jest formułą spełnialną} \end{aligned}$$

Która z relacji R_1 , R_2 oraz R_3 jest relacją równoważności? W każdym przypadku w razie pozytywnej odpowiedzi wyznacz moc zbioru klas abstrakcji danej relacji.

Zadanie 455. Niech $\mathcal{F}$ będzie zbiorem formuł zdaniowych zbudowanych ze zmiennych ze zbioru $V = \{p, q, r, \dots\}$ i spójników implikacji $\Rightarrow$, fałszu $\perp$ i prawdy $\top$. Binarna relacja R na zbiorze $\mathcal{F}$ jest *monotoniczna*, jeśli

1. $\perp R \phi$,
2. $\phi R \top$,
3. jeśli $\phi_1 R \phi_2$ i $\psi_1 R \psi_2$, to $(\phi_2 \Rightarrow \psi_1) R (\phi_1 \Rightarrow \psi_2)$,

dla wszelkich formuł $\phi, \phi_1, \phi_2, \psi_1, \psi_2 \in \mathcal{F}$.

1. Pokaż, że w zbiorze relacji monotonicznych na $\mathcal{F}$ uporządkowanym relacją inkluzji istnieje element najmniejszy. Relację tę będziemy oznaczać $\sqsubseteq$.
2. Pokaż, że relacja $\sqsubseteq$ jest częściowym porządkiem na $\mathcal{F}$. Pokaż, że nie jest to porządek liniowy.
3. Pokaż, że $\langle \mathcal{F}, \sqsubseteq \rangle$ jest kratą.
4. Pokaż, że jeśli $\phi \sqsubseteq \psi$, to $\phi \Rightarrow \psi$ jest tautologią. Pokaż, że implikacja odwrotna nie zachodzi.

10

Dobre porządki i indukcja

10.1. Porządki regularne

Definicja 140. Porządek częściowy $\langle P, \leq \rangle$ jest *regularny* (dobrze ufundowany), jeśli w każdym niepustym zbiorze $X \subseteq P$ istnieje element minimalny. Mówimy, że porządek jest *dobry*, jeśli jest liniowy i regularny.

Twierdzenie 141.¹ Jeśli porządek $\langle P, \leq \rangle$ jest regularny, to w zbiorze P nie istnieje nieskończony ciąg ściśle malejący, tj taki ciąg $a_0, a_1, a_2, \dots$, że $a_{i+1} < a_i$ dla wszystkich $i \in \mathbb{N}$.

Zadanie 456. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą zbiorami uporządkowanymi, w których porządki $\leq_A$ i $\leq_B$ są regularne. Na zbiorze $A \times B$ definiujemy relację $\leq$ przyjmując, że $\langle x_1, y_1 \rangle \leq \langle x_2, y_2 \rangle$ wtedy i tylko wtedy, gdy $x_1 \leq_A x_2$ i $y_1 \leq_B y_2$, dla wszelkich $x_1, x_2 \in A$ i $y_1, y_2 \in B$. Wykaż, że relacja $\leq$ jest porządkiem regularnym na zbiorze $A \times B$.

Zadanie 457. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą dobrymi porządkami. W produkcie $A \times B$ definiujemy relację $\leq$ jako rozszerzenie leksykograficzne obu porządków, czyli $\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle$ wtedy i tylko wtedy, gdy $a_1 <_A a_2$ lub gdy $a_1 = a_2$ i $b_1 \leq_B b_2$. Udowodnij, że $\langle A \times B, \leq \rangle$ jest dobrym porządkiem.

Zadanie 458. Podaj przykład takiego dobrego porządku $\langle A, \leq \rangle$, że porządek leksykograficzny na A^* generowany przez $\leq$ nie jest dobry.

Zadanie 459. Załóżmy, że zbiór $\langle X, R \rangle$ jest dobrze uporządkowany. Znajdź warunek konieczny i dostateczny na to, by zbiór $\langle X, R^{-1} \rangle$ był także dobrze uporządkowany.

Zadanie 460. Udowodnij, że jeśli $f : A \rightarrow B$ jest monotoniczną bijekcją między dobrymi porządkami $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$, to funkcja odwrotna f^{-1} też jest monotoniczna. Czy założenie, że porządki $\leq_A$ i $\leq_B$ są dobre jest istotne?

¹Przy założeniu aksjomatu wyboru prawdziwe jest również twierdzenie odwrotne.

Zadanie 461. W zbiorze $\mathbb{N} \setminus \{0\}$ wprowadzamy relację R wzorem

$$x R y \Leftrightarrow (2|x \wedge 2|y \wedge y \leq x) \vee (2|x \wedge \neg(2|y)) \vee (\neg(2|x) \wedge \neg(2|y) \wedge x \leq y).$$

Udowodnij, że zbiór $\langle \mathbb{N} \setminus \{0\}, R \rangle$ jest liniowo uporządkowany. Czy jest to dobry porządek?

Zadanie 462. Udowodnij, że w zbiorze dobrze uporządkowanym każdy element (poza co najwyżej elementem największym) posiada następnik. Czy każdy element poza elementem pierwszym musi posiadać poprzednik?

Zadanie 463. Dany jest zbiór

$$A = \left\{ n + \frac{m}{m+1} \mid n, m \in \mathbb{N} \right\}.$$

1. Czy $\langle A, \leq \rangle$ jest dobrym porządkiem ($\leq$ jest zwykłą relacją porządku w zbiorze liczb rzeczywistych)?
2. Ile jest nierosnących funkcji z $\mathbb{N}$ w A ?

Zadanie 464. W zbiorze $\mathcal{F} = \mathbb{N}^{\mathbb{N}}$ funkcji z $\mathbb{N}$ w $\mathbb{N}$ wprowadzamy relację $\leq_F$ kładąc

$$f \leq_F g \Leftrightarrow (\forall n \in \mathbb{N})(f(n) \leq g(n)).$$

Czy porządek częściowy $\langle \mathcal{F}, \leq_F \rangle$ jest

1. krata,
2. kratą zupełną,
3. porządkiem zupełnym,
4. porządkiem regularnym?

Zadanie 465. Niech $\mathcal{F} = \{f \in 2^{\mathbb{N}} \mid \{n \in \mathbb{N} \mid f(n) = 1\} \text{ jest skończony}\}$. W zbiorze $\mathcal{F}$ wprowadzamy relacje $\leq_F$ i $\leq_L$ kładąc

$$f \leq_F g \Leftrightarrow \forall n \in \mathbb{N} (f(n) \leq g(n)) \quad \text{oraz}$$

$$f \leq_L g \Leftrightarrow f = g \vee \exists m \in \mathbb{N} (f(m) < g(m) \wedge \forall n \in \mathbb{N} (n < m \Rightarrow f(n) = g(n))).$$

1. Czy $\langle \mathcal{F}, \leq_F \rangle$ jest porządkiem liniowym?
2. Czy $\langle \mathcal{F}, \leq_L \rangle$ jest porządkiem liniowym?
3. Czy $\langle \mathcal{F}, \leq_F \rangle$ jest porządkiem regularnym?
4. Czy $\langle \mathcal{F}, \leq_L \rangle$ jest porządkiem regularnym?
5. Czy $\langle \mathcal{F}, (\leq_F)^{-1} \rangle$ jest porządkiem regularnym?

6. Czy $\langle \mathcal{F}, (\leq_L)^{-1} \rangle$ jest porządkiem regularnym?

Zadanie 466. Czy porządek zadany definicją 131 jest regularny?

Zadanie 467. Czy na zbiorze A o mocy większej niż 1 można zdefiniować porządek jednocześnie dobry i gęsty?

Definicja 142. Binarna relacja R na zbiorze X jest *słabo konfluentna*, jeśli dla każdych $x_1, x_2, x_3 \in X$ istnieje taki $x_4 \in X$, że jeśli $x_1 R x_2$ i $x_1 R x_3$, to $x_2 \bar{R} x_4$ i $x_3 \bar{R} x_4$, gdzie $\bar{R}$ jest przechodnim domknięciem relacji R . Relacja R jest *konfluentna*, jeśli dla każdych $x_1, x_2, x_3 \in X$ istnieje taki $x_4 \in X$, że jeśli $x_1 \bar{R} x_2$ i $x_1 \bar{R} x_3$, to również $x_2 \bar{R} x_4$ i $x_3 \bar{R} x_4$, gdzie $\bar{R}$ jest przechodnim domknięciem relacji R .

Zadanie 468. Pokaż, że istnieje relacja R słabo konfluentna, która nie jest konfluentna.

Zadanie 469. Pokaż, że istnieje relacja R słabo konfluentna, której graf jest acykliczny i która nie jest konfluentna.

Definicja 143. Binarna relacja R na zbiorze X jest *ufundowana* jeśli nie istnieje taki nieskończony ciąg $a_0, a_1, a_2, \dots$, że $a_i R a_{i+1}$ dla wszystkich $i \in \mathbb{N}$.

Zadanie 470. Pokaż, że jeśli relacja R jest ufundowana i słabo konfluentna, to jest konfluentna.

Zadanie 471. Niech $\mathcal{K}$ będzie rodziną podzbiorów zbioru liczb naturalnych taką, że relacja zawierania na tej rodzinie jest porządkiem regularnym. Pokaż, że każdy łańcuch w tym porządku jest przeliczalny.

Zadanie 472. Dane są dwa niemalejące ciągi liczb naturalnych $\langle a_0, a_1, a_2, \dots \rangle$ oraz $\langle b_0, b_1, ab_2, \dots \rangle$. Przypuśćmy, że te ciągi „podobnie rosną”, tzn. dla dowolnej liczby naturalnej n spełnione są warunki:

1. jeżeli $a_n < b_n$, to $a_n < a_{n+1}$ oraz $b_n = b_{n+1}$,
2. jeżeli $b_n < a_n$, to $b_n < b_{n+1}$ oraz $a_n = a_{n+1}$.

Udowodnij, że jeżeli liczba c jest wyrazem obu tych ciągów, to c jest wyrazem tych ciągów o tym samym numerze (tj. istnieje taka liczba $i \in \mathbb{N}$, że $a_i = c = b_i$).

Zadanie 473. Czy porządek z zadania 365 jest regularny?

10.2. Indukcja

Twierdzenie 144 (zasada indukcji). Niech $\langle P, \leq \rangle$ będzie regularnym porządkiem częściowym. Jeśli $X \subseteq P$ spełnia warunek $\forall x ((\forall y < x \ y \in X) \Rightarrow x \in X)$, to $X = P$.

Przykład 145. Pokażemy, że dla wszystkich dodatnich liczb naturalnych zachodzi równość

$$1 + 2 + \dots + n = \frac{n(n+1)}{2}. \quad (1)$$

Skorzystamy w tym celu z zasady indukcji dla $\langle \mathbb{N}^+, \leq \rangle$ (oczywiście jest to porządek regularny).

Niech $X = \{n \in \mathbb{N}^+ \mid 1 + 2 + \dots + n = \frac{n(n+1)}{2}\}$. Pokażemy, że spełniony jest warunek

$$\forall n \in \mathbb{N}^+ ((\forall i < n \ i \in X) \Rightarrow n \in X) \quad (2)$$

Weźmy dowolną liczbę $n \in \mathbb{N}^+$ i rozważmy następujące dwa przypadki.

Przypadek 1: $n = 1$. Wtedy $1 = \frac{1 \cdot 2}{2}$, czyli $1 \in X$, a zatem w tym przypadku implikacja

$$(\forall i < n \ i \in X) \Rightarrow n \in X \quad (3)$$

jest prawdziwa.

Przypadek 2: $n > 1$. Załóżmy, że prawdziwy jest warunek

$$\forall i < n \ i \in X. \quad (4)$$

Z założenia (4) wiemy, że $n-1 \in X$, czyli $1 + 2 + \dots + (n-1) = \frac{(n-1)n}{2}$. Stąd

$$1 + 2 + \dots + n = \frac{(n-1)n}{2} + n = n \left(\frac{(n-1)}{2} + \frac{1}{2} \right) = \frac{n(n+1)}{2}$$

a zatem

$$n \in X, \quad (5)$$

czyli również w tym przypadku implikacja (3) jest prawdziwa, co wobec dowolności wyboru liczby n dowodzi prawdziwości warunku (2). Na mocy zasady indukcji otrzymujemy, że $X = \mathbb{N}^+$, czyli dla wszystkich dodatnich liczb naturalnych zachodzi równość (1). ■

W powyższym rozumowaniu zwyczajowo przypadek 1 nazywa się *podstawą indukcji* a przypadek 2 *krokiem indukcyjnym*. Warunek (4) nazywany jest *założeniem indukcyjnym* a warunek (5) *tezą indukcji*.

Przykład 146. *Grafem prostym* o wierzchołkach V i krawędziach E nazywamy taką parę $\langle V, E \rangle$, że V jest skończonym zbiorem oraz $E \subseteq V \times V$ jest relacją antyzwrotną i symetryczną.² Pokażemy, że dla wszystkich dodatnich liczb naturalnych n każdy n -wierzchołkowy graf prosty ma nie więcej niż $\frac{n(n-1)}{2}$ krawędzi. Niech

$$X = \{n \in \mathbb{N}^+ \mid \text{każdy } n\text{-wierzchołkowy graf prosty} \\ \text{ma nie więcej niż } \frac{n(n-1)}{2} \text{ krawędzi}\}.$$

Weźmy dowolną liczbę $n \in \mathbb{N}^+$ i rozważmy następujące dwa przypadki.

Przypadek 1: $n = 1$. Rozważmy dowolny 1-wierzchołkowy graf $G = \langle V, E \rangle$. Ponieważ relacja E jest antyzwrotna, więc graf G nie ma wcale krawędzi (ich liczba jest ograniczona przez 0). Mamy $0 = \frac{1 \cdot 0}{2}$, co pokazuje, że w tym przypadku $n \in X$ i implikacja (3) jest prawdziwa.

Przypadek 2: $n > 1$. Załóżmy, że prawdziwy jest warunek $\forall i < n \ i \in X$. Chcemy pokazać, że $n \in X$, czyli że każdy n -wierzchołkowy graf prosty ma nie więcej niż $\frac{n(n-1)}{2}$ krawędzi. Rozważmy zatem dowolny n -wierzchołkowy graf $G = \langle V, E \rangle$. Wybierzmy w zbiorze V dowolny wierzchołek v i usuńmy go z grafu otrzymując graf $G' = \langle V', E' \rangle$, gdzie $V' = V - \{v\}$ oraz $E' = E \cap (V' \times V')$. Graf G' jest $(n-1)$ -wierzchołkowy, więc z założenia indukcyjnego liczba krawędzi w E' jest ograniczona przez $\frac{(n-1)(n-2)}{2}$. W zbiorze $E - E'$ jest co najwyżej $n-1$ krawędzi, a zatem łączna liczba krawędzi w E nie przekracza $\frac{n(n-1)}{2}$. Ponieważ graf G był wybrany dowolnie, więc każdy n -wierzchołkowy graf ma nie więcej niż $\frac{n(n-1)}{2}$ krawędzi, a zatem $n \in X$ i również w tym przypadku implikacja (3) jest prawdziwa. Ponieważ liczba n była wybrana jako dowolna, dowiedliśmy prawdziwości warunku (2). Na mocy zasady indukcji otrzymujemy, że $X = \mathbb{N}^+$, czyli dla wszystkich dodatnich liczb naturalnych n każdy n -wierzchołkowy graf prosty ma nie więcej niż $\frac{n(n-1)}{2}$ krawędzi. ■

Okazuje się, że samodzielne sformułowanie powyższego rozumowania sprawia ogromne kłopoty wielu studentom. Poniżej wymieniamy najczęściej spotykane błędy w tego typu rozumowaniach.

- Sprawdzenie podstawy indukcji dla $n = 1$, $n = 2$ i $n = 3$: Zwykle wystarcza rozważenie jednego przypadku bazowego. Sprawdzenie prawdziwości twierdzenia dla drugiej z kolei liczby jest konieczne tylko wtedy, gdy chcemy skorzystać z założenia, że $n - 2 \in X$ (bo dla $n = 2$ mamy $n - 2 \notin \mathbb{N}^+$ i z takiego założenia nie da się skorzystać); tutaj natomiast nie ma takiej potrzeby.

²W języku teorii grafów oznacza to, że nie ma pętli w wierzchołkach i krawędzie nie są skierowane.

- Użycie sformułowania „teza z zadania dla $n = k$ ”: zwykle student używający takiego sformułowania nie wie, co ono oznacza. W szczególności nie wiadomo, czy oznacza ono zdanie „ $k \in X$ ” czy może „ $k \in X \Rightarrow (k + 1) \in X$ ”, czy też „ $\forall k \, k \in X \Rightarrow (k + 1) \in X$ ” czy „ $\forall k \, k \in X$ ”.
- Oparcie dowodu kroku indukcyjnego na schemacie „weźmy dowolny graf $(n - 1)$ -wierzchołkowy i dodajmy do niego wierzchołek”: tu błąd polega na tym, że mamy coś dowieść dla *wszystkich* grafów n -wierzchołkowych, ale nie da się otrzymać dowolnego grafu n -wierzchołkowego dodając wierzchołek do dowolnego grafu $(n - 1)$ -wierzchołkowego. W szczególności dla $n = 4$ nie da się otrzymać trójramienną gwiazdy dodając wierzchołek do trójkąta.
- Rozpoczęcie dowodu kroku indukcyjnego od sformułowania „niech k będzie liczbą krawędzi w grafie”: tu nie wiadomo o jaki graf chodzi, a nie każdy graf ma tyle samo krawędzi.

Zadania poniżej należy rozwiązywać korzystając z zasady indukcji podanej w Twierdzeniu 144. Z innej wersji zasady indukcji można skorzystać tylko pod warunkiem, że umie się tę inną wersję udowodnić.³

Zadanie 474. W klasie jest $2n$ dzieci i n dwuosobowych ławek. Wykaż przez indukcję, że dzieci można podzielić w pary na $\frac{(2n)!}{2^n n!}$ sposobów i rozsadzić w ławkach na $\frac{(2n)!}{2^n}$ sposobów.

Zadanie 475. Skończony zbiór liniowo uporządkowany $\langle A, \leq_A \rangle$ ma n elementów, a zbiór uporządkowany $\langle B, \leq_B \rangle$ ma 2 elementy, przy czym $A \cap B = \emptyset$. Na ile sposobów można porządek liniowy na A rozszerzyć o elementy zbioru B (to znaczy znaleźć taki porządek liniowy $\langle A \cup B, \leq \rangle$, że $(a_1 \leq_A a_2) \Leftrightarrow (a_1 \leq a_2)$, dla $a_1, a_2 \in A$ oraz $(b_1 \leq_B b_2) \Leftrightarrow (b_1 \leq b_2)$, dla $b_1, b_2 \in B$)? Odpowiedź uzasadnij przy pomocy dowodu przez indukcję.

Zadanie 476. Udowodnij, że jeśli wyrazy ciągu spełniają warunki $a_0 = 2$, $a_1 = 3$ i $a_{n+1} = 3a_n - 2a_{n-1}$ dla $n \geq 2$, to $a_n = 2^n + 1$.

Zadanie 477. Dany jest ciąg a_n taki, że $a_0 = 0$, $a_1 = 1$ oraz $a_{n+1} = a_n + a_{n-1}$ dla $n \geq 2$. Udowodnij, że jeśli $n > 0$, to $a_{n+1} = 1 + \sum_{i=0}^{n-1} a_i$.

Zadanie 478. Dany jest ciąg a_n taki, że $a_0 = 0$, $a_1 = 1$ oraz $a_{n+1} = a_n + a_{n-1}$ dla $n \geq 2$. Udowodnij, że jeśli $n > 0$, to $a_n^2 = (-1)^{n+1} + a_{n-1}a_{n+1}$.

³Dlaczego? Otóż w przyszłości będziecie musieli często korzystać z indukcji strukturalnej (w której porządek zadany jest przez strukturę termów, grafów, dowodów itp.) Np. przy uzasadnianiu poprawności algorytmu wyprowadzania typu potrzebna będzie indukcja względem budowy dowodu osądu typowego. Teraz nie wiemy jeszcze co to jest osąd typowy, ale jak się dowiemy to nie będzie już czasu na zastanawianie się co to jest indukcja.

Zadanie 479. Dany jest taki ciąg a_n , że $a_0 = 0$, $a_1 = 1$ oraz $a_{n+1} = a_n + a_{n-1}$ dla $n \geq 2$. Udowodnij, że jeśli $n > 0$, to $a_{2n+1} = a_n^2 + a_{n+1}^2$.

Zadanie 480. Udowodnij, że obszary wyznaczone przez dowolną skończoną liczbę prostych na płaszczyźnie można pokolorować dwoma kolorami tak, by żadne dwa obszary o tym samym kolorze nie miały wspólnego boku.

Zadanie 481. Wykaż indukcyjnie, że $2^n \geq n^2$ dla każdego $n \geq 5$.

Zadanie 482. Zbiór W na płaszczyźnie jest *wypukły*, jeśli wraz z każdymi dwoma punktami zawiera cały łączący je odcinek, tj. gdy $\overline{ab} \subseteq W$ dla dowolnych punktów $a, b \in W$. Niech $\langle W_i : i \in \mathbb{N} \rangle$ będzie ciągiem takich zbiorów wypukłych, że $W_i \subseteq W_{i+1}$ dla każdego $i \in \mathbb{N}$. Pokaż, że zbiór $W = \bigcup_{n \in \mathbb{N}} W_n$ jest wypukły.

Zadanie 483. Niech $X \subseteq \mathbb{N}$ będzie takim zbiorem, że spełniona jest koniunkcja warunków

1. $0, 1 \in X$
2. $\forall n (n \in X \Rightarrow 2n \in X)$
3. $\forall n (n + 1 \in X \Rightarrow n \in X)$

Udowodnij, że $X = \mathbb{N}$.

Zadanie 484. Dany jest zbiór $X \subseteq \mathbb{N}$ spełniający warunki:

1. $0, 1 \in X$,
2. jeśli $x \in X$ oraz $x + 1 \in X$ to $x + 2 \in X$, dla każdej liczby naturalnej x .

Wykaż, że $X = \mathbb{N}$. Czy to twierdzenie pozostanie słuszne, jeśli warunek 1. zastąpimy przez słabszy warunek $0 \in X$?

Zadanie 485. Rozważmy grę, w której ruchy wykonują na zmianę gracz A i gracz B . Gracz A dostaje n cukierków i rozpoczyna grę. W każdym kroku gracz, który ma cukierki, zjada jeden lub dwa cukierki i przekazuje resztę cukierków przeciwnikowi. Wygrywa ten gracz, który zje ostatniego cukierka. Wykaż, że jeśli n dzieli się przez 3, to gracz B potrafi wygrać niezależnie od ruchów gracza A , natomiast jeśli n nie dzieli się przez 3, to gracz A potrafi wygrać niezależnie od ruchów gracza B .

Zadanie 486. Wykaż, że n prostych przecina się na płaszczyźnie w co najwyżej $\frac{n(n-1)}{2}$ punktach.

Zadanie 487. Pokaż przez indukcję, że dla każdej formuły zbudowanej ze zmiennych zdaniowych oraz spójników $\vee, \wedge, \Rightarrow, \neg$, liczba wystąpień zmiennych jest o 1 większa od liczby wystąpień binarnych spójników zdaniowych.

Zadanie 488. Pokaż przez indukcję, że dla każda formuła zbudowana ze zmiennych zdaniowych i spójników $\wedge, \vee$ jest spełnialna.

Zadanie 489. Pokaż przez indukcję, że dla każdego zbioru A mocy $n \in \mathbb{N}$ istnieje $n!$ bijekcji $f : A \rightarrow A$.

Zadanie 490. Udowodnij przez indukcję, że każdą liczbę naturalną większą od 1 można przedstawić w postaci iloczynu liczb pierwszych. *Wskazówka:* wybierz odpowiednią zasadę indukcji.

Zadanie 491. Niech $X \subseteq \mathbb{N}$. Udowodnij, że jeśli

- $0 \in X, 1 \in X$ oraz $2 \in X$,
- dla dowolnego $x \in \mathbb{N}$, z tego, że $x \in X, x + 1 \in X$ oraz $x + 2 \in X$ wynika, że $x + 3 \in X$,

to $X = \mathbb{N}$.

Zadanie 492. Mówimy, że graf $G = \langle V, E \rangle$ jest *spójny*, jeśli zwrotne i przechodnie domknięcie relacji E jest równe $V \times V$ (w języku teorii grafów oznacza to, że każde dwa wierzchołki są połączone ścieżką). Pokaż przez indukcję, że (dla wszystkich dodatnich liczb naturalnych n) każdy n -wierzchołkowy graf spójny ma co najmniej $n - 1$ krawędzi.

Twierdzenie 147 (o definiowaniu przez indukcję). Niech A i B będą dowolnymi zbiorami. Niech $g : A \rightarrow B$ oraz $h : B \times A \times \mathbb{N} \rightarrow B$ będą dowolnymi funkcjami. Wtedy istnieje dokładnie jedna funkcja $f : A \times \mathbb{N} \rightarrow B$ spełniająca warunki:

1. $\forall a \in A \ f(a, 0) = g(a)$,
2. $\forall a \in A \ \forall n \in \mathbb{N} \ f(a, n + 1) = h(f(a, n), a, n)$.

Twierdzenie 148 (drugie twierdzenie o definiowaniu przez indukcję).

Niech A i B będą dowolnymi zbiorami. Niech $g : A \rightarrow B$ oraz $h : B^* \times A \times \mathbb{N} \rightarrow B$ będą dowolnymi funkcjami. Wtedy istnieje dokładnie jedna funkcja $f : A \times \mathbb{N} \rightarrow B$ spełniająca warunki:

1. $\forall a \in A \ f(a, 0) = g(a)$,
2. $\forall a \in A \ \forall n \in \mathbb{N} \ f(a, n + 1) = h((f(a, 0), \dots, f(a, n)), a, n)$.

Twierdzenie 149 (O definiowaniu funkcji przez indukcję noetherowską).

Niech $\langle A, \leq \rangle$ będzie zbiorem regularnym i niech B, C będą dowolnymi zbiorami. Niech $B^{\subseteq A \times C}$ oznacza zbiór funkcji częściowych z $A \times C$ w B . Dla dowolnej funkcji $h : B^{\subseteq A \times C} \times A \times C \rightarrow B$ istnieje dokładnie jedna funkcja spełniająca warunek:

$$f(x, c) = h(f \cap (\{y \in A \mid y < x\} \times C \times B), x, c).$$

Zadanie 493. Udowodnij, że istnieje dokładnie jedna funkcja $\textit{suma} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ i dokładnie jedna funkcja $\textit{iloczyn} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ spełniające równania

$$\textit{suma}(n, 0) = n$$

$$\textit{suma}(n, m + 1) = \textit{suma}(n, m) + 1$$

$$\textit{iloczyn}(n, 0) = 0$$

$$\textit{iloczyn}(n, m + 1) = n + \textit{iloczyn}(n, m).$$

11

Elementy algebry uniwersalnej

11.1. Algebra termów

Definicja 150. *Sygnaturą* nazywamy rodzinę $\{\Sigma_n \mid n \in N\}$ zbiorów parami rozłącznych. Elementy zbioru Σ_n nazywamy *symbolami n -argumentowymi*. Elementy Σ_0 nazywamy *symbolami stałych* (lub po prostu *stałymi*). Kładziemy też $\Sigma = \bigcup_{n=0}^{\infty} \Sigma_n$.

Definicja 151. *Algebrą nad Σ* (lub *Σ -algebrą*) nazywamy niepusty zbiór A wraz z interpretacją $\cdot^A$, czyli przyporządkowaniem, które każdemu symbolowi $f \in \Sigma_n$ przyporządkowuje funkcję $f^A : A^n \rightarrow A$. Tak opisaną algebrę oznaczamy przez $\mathcal{A}$ lub $\langle A, f^A \mid f \in \Sigma \rangle$. Zbiór A nazywamy *nośnikiem* algebry $\mathcal{A}$.

Definicja 152 (Algebra termów). Niech Σ będzie sygnaturą i niech $V = \{v_i \mid i \in \mathbb{N}\}$ będzie zbiorem zmiennych (zakładamy, że $\Sigma \cap V = \emptyset$). Przez $T(\Sigma, V)$ będziemy oznaczać zbiór termów nad Σ , czyli najmniejszy zbiór zawierający zmienne i symbole stałych (to znaczy $V \subseteq T(\Sigma, V)$ i $\Sigma_0 \subseteq T(\Sigma, V)$) i zamknięty względem Σ (to znaczy jeśli $f \in \Sigma_n, t_1, \dots, t_n \in T(\Sigma, V)$, to $f(t_1, \dots, t_n) \in T(\Sigma, V)$).

Przez $T(\Sigma)$ będziemy oznaczać zbiór *termów stałych* nad Σ , czyli najmniejszy zbiór zawierający symbole stałych (to znaczy $\Sigma_0 \subseteq T(\Sigma)$) i zamknięty względem Σ (to znaczy jeśli $f \in \Sigma_n, t_1, \dots, t_n \in T(\Sigma)$, to $f(t_1, \dots, t_n) \in T(\Sigma)$).

Zbiór termów stałych można też zdefiniować jako zbiór tych termów, w których nie występują zmienne.

W zbiorze termów $T(\Sigma, V)$ łatwo określić interpretację $\cdot^{\mathcal{F}}$ sygnatury Σ , czyli algebrę

$$\langle T(\Sigma, V), f^{\mathcal{F}} : f \in \Sigma \rangle,$$

kładąc $f^{\mathcal{F}}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$ dla $f \in \Sigma_n, t_1, \dots, t_n \in T(\Sigma, V)$. Podobnie jeśli $\Sigma_0 \neq \emptyset$, można określić interpretację $\mathcal{H}$ sygnatury Σ w $T(\Sigma)$.

Algebry $\mathcal{F}$ i $\mathcal{H}$ są przykładami algebr wolnych nad Σ . Algebra $\mathcal{H}$ jest nazywana *algebrą Herbranda* nad Σ .

Definicja 153. Niech $t, t' \in T(\Sigma, V)$. Mówimy, że t' jest *podtermem* t , jeśli $t = t'$ lub $t = f(t_1, \dots, t_n)$ i t' jest podtermem t_i dla pewnego $i \leq n$. Jeśli t' jest podtermem t to piszemy $t' \sqsubseteq t$.

11.1.1. Inna definicja zbioru termów. Drzewa

Definicja 154. Niech A będzie dowolnym zbiorem. Zbiór $T \subseteq A^*$ jest *drzewem* jeśli jest zamknięty na przedrostki (to znaczy, jeśli $u \prec w$ (u jest przedrostkiem w) oraz $w \in T$, to $u \in T$).

Elementy drzewa nazywamy *wierzchołkami*. Każde drzewo zawiera słowo puste ϵ . Słowo puste nazywamy *korzeniem drzewa*. Jeśli $w \in T$ oraz $wa \in T$ dla $w \in A^*$, $a \in A$, to mówimy, że wa jest *następnikiem* (*synem*) w w T , w nazywamy *poprzednikiem* (*ojcem*) wa . Wierzchołek T , który nie ma następników nazywamy *liściem*. *Ścieżką* w drzewie T nazywamy dowolny podzbiór T liniowo uporządkowany relacją $\prec$. *Ścieżka* w drzewie T jest *gałęzią*, jeśli jest maksymalnym podzbiorem T liniowo uporządkowanym relacją $\prec$. Każda gałąź zawiera korzeń drzewa. Jeśli gałąź jest skończona, to zawiera dokładnie jeden liść. *Stopniem* wierzchołka w w drzewie T nazywamy liczbę następników w . *Długością ścieżki* π nazywamy moc zbioru π . *Wysokością drzewa* T nazywamy kres górny długości ścieżek w T . Jeśli drzewo T jest skończone, to jego wysokość jest równa długości najdłuższej gałęzi w T .

Definicja 155. Niech T będzie drzewem i niech $w \in T$. Kładziemy

$$T_w = \{u \in A^* \mid wu \in T\}.$$

Łatwo sprawdzić, że T_w jest drzewem. T_w nazywamy *poddrzewem drzewa* T *ukorze-nionym w* w . Drzewo U jest poddrzewem T , jeśli $U = T_w$ dla pewnego $w \in T$.

Definicja 156. *Drzewem adresów* nazywamy drzewo T nad $\mathbb{N}$ o tej własności, że dla każdego $w \in T$ zbiór następników w jest odcinkiem początkowym $\mathbb{N}$, to znaczy jeśli $wn \in T$ dla pewnego $n \in \mathbb{N}$, oraz $m < n$, to $wm \in T$.

Definicja 157. Niech Σ będzie sygnaturą. *Termem* nad Σ nazywamy dowolną parę $t = \langle T, e \rangle$, gdzie T jest drzewem adresów, $e : T \rightarrow \Sigma$ zaś taką funkcją, że jeśli $w \in T$, $e(w) \in \Sigma_n$, to w ma stopień n .

Definicja 158. Niech $t = \langle T, e \rangle$ będzie termem i niech $w \in T$. *Podtermem* t w w nazywamy term $t_w = \langle T_w, e_w \rangle$, gdzie $e_w(u) = e(wu)$. t' jest podtermem t , jeśli $t' = t_w$ dla pewnego $w \in T$.

11.1.2. Wartość termu

Definicja 159. Niech $\mathcal{A} = \langle A, f^{\mathcal{A}} : f \in \Sigma \rangle$ będzie algebrą nad sygnaturą Σ . Niech $T(\Sigma, X)$ będzie zbiorem termów sygnatury Σ ze zmiennymi ze zbioru X . *Wartościowaniem* X w algebrze $\mathcal{A}$ nazywamy funkcję $\sigma : X \rightarrow A$. *Wartością termu*

$t \in T(\Sigma, X)$ przy wartościowaniu σ nazywamy element $\mathcal{A}$ otrzymany z termu t po zastąpieniu każdej zmiennej x przez $\sigma(x)$, zastąpieniu symboli funkcji z Σ przez ich interpretację w $\mathcal{A}$ oraz obliczenie tak otrzymanego wyrażenia w $\mathcal{A}$.

Formalnie, wartościowanie σ rozszerza się do funkcji $\sigma^* : T(\Sigma, X) \rightarrow \mathcal{A}$ zdefiniowanej w następujący sposób:

$$\begin{aligned}\sigma^*(x) &= \sigma(x), \text{ dla } x \in X \text{ oraz} \\ \sigma^*(f(t_1, \dots, t_n)) &= f^{\mathcal{A}}(\sigma(t_1), \dots, \sigma(t_n)), \text{ dla } f \in \Sigma_n, t_1, \dots, t_n \in T(\Sigma, X)\end{aligned}$$

Jeśli nie będzie prowadzić to do nieporozumień, będziemy pisali σ zamiast σ^* . Funkcję σ nazywamy *wartościowaniem zmiennych*, a funkcję σ^* *wartościowaniem termów*. Element $\sigma^*(t)$ algebry $\mathcal{A}$ nazywamy wartością termu t w algebrze $\mathcal{A}$. Zauważmy, że jeśli term t nie zawiera zmiennych, to $\sigma^*(t)$ nie zależy od σ . Ogólniej, jeśli zmienna x nie występuje w t to $\sigma^*(t)$ nie zależy od $\sigma(x)$.

Definicja 160. Niech Σ będzie sygnaturą. Podstawienie σ w algebrze termów $\mathcal{F} = \langle T(\Sigma, V), f : f \in \Sigma \rangle$ jest funkcją przyporządkowującą zmiennym ze zbioru $X \subseteq V$ elementy $T(\Sigma, V)$. Jest to więc wartościowanie w algebrze termów. Jak poprzednio wartościowanie σ rozszerzamy do $\sigma^* : T(\Sigma, V) \rightarrow T(\Sigma, V)$ kładąc $\sigma(y) = y$ dla $y \in V \setminus X$. Oczywiście, tak jak poprzednio $\sigma^*(x) = \sigma(x)$ dla $x \in X$ oraz $\sigma^*(f(t_1, \dots, t_n)) = f(\sigma^*(t_1), \dots, \sigma^*(t_n))$. Term $\sigma^*(t)$ nazywamy wartością termu t przy podstawieniu σ . Podobnie jak poprzednio, jeśli nie prowadzi to do nieporozumień, piszemy σ zamiast σ^* . Wartość termu t przy podstawieniu σ jest termem uzyskanym z termu t przez zastąpienie każdego wystąpienia zmiennej x w termie t przez term $\sigma(x)$.

11.2. Homomorfizmy

Definicja 161. Niech $\mathcal{A}$ i $\mathcal{B}$ będą algebrami nad sygnaturą Σ . Funkcja $h : \mathcal{A} \rightarrow \mathcal{B}$ jest homomorfizmem algebry $\mathcal{A}$ w algebrę $\mathcal{B}$, jeśli dla każdego n , dla każdego $f \in \Sigma_n$ i dowolnych $a_1, \dots, a_n \in \mathcal{A}$ zachodzi równość

$$h(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(h(a_1), \dots, h(a_n)).$$

Przykład 162. Wartościowanie termów w algebrze $\mathcal{A}$ jest homomorfizmem algebry termów w algebrę $\mathcal{A}$.

Przykład 163. Podstawienie jest homomorfizmem algebry termów w siebie.

Zadanie 494. Niech Σ będzie dowolną sygnaturą i niech $\mathcal{A}$ i $\mathcal{B}$ będą dowolnymi algebrami sygnatury Σ . Wykaż, że istnieje algebra $\mathcal{C}$ o sygnaturze Σ , dla której istnieją homomorfizmy: g algebry $\mathcal{C}$ na $\mathcal{A}$ i h algebry $\mathcal{C}$ na $\mathcal{B}$.

Zadanie 495. Udowodnij, że pierścień $\mathbb{Z}_p = (\{0, \dots, p-1\}, +, \cdot, 0, 1)$ dla dowolnej liczby pierwszej p spełnia formułę $\forall x (x \neq 0 \Rightarrow \exists y (x \cdot y = 1))$.

Zadanie 496. Znajdź wszystkie homomorfizmy algebry $\langle \{a\}^*, \cdot, \epsilon \rangle$ w algebrę $\langle \{a, b\}^*, \cdot, \epsilon \rangle$, gdzie $\cdot$ oznacza konkatenację (złączenie) słów, a ϵ oznacza słowo puste.

Zadanie 497. Niech $\langle \{a, b\}^*, \cdot \rangle$ będzie algebrą słów nad alfabetem $\{a, b\}$ z konkatenacją „ $\cdot$ ”. Jaka jest moc zbioru wszystkich homomorfizmów $h : \{a, b\}^* \rightarrow \{a, b\}^*$ algebry $\langle \{a, b\}^*, \cdot \rangle$ w siebie?

Zadanie 498. Niech $\mathbb{Z}_n$ oznacza algebrę $\langle \{0, 1, \dots, n-1\}, + \rangle$, gdzie $+$ oznacza dodawanie modulo n . Ile jest homomorfizmów

1. $h : \mathbb{Z}_5 \rightarrow \mathbb{Z}_3$,
2. $h : \mathbb{Z}_3 \rightarrow \mathbb{Z}_5$?

Zadanie 499. Ile jest homomorfizmów $h : \mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_k$, dla $k \leq 2^n$.

Zadanie 500. Niech $\mathfrak{B}_n$ oznacza algebrę $\langle \mathcal{P}(\{0, \dots, n-1\}), \cup, \cap, \setminus \rangle$. Ile jest homomorfizmów:

1. $h : \mathfrak{B}_5 \rightarrow \mathfrak{B}_3$?
2. $h : \mathfrak{B}_3 \rightarrow \mathfrak{B}_5$?

Zadanie 501. Niech $\mathfrak{B}_n$ oznacza algebrę $\langle \mathcal{P}(\{0, \dots, n-1\}), \cup, \cap, {}^c \rangle$, gdzie c oznacza dopełnienie zbioru. Ile jest homomorfizmów:

1. $h : \mathfrak{B}_5 \rightarrow \mathfrak{B}_3$?
2. $h : \mathfrak{B}_3 \rightarrow \mathfrak{B}_5$?

Zadanie 502. Niech $\mathfrak{B}_n$ oznacza algebrę $\langle \mathcal{P}(\{0, \dots, n-1\}), \cup, \cap \rangle$. Ile jest homomorfizmów:

1. $h : \mathfrak{B}_5 \rightarrow \mathfrak{B}_3$?
2. $h : \mathfrak{B}_3 \rightarrow \mathfrak{B}_5$?

Zadanie 503. Niech $\mathfrak{B}_n$ oznacza algebrę $\langle \mathcal{P}(\{0, \dots, n-1\}), \cup \rangle$. Ile jest homomorfizmów:

1. $h : \mathfrak{B}_5 \rightarrow \mathfrak{B}_3$?
2. $h : \mathfrak{B}_3 \rightarrow \mathfrak{B}_5$?

Zadanie 504. Przyjmijmy, że $[0, 1) = \{r \in \mathbb{R} : 0 \leq r < 1\}$, funkcja $f : \mathbb{R} \rightarrow [0, 1)$ przyporządkowuje liczbie x część ułamkową x (tj. $f(x) \in [0, 1)$ i $x - f(x)$ jest liczbą całkowitą dla każdego $x \in \mathbb{R}$), a funkcja $g : [0, 1) \rightarrow \mathbb{R}$ jest identycznością na $[0, 1)$ (to znaczy $g(x) = x$ dla $x \in [0, 1)$). W zbiorze $[0, 1)$ definiujemy działanie $\oplus$ kładąc $x \oplus y = f(x + y)$. Rozważamy algebry

$$\begin{aligned}\mathcal{R}_1 &= \langle \mathbb{R}, + \rangle \\ \mathcal{R}_2 &= \langle \mathbb{R}, +, \times \rangle \\ \mathcal{R}_3 &= \langle [0, 1), \oplus \rangle \\ \mathcal{R}_4 &= \langle [0, 1), \oplus, \times \rangle\end{aligned}$$

- Czy f jest homomorfizmem algebry $\mathcal{R}_1$ w $\mathcal{R}_3$?
- Czy f jest homomorfizmem algebry $\mathcal{R}_2$ w $\mathcal{R}_4$?
- Czy g jest homomorfizmem algebry $\mathcal{R}_3$ w $\mathcal{R}_1$?
- Czy g jest homomorfizmem algebry $\mathcal{R}_4$ w $\mathcal{R}_2$?

Zadanie 505. Niech Σ będzie sygnaturą, zawierającą co najmniej jeden binarny symbol funkcyjny i niech V oznacza przeliczalny nieskończony zbiór zmiennych. Niech $\mathcal{T}(\Sigma, V)$ oznacza algebrę termów nad sygnaturą Σ ze zmiennymi z V . Rozważamy homomorfizmy

$$h : \mathcal{T}(\Sigma, V) \rightarrow \mathcal{T}(\Sigma, V).$$

Czy jest taki homomorfizm h i term t , dla których zbiór $h^{-1}(\{t\})$ jest nieskończony? Podaj wszystkie liczby naturalne n , takie, że istnieją h i t , dla których zbiór $h^{-1}(\{t\})$ ma n elementów.

11.3. Problem unifikacji

Definicja 164. Niech Σ będzie sygnaturą. *Problemem unifikacji* nazywamy następujące zadanie: „mając dany zbiór $\{(t_1, u_1), \dots, (t_n, u_n)\}$, znaleźć takie podstawienie σ , żeby dla każdego $i \leq n$ zachodziło $\sigma(t_i) = \sigma(u_i)$.” To znaczy, należy znaleźć takie przyporządkowanie termów zmiennym występującym w termach $t_1, u_1, \dots, t_n, u_n$, żeby po podstawieniu tych termów za odpowiednie zmienne uzyskać termy równe. Podstawienie σ nazywamy *unifikatorem* zbioru $\{(t_1, u_1), \dots, (t_n, u_n)\}$. Często ten zbiór (nazywany czasem *instancją problemu unifikacji*) zapisujemy jako

$$\{t_1 \stackrel{?}{=} u_1, \dots, t_n \stackrel{?}{=} u_n\}.$$

Definicja 165. Jeśli σ i τ są unifikatorami zbioru $\{(t_1, u_1), \dots, (t_n, u_n)\}$, to mówimy, że σ jest *ogólniejsze* od τ , (co oznaczamy $\tau \leq \sigma$) jeśli istnieje takie podstawienie ϱ , że $\tau = \varrho(\sigma)$, gdzie $(\varrho(\sigma))(x) = \varrho(\sigma(x))$. Podstawienie σ nazywamy

najogólniejszym unifikatorem zbioru

$$PU = \{t_1 \stackrel{?}{=} u_1, \dots, t_n \stackrel{?}{=} u_n\},$$

jeśli σ jest unifikatorem PU oraz σ jest ogólniejsze od każdego innego unifikatora PU .

Twierdzenie 166. Istnieje algorytm, który dla zadanej instancji

$$\{t_1 \stackrel{?}{=} u_1, \dots, t_n \stackrel{?}{=} u_n\}$$

problemu unifikacji znajduje jego najogólniejszy unifikator lub odpowiada „nie ma unifikatora”.

Zadanie 506. W tym zadaniu będziemy rozważać zadania unifikacji składające się z nieskończonej liczby par termów. Udowodnij następujące twierdzenie o zwartości dla problemu unifikacji: zadanie unifikacji $\{t_i \stackrel{?}{=} s_i\}_{i \in I}$, w którym występuje jedynie skończenie wiele różnych zmiennych, ma rozwiązanie wtedy i tylko wtedy, gdy każde jego skończone podzadanie $\{t_i \stackrel{?}{=} s_i\}_{i \in I_0}$, dla $I_0 \subseteq I$, $|I_0| < \infty$, ma rozwiązanie. Pokaż, że twierdzenie jest fałszywe, jeśli zadanie zawiera nieskończenie wiele zmiennych.

W poniższych zadaniach znajdź najogólniejszy unifikator dla podanych instancji problemu unifikacji (lub uzasadnij, że takowy nie istnieje) w algebrze termów o sygnaturze $\Sigma = \{c, d, g, f\}$ i zbiorze zmiennych $\mathcal{X} = \{x, y, z, u, v, \dots\}$.

Zadanie 507. $\{f(x, f(x, c, g(z))), f(g(g(z)), x, g(c))\} \stackrel{?}{=} f(f(u, v, v), y, y)$

Zadanie 508. $\{f(f(d, y), f(z, x))\} \stackrel{?}{=} f(f(y, z), f(x, c))\}$

Zadanie 509. $\{f(f(x, y), f(z, u))\} \stackrel{?}{=} f(f(f(f(u, u), f(u, u)), f(f(x, x), f(x, x))), f(f(f(y, y), f(y, y)), f(f(u, u), f(u, u))))\}$

Zadanie 510. $\{f(x_1, x_1) \stackrel{?}{=} x_2, f(x_2, x_2) \stackrel{?}{=} x_3, \dots, f(x_{n-1}, x_{n-1}) \stackrel{?}{=} x_n\}$

Zadanie 511. W tym zadaniu u, v, w, x, y, z są zmiennymi, natomiast a, f, g, h, p symbolami funkcyjnymi. Dla każdej z poniższych par termów podaj najogólniejszy unifikator lub uzasadnij, że dane termy nie są unifikowalne.

1. $p(f(y), w, g(z)) \stackrel{?}{=} p(v, u, v)$
2. $p(a, x, f(g(y))) \stackrel{?}{=} p(z, h(w), f(w))$
3. $p(z, h(w), g(z)) \stackrel{?}{=} p(v, u, v)$
4. $p(a, h(w), f(g(y))) \stackrel{?}{=} p(z, x, f(w))$

Elementy logiki formalnej

12.1. Rezolucja dla rachunku zdań

Definicja 167. *Literal* w rachunku zdań to zmienna zdaniowa lub negacja zmiennej zdaniowej. *Klauzulą* nazywamy alternatywę skończenie wielu literalów. Alternatywę zera literalów nazywamy klauzulą pustą i oznaczamy $\perp$.

W tym rozdziale przyjmujemy konwencję utożsamiającą klauzulę ze zbiorem jej literalów. W szczególności klauzule $p \vee q$ i $q \vee p$, podobnie jak $p \vee p$ i p będziemy uważać za identyczne.

Definicja 168. Mówimy, że zbiór formuł $\mathcal{F}$ jest spełnialny jeśli istnieje takie wartościowanie σ , że $\hat{\sigma}(\phi) = \text{T}$ dla wszystkich $\phi \in \mathcal{F}$; w przeciwnym przypadku mówimy że $\mathcal{F}$ jest *sprzeczny*. Formułę ϕ nazywamy *logiczną konsekwencją* zbioru formuł $\mathcal{F}$ jeśli dla każdego wartościowania σ spełniającego $\mathcal{F}$ zachodzi $\hat{\sigma}(\phi) = \text{T}$.

Definicja 169. Jeśli C i D są klauzulami a p jest zmienną zdaniową to klauzulę $C \vee D$ nazywamy *rezolwentą* klauzul $C \vee p$ i $D \vee \neg p$. Rezolucyjnym dowodem sprzeczności zbioru $\mathcal{F}$ nazywamy ciąg klauzul $C_0, \dots, C_n$ spełniający warunki

- dla wszystkich $i \in \{0, \dots, n\}$ zachodzi $C_i \in \mathcal{F}$ lub istnieją takie $j, k < i$, że C_i jest rezolwentą C_j i C_k .
- $C_n = \perp$.

W systemie rezolucji dość łatwo dowodzi się twierdzenie o poprawności (*jeśli istnieje rezolucyjny dowód sprzeczności zbioru $\mathcal{F}$, to zbiór $\mathcal{F}$ jest sprzeczny*). Natomiast dowód twierdzenia o zupełności (*jeśli zbiór $\mathcal{F}$ jest sprzeczny, to istnieje rezolucyjny dowód jego sprzeczności*) jest trudniejszy i wybiega poza ramy tego wykładu.

Zadanie 512. Udowodnij, że dla dowolnych klauzul C i D oraz dowolnej zmiennej zdaniowej p rezolwenta $C \vee D$ jest logiczną konsekwencją zbioru $\{C \vee p, D \vee \neg p\}$.

Zadanie 513. Podaj rezolucyjny dowód sprzeczności dla zbioru klauzul $\{\neg p \vee q, \neg p \vee \neg r \vee s, \neg q \vee r, p, \neg s\}$.

Zadanie 514. Podaj rezolucyjny dowód sprzeczności dla zbioru klauzul

$$\left\{ \begin{array}{ll} p \vee r, & \neg r \vee \neg s, \\ q \vee s, & q \vee r, \\ \neg p \vee \neg q, & s \vee p \end{array} \right\}.$$

Zadanie 515. Sprawdź, czy zbiór klauzul

$$\{p \vee q \vee r, \neg r \vee \neg q \vee \neg p, \neg q \vee r, \neg r \vee p\}$$

jest sprzeczny. Jeśli jest sprzeczny, podaj dla niego rezolucyjny dowód sprzeczności. Jeśli nie jest, podaj wartościowanie spełniające ten zbiór.

12.2. System Hilberta dla rachunku zdań ze spójnikami implikacji i fałszu

Definicja 170. Litera Δ oznacza dowolny zbiór formuł zdaniowych, zaś litery α, β, γ oznaczają dowolne formuły. Dla dowolnej formuły α zapis $\neg\alpha$ jest skrótem zapisu $\alpha \rightarrow \perp$.

Wyrażenie postaci $\Delta \vdash \alpha$ nazywamy *sekwentem*. Wyrażenie $\vdash \alpha$ oznacza $\emptyset \vdash \alpha$. Wyrażenie Δ, α oznacza $\Delta \cup \{\alpha\}$.

Aksjomaty systemu Hilberta

$$\begin{array}{l} \Delta, \alpha \vdash \alpha \\ \Delta \vdash \alpha \rightarrow (\beta \rightarrow \alpha) \\ \Delta \vdash (\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow \alpha \rightarrow \gamma) \\ \Delta \vdash \neg\neg\alpha \rightarrow \alpha \end{array}$$

Reguła dowodzenia (reguła odrywania)

$$\frac{\Delta \vdash \alpha \quad \Delta \vdash \alpha \rightarrow \beta}{\Delta \vdash \beta}$$

Sekwenty nad poziomą kreską nazywamy *przesłankami*, a sekwent pod kreską nazywamy *konkluzją*. Dowodem (sekwentu $\Delta \vdash \alpha$) nazywamy skończone drzewo etykietowane sekwentami, którego korzeń ma etykietę $\Delta \vdash \alpha$, liście są etykietowane aksjomatami oraz dla każdego wierzchołka jego etykieta jest konkluzją reguły wnioskowania, której przesłankami są etykiety następników tego wierzchołka. Jeśli istnieje dowód, którego korzeń jest etykietowany sekwentem $\Delta \vdash \alpha$, to mówimy, że sekwent $\Delta \vdash \alpha$ jest *wyprowadzalny* w systemie Hilbertowskim.

W systemie Hilberta zachodzą twierdzenia o poprawności i zupełności (sekwent $\vdash \alpha$ jest wyprowadzalny wtedy i tylko wtedy, gdy α jest tautologią), jednak ich dowody wybiegają poza ramy tego wykładu.

12.3. System naturalnej dedukcji

System naturalnej dedukcji kładzie nacisk na reguły dowodzenia, przy zachowaniu tylko jednego, bardzo prostego, aksjomatu. Jego intencją jest zachowanie jak największej zgodności struktury dowodów z naturalnym sposobem rozumowania w matematyce. Reguły dowodzenia (poza regułą *przez sprzeczność*) podzielone są na dwie grupy: reguły wprowadzania spójników logicznych, mówiące jak dowodzi się zdań z użyciem danego spójnika, oraz reguły eliminacji spójników logicznych mówiące jakie wnioski można wyciągnąć ze zdań używających danego spójnika. Podobnie jak w poprzednim rozdziale, zapis $\neg\alpha$ jest skrótem zapisu $\alpha \rightarrow \perp$. **Aksjomat systemu naturalnej dedukcji**

$$\Delta, \alpha \vdash \alpha$$

Reguły dowodzenia systemu naturalnej dedukcji

Reguły wprowadzania:

$$\frac{\Delta, \alpha \vdash \beta}{\Delta \vdash \alpha \rightarrow \beta} (\rightarrow -\text{intro})$$

$$\frac{\Delta \vdash \alpha \quad \Delta \vdash \beta}{\Delta \vdash \alpha \wedge \beta} (\wedge -\text{intro})$$

$$\frac{\Delta \vdash \alpha}{\Delta \vdash \alpha \vee \beta} (\vee -\text{intro}) \quad \frac{\Delta \vdash \beta}{\Delta \vdash \alpha \vee \beta} (\vee -\text{intro})$$

Reguły eliminacji:

$$\frac{\Delta \vdash \alpha \quad \Delta \vdash \alpha \rightarrow \beta}{\Delta \vdash \beta} (\rightarrow -\text{elim})$$

$$\frac{\Delta \vdash \alpha \wedge \beta}{\Delta \vdash \alpha} (\wedge -\text{elim}) \quad \frac{\Delta \vdash \alpha \wedge \beta}{\Delta \vdash \beta} (\wedge -\text{elim})$$

$$\frac{\Delta \vdash \alpha \vee \beta \quad \Delta, \alpha \vdash \gamma \quad \Delta, \beta \vdash \gamma}{\Delta \vdash \gamma} (\vee -\text{elim})$$

Reguła “przez sprzeczność”

$$\frac{\Delta, \neg\alpha \vdash \perp}{\Delta \vdash \alpha} (\text{PS})$$

Można udowodnić, że sekwent $\Delta \vdash \alpha$ jest wyprowadzalny w systemie naturalnej dedukcji wtedy i tylko wtedy gdy jest on wyprowadzalny w systemie Hilberta. W szczególności system ten ma własność poprawności i zupełności.

12.4. Składnia języka pierwszego rzędu

Definicja 171. *Sygnaturą* języka pierwszego rzędu nazywamy zbiór $\Sigma = \Sigma^F \cup \Sigma^R$, gdzie Σ^F jest zbiorem *symboli funkcyjnych* a Σ^R zbiorem *symboli relacyjnych*, przy czym $\Sigma^F = \bigcup_{i \in \mathbb{N}} \Sigma_i^F$ i $\Sigma^R = \bigcup_{i \in \mathbb{N}} \Sigma_i^R$, gdzie Σ_i^F i Σ_i^R są odpowiednio zbiorami i -argumentowych ($i \geq 0$) symboli funkcyjnych i relacyjnych.

Definicja 172. Zbiór termów $\mathcal{T}(\Sigma, V) = \mathcal{T}(\Sigma^F, V)$ definiujemy jako najmniejszy zbiór zawierający zmienne ze zbioru V i zamknięty ze względu na tworzenie termów złożonych zawierających symbole funkcji z Σ^F , tj. jeśli $t_1, \dots, t_n$ są termami, zaś $f \in \Sigma_n^F$, to $f(t_1, \dots, t_n)$ też jest termem.

Definicja 173. Zbiór formuł atomowych jest zbiorem napisów postaci $R(t_1, \dots, t_n)$, gdzie $R \in \Sigma_n^R$, zaś $t_1, \dots, t_n$ są termami.

Definicja 174. Zbiór *formuł języka pierwszego rzędu* jest najmniejszym zbiorem napisów zawierającym formuły atomowe, zamkniętym ze względu na spójniki zdaniowe $\vee, \wedge, \neg, \perp, \Rightarrow, \Leftrightarrow$, oraz kwantyfikatory $\forall$ i $\exists$, tzn. jeśli α i β są formułami, zaś x jest zmienną (z V), to formułami są także $\perp, \neg\alpha, \alpha \vee \beta, \alpha \wedge \beta, \alpha \Rightarrow \beta, \alpha \Leftrightarrow \beta, \forall x \alpha, \exists x \alpha$.

Definicja 175. Zbiór zmiennych *wolnych* $FV(\alpha)$ formuły α definiujemy indukcyjnie:

$$\begin{aligned} FV(\perp) &= \emptyset \\ FV(R(t_1, \dots, t_n)) &= FV(t_1) \cup \dots \cup FV(t_n) \\ FV(\alpha \vee \beta) = FV(\alpha \wedge \beta) = FV(\alpha \Rightarrow \beta) = FV(\alpha \Leftrightarrow \beta) &= FV(\alpha) \cup FV(\beta) \\ FV(\forall x \alpha) = FV(\exists x \alpha) &= FV(\alpha) \setminus \{x\} \end{aligned}$$

gdzie dla termów $FV(t_i)$ oznacza zbiór wszystkich zmiennych występujących w t_i .

Definicja 176. Wszystkie wolne wystąpienia zmiennej x w formule α stają się *związane* w formule $\forall x \alpha$ i $\exists x \alpha$. Mówimy że kwantyfikator *wiąże* te wystąpienia.

Definicja 177. Formuła bez zmiennych wolnych nazywa się *zdaniem*.

12.5. Semantyka języka pierwszego rzędu

Definicja 178. *Struktura* $\mathfrak{A}$ *sygnatury* Σ to niepusty zbiór A zwany jej *uniwersum* i *interpretacja*, czyli funkcja $\cdot^{\mathfrak{A}}$, która każdemu symbolowi funkcji $f \in \Sigma_n^F$, gdzie $n \geq 0$, przyporządkowuje funkcję $f^{\mathfrak{A}} : A^n \rightarrow A$, każdemu symbolowi relacji $R \in \Sigma_n^R$, gdzie $n > 0$, przyporządkowuje relację $R^{\mathfrak{A}} \subseteq A^n$ i każdemu symbolowi $R \in \Sigma_0^R$ przyporządkowuje wartość logiczną ze zbioru $\{T, F\}$.

Definicja 179. *Wartościowaniem* w strukturze $\mathfrak{A}$ nazywamy dowolną funkcję $v : V \rightarrow A$. Ponadto niech

$$(v_x^a)(y) = \begin{cases} v(y), & \text{gdy } x \neq y, \\ a, & \text{gdy } x = y, \end{cases}$$

dla dowolnego wartościowania $v : V \rightarrow A$, zmiennej $x \in V$ i elementu $a \in A$.

Definicja 180. Dla dowolnego termu z $\mathcal{T}(\Sigma^F, V)$ definiujemy indukcyjnie jego *interpretację* $t^{\mathfrak{A}}[v]$ przy zadanym wartościowaniu zmiennych $v : V \rightarrow A$:

$$\begin{aligned} x^{\mathfrak{A}}[v] &= v(x) \\ (f(t_1, \dots, t_n))^{\mathfrak{A}}[v] &= f^{\mathfrak{A}}(t_1^{\mathfrak{A}}[v], \dots, t_n^{\mathfrak{A}}[v]) \end{aligned}$$

Definicja 181. Poniżej definiujemy indukcyjnie relację $\models$. Gdy ona zachodzi, co oznaczamy $\mathfrak{A} \models \alpha[v]$, to mówimy że *struktura* $\mathfrak{A}$ *spełnia formułę* α *przy wartościowaniu* v .

1. Nigdy nie zachodzi $\mathfrak{A} \models \perp[v]$.
2. $\mathfrak{A} \models R(t_1, \dots, t_n)[v]$ wtw $(t_1^{\mathfrak{A}}[v], \dots, t_n^{\mathfrak{A}}[v]) \in R^{\mathfrak{A}}$.
3. $\mathfrak{A} \models (t_1 = t_2)[v]$ wtw $t_1^{\mathfrak{A}}[v] = t_2^{\mathfrak{A}}[v]$.
4. $\mathfrak{A} \models (\alpha \wedge \beta)[v]$ wtw gdy zachodzą jednocześnie $\mathfrak{A} \models \alpha[v]$ i $\mathfrak{A} \models \beta[v]$.
5. $\mathfrak{A} \models (\alpha \vee \beta)[v]$ wtw gdy $\mathfrak{A} \models \alpha[v]$ lub $\mathfrak{A} \models \beta[v]$.
6. $\mathfrak{A} \models (\alpha \Rightarrow \beta)[v]$ wtw gdy nie zachodzi $\mathfrak{A} \models \alpha[v]$ lub zachodzi $\mathfrak{A} \models \beta[v]$.
7. $\mathfrak{A} \models (\alpha \Leftrightarrow \beta)[v]$ wtw jednocześnie nie zachodzą $\mathfrak{A} \models \alpha[v]$ i $\mathfrak{A} \models \beta[v]$, lub jednocześnie zachodzą $\mathfrak{A} \models \alpha[v]$ i $\mathfrak{A} \models \beta[v]$.
8. $\mathfrak{A} \models (\forall x. \alpha)[v]$ wtw dla każdego elementu $a \in A$ zachodzi $\mathfrak{A} \models \alpha[v_x^a]$.
9. $\mathfrak{A} \models (\exists x. \alpha)[v]$ wtw istnieje element $a \in A$ dla którego zachodzi $\mathfrak{A} \models \alpha[v_x^a]$.

Definicja 182. Formuła α jest *spełnialna* w $\mathfrak{A}$, jeśli istnieje wartościowanie $v : V \rightarrow A$ dla którego zachodzi $\mathfrak{A} \models \alpha[v]$. Formuła α jest *spełnialna*, jeśli istnieje struktura $\mathfrak{A}$, w której α jest spełnialna. Formuła α jest *prawdziwa* w $\mathfrak{A}$ (struktura $\mathfrak{A}$ jest *modelem dla* α), jeśli dla każdego wartościowania $v : V \rightarrow A$ zachodzi $\mathfrak{A} \models \alpha[v]$. Formuła α jest *prawdziwa* (jest *tautologią*), jeśli dla każdej struktury $\mathfrak{A}$, formuła α jest prawdziwa w $\mathfrak{A}$.

Zadanie 516. Niech ϕ i ψ będą formułami rachunku kwantyfikatorów. Udowodnij, że następujące formuły są tautologiami.

- $(\exists x \phi \Rightarrow \psi) \Rightarrow \forall x \phi \Rightarrow \exists x \psi$
- $(\forall x \phi \Rightarrow \psi) \Rightarrow \exists x \phi \Rightarrow \exists x \psi$

12.6. Podstawienia

Definicja 183. Dla dowolnej formuły α napis $\alpha[x/t]$ oznacza wynik podstawienia termu t w każde wolne wystąpienie x w α . Podstawienie $[x/t]$ jest *dopuszczalne* w α , jeśli w wyniku tego podstawienia żadna zmienna z t nie staje się związana, tj. każde wystąpienie x w α nie znajduje się w zasięgu żadnego kwantyfikatora wiążącego zmienną występującą w t .

Twierdzenie 184 (o podstawianiu). Dla dowolnych termów s i t i zmiennej x zachodzi

$$(t[x/s])^{\mathfrak{A}}[v] = t^{\mathfrak{A}}[v_x^{s^{\mathfrak{A}}[v]}].$$

Dla dowolnej formuły α , jeśli podstawienie $[x/s]$ jest dopuszczalne w α , to

$$\mathfrak{A} \models (\alpha[x/s])[v] \quad \text{wtw} \quad \mathfrak{A} \models \alpha[v_x^{s^{\mathfrak{A}}[v]}].$$

Fakt 185. Dla dowolnej formuły α , zmiennej x i termu s , jeśli podstawienie $[x/s]$ jest dopuszczalne w α , to formuła $(\forall x.\alpha) \Rightarrow (\alpha[x/s])$ jest tautologią.

12.7. Rezolucja dla rachunku I rzędu

Definicja 186. *Literał* w rachunku kwantyfikatorów to formuła atomowa lub negacja formuły atomowej. *Klauzulą* nazywamy alternatywę skończenie wielu literałów. Alternatywę zera literałów nazywamy klauzulą pustą i oznaczamy $\perp$.

Definicja 187. Jeśli C i D są klauzulami, A i B formułami atomowymi i σ najogólniejszym unifikatorem A i B to klauzulę $\sigma(C \vee D)$ nazywamy *rezolwentą* klauzul $C \vee A$ i $D \vee \neg B$ a klauzulę $\sigma(C \vee A)$ *faktorem* klauzuli $C \vee A \vee B$. Rezolucyjnym dowodem sprzeczności zbioru klauzul $\mathcal{F}$ nazywamy ciąg klauzul $C_0, \dots, C_n$ spełniający warunki

- $C_n = \perp$, oraz
- dla wszystkich $i \in \{0, \dots, n\}$ zachodzi
 - $C_i \in \mathcal{F}$, lub

- istnieją takie $j, k < i$, że C_i jest rezolwentą C_j i C_k , lub
- istnieje takie $j < i$, że C_i jest faktorem C_j .

Zadanie 517. Mówimy, że formuła φ logiki I rzędu jest logiczną konsekwencją zbioru formuł $\mathcal{F}$ jeśli w każdej strukturze, w której prawdziwe są wszystkie formuły ze zbioru $\mathcal{F}$ prawdziwa jest również formuła φ .

Udowodnij, że jeśli C i D są klauzulami w logice I rzędu, A i B formułami atomowymi a σ najogólniejszym unifikatorem A i B , to rezolwenta $\sigma(C \vee D)$ jest logiczną konsekwencją klauzul $C \vee A$ i $D \vee \neg B$.

Zadanie 518. Podaj rezolucyjny dowód sprzeczności dla zbioru klauzul

$$\{\neg p(x) \vee \neg p(f(a)) \vee q(y), \quad p(z), \quad \neg p(g(b, u)) \vee \neg q(b)\},$$

gdzie a, b, f, g są symbolami funkcyjnymi, p i q są symbolami relacyjnymi a u, x, y, z są zmiennymi.

13

Zadania egzaminacyjne z rozwiązaniami*

Zadanie 519. Niech ϕ będzie formułą zdaniową zbudowaną ze zmiennych zdaniowych i spójników alternatywy, koniunkcji i negacji (do jej zapisania można oczywiście używać nawiasów). Przez *wartościowanie* rozumiemy w tym zadaniu funkcję, która zmiennym *występującym* w formule ϕ przyporządkowuje wartości ze zbioru $\{0, 1\}$. Niech n będzie dodatnią liczbą naturalną.

- a) Udowodnij, że dla każdej liczby naturalnej $k \leq 2^n$ istnieje formuła zdaniowa ϕ zawierająca n zmiennych i spełniona przez dokładnie k wartościowań.
- b) Dla jakich liczb k istnieje formuła ϕ zawierająca n zmiennych, w której każda ze zmiennych występuje dokładnie jeden raz i która jest spełniona przez dokładnie k wartościowań?

Rozwiązanie. Część a) jest oczywistą konsekwencją zupełności zbioru spójników złożonego z alternatywy, koniunkcji i negacji. Bierzymy dowolną funkcję boolowską n zmiennych przyjmującą wartość 1 dla k argumentów i korzystając z zupełności stwierdzamy, że jest to funkcja przyporządkowująca układowi zer i jedynej wartości logicznej pewnej formuły przy wartościowaniu wyznaczonym przez ten układ. Dokładniej, bierzemy n zmiennych zdaniowych $p_1, \dots, p_n$ i tworzymy formuły będące koniunkcją tych zmiennych bądź ich negacji (np. $\neg p_1 \wedge p_2 \wedge \dots \wedge p_n$). Formuły tej postaci są spełnione przez dokładnie jedno wartościowanie. Alternatywa k różnych formuł takiej postaci (dowolnie wybranych) jest formułą spełnioną przez dokładnie k wartościowań.

Bardziej szczegółowo przedstawimy inne rozwiązanie tego zadania. Przyjmijmy, że $W(\phi)$ oznacza zbiór wartościowań spełniających formułę ϕ . Symbolem $|X|$ oznaczamy liczbę elementów zbioru X .

Fakt 188. Jeżeli w formule ϕ występuje n zmiennych, to $|W(\neg\phi)| = 2^n - |W(\phi)|$.

*Rozdział przygotował A. Kościelski.

Dowód. Jest to oczywisty fakt. Dla formuły ϕ z n zmiennymi jest 2^n wartościowań. Każde z nich spełnia albo ϕ , albo $\neg\phi$, żadne nie może jednocześnie spełniać obu tych formuł.

Fakt 189. Jeżeli żadna zmienna nie występuje jednocześnie w formułach ϕ i ψ , to

$$|W(\phi \wedge \psi)| = |W(\phi)| \cdot |W(\psi)|.$$

Dowód. Rozważmy funkcję, która wartościowaniu h formuły $\phi \wedge \psi$ przyporządkowuje parę dwóch wartościowań: wartościowania będącego obcięciem h do zmiennych formuły ϕ i wartościowania będącego obcięciem h do zmiennych formuły ψ . Różnowartościowość tej funkcji jest oczywista.

Wystarczy teraz zauważyć, że funkcja ta przekształca zbiór $W(\phi \wedge \psi)$ na iloczyn kartezjański $W(\phi) \times W(\psi)$. (Gdzie w tym dowodzie korzysta się z założenia o zmiennych formuł ϕ i ψ ?)

Wniosek. Jeżeli zmienna p nie występuje w formule ϕ , to $|W(\phi \wedge p)| = |W(\phi)|$.

Wniosek. Jeżeli w formule ϕ występuje n zmiennych i nie ma wśród nich zmiennej p , to $|W(\phi \vee p)| = 2^n + |W(\phi)|$.

Dowód. Zauważmy, że

$$\begin{aligned} |W(\phi \vee p)| &= |W(\neg(\neg\phi \wedge \neg p))| \\ &= 2^{n+1} - |W(\neg\phi \wedge \neg p)| \\ &= 2^{n+1} - |W(\neg\phi)| \cdot |W(\neg p)| \\ &= 2^{n+1} - (2^n - |W(\phi)|) \cdot (2 - |W(p)|) \\ &= 2^{n+1} - 2^n + |W(\phi)| \\ &= 2^n + |W(\phi)|. \end{aligned}$$

Fakt 190. Dla każdej liczby naturalnej $k \leq 2^n$ istnieje formuła zdaniowa z n zmiennymi spełniona przez dokładnie k wartościowań.

Dowód. Fakt ten dowodzimy przez indukcję ze względu na n .

Zauważmy, że $|W(p \wedge \neg p)| = 0$, $|W(p)| = 1$ i $|W(p \vee \neg p)| = 2$. Tym samym twierdzenie jest prawdziwe dla $n = 1$.

Załóżmy, że twierdzenie to zachodzi dla liczby n i weźmy $k \leq 2^{n+1}$. Zachodzi jeden z dwóch przypadków: albo $k \leq 2^n$, albo $2^n < k \leq 2^{n+1}$.

Jeżeli $k \leq 2^n$, to znajdujemy formułę ϕ z n zmiennymi, która jest spełniona przez k wartościowań, i zmienną p , która nie występuje w ϕ . Formuła $\phi \wedge p$ jest spełniona przez k wartościowań i występuje w niej $n + 1$ zmiennych.

Jeżeli $2^n < k \leq 2^{n+1}$, to bierzemy formułę ϕ z n zmiennymi, spełnioną przez $k - 2^n$ wartościowań. Wtedy dla dowolnej zmiennej p nie występującej w ϕ formuła $\phi \vee p$ jest spełniona przez k wartościowań i występuje w niej $n + 1$ zmiennych.

Podobnie dowodzimy następujący fakt:

Fakt 191. Dla każdej nieparzystej liczby naturalnej $k \leq 2^n$ istnieje formuła zdaniowa z n zmiennymi, w której każda zmienna występuje dokładnie jeden raz i która jest spełniona przez dokładnie k wartościowań.

Dowód. Twierdzenie to także dowodzimy przez indukcję ze względu na n . Formułę, w której każda zmienna występuje najwyżej jeden raz, będziemy nazywać *formułą prostą*.

Zauważmy, że $|W(p)| = 1$. Wobec tego dowodzone twierdzenie jest prawdziwe dla $n = 1$.

Załóżmy, że twierdzenie to zachodzi dla liczby n i weźmy nieparzystą liczbę $k \leq 2^{n+1}$. Liczba k jest albo $\leq 2^n$, albo też spełnia nierówności $2^n < k \leq 2^{n+1}$.

Jeżeli $k \leq 2^n$, to znajdujemy prostą formułę ϕ z n zmiennymi, która jest spełniona przez k wartościowań, i zmienną p , która nie występuje w ϕ . Formuła $\phi \wedge p$ jest prosta i spełniona przez k wartościowań, oraz występuje w niej $n + 1$ zmiennych.

Jeżeli $2^n < k \leq 2^{n+1}$, to bierzemy prostą formułę ϕ z n zmiennymi, spełnioną przez $k - 2^n$ wartościowań. Wtedy dla dowolnej zmiennej p nie występującej w ϕ , formuła $\phi \vee p$ jest prosta, spełniona przez k wartościowań i występuje w niej $n + 1$ zmiennych.

Fakt 192. Jeżeli ϕ jest formułą, w której każda zmienna występuje najwyżej jeden raz, to ϕ jest spełniona przez nieparzystą liczbę wartościowań.

Dowód. Dowód przeprowadzimy przez indukcję ze względu na liczbę znaków występujących w formule. Formuła, która daje się zapisać za pomocą jednego znaku, jest zmienną i jest spełniona przez jedno wartościowanie.

Przypuśćmy, że $\phi = \neg\psi$ i występuje w niej n zmiennych. Oczywiście, każda zmienna występuje tyle samo razy w ϕ , co w ψ . Z założenia indukcyjnego wynika więc, że ψ jest spełniona przez nieparzystą liczbę wartościowań równą $|W(\psi)|$. Liczba $2^n - |W(\psi)|$ jest nieparzysta i jest równa liczbie wartościowań spełniających ϕ .

Jeżeli w koniunkcji $\phi \wedge \psi$ każda zmienna występuje najwyżej jeden raz (jeżeli koniunkcja ta jest prosta), to ϕ i ψ są proste, i żadna zmienna nie występuje jednocześnie w obu tych formułach. Wobec tego, formuła $\phi \wedge \psi$ jest spełniona przez $|W(\phi)| \cdot |W(\psi)|$ wartościowań. Na mocy założenia indukcyjnego, oba czynniki tego iloczynu są liczbami nieparzystymi. Iloczyn liczb nieparzystych też jest nieparzysty.

Jeszcze trzeba pokazać (można to zrobić w podobny sposób), że alternatywa będąca formułą prostą jest spełniona przez nieparzystą liczbę wartościowań. ■

Zadanie 520. Wykaż przez indukcję, że dla każdej formuły zdaniowej ϕ zbudowanej ze zmiennych oraz spójników $\wedge$ i $\vee$ (oczywiście do jej zapisania można też używać nawiasów) istnieje formuła ψ postaci $\psi_1 \vee \psi_2 \vee \dots \vee \psi_n$, taka, że dla każdego $i \leq n$ formuła ψ_i jest koniunkcją zmiennych oraz $(\phi \Leftrightarrow \psi)$ jest tautologią.

Rozwiązanie (szkic). Formuły ϕ i ψ są równoważne wtedy i tylko wtedy, gdy formuła $\phi \Leftrightarrow \psi$ jest tautologią. Zauważmy, że

Fakt 193. Formuła $(\phi_1 \vee \phi_2) \wedge \psi$ jest równoważna $(\phi_1 \wedge \psi) \vee (\phi_2 \wedge \psi)$, czyli formuła

$$(\phi_1 \vee \phi_2) \wedge \psi \Leftrightarrow (\phi_1 \wedge \psi) \vee (\phi_2 \wedge \psi)$$

jest tautologią.

Fakt 194. Formuła

$$(\phi_1 \vee \dots \vee \phi_n) \wedge \psi \Leftrightarrow (\phi_1 \wedge \psi) \vee \dots \vee (\phi_n \wedge \psi)$$

jest tautologią. Tautologią jest także formuła

$$\psi \wedge (\phi_1 \vee \dots \vee \phi_n) \Leftrightarrow (\psi \wedge \phi_1) \vee \dots \vee (\psi \wedge \phi_n).$$

Fakt 195. Formuła

$$(\phi_1 \vee \dots \vee \phi_n) \wedge (\phi'_1 \vee \dots \vee \phi'_m) \Leftrightarrow (\phi_1 \wedge \phi'_1) \vee \dots \vee (\phi_n \wedge \phi'_1) \vee \dots \vee (\phi_1 \wedge \phi'_m) \vee \dots \vee (\phi_n \wedge \phi'_m)$$

jest tautologią.

Korzystając z ostatniego faktu można dowieść własność podaną w zadaniu przez indukcję ze względu na liczbę spójników występujących w formule ϕ .

Jeżeli w formule ϕ nie występują spójniki, to jest ona zmienną. Każda zmienna jest jednoczłonową alternatywą, której jedynym członem jest jednoczłonowa koniunkcja. Tak więc w tym przypadku formuła ϕ ma odpowiednią postać i możemy przyjąć, że $\psi = \phi$.

Jeżeli w formule ϕ występuje przynajmniej jeden spójnik, to jest ona koniunkcją lub alternatywą formuł z mniejszą liczbą spójników. W przypadku alternatywy dalszy dowód jest prosty i zostaje pominięty. Jeżeli $\phi = \phi_1 \wedge \phi_2$, to na podstawie założenia indukcyjnego znajdujemy alternatywy ψ_1 i ψ_2 wymaganej postaci równoważne odpowiednio ϕ_1 i ϕ_2 . Wprowadzając odpowiednie oznaczenia możemy przyjąć, że lewa strona równoważności z ostatniego faktu jest równa $\psi_1 \wedge \psi_2$. Formułę ψ definiujemy jako prawą stronę równoważności z tego faktu.

Rozwiązanie (inny sposób). Najpierw sformalizujemy treść zadania.

Symbolem $\mathcal{K}$ będziemy oznaczać najmniejszy w sensie inkluzji spośród zbiorów X spełniających warunki:

1. wszystkie zmienne zdaniowe należą do X ,
2. jeżeli ϕ i ψ należą do X , to także formuła $\phi \wedge \psi$ należy do X .

Tak więc $\mathcal{K}$ jest zbiorem koniunkcji zmiennych zdaniowych. Symbolem $\mathcal{A}$ będziemy zaś oznaczać najmniejszy w sensie inkluzji spośród zbiorów X spełniających warunki:

1. $\mathcal{K} \subseteq X$,
2. jeżeli ϕ i ψ należą do X , to także formuła $\phi \vee \psi$ należy do X .

Tak więc $\mathcal{A}$ jest zbiorem alternatyw koniunkcji zmiennych zdaniowych. Posługując się wprowadzonymi oznaczeniami rozwiązywane zadanie można sformułować następująco: dowieść, że dla każdej formuły ϕ , w której występują tylko spójniki $\wedge$ i $\vee$, istnieje formuła $\psi \in \mathcal{A}$ taka, że formuła $\phi \Leftrightarrow \psi$ jest tautologią.

Dowód zostanie przeprowadzony przez indukcję ze względu na liczbę spójników występujących w formule ϕ .

Niech n będzie liczbą naturalną, a ϕ formułą, w której występuje n spójników i są to jedynie spójniki $\wedge$ i $\vee$. Będziemy zakładać, że jeżeli w pewnej formule występuje mniej niż n spójników, to jest ona równoważna formule należącej do $\mathcal{A}$. Przy tym założeniu wykazemy, że ψ też jest równoważna formule należącej do $\mathcal{A}$.

W dowodzie będziemy rozważać kilka przypadków. Najpierw przyjmijmy dodatkowo, że $n = 0$. Wtedy w formule ϕ nie ma spójników, a więc ϕ jest zmienną i — w konsekwencji — należy do $\mathcal{K}$ oraz do $\mathcal{A}$. W tym przypadku przyjmujemy, że $\psi = \phi$. Oczywiście, $\psi \in \mathcal{A}$, a ponadto, formuły ϕ i ψ są w oczywisty sposób równoważne.

Jeżeli $n > 0$, to w ϕ jest przynajmniej jeden spójnik. Wtedy ϕ jest albo koniunkcją, albo alternatywą formuł zawierających mniejszą liczbę spójników niż ϕ . Najpierw założymy, że $\phi = \phi_1 \vee \phi_2$. Dla formuł ϕ_1 i ϕ_2 możemy skorzystać z założenia indukcyjnego. Istnieją więc w $\mathcal{A}$ formuły ψ_1 i ψ_2 równoważne odpowiednio ϕ_1 i ϕ_2 . Oczywiście, $\psi_1 \vee \psi_2 \in \mathcal{A}$ oraz $\psi_1 \vee \psi_2$ jest równoważne z $\phi_1 \vee \phi_2$.

Jeżeli $\phi = \phi_1 \wedge \phi_2$, to także znajdujemy w $\mathcal{A}$ formuły ψ_1 i ψ_2 równoważne odpowiednio ϕ_1 i ϕ_2 . Formuły z $\mathcal{A}$ albo należą do $\mathcal{K}$, albo są alternatywami.

Jeżeli ψ_1 i ψ_2 należą do $\mathcal{K}$, to przyjmujemy, że $\psi = \psi_1 \wedge \psi_2$. Także w tym przypadku jest oczywiste, że $\psi \in \mathcal{K} \subseteq \mathcal{A}$ oraz, że ϕ jest równoważne ψ .

Pozostał do rozważania przypadek, w którym przynajmniej jedna z formuł ψ_1 i ψ_2 jest alternatywą. Założymy, że $\psi_1 = \psi_{11} \vee \psi_{12}$. Jeżeli okaże się, że alternatywą jest tylko ψ_2 będziemy postępować dokładnie tak samo. Na mocy prawa rozdzielności koniunkcji względem alternatywy (prawo $(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$) otrzymujemy, że formuła

$$\phi = (\phi_{11} \vee \psi_{12}) \wedge \phi_2$$

jest równoważna formule

$$(\phi_{11} \wedge \phi_2) \vee (\psi_{12} \wedge \phi_2).$$

Nietrudno zauważyć, że w obu członach tej alternatywy jest mniej spójników, niż w formule ϕ . Do tych członów możemy więc zastosować założenie indukcyjne. W ten sposób znajdujemy formuły ψ_1 i ψ_2 takie, że

$$\psi_1 \Leftrightarrow (\phi_{11} \wedge \phi_2) \text{ oraz } \psi_2 \Leftrightarrow (\phi_{12} \wedge \phi_2)$$

są tautologiami. Bez trudu dowodzimy, że formuła

$$\phi \Leftrightarrow (\psi_1 \vee \psi_2)$$

jest tautologią. Ponieważ $\psi_1, \psi_2 \in \mathcal{A}$, więc także $\psi_1 \vee \psi_2 \in \mathcal{A}$. W rozważanym przypadku możemy przyjąć, że $\psi = \psi_1 \vee \psi_2$.

Przedstawiony dowód można rozbić na dwie części dowodząc najpierw, że koniunkcja formuł należących do $\mathcal{A}$ jest równoważna formule należącej do $\mathcal{A}$. ■

Zadanie 521. Używając jedynie zmiennych, kwantyfikatorów, spójników logicznych, nawiasów i symboli $\in, \mathbb{N}, +, \times, =$ napisz formułę mówiące, że:

- nie ma największej liczby pierwszej,
- istnieje taka liczba naturalna, że każda liczba naturalna większa od niej jest sumą nie więcej niż czterech kwadratów liczb pierwszych,
- istnieje nieskończenie wiele par liczb bliźniaczych.

Para liczb bliźniaczych, to dwie liczby pierwsze różniące się o 2.

Rozwiązanie. Najpierw napiszemy pomocniczą formułę $P(x)$ równą

$$\neg \exists a \in \mathbb{N} \exists b \in \mathbb{N} \exists r \in \mathbb{N} \exists s \in \mathbb{N} (\neg x = a \wedge \neg x = b \wedge x = a + r \wedge x = b + s \wedge x = a \times b).$$

Zauważmy, że formuła $\exists r \in \mathbb{N} (x = a + r)$ jest równoważna nierówności $x \geq a$. Wobec tego formuła $P(x)$ stwierdza, że liczba x nie jest iloczynem dwóch liczb mniejszych od x , a więc stwierdza, że x jest liczbą pierwszą.

Własność „nie ma największej liczby pierwszej” można wyrazić pisząc

$$\neg \exists x \in \mathbb{N} (P(x) \wedge \forall y \in \mathbb{N} (P(y) \Rightarrow \exists r \in \mathbb{N} (x = y + r))).$$

Formuła

$$\begin{aligned} &\exists x \in \mathbb{N} \forall y \in \mathbb{N} \exists a \in \mathbb{N} \exists b \in \mathbb{N} \exists c \in \mathbb{N} \exists d \in \mathbb{N} \\ &((P(a) \vee a + a = a) \wedge (P(b) \vee b + b = b) \wedge (P(c) \vee c + c = c) \\ &\wedge (P(d) \vee d + d = d) \wedge x + y = a \times a + b \times b + c \times c + d \times d) \end{aligned}$$

stwierdza, że „istnieje taka liczba naturalna, że każda liczba naturalna większa od niej jest sumą nie więcej niż czterech kwadratów liczb pierwszych”. Zauważmy, że własność $a + a = a$ jest równoważna stwierdzeniu $a = 0$.

Ostatnią z wymienionych w zadaniu własności („istnieje nieskończenie wiele par liczb bliźniaczych”) można wyrazić pisząc

$$\forall x \in \mathbb{N} \exists y \in \mathbb{N} \exists d \in \mathbb{N} \exists r \in \mathbb{N} \\ ((\neg(d + d = d) \wedge d \times d = d + d) \wedge y = x + r \wedge P(y) \wedge P(y + d)).$$

Aby się o tym przekonać wystarczy zauważyć, że własności $\neg(d + d = d) \wedge d \times d = d + d$ oraz $d = 2$ są równoważne a także, że zbiór $\{y \in \mathbb{N} \mid \phi(y)\}$ jest nieskończony wtedy i tylko wtedy, gdy $\forall x \in \mathbb{N} \exists y \in \mathbb{N} (x \leq y \wedge \phi(y))$. ■

Zadanie 522. Pokaż, że

$$(A_1 \cup A_2) \div (B_1 \cup B_2) \subseteq (A_1 \div B_1) \cup (A_2 \div B_2). \quad (1)$$

Czy zawieranie

$$(A_1 \cap A_2) \div (B_1 \cap B_2) \subseteq (A_1 \div B_1) \cup (A_2 \div B_2) \quad (2)$$

jest prawdziwe dla dowolnych zbiorów A_1, A_2, B_1 i B_2 ?

Rozwiązanie. Zaczynamy od pierwszej inkluzji. Zgodnie z definicją, aby dowieść zawieranie $X \subseteq Y$ powinniśmy wziąć dowolny element $x \in X$ i o tym elemencie dowieść, że należy do zbioru Y . Weźmy więc $x \in (A_1 \cup A_2) \div (B_1 \cup B_2)$. Z definicji różnicy symetrycznej wiemy, że element ten spełnia równoważność

$$x \in (A_1 \cup A_2) \Leftrightarrow x \notin (B_1 \cup B_2). \quad (3)$$

Na podstawie tej równoważności niewiele potrafimy rozstrzygnąć. Załóżmy więc dodatkowo, że zachodzi

Przypadek 1: $x \in (A_1 \cup A_2)$. Z równoważności (3) otrzymujemy, że $x \notin (B_1 \cup B_2)$. Wobec tego, zarówno $x \notin B_1$, jak i $x \notin B_2$. Dalsze rozumowanie też będzie polegać na rozważeniu kolejnych przypadków.

Przypadek 1.1: $x \in A_1$. Wiemy już, że $x \notin B_1$. Zachodzi więc także równoważność

$$x \in A_1 \Leftrightarrow x \notin B_1, \quad (4)$$

np. dlatego, że w rozważanym przypadku obie strony tej równoważności są prawdziwe, albo dlatego, że dowodzenie tej równoważności polega na wykazaniu dwóch implikacji stwierdzających, że przy pewnych założeniach zachodzą fakty, których prawdziwość udało nam się wcześniej ustalić. Równoważność (4) oznacza, że $x \in (A_1 \div B_1)$, i tym bardziej, x należy do prawej strony wzoru (1).

Przypadek 1.2: $x \in A_2$. W tym przypadku, tak jak w poprzednim, dowodzimy, że $x \in A_2 \Leftrightarrow x \notin B_2$, i w konsekwencji, x należy do drugiego składnika prawej strony wzoru (1).

Przypadek 2: $x \notin (A_1 \cup A_2)$. Z równoważności (3) otrzymujemy teraz, że $x \in (B_1 \cup B_2)$. Mamy więc sytuację analogiczną do opisanej w przypadku 1. Dalszy dowód prowadzimy tak, jak w przypadku 1 zastępując A_1 i A_2 zbiorami B_1 oraz B_2 , i odwrotnie.

Zawieranie (2) jest też prawdziwe dla wszystkich zbiorów i można się o tym przekonać w bardzo podobny sposób. Proponuję, aby zainteresowane osoby same przekształciły podany dowód zawierania (1) w dowód inkluzji (2). W przypadku 1 w przekształconym dowodzie powinna być rozważana sytuacja, w której $x \notin B_1 \cap B_2$.

Rozwiązanie (inny sposób). Będziemy korzystać z następujących praw rachunku zbiorów:

$$\begin{aligned} X \dot{-} Y &= (X \setminus Y) \cup (Y \setminus X), \\ (X \cup Y) \setminus Z &= (X \setminus Z) \cup (Y \setminus Z), \\ X \setminus (Y \cup Z) &\subseteq X \setminus Y. \end{aligned}$$

Posługując się tymi prawami oraz monotonicznością sumy mnogościowej można wykazać, że

$$\begin{aligned} (A_1 \cup A_2) \dot{-} (B_1 \cup B_2) &= ((A_1 \cup A_2) \setminus (B_1 \cup B_2)) \cup ((B_1 \cup B_2) \setminus (A_1 \cup A_2)) \\ &= (A_1 \setminus (B_1 \cup B_2)) \cup (A_2 \setminus (B_1 \cup B_2)) \cup (B_1 \setminus (A_1 \cup A_2)) \cup (B_2 \setminus (A_1 \cup A_2)) \\ &\subseteq (A_1 \setminus B_1) \cup (A_2 \setminus B_2) \cup (B_1 \setminus A_1) \cup (B_2 \setminus A_2) = (A_1 \dot{-} B_1) \cup (A_2 \dot{-} B_2). \end{aligned}$$

Jeżeli wprowadzimy pojęcie dopełnienia zbioru, to w dowodzie zawierania (2) możemy wykorzystać wzór

$$X \dot{-} Y = X^c \dot{-} Y^c.$$

Zauważmy, że

$$\begin{aligned} (A_1 \cap A_2) \dot{-} (B_1 \cap B_2) &= (A_1 \cap A_2)^c \dot{-} (B_1 \cap B_2)^c = (A_1^c \cup A_2^c) \dot{-} (B_1^c \cup B_2^c) \\ &\subseteq (A_1^c \dot{-} B_1^c) \cup (A_2^c \dot{-} B_2^c) = (A_1 \dot{-} B_1) \cup (A_2 \dot{-} B_2). \end{aligned}$$

Zadanie 523. Pokaż, że

1. $A_1 \dot{-} \dots \dot{-} A_n$ zawiera te i tylko te elementy, które należą do nieparzystej liczby zbiorów A_i , gdzie $i = 1, \dots, n$;
2. jeśli zbiory $A_1, \dots, A_n$ są skończone, to

$$|A_1 \dot{-} \dots \dot{-} A_n| = \sum_{i=1}^n (-2)^{i-1} \sum_{\substack{I \subseteq \{1, \dots, n\} \\ |I|=i}} \left| \bigcap_{j \in I} A_j \right|.$$

Rozwiązanie. *Część I.* Tak naprawdę rozwiążemy ogólniejsze zadanie, a mianowicie pokażemy, że dla dowolnych zbiorów $A_1, \dots, A_n$, dla dowolnego wyrażenia $A_1 \dot{\cup} \dots \dot{\cup} A_n$ (z dowolnym rozmieszczeniem nawiasów) i dla dowolnego x zachodzi następująca równoważność:

$$x \in A_1 \dot{\cup} \dots \dot{\cup} A_n \Leftrightarrow x \text{ należy do nieparzystej liczby zbiorów spośród } A_1, \dots, A_n.$$

Najpierw musimy nieco uściślić sformułowanie zadania, które nie jest precyzyjne np. w przypadku, gdy $A_1 = \dots = A_n$. Przypuśćmy, że rozważamy rodzinę zbiorów $(A_i)_{i \in I}$ indeksowanych zbiorem I . Tak więc, jeżeli rozważamy rodzinę $A_1, \dots, A_n$, to $I = \{1, \dots, n\}$. Dla takiej rodziny i dla dowolnego elementu x definiujemy zbiór

$$I(x) = \{i \in I \mid x \in A_i\}.$$

Posługując się wprowadzonym oznaczeniem równoważność z treści zadania możemy zapisać w postaci

$$x \in A_1 \dot{\cup} \dots \dot{\cup} A_n \Leftrightarrow |I(x)| \text{ jest nieparzysta.}$$

Zauważmy od razu, że dla $n = 1$ ta równoważność jest oczywista.

Dowód będziemy prowadzić przez indukcję. Musimy więc sformułować zadanie tak, aby było możliwe zastosowanie zasady indukcji. Będziemy dowodzić, że dla każdej liczby naturalnej $n \geq 1$, dla dowolnej rodziny zbiorów $A_1, \dots, A_n$ indeksowanej zbiorem $\{1, \dots, n\}$ zachodzi teza zadania. Fakt, że dla dowolnej rodziny zbiorów $A_1, \dots, A_n$ zachodzi teza zadania, oznaczmy symbolem $\phi(n)$. W dowodzie skorzystamy z zasady indukcji, która stwierdza, że aby dowieść zdanie postaci $\forall n \geq 1 \phi(n)$ wystarczy pokazać, że dla dowolnego $n \geq 1$, z tego, że $\phi(k)$ zachodzi dla $k < n$ wynika, że także zachodzi $\phi(n)$. Osoby, które nie są przekonane do tego schematu indukcji, mogą spróbować przerobić podany dowód na dowód korzystający ze zwykłego schematu indukcji, ale wtedy trzeba dowodzić tezę w postaci $\forall n \geq 1 \forall k \leq n \phi(k)$.

Przypuśćmy, że $n \geq 2$ oraz

$$A_1 \dot{\cup} \dots \dot{\cup} A_n = (A_1 \dot{\cup} \dots \dot{\cup} A_k) \dot{\cup} (A_{k+1} \dot{\cup} \dots \dot{\cup} A_n).$$

Weźmy dowolny element x . Będziemy rozważać dwa przypadki: $x \in A_{k+1} \dot{\cup} \dots \dot{\cup} A_n$ oraz $x \notin A_{k+1} \dot{\cup} \dots \dot{\cup} A_n$.

W pierwszym przypadku, z założenia indukcyjnego wynika, że x należy do nieparzystej liczby zbiorów spośród $A_{k+1}, \dots, A_n$. Zauważmy także, że następujące warunki są równoważne:

1. $x \in A_1 \dot{\cup} \dots \dot{\cup} A_n$,
2. $x \notin A_1 \dot{\cup} \dots \dot{\cup} A_k$,
3. x należy do parzystej liczby zbiorów spośród $A_1, \dots, A_k$,

4. x należy do nieparzystej liczby zbiorów spośród $A_1, \dots, A_n$.

W drugim przypadku przeprowadzamy analogiczne rozumowanie. Zauważmy też, że z rozwiązanego, ogólniejszego zadania wynika, że różnica symetryczna jest łączna.

Część 1, rozwiązanie wymagające łączności różnicy symetrycznej. Oczywiście, $A \dot{\cup} B \subseteq A \cup B$. Stąd przez łatwą indukcję otrzymujemy, że $A_1 \dot{\cup} \dots \dot{\cup} A_n \subseteq A_1 \cup \dots \cup A_n$. Z tego wzoru wynika, że elementy nie należące do żadnego ze zbiorów $A_1, \dots, A_n$ nie należą także do różnicy $A_1 \dot{\cup} \dots \dot{\cup} A_n$.

Przypuśćmy, że element x należy do parzystej liczby zbiorów spośród $A_1, \dots, A_n$. Przetawmy zbiory $A_1, \dots, A_n$ tak, aby te zbiory, do których należy x , znalazły się na pierwszych miejscach. Jeżeli po takim przestawieniu zbiory znalazły się w porządku $A_{i_1}, \dots, A_{i_n}$ i x należy do $2 \cdot k$ tych zbiorów, to z łączności i przemienności różnicy symetrycznej otrzymujemy, że

$$A_1 \dot{\cup} \dots \dot{\cup} A_n = (A_{i_1} \dot{\cup} A_{i_2}) \dot{\cup} \dots \dot{\cup} (A_{i_{2k-1}} \dot{\cup} A_{i_{2k}}) \dot{\cup} A_{i_{2k+1}} \dot{\cup} \dots \dot{\cup} A_{i_n}.$$

Zauważmy, że x nie należy do zbiorów

$$(A_{i_1} \dot{\cup} A_{i_2}), \dots, (A_{i_{2k-1}} \dot{\cup} A_{i_{2k}}), A_{i_{2k+1}}, \dots, A_{i_n}.$$

Stąd wynika, że x nie należy także do różnicy $A_1 \dot{\cup} \dots \dot{\cup} A_n$.

Udowodniliśmy więc, że elementy należące do parzystej liczby zbiorów spośród $A_1, \dots, A_n$ nie należą do różnicy $A_1 \dot{\cup} \dots \dot{\cup} A_n$. Oznacza to, że elementy należące do różnicy $A_1 \dot{\cup} \dots \dot{\cup} A_n$ należą do nieparzystej liczby zbiorów spośród $A_1, \dots, A_n$.

Udowodnimy jeszcze implikację odwrotną. Załóżmy więc, że element x należy do nieparzystej liczby zbiorów spośród $A_1, \dots, A_n$, w tym do zbioru A_1 . Element ten należy do parzystej liczby zbiorów spośród $A_2, \dots, A_n$. Wobec tego nie należy do różnicy $A_2 \dot{\cup} \dots \dot{\cup} A_n$. Tym samym należy do różnicy

$$A_1 \dot{\cup} (A_2 \dot{\cup} \dots \dot{\cup} A_n) = A_1 \dot{\cup} \dots \dot{\cup} A_n.$$

Część 2. Jeśli zbiory $A_1, \dots, A_n$ są skończone, to

$$|A_1 \dot{\cup} \dots \dot{\cup} A_n| = \sum_{i=1}^n (-2)^{i-1} \sum_{|I|=i} \left| \bigcap_{j \in I} A_j \right|.$$

Weźmy skończony zbiór X zawierający zbiory $A_1, \dots, A_n$. Niech Ch_A oznacza funkcję określoną w zbiorze X , przyjmującą wartości 0 i 1, przyjmującą wartość 1 dokładnie dla tych argumentów, które należą do A . Zauważmy, że

$$\sum_{x \in X} \text{Ch}_A(x) = |A|.$$

Będziemy przekształcać prawą stronę dowodzonego wzoru. Mamy więc

$$\begin{aligned} \sum_{i=1}^n (-2)^{i-1} \sum_{|I|=i} \left| \bigcap_{j \in I} A_j \right| &= \sum_{i=1}^n (-2)^{i-1} \sum_{|I|=i} \sum_{x \in X} \text{Ch}_{\bigcap_{j \in I} A_j}(x) \\ &= \sum_{x \in X} \sum_{i=1}^n (-2)^{i-1} \sum_{|I|=i} \text{Ch}_{\bigcap_{j \in I} A_j}(x). \end{aligned}$$

Przyjmijmy, że $I(x) = \{i \leq n \mid x \in A_i\}$. Nietrudno zauważyć, że warunek

$$\text{Ch}_{\bigcap_{j \in I} A_j}(x) = 1$$

jest równoważny ze stwierdzeniem $I \subseteq I(x)$. Wobec tego (po rozbiciu sumy na składniki równe 0 i równe 1) otrzymujemy, że dla $i \leq |I(x)|$

$$\sum_{|I|=i} \text{Ch}_{\bigcap_{j \in I} A_j}(x) = \sum_{\substack{|I|=i \\ \text{Ch}_{\bigcap_{j \in I} A_j}(x)=1}} 1 = \sum_{\substack{|I|=i \\ I \subseteq I(x)}} 1 = \binom{|I(x)|}{i}.$$

Ponadto, dla $i > |I(x)|$ suma ta jest równa 0. Wróćmy do przerwanych przekształceń:

$$\begin{aligned} \sum_{x \in X} \sum_{i=1}^n (-2)^{i-1} \sum_{|I|=i} \text{Ch}_{\bigcap_{j \in I} A_j}(x) &= \sum_{x \in X} \sum_{i=1}^{|I(x)|} (-2)^{i-1} \sum_{|I|=i} \text{Ch}_{\bigcap_{j \in I} A_j}(x) \\ &= \sum_{x \in X} \sum_{i=1}^{|I(x)|} (-2)^{i-1} \binom{|I(x)|}{i} = \sum_{x \in X} (-2)^{-1} \left(\sum_{i=0}^{|I(x)|} (-2)^i \binom{|I(x)|}{i} - 1 \right) \\ &= \sum_{x \in X} (-2)^{-1} ((1-2)^{|I(x)|} - 1) = \sum_{x \in X} 2^{-1} (1 - (-1)^{|I(x)|}). \end{aligned}$$

Teraz zauważmy, że liczba $2^{-1}(1 - (-1)^m)$ jest równa 0 lub 1, i jest równa 1 wtedy i tylko wtedy, gdy m jest liczbą nieparzystą. Stąd otrzymujemy, że

$$\sum_{x \in X} 2^{-1} (1 - (-1)^{|I(x)|}) = |\{x \in X : |I(x)| \text{ jest nieparzyste}\}| = |A_1 \dot{-} \dots \dot{-} A_n|,$$

i to kończy dowód. ■

Zadanie 524. Dla jakich zbiorów C prawdziwe jest zdanie stwierdzające, że dla dowolnych zbiorów A i B zachodzi

$$A \times C \subseteq B \times C \Rightarrow A \subseteq B? \quad (1)$$

Rozwiązanie. Najpierw spróbujemy dowieść implikację (1). Mamy więc zbiory A , B i C , zakładamy, że zbiory te spełniają założenie $A \times C \subseteq B \times C$. W tej sytuacji staramy się dowieść, że $A \subseteq B$. Aby dowieść to zawieranie, bierzemy $x \in A$ i próbujemy wykazać, że $x \in B$. Oczywiście, powinniśmy skorzystać z założenia. Łatwo zauważyć, że w tym celu przydałaby się para o pierwszej współrzędnej x i drugiej należącej do C . Aby taką parę utworzyć, musimy mieć element zbioru C . Jest to proste pod warunkiem, że C jest zbiorem niepustym. Wtedy zbiór C ma przynajmniej jeden element. Jeden z elementów zbioru C oznaczamy symbolem c i tworzymy parę $\langle x, c \rangle$. Ta para należy do iloczynu kartezjańskiego $A \times C$. Na podstawie założenia stwierdzamy, że należy także do iloczynu $B \times C$. Jeżeli $\langle x, c \rangle \in B \times C$, to także $x \in B$.

Przedstawione rozumowanie pozwala dowieść implikację (1), ale wymaga dodatkowego założenia, że zbiór C jest niepusty. Nietrudno zauważyć, że w przypadku, gdy C jest zbiorem pustym, to puste są także zbiory $A \times C$ i $B \times C$, i w konsekwencji, poprzednik implikacji (1) jest prawdziwy dla dowolnych zbiorów A i B . Jeżeli przyjmujemy, że A jest dowolnym zbiorem niepustym (np. zbiorem liczb naturalnych), a B jest zbiorem pustym, to następnik implikacji (1) będzie fałszywy, i to samo będzie można powiedzieć o całej implikacji.

Ostatecznie otrzymujemy, że implikacja $A \times C \subseteq B \times C \Rightarrow A \subseteq B$ zachodzi dla wszystkich zbiorów A i B wtedy i tylko wtedy, gdy C nie jest zbiorem pustym. ■

Zadanie 525. Inwolucją nazywamy odwzorowanie $f : A \rightarrow A$ takie, że ff jest identycznością na A . Czy involucja jest bijekcją na A ? Pokaż, że każdą bijekcję można przedstawić jako złożenie dwóch involucji.

Rozwiązanie. *Część 1: każda involucja jest bijekcją.* Przypuśćmy, że $f : A \rightarrow A$ jest involucją. Spełnia więc dla dowolnego $x \in A$ równość $f(f(x)) = x$. Taka funkcja f jest typu „na”: wartość $x \in A$ przyjmuje dla argumentu $f(x)$. Jest to też funkcja różnowartościowa. Aby się o tym przekonać, weźmy dwa argumenty $x, y \in A$ takie, że $f(x) = f(y)$. Dla takich argumentów zachodzi też równość $f(f(x)) = f(f(y))$. Jeżeli f jest involucją, to stąd wynika, że $x = y$.

Część 2. Ta część zadania jest znacznie trudniejsza. Rozwiązując to zadanie zauważyłem, że jest właściwie tylko jedna bijekcja, którą trzeba przedstawić jako złożenie involucji. Tą bijekcją jest funkcja S przekształcająca zbiór liczb całkowitych $\mathbb{Z}$ w $\mathbb{Z}$ zdefiniowana wzorem $S(n) = n + 1$.

Krok 1. Aby przedstawić S jako złożenie involucji, weźmy funkcje $f, g : \mathbb{Z} \rightarrow \mathbb{Z}$ zdefiniowane wzorami $f(n) = -n$ oraz $g(n) = -(n + 1)$. Funkcje te są involucjami. Sprawdzenie tego faktu wymaga jedynie elementarnych rachunków. Mamy też

$$f(g(n)) = f(-(n + 1)) = n + 1 = S(n).$$

Tak więc $S = fg$.

Krok 2. Załóżmy, że $m > 0$. Symbolem $k \bmod m$ będziemy oznaczać resztę z dzielenia liczby k przez m , a więc najmniejszą nieujemną liczbę x taką, że $k - x$ dzieli się przez m . Korzystając z przedstawienia z kroku 1 można bez trudu przedstawić w postaci złożenia inwolucji funkcję $S_m : \{i \in \mathbb{N} : i < m\} \rightarrow \{i \in \mathbb{N} : i < m\}$ zdefiniowaną wzorem

$$S_m(n) = S(n) \bmod m = (n + 1) \bmod m = \begin{cases} n + 1 & \text{jeżeli } n < m - 1 \\ 0 & \text{jeżeli } n = m - 1. \end{cases}$$

Weźmy funkcję $f_m : \{i \in \mathbb{N} \mid i < m\} \rightarrow \{i \in \mathbb{N} \mid i < m\}$ taką, że

$$f_m(n) = f(n) \bmod m = (-n) \bmod m = \begin{cases} m - n & \text{jeżeli } n > 0 \\ 0 & \text{jeżeli } n = 0 \end{cases}$$

oraz funkcję $g_m : \{i \in \mathbb{N} \mid i < m\} \rightarrow \{i \in \mathbb{N} \mid i < m\}$ taką, że

$$g_m(n) = g(n) \bmod m = (-(n + 1)) \bmod m = m - n - 1.$$

Ponieważ dodawanie i dodawanie modulo m mają własności przysługujące dodawaniu w pierścieniu, i tylko takie własności były wykorzystywane w kroku 1, więc funkcje f_m i g_m są inwolucjami i zachodzi równość $S_m = f_m g_m$. Osoby, dla których przytoczony argument nie jest jasny, mogą sprawdzić bezpośrednio wymagane równości.

Krok 3. Weźmy teraz bijekcję $s : A \rightarrow A$ i załóżmy, że zbiór A jest rozłączną sumą dwóch zbiorów A_1 i A_2 przekształcanych przez funkcję s w siebie (zakładamy więc, że $A_1 \cap A_2 = \emptyset$, $A = A_1 \cup A_2$, $s(x) \in A_1$ dla dowolnego $x \in A_1$ oraz analogiczną własność dla zbioru A_2).

Niech $s^{(1)}$ oznacza obcięcie funkcji s do zbioru A_1 (tak więc $s^{(1)} : A_1 \rightarrow A_1$ i $s^{(1)}(x) = s(x)$ dla wszystkich $x \in A_1$). Podobnie, niech $s^{(2)}$ oznacza obcięcie funkcji s do A_2 . Funkcje $s^{(1)}$ i $s^{(2)}$ są bijekcjami. Zauważmy, że jeżeli $s^{(1)}$ i $s^{(2)}$ są złożeniami inwolucji, to złożeniem inwolucji jest również funkcja s .

Jeżeli $s^{(1)} = f^{(1)}g^{(1)}$ i $s^{(2)} = f^{(2)}g^{(2)}$ dla inwolucji $f^{(1)}$, $g^{(1)}$, $f^{(2)}$ i $g^{(2)}$, to $s = fg$ dla inwolucji $f, g : A \rightarrow A$ zdefiniowanych wzorami

$$f(x) = \begin{cases} f^{(1)}(x) & \text{jeżeli } x \in A_1 \\ f^{(2)}(x) & \text{jeżeli } x \in A_2 \end{cases} \quad \text{oraz} \quad g(x) = \begin{cases} g^{(1)}(x) & \text{jeżeli } x \in A_1 \\ g^{(2)}(x) & \text{jeżeli } x \in A_2. \end{cases}$$

Sprawdzenie podanych wyżej własności pozostawiam zainteresowanym.

Przedstawioną konstrukcję bez trudu można uogólnić na przypadek, w którym zbiór A jest sumą trzech zbiorów, lub jest sumą dowolnej skończonej liczby zbiorów. Można też ją uogólnić na przypadek dowolnego podziału zbioru A , także nieskończonego.

Krok 4. Mając bijekcję $s : A \rightarrow A$ podzielę zbiór A na takie fragmenty, dla których s będzie można łatwo przedstawić w postaci złożenia inwolucji.

Przyjmijmy, że jeżeli n jest dodatnią liczbą naturalną, to s^n oznacza n -krotne złożenie funkcji s . Tak więc $s^1 = s$, $s^2 = ss$, $s^{n+1} = ss^n$. Umówmy się także, że s^0 jest funkcją identycznościową w zbiorze A . Jeżeli natomiast n jest liczbą ujemną, to s^n oznacza $(-n)$ -krotne złożenie $(s^{-1})^{-n}$ funkcji odwrotnej do s . Dowodzi się, że dla dowolnych liczb całkowitych n i m zachodzi wzór $s^{n+m} = s^n s^m$ lub nieco inaczej, dla dowolnego $x \in A$ zachodzi wzór $s^{n+m}(x) = s^n(s^m(x))$.

Zdefiniujemy teraz relację R w zbiorze A przyjmując, że

$$x R y \Leftrightarrow \exists n \in \mathbb{Z} \ y = s^n(x)$$

dla dowolnych $x, y \in A$. Relacja R jest relacją równoważności. Rozbija więc zbiór A na klasy abstrakcji, czyli na zbiory postaci $\{y \in A \mid x R y\}$. Różne klasy abstrakcji są rozłączne. Jest też oczywiste, że jeżeli $z \in \{y \in A \mid x R y\}$, to także $s(z) \in \{y \in A \mid x R y\}$. W dalszym ciągu będziemy przedstawiać funkcję s (a właściwie jej obcięcie) w postaci złożenia inwolucji na każdej klasie abstrakcji relacji R .

Krok 5. Przypuśćmy, że prócz bijekcji $s : X \rightarrow X$ mamy bijekcje $t : Y \rightarrow Y$ i $\phi : Y \rightarrow X$ takie, że $s\phi = \phi t$. Jeżeli wtedy funkcja t jest złożeniem dwóch inwolucji, to funkcja s też ma tę własność.

Jeżeli $t = fg$ dla inwolucji $f, g : Y \rightarrow Y$, to

$$s(\phi(y)) = (s\phi)(y) = (\phi t)(y) = (\phi fg)(y) = ((\phi f \phi^{-1})(\phi g \phi^{-1}))(\phi(y)).$$

Ponieważ funkcja ϕ jest typu „na”, z udowodnionej równości wynika, że

$$s = (\phi f \phi^{-1})(\phi g \phi^{-1}).$$

Wystarczy jeszcze zauważyć, że złożenia $(\phi f \phi^{-1})$ i $(\phi g \phi^{-1})$ są inwolucjami.

Krok 6. W dalszym ciągu będziemy zajmować się klasą abstrakcji ustalonego elementu $a_0 \in A$, a więc zbiorem $A_0 = \{y \in A \mid a_0 R y\}$. Zdefiniujmy pomocniczą funkcję $\phi : \mathbb{Z} \rightarrow A_0$ przyjmując, że

$$\phi(n) = s^n(a_0).$$

Funkcji ϕ przekształca zbiór liczb całkowitych na klasę A_0 . Dalej będziemy badać funkcję ϕ . Są możliwe dwa przypadki: albo dla pewnej liczby $m > 0$ zachodzi równość $\phi(m) = a_0$, albo też dla wszystkich $m > 0$ mamy $\phi(m) \neq a_0$. Najpierw zajmiemy się drugim przypadkiem.

Krok 7. Jeżeli $\phi(m) \neq a_0$ dla wszystkich liczb naturalnych m , to funkcja ϕ jest różnowartościowa. Aby się o tym przekonać założmy, że jest przeciwnie, a więc, że $\phi(m_1) = \phi(m_2)$ dla pewnych m_1 i $m_2 > m_1$. Jeżeli $m_1 < 0$, to

$$a_0 = s^{-m_1}(\phi(m_1)) = s^{-m_1}(\phi(m_2)) = s^{-m_1}(s^{m_2}(a_0)) = \phi(m_2 - m_1),$$

a to nie jest możliwe w rozważanym przypadku. Jeżeli natomiast $m_1 \geq 0$, to

$$s^{m_1}(a_0) = \phi(m_1) = \phi(m_2) = s^{m_1}(\phi(m_2 - m_1))$$

i z różnowartościowości s^{m_1} otrzymujemy, że $a_0 = \phi(m_2 - m_1)$. To też w rozważanym przypadku nie może zachodzić.

Zauważmy jeszcze, że

$$(s\phi)(n) = s(\phi(n)) = s(s^n(a_0)) = s^{n+1}(a_0) = \phi(n+1) = \phi(S(n)) = (\phi S)(n).$$

Tak więc $s\phi = \phi S$. W kroku 1 jest pokazane, że S jest złożeniem inwolucji. Wobec tego, z własności podanej w kroku 5 otrzymujemy, że s jest złożeniem inwolucji na zbiorze A_0 .

Krok 8. Jeżeli $\phi(m) = a_0$ dla pewnej liczby naturalnej $m > 1$, to bierzemy najmniejszą liczbę m_0 o tej własności. Następnie pokazujemy, że funkcja ϕ przekształca różnowartościowo zbiór $\{x \in \mathbb{N} \mid x < m_0\}$ na klasę abstrakcji A_0 . Fakt ten pozwala powtórzyć rozumowanie z kroku 7. Tym razem korzystamy z rozkładu na inwolucje funkcji S_{m_0} , opisanego w kroku 2. ■

Zadanie 526. Przypuśćmy, że $f : X \rightarrow Y$, $A \subseteq X$ oraz $B \subseteq Y$. Udowodnij, że

$$f(A \cap f^{-1}(B)) = f(A) \cap B$$

Rozwiązanie. Pokażemy, że

$$y \in f(A \cap f^{-1}(B)) \Leftrightarrow y \in f(A) \cap B$$

dla dowolnego y . Stąd i z zasady ekstensjonalności wynika dowodzona równość. Aby dowieść podaną równoważność zauważmy, że następujące formuły są równoważne:

1. $y \in f(A \cap f^{-1}(B))$,
2. $\exists x(x \in A \cap f^{-1}(B) \wedge f(x) = y)$,
3. $\exists x(x \in A \wedge x \in f^{-1}(B) \wedge f(x) = y)$,
4. $\exists x(x \in A \wedge f(x) \in B \wedge f(x) = y)$,
5. $\exists x(x \in A \wedge f(x) = y \wedge y \in B)$,
6. $(\exists x(x \in A \wedge f(x) = y)) \wedge y \in B$,
7. $y \in f(A) \wedge y \in B$,
8. $y \in f(A) \cap B$.

Rozwiązanie (inny sposób). Najpierw udowodnimy zawieranie $f(A \cap f^{-1}(B)) \subseteq f(A) \cap B$. Przypuśćmy, że $y \in f(A \cap f^{-1}(B))$. Istnieje więc $x \in A \cap f^{-1}(B)$ taki, że $f(x) = y$. Ten istniejący x oznaczmy symbolem x_0 . Mamy więc $x_0 \in A \cap f^{-1}(B)$ oraz $f(x_0) = y$. Oczywiście, element x_0 ma dwie własności: $x_0 \in A$ oraz $f(x_0) = y$. Istnieje więc taki x , że $x \in A$ oraz $f(x) = y$. Stąd wynika, że $y \in f(A)$.

Element x_0 należy także do $f^{-1}(B)$. Jeżeli skorzystamy z definicji przeciwobrazu, to otrzymamy, że $y = f(x_0) \in B$. Rozważany y należy więc do $f(A)$ i do B , czyli $y \in f(A) \cap B$. To kończy dowód interesującego nas zawierania.

Udowodnimy jeszcze zawieranie przeciwne, czyli $f(A) \cap B \subseteq f(A \cap f^{-1}(B))$. W tym celu weźmy $y \in f(A) \cap B$. Taki y należy do $f(A)$, a więc istnieje $x \in A$ takie, że $f(x) = y$. Jeden z tych elementów oznaczmy symbolem x_0 . Mamy więc, że $x_0 \in A$ oraz $f(x_0) = y$. Ponieważ $y \in B$, więc także $f(x_0) \in B$. Ta ostatnia własność implikuje, że $x_0 \in f^{-1}(B)$. Element x_0 jest jednym z takich x , dla których $x \in A$, $x \in f^{-1}(B)$ oraz $f(x) = y$. Istnieje więc x takie, że $x \in A \cap f^{-1}(B)$ oraz $f(x) = y$. Stąd i z definicji pojęcia obrazu wynika, że $y \in f(A \cap f^{-1}(B))$ i tym samym zostało wykazane dowodzone zawieranie.

Interesująca nas równość wynika z udowodnionych zawierania i zasady ekstensjonalności.

Rozwiązanie (inny dowód jednego z zawierania). Skorzystamy teraz z dwóch własności pojęcia obrazu: monotoniczności

$$\text{jeśli } C \subseteq D \text{ to } f(C) \subseteq f(D)$$

oraz zawierania

$$f(f^{-1}(B)) \subseteq B,$$

a także z dwóch znanych własności przekroju:

$$\text{jeśli } E \subseteq C \text{ i } E \subseteq D \text{ to } E \subseteq C \cap D$$

i

$$C \cap D \subseteq C \text{ oraz } C \cap D \subseteq D.$$

Z podanych własności wynika, że

$$f(A \cap f^{-1}(B)) \subseteq f(A),$$

$$f(A \cap f^{-1}(B)) \subseteq f(f^{-1}(B)) \subseteq B,$$

i — w konsekwencji —

$$f(A \cap f^{-1}(B)) \subseteq f(A) \cap B.$$

Zadanie 527. Udowodnij, że na to, by relacja R była:

1. zwrotna, potrzeba i wystarcza, by $I \subseteq R$, gdzie I jest relacją identyczności;
2. symetryczna, potrzeba i wystarcza, by $R^{-1} = R$;
3. przechodnia, potrzeba i wystarcza, by $RR \subseteq R$;
4. relacją równoważności, potrzeba i wystarcza, by $I \subseteq R \wedge R^{-1} = R \wedge RR \subseteq R$.

Rozwiązanie. Jest to bardzo proste zadanie, tak proste, że chciałoby się napisać tylko, że jest oczywiste. Warunki $I \subseteq R$ i $RR \subseteq R$ są niemal identyczne odpowiednio z warunkami z definicji zwrotności i symetryczności relacji R . Z tego powodu przedstawiony dowód może będzie zbyt szczegółowy. Weźmy zbiór X i relację $R \subseteq X \times X$.

Część 1. Pokażemy, że R jest relacją zwrotną w zbiorze X wtedy i tylko wtedy, gdy $I \subseteq R$. Dowód równoważności składa się oczywiście z dowodu dwóch implikacji.

Najpierw założmy, że R jest relacją zwrotną w zbiorze X . Aby dowieść, że $I \subseteq R$, weźmy dowolny element $p \in I$. Oczywiście, p jest parą uporządkowaną (ponieważ I jest relacją), obie współrzędne p należą do X (gdyż I jest relacją w zbiorze X) i są sobie równe (dlatego, że I jest relacją identyczności). Tak więc $p = \langle x, x \rangle$ dla pewnego $x \in X$. Ponieważ R jest zwrotna, więc $p = \langle x, x \rangle \in R$. W ten sposób dowód zawierania $I \subseteq R$ został zakończony.

Aby dowieść zwrotność relacji R , wystarczy dla dowolnego elementu $x \in X$ pokazać, że para $\langle x, x \rangle$ należy do R . Oczywiście, $\langle x, x \rangle \in I$ na podstawie definicji relacji identycznościowej. Stąd i z zawierania $I \subseteq R$ otrzymujemy, że $\langle x, x \rangle \in R$.

Część 2. Teraz pokażemy, że relacja R jest symetryczna wtedy i tylko wtedy, gdy $R^{-1} = R$. Podobnie jak w części 1 udowodnimy dwie implikacje.

Jeżeli relacja R jest symetryczna, to dowolna para $\langle x, y \rangle$ z relacji R (a właściwie dowolny element relacji R) należy także do relacji R^{-1} . Tak jest, ponieważ z warunku $\langle x, y \rangle \in R$ wynika, że $\langle y, x \rangle \in R$, a to z kolei oznacza, że $\langle x, y \rangle \in R^{-1}$. Przedstawione rozumowanie świadczy o tym, że symetryczna relacja R spełnia warunek $R \subseteq R^{-1}$. Podobnie dowodzimy zawieranie odwrotne: jeżeli $\langle x, y \rangle \in R^{-1}$, to korzystając z definicji relacji odwrotnej otrzymujemy, że $\langle y, x \rangle \in R$, a jeżeli skorzystamy jeszcze z symetryczności R , to otrzymamy, że $\langle x, y \rangle \in R$. Dla relacji symetrycznej prawdziwe są więc dwa zawierania: $R \subseteq R^{-1}$ i $R^{-1} \subseteq R$. Wobec tego, prawdziwa jest też równość $R = R^{-1}$.

W drugą stronę, relacja spełniająca warunek $R = R^{-1}$ spełnia także zawieranie $R \subseteq R^{-1}$. To zawieranie oznacza, że R jest relacją symetryczną. Jeżeli bowiem $\langle x, y \rangle \in R$, to na podstawie tego zawierania mamy, że $\langle y, x \rangle \in R^{-1}$. Jeżeli teraz skorzystamy z definicji relacji odwrotnej, to otrzymamy, że $\langle y, x \rangle \in R$.

Część 3. Pokażemy jeszcze, że przechodność relacji R jest równoważna zawieraniu $RR \subseteq R$.

Założmy, że R jest relacją przechodnią i $\langle x, y \rangle \in RR$. Z definicji złożenia relacji wynika, że istnieje z taki, że $\langle x, z \rangle \in R$ i $\langle z, y \rangle \in R$. Jeden z takich z oznaczmy symbolem z_0 . Element z_0 ma więc dwie własności: $\langle x, z_0 \rangle \in R$ oraz $\langle z_0, y \rangle \in R$. Z przechodności relacji R otrzymujemy, że $\langle x, y \rangle \in R$. Kończy to dowód zawierania $RR \subseteq R$.

Jeżeli $RR \subseteq R$, to relacja R jest przechodnia. Aby się o tym przekonać weźmy x, y i z takie, że $\langle x, y \rangle \in R$ i $\langle y, z \rangle \in R$. Z definicji złożenia relacji wynika, że $\langle x, z \rangle \in RR$. Założone zawieranie implikuje więc, że $\langle x, z \rangle \in R$, i to kończy dowód przechodności relacji R .

Część 4. Z części 1, 2 i 3 wynika równoważność z części 4. Aby się o tym przekonać, wystarczy zauważyć, że jeżeli zdania ϕ_i są równoważne zdaniom ψ_i dla $i = 1, 2, 3$, to koniunkcja $\phi_1 \wedge \phi_2 \wedge \phi_3$ jest równoważna koniunkcji $\psi_1 \wedge \psi_2 \wedge \psi_3$. ■

Zadanie 528. Niech f będzie bijekcją przekształcającą zbiór A w A . Zdefiniujmy relację $R \subseteq A^2$ przyjmując, że

$$xRy \Leftrightarrow f(x) = y.$$

Symbolem R_∞ oznaczamy przechodnie domknięcie relacji R , czyli relację $\bigcup_{n=1}^{\infty} R^n$, gdzie $R^1 = R$ oraz $R^{n+1} = R^n R$. Czy

1. R_∞ jest relacją równoważności?
2. R_∞ jest relacją równoważności, jeśli A jest zbiorem skończonym?

Rozwiązanie. *Część 1.* Najpierw zauważmy, że jeżeli funkcję f będziemy traktować jak relację, to warunek $f(x) = y$ będzie równoważny z $\langle x, y \rangle \in f$. Tak więc relacja R jest tożsama z funkcją f . Wobec tego, relacja R^n jest niczym innym, jak n -krotnym złożeniem funkcji f .

Na ogół przechodnie domknięcie relacji R zdefiniowanej w zadaniu nie jest relacją równoważności. Tak jest np. dla zbioru liczb całkowitych $\mathbb{Z}$ i funkcji $f : \mathbb{Z} \rightarrow \mathbb{Z}$ zdefiniowanej wzorem $f(k) = k + 1$. Funkcja f jest oczywiście bijekcją. Dla dowolnego $n \in \mathbb{N}$ relacja R^n spełnia dla wszystkich $x, y \in \mathbb{Z}$ równoważność

$$xR^n y \Leftrightarrow y = x + n.$$

Jeżeli przedstawione argumenty nie implikują tej równoważności w sposób oczywisty, to proponuję sprawdzenie jej przez indukcję ze względu na n .

Dla tej funkcji f relacja R_∞ nie jest zwrotna, a nawet jest antyzwrotna. Dla wszystkich $x \in \mathbb{Z}$, założenie $xR_\infty x$ można sprowadzić do sprzeczności w następujący sposób: warunek $xR_\infty x$ oznacza, że $\langle x, x \rangle \in \bigcup_{n=1}^{\infty} R^n$. Tak więc dla pewnej

liczby $m > 0$ mamy $\langle x, x \rangle \in R^m$, czyli $x R^m x$. Z podanej charakteryzacji relacji R^m wynika, że $x = x + m$. Jest to możliwe tylko, gdy $m = 0$. Przeczy to jednak warunkowi $m > 0$.

Jeżeli R_∞ nie jest zwrotna, to nie jest relacją równoważności. Można też dowieść w podobny sposób, że R_∞ nie jest też symetryczna.

Część 2. Założenie o skończoności zbioru A implikuje, że R_∞ jest relacją równoważności. Dla dowolnego $x \in A$, rozważamy funkcję $I : \mathbb{N} \rightarrow A$ taką, że $I(n) = f^n(x)$ dla wszystkich $n \in \mathbb{N}$ ($I(n)$ to wartość n -krotnego złożenia funkcji f dla argumentu x , $f^0(x) = x$). Gdyby funkcja I była różnowartościowa, to zbiór A byłby nieskończony. Dla skończonego zbioru A funkcja I nie jest różnowartościowa. Tak więc możemy znaleźć dwie liczby naturalne p i q , takie, że $p < q$ oraz $f^p(x) = I(p) = I(q) = f^q(x)$. Składanie funkcji jest operacją łączną i zachowuje różnowartościowość. Wobec tego, $f^p(x) = f^q(x) = f^p(f^{q-p}(x))$. Różnowartościowość funkcji f^p implikuje także równość $f^{p-q}(x) = x$. Udowodniliśmy więc, że jeżeli A jest zbiorem skończonym, to dla dowolnego $x \in A$ istnieje liczba dodatnia r taka, że

$$f^r(x) = x. \quad (1)$$

Udowodniona własność oznacza, że relacja R_∞ jest zwrotna. Aby się o tym przekonać, bierzemy $x \in A$ i liczbę $r > 0$ spełniającą (1). Z równości (1) wynika, że $\langle x, x \rangle \in f^r = R^r$. Zawieranie $R^r \subseteq R_\infty$ implikuje zaś, że $\langle x, x \rangle \in R_\infty$.

Równość (1) implikuje także, że jeżeli iterujemy obliczanie wartości funkcji f zaczynając od argumentu x , to otrzymujemy w kółko te same wartości

$$f(x), f^2(x), \dots, f^r(x) = x, f(x), f^2(x), \dots, f^r(x) = x, f(x), \dots$$

Spostrzeżenie to pozwala dowieść symetryczność relacji R_∞ . Najpierw jednak zauważmy, że równość (1) zachodzi także dla wszystkich wielokrotności r . Świadczą o tym następujące obliczenia będące fragmentem dowodu indukcyjnego:

$$f^{(k+1)r}(x) = f^{kr}(f^r(x)) = f^{kr}(x) = x.$$

Teraz możemy przystąpić do dowodu, że relacja R_∞ jest symetryczna. Przypuścimy, że $\langle x, y \rangle \in R_\infty$. Na podstawie definicji R_∞ stwierdzamy, że $\langle x, y \rangle \in R^n$ dla pewnej dodatniej liczby naturalnej n . Ponieważ relacja R^n jest równa f^n , więc $f^n(x) = y$. Weźmy liczbę naturalną k taką, że $n < kr$. Dla tej liczby k mamy $kr - n > 0$ oraz

$$f^{kr-n}(y) = f^{kr-n}(f^n(x)) = f^{kr}(x) = x.$$

Udowodniona równość oznacza, że

$$\langle y, x \rangle \in f^{kr-n} = R^{kr-n} \subseteq R_\infty.$$

Przechodniość relacji R_∞ wynika z zadania 203.

Z przedstawionych rozumowań otrzymujemy, że jeżeli zbiór A jest skończony, to relacja R_∞ jest zwrotna i symetryczna. Wiemy też, że jest przechodnia. Tak więc dla zbioru skończonego A , relacją R_∞ jest równoważność. ■

Zadanie 529. Przypuśćmy, że V jest skończonym zbiorem zmiennych zdaniowych, $R \subseteq V^2$ jest przechodnią relacją w zbiorze V , a $p_0, q_0 \in V$ są dwiema różnymi zmiennymi zdaniowymi. Niech Φ będzie formułą zdaniową

$$p_0 \wedge \neg q_0 \wedge \bigwedge_{(p,q) \in R} (p \Rightarrow q).$$

Pokaż, że formuła Φ jest sprzeczna wtedy i tylko wtedy, gdy $(p_0, q_0) \in R$.

Rozwiązanie. Najpierw udowodnimy, że jeżeli $(p_0, q_0) \notin R$, to formuła Φ jest spełnialna. Zrobimy to definiując wartościowanie spełniające Φ .

Zauważmy, że chcemy zdefiniować wartościowanie, przy którym będzie prawdziwa formuła p_0 , będą prawdziwe wszystkie implikacje $p \Rightarrow q$ takie, że $(p, q) \in R$, i — w konsekwencji — będą prawdziwe wszystkie zmienne q takie, że $(p_0, q) \in R$, oraz możliwie dużo zmiennych będzie fałszywych, gdyż q_0 powinna być fałszywa. Weźmy więc wartościowanie w , przy którym prawdziwa jest zmienna p_0 oraz wszystkie zmienne q takie, że $(p_0, q) \in R$, a pozostałe zmienne są fałszywe.

Pokażemy, że przy wartościowaniu w koniunkcja Φ jest prawdziwa. W tym celu wystarczy pokazać, że wszystkie jej człony są prawdziwe.

Oczywiście, pierwszy człon (p_0) jest prawdziwy przy wartościowaniu w . Ponieważ $q_0 \neq p_0$ i $(p_0, q_0) \notin R$, więc zmienna q_0 jest fałszywa przy wartościowaniu w , a drugi człon formuły Φ (negacja q_0) jest prawdziwy.

Pozostałe człony koniunkcji Φ są postaci $p \Rightarrow q$ dla zmiennych p i q takich, że $(p, q) \in R$. Weźmy więc p i q takie, że $(p, q) \in R$. Jeżeli zmienna p jest fałszywa przy wartościowaniu w , to implikacja $p \Rightarrow q$ jest przy tym wartościowaniu prawdziwa.

Przypuśćmy więc, że zmienna p jest prawdziwa przy wartościowaniu w . Wtedy są możliwe dwa przypadki: albo $p = p_0$, albo $(p_0, p) \in R$. W każdym przypadku (w drugim z przechodniości R) mamy, że $(p_0, q) \in R$. Tak więc zmienna q oraz implikacja $p \Rightarrow q$ są prawdziwe przy wartościowaniu w . W ten sposób dowiedliśmy spełnialności formuły Φ .

Udowodnimy jeszcze metodą nie wprost, że jeżeli $(p_0, q_0) \in R$, to formuła Φ jest sprzeczna. Załóżmy więc, że koniunkcja Φ jest prawdziwa przy pewnym wartościowaniu. Przy tym wartościowaniu są prawdziwe wszystkie człony Φ , a więc m.in. formuły p_0 , $\neg q_0$ oraz — na mocy założenia $(p_0, q_0) \in R$ — implikacja $p_0 \Rightarrow q_0$. Oczywiście, nie jest to możliwe, gdyż implikacja $p_0 \Rightarrow q_0$ jest fałszywa przy każdym wartościowaniu, przy którym formuły p_0 i $\neg q_0$ są prawdziwe. ■

Zadanie 530. Na zbiorze X określone są takie relacje równoważności Q i R , że

1. każda klasa równoważności relacji Q ma q elementów,
2. każda klasa relacji R ma r elementów oraz
3. istnieje klasa równoważności relacji Q , która ma dokładnie jeden element wspólny z każdą klasą równoważności relacji R .

Ile elementów ma zbiór X ?

Rozwiązanie. Przyjmijmy, że A oznacza tę klasę równoważności relacji Q , o której jest mowa w punkcie 3), a K — zbiór klas równoważności relacji R .

Wszystkie przedstawione rozwiązania korzystają z faktu, że zbiory K i A mają tyle samo elementów. Jeżeli to wiemy, to na podstawie warunku 1) stwierdzamy, że K ma q elementów. Relacja równoważności R wyznacza więc podział zbioru X na q rozłącznych klas równoważności, które mają po r elementów. Stąd otrzymujemy, że X ma $q \cdot r$ elementów. Dalej pokażę, jak dowodzić, że $|A| = |K|$.

Sposób 1. Niech $f : K \rightarrow A$ będzie funkcją, która dla klasy $Y \in K$ przyjmuje wartość $f(Y) \in Y \cap A$. Punkt 3) ze sformułowania zadania gwarantuje poprawność tej definicji.

Pokażemy, że funkcja f jest bijekcją. Jeżeli $f(Y) = f(Z)$ dla pewnych klas $Y, Z \in K$, to $f(Y) \in (Y \cap A) \cap (Z \cap A) \subseteq Y \cap Z$. W tym przypadku klasy Y i Z nie są rozłączne, a to jest możliwe tylko wtedy, gdy $Y = Z$. Wobec tego f jest różnowartościowa.

Weźmy teraz $a \in A$. Oczywiście, klasa równoważności $[a]_R$ należy do K . Gdyby $f([a]_R) \neq a$, to zbiór $[a]_R \cap A$ miałby przynajmniej dwa elementy: $f([a]_R)$ oraz a , a to przeczy warunkowi 3). Tak więc funkcja f jest typu „na”.

Sposób 2. Tym razem definiujemy funkcję $g : A \rightarrow K$, która elementowi $a \in A$ przyporządkowuje klasę $[a]_R$ (przyjmujemy, że $g(a) = [a]_R$). Podobnie jak w pierwszym rozwiązaniu, funkcja g jest bijekcją.

Jeżeli $[a]_R = [b]_R$ dla $a, b \in A$, to do klasy $[a]_R$ należy zarówno a , jak i b . Z wyboru A mamy jednak, że do dowolnej klasy równoważności może należeć tylko jeden element zbioru A , więc $a = b$.

Jeżeli Y jest dowolną klasą równoważności relacji R , to z warunku 3) (a raczej z wyboru A) znajdujemy w niej pewien element $a \in A$. Wobec tego, klasy równoważności $[a]_R$ i Y nie są rozłączne. Takie klasy muszą być równe. Otrzymaliśmy więc, że $g(a) = [a]_R = Y$.

Sposób 3. Zauważmy, że

$$A = A \cap X = A \cap \bigcup_{Y \in K} Y = \bigcup_{Y \in K} A \cap Y$$

(druga równość wynika stąd, że suma klas równoważności jest równa dziedzinie relacji równoważności). Zbiory $A \cap Y_1$ i $A \cap Y_2$ dla różnych klas równoważności Y_1 i Y_2 są rozłączne, ponieważ klasy te są rozłączne. Wobec tego

$$|A| = \left| \bigcup_{Y \in K} A \cap Y \right| = \sum_{Y \in K} |A \cap Y| = \sum_{Y \in K} 1 = |K|.$$

■

Zadanie 531. Niech A, B będą dowolnymi zbiorami. Kiedy równanie

$$A \cup X = B$$

1. ma dokładnie jedno rozwiązanie,
2. ma nieskończenie wiele rozwiązań,
3. nie ma rozwiązań?

Rozwiązanie. Jeżeli równanie $A \cup X = B$ ma rozwiązanie, to jest taki zbiór C , że $A \cup C = B$. Wtedy oczywiście zbiór A jest podzbiorem B . Także na odwrót, jeżeli $A \subseteq B$, to zbiór $X = B \setminus A$ spełnia równanie $A \cup X = B$.

Udowodniliśmy więc, że równanie $A \cup X = B$ ma rozwiązanie wtedy i tylko wtedy, gdy $A \subseteq B$. Tym samym odpowiedzieliśmy na pytanie 3: równanie $A \cup X = B$ nie ma rozwiązania wtedy i tylko wtedy, gdy $A \not\subseteq B$.

Żałujemy, że $A \subseteq B$. Scharakteryzujemy rozwiązania równania $A \cup X = B$. Warunek $A \cup C = B$ implikuje, że C jest podzbiorem B oraz zawiera różnicę $B \setminus A$. Prawdziwa jest także implikacja odwrotna: jeżeli $B \setminus A \subseteq C \subseteq B$, to

$$B = A \cup (B \setminus A) \subseteq A \cup C \subseteq A \cup B = B,$$

a więc C spełnia równanie $A \cup X = B$. Tak więc zbiorem rozwiązań równania $A \cup X = B$ jest

$$\{X : B \setminus A \subseteq X \subseteq B\}.$$

Policzymy jeszcze liczbę elementów tego zbioru, albo jego moc. W tym celu definiujemy funkcję f określoną w zbiorze $\mathcal{P}(A)$ wszystkich podzbiorów zbioru A i przyjmującą wartości dane wzorem

$$f(Y) = Y \cup (B \setminus A).$$

Łatwo dowodzi się, że funkcja f przekształca $\mathcal{P}(A)$ na zbiór rozwiązań równania $A \cup X = B$. Co więcej, jest to funkcja różnowartościowa. Jeżeli bowiem $f(Y_1) = f(Y_2)$ dla pewnych $Y_1, Y_2 \in \mathcal{P}(A)$, to

$$Y_1 = (Y_1 \cup (B \setminus A)) \cap A = f(Y_1) \cap A = f(Y_2) \cap A = (Y_2 \cup (B \setminus A)) \cap A = Y_2.$$

Tak więc funkcja f ustala równoliczność zbioru $\mathcal{P}(A)$ i zbioru rozwiązań równania $A \cup X = B$. Oznacza to, że równanie $A \cup X = B$ ma tyle elementów, co zbiór $\mathcal{P}(A)$ (albo zbiór rozwiązań równania $A \cup X = B$ jest tej samej mocy, co zbiór $\mathcal{P}(A)$).

Teraz łatwo odpowiedzieć na pytania 1 i 2. Jeżeli A jest niepusty to ma przynajmniej dwa podzbiory: zbiór pusty i samego siebie. Tak więc równanie $A \cup X = B$ ma dokładnie jedno rozwiązanie wtedy i tylko wtedy, gdy A jest zbiorem pustym.

Zbiory skończone mają skończenie wiele podzbiorów, a nieskończone — nieskończenie wiele. Wobec tego, równanie $A \cup X = B$ ma nieskończenie wiele rozwiązań wtedy i tylko wtedy, gdy A jest zbiorem nieskończonym. ■

Zadanie 532. Niech $\alpha : \mathbb{N} \rightarrow \{0, 1\}$ będzie ciągiem zerowyjedyńkowym. Symbolem $\sim_\alpha$ oznaczamy relację w zbiorze $\{0, 1\}^{\mathbb{N}}$ nieskończonych ciągów zerowyjedyńkowych zdefiniowaną formułą

$$\beta \sim_\alpha \gamma \iff \forall n \in \mathbb{N} (\alpha(n)\beta(n) = \alpha(n)\gamma(n)).$$

Czy istnieje taki ciąg α , dla którego:

- relacja $\sim_\alpha$ ma przeliczalnie i nieskończenie wiele klas równoważności?
- wszystkie klasy równoważności relacji $\sim_\alpha$ są przeliczalne i nieskończone?
- istnieje przeliczalna i nieskończona klasa równoważności relacji $\sim_\alpha$?

Rozwiązanie. Ustalmy α i przyjmijmy, że $A = \{n \in \mathbb{N} \mid \alpha(n) = 1\}$. Oczywiście, $\sim_\alpha$ jest relacją równoważności. Przyjmijmy, że N_α jest zbiorem klas równoważności tej relacji. Symbolem $[x]_\alpha$ będziemy oznaczać klasy abstrakcji relacji $\sim_\alpha$.

Fakt 196. Zbiór N_α i zbiór $\{0, 1\}^A$ są równoliczne.

Dowód. Dla funkcji $\xi : A \rightarrow \{0, 1\}$ definiujemy funkcję $\bar{\xi} : \mathbb{N} \rightarrow \{0, 1\}$ przyjmując, że

$$\bar{\xi}(n) = \begin{cases} \xi(n), & \text{jeżeli } n \in A, \\ 0, & \text{w przeciwnym razie.} \end{cases}$$

Zdefiniujmy jeszcze wzorem

$$f(\xi) = [\bar{\xi}]_\alpha$$

funkcję $f : \{0, 1\}^A \rightarrow N_\alpha$. Funkcja ta jest różnowartościowa i typu „na”.

Aby dowieść różnowartościowość funkcji f weźmy dwa (różne) argumenty ξ_1 i ξ_2 tej funkcji. Są to funkcje określone w zbiorze A . Istnieje więc liczba $n \in A$ taka, że $\xi_1(n) \neq \xi_2(n)$. Funkcje $\bar{\xi}_1$ i $\bar{\xi}_2$ też przyjmują różne wartości dla argumentu n :

$$\bar{\xi}_1(n) = \xi_1(n) \neq \xi_2(n) = \bar{\xi}_2(n).$$

Oznacza to, że $\bar{\xi}_1 \not\sim_\alpha \bar{\xi}_2$. Stąd otrzymujemy, że klasy $[\bar{\xi}_1]_\alpha$ i $[\bar{\xi}_2]_\alpha$ są różne (różnią się np. elementem $\bar{\xi}_1$).

Weźmy dowolną klasę ze zbioru N_α i jej reprezentanta γ . Pokażemy, że $[\gamma]_\alpha$ jest wartością funkcji f . W tym celu weźmy funkcję $\delta : A \rightarrow \{0, 1\}$ będącą obcięciem γ do zbioru A (a więc spełniającą $\delta(n) = \gamma(n)$ dla wszystkich $n \in A$) i zauważmy, że także $\bar{\delta}(n) = \gamma(n)$ dla wszystkich $n \in A$. To jednak oznacza, że $\bar{\delta} \sim_\alpha \gamma$. Wobec tego, $f(\delta) = [\bar{\delta}]_\alpha = [\gamma]_\alpha$.

Dowód (inny sposób). Weźmy funkcję $g : \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^A$ przyporządkowującą funkcji $\gamma \in \{0, 1\}^{\mathbb{N}}$ obcięcie funkcji γ do zbioru A . Oczywiście, funkcja g jest typu „na”. Świadczy o tym np. równość $g(\bar{\xi}) = \bar{\xi}$.

Funkcja g spełnia także równoważność

$$g(\gamma_1) = g(\gamma_2) \Leftrightarrow \gamma_1 \sim_\alpha \gamma_2.$$

Równoważność ta implikuje, że wzór

$$G([\gamma]_\alpha) = g(\gamma)$$

jest poprawną definicją funkcji $G : N_\alpha \rightarrow \{0, 1\}^A$ i – co więcej – funkcja ta jest różnowartościowa. Ponieważ g jest typu „na”, więc także G jest typu „na”.

Fakt 197. Klasy równoważności relacji $\sim_\alpha$ są równoliczne ze zbiorem $\{0, 1\}^{\mathbb{N} \setminus A}$.

Dowód. Weźmy dowolną funkcję $\beta \in \{0, 1\}^{\mathbb{N}}$ i zdefiniujmy funkcję $f : [\beta]_\alpha \rightarrow \{0, 1\}^{\mathbb{N} \setminus A}$. Funkcja f elementowi $\gamma \in [\beta]_\alpha$ przyporządkowuje obcięcie γ do zbioru $\mathbb{N} \setminus A$. Aby dowieść podany fakt pokażemy, że funkcja f jest bijekcją.

Weźmy więc różne funkcje $\gamma_1, \gamma_2 \in [\beta]_\alpha$. Ponieważ należą do jednej klasy równoważności relacji $\sim_\alpha$, więc przyjmują te same wartości dla dowolnego argumentu ze zbioru A . Wobec tego, przyjmują różne wartości dla pewnego $n \notin A$. Ich obcęcia od zbioru $\mathbb{N} \setminus A$ też przyjmują różne wartości dla tego samego argumentu, a więc są różne. To dowodzi, że funkcja f jest różnowartościowa.

Aby dowieść, że funkcja f jest typu „na”, weźmy dowolną funkcję $\xi \in \{0, 1\}^{\mathbb{N} \setminus A}$ i zdefiniujmy $\gamma \in \{0, 1\}^{\mathbb{N}}$ takie, że

$$\gamma(n) = \begin{cases} \beta(n), & \text{jeżeli } n \in A, \\ \xi(n), & \text{w przeciwnym razie.} \end{cases}$$

Oczywiście, funkcje γ i β są w relacji $\sim_\alpha$ oraz obcięcie γ do $\mathbb{N} \setminus A$ jest równe ξ . Tak więc $f(\gamma) = \xi$.

Fakt 198. Jeżeli zbiór $A \subseteq \mathbb{N}$ jest nieskończony, to zbiór $\{0, 1\}^A$ jest nieprzeliczalny.

Dowód. Nieskończony podzbiór A zbioru liczb naturalnych jest równoliczny ze zbiorem liczb naturalnych $\mathbb{N}$. Jeżeli zbiór A jest równoliczny z $\mathbb{N}$, to także zbiory $\{0, 1\}^A$ i $\{0, 1\}^{\mathbb{N}}$ są równoliczne. Ten ostatni zbiór jest nieprzeliczalny na podstawie twierdzenia Cantora. Oznacza to, że także zbiór $\{0, 1\}^A$ jest nieprzeliczalny.

Wniosek. Zbiór N_α klas równoważności relacji $\sim_\alpha$ jest albo skończony, albo nieprzeliczalny.

Dowód. Są możliwe dwa przypadki: albo zbiór A jest skończony i wtedy zbiór $\{0, 1\}^A$ i równoliczny z nim zbiór N_α są skończone, albo zbiór A jest nieskończony i zarówno zbiór $\{0, 1\}^A$ jak i równoliczny z nim zbiór N_α są nieprzeliczalne.

Z powyższego wniosku wynika negatywna odpowiedź na pytanie a): dla żadnego α zbiór klas równoważności relacji $\sim_\alpha$ nie jest przeliczalny i nieskończony.

Wniosek. Klasy abstrakcji relacji $\sim_\alpha$ są albo skończone, albo nieprzeliczalne.

Dowód. Ten wniosek dowodzimy dokładnie tak, jak poprzedni.

Z ostatniego wniosku otrzymujemy negatywną odpowiedź na pytanie c): dla żadnego α żadna klasa równoważności nie jest nieskończona przeliczalna.

Negatywna odpowiedź na pytanie c) implikuje także negatywną odpowiedź na pytanie b). Odpowiedź na pytanie b) można też łatwo wyprowadzić z ostatniego wniosku. ■

Zadanie 533. Niech $f : \mathbb{R} \rightarrow \mathbb{R}$. Mówimy, że $x \in \mathbb{R}$ jest lokalnym maksimum funkcji f , jeżeli istnieje taka dodatnia liczba rzeczywista r , że dla każdego $y \in \mathbb{R}$

$$(x - r < y < x + r \wedge x \neq y) \Rightarrow f(x) > f(y)$$

Udowodnij, że dla każdej funkcji $f : \mathbb{R} \rightarrow \mathbb{R}$ zbiór jej lokalnych maksimów jest przeliczalny.

Rozwiązanie. Nie należy ulec pokusie i próbować udowodnić powyższe twierdzenie w następujący, niesłuszny sposób:

Dowód (fałszywy!). Z każdym z maksimów lokalnych x związujemy taki przedział zawierający x , że dla każdej liczby z tego przedziału z wyjątkiem x funkcja f przyjmuje wartości mniejsze niż $f(x)$ (taki przedział istnieje na mocy definicji). Z każdego takiego przedziału wybieramy liczbę wymierną. Zbudowaliśmy więc odwzorowanie przekształcające zbiór maksimów funkcji w zbiór liczb wymiernych, który jest przeliczalny.

Niestety nie zadbałszy o to, by odwzorowanie powyższe było różnowartościowe! Jednym z warunków, który by to zagwarantował, jest wymaganie, by przedziały otaczające maksima były rozłączne. Nie zawsze jednak takie przedziały da się wybrać. Podam przykłady funkcji, dla których nie można skonstruować takiej rodziny pami rozłącznych przedziałów zawierających wszystkie maksima lokalne, że w każdym przedziale jest najwyżej jedno maksimum.

Rozważmy funkcję $f_1 : \mathbb{R} \rightarrow \mathbb{R}$ zdefiniowaną wzorem

$$f_1(x) = \begin{cases} \sin\left(\frac{1}{x}\right), & \text{dla } x \neq 0, \\ 2, & \text{dla } x = 0. \end{cases}$$

Łatwo sprawdzić, że funkcja f_1 przyjmuje maksimum lokalne dla $x = 0$ i dla wszystkich $x = \frac{1}{2k\pi}$ dla $k \in \mathbb{Z}$.

Podobnie jest w przypadku funkcji f_2 zdefiniowanej wzorem

$$f_2(x) = \begin{cases} x^2 \left(\sin\left(\frac{1}{x}\right) - 2 \right), & \text{dla } x \neq 0, \\ 0, & \text{dla } x = 0, \end{cases}$$

która dodatkowo jest ciągła, a nawet różniczkowalna.

Weźmy teraz funkcję $f : \mathbb{R} \rightarrow \mathbb{R}$ przyjmującą wartości

$$f(x) = \begin{cases} \frac{1}{n}, & \text{jeżeli } x = \frac{m}{n}, \text{ gdzie } n \text{ i } m \text{ są liczbami} \\ & \text{względnie pierwszymi i } n > 0, \\ 1, & \text{jeżeli } x = 0, \\ 0, & \text{jeżeli } x \notin \mathbb{Q}. \end{cases}$$

Dla tej funkcji zbiór lokalnych maksimów jest równy zbiorowi liczb wymiernych. Zauważmy od razu ważną własność funkcji f : dla dowolnej dodatniej liczby k i dla dowolnej liczby całkowitej a , funkcja f nie przyjmuje wartości $1/k$ dla argumentów $x \in (a/k, (a+1)/k)$.

Najpierw pokażemy, że $3/7$ jest lokalnym maksimum f . Oczywiście, $f(3/7) = 1/7$. Zauważmy, że w przedziale $(2/7, 4/7)$ funkcja f przyjmuje wartość $1/7$ tylko dla $x = 3/7$. Funkcja f przyjmuje też wartości większe od $1/7$ i są to wartości 1 , $1/2$, $1/3$, $1/4$, $1/5$ i $1/6$. Ale f nie przyjmuje wartości 1 w przedziale $(0, 1)$, nie przyjmuje wartości $1/2$ w przedziale $(0, 1/2)$, nie przyjmuje wartości $1/3$ dla $x \in (1/3, 2/3)$, wartości $1/4$ dla $x \in (1/4, 2/4)$, wartości $1/5$ dla $x \in (2/5, 3/5)$ oraz wartości $1/6$ dla $x \in (2/6, 3/6)$. Zauważmy, że do wszystkich wymienionych przedziałów należy $3/7$. Co więcej, dla argumentów należących do przekroju wymienionych przedziałów (z wyjątkiem $x = 3/7$) funkcja f nie przyjmuje wartości $\geq 1/7$. Przekrojem tym jest $(2/5, 1/2)$. Dla $x \in (2/5, 1/2)$ z wyjątkiem $x = 3/7$ funkcja f przyjmuje wartości mniejsze od $1/7$. Zmniejszając ten przedział można spowodować, że

jego środkiem stanie się punkt $3/7$. Tak więc $3/7$ jest jednym z maksimów lokalnych funkcji f .

Przedstawione rozumowanie można powtórzyć dla każdej z liczb wymiernych. Jeżeli m/n jest nieskracalnym przedstawieniem liczby wymiernej i $n > 0$, to definiujemy

$$a_k = \max \left\{ a \in \mathbb{Z} \mid \frac{a}{k} < \frac{m}{n} \right\}.$$

Oczywiście, $\frac{a_k}{k} < \frac{m}{n} \leq \frac{a_{k+1}}{k+1}$. Jeżeli $0 < k < n$, to także $\frac{m}{n} < \frac{a_{k+1}}{k+1}$, gdyż przedstawienie liczby wymiernej w postaci nieskracalnego ułamka z dodatnim mianownikiem jest jednoznaczne i liczba m/n nie daje się przedstawić w postaci l/k .

Przyjmijmy, że

$$p = \max\{a_1, \dots, a_n\} \text{ oraz } q = \min\{a_1 + 1, \dots, a_{n-1} + 1, a_n + 2\}.$$

Liczby p i q są tak dobrane, że

$$(p, q) = \bigcap_{k=1}^{n-1} (a_k, a_k + 1) \cap (a_n, a_n + 2).$$

Oczywiście, $m/n \in (p, q)$. Ze wspomnianej własności funkcji f otrzymujemy, że na przedziale (p, q) nie przyjmuje ona wartości $> 1/n$ oraz – z wyjątkiem argumentu m/n – nie przyjmuje wartości $1/n$. Wobec tego, na przedziałach $(p, m/n)$ i $(m/n, q)$ funkcja f przyjmuje tylko wartości $< 1/n$. Aby wykazać, że liczba m/n spełnia warunek z definicji maksimum lokalnego wystarczy zastąpić przedział (p, q) mniejszym i symetrycznym względem punktu m/n .

Można konstruować jeszcze bardziej skomplikowane funkcje o interesujących nas własnościach. Prawdopodobnie można dowieść, że dla dowolnego przeliczalnego zbioru $X \subseteq \mathbb{R}$ istnieje funkcja $f : \mathbb{R} \rightarrow \mathbb{R}$, która ma maksima lokalne dokładnie w punktach należących do X .

Dowód (poprawny). Weźmy funkcję $f : \mathbb{R} \rightarrow \mathbb{R}$ i zdefiniujmy zbiór

$$M = \{x \in \mathbb{R} \mid x \text{ jest maksimum lokalnym funkcji } f\}.$$

Aby rozwiązać zadanie wystarczy dowieść, że M jest przeliczalny. Przeliczalność zbioru M wykażemy dowodząc, że istnieje różnowartościowa funkcja

$$g : M \rightarrow \mathbb{Q} \times \mathbb{Q}.$$

Od funkcji g będziemy wymagać, aby dla argumentu $m \in M$ jej wartością była para liczb wymiernych r_1 i r_2 taka, że $r_1 < m < r_2$ i dla wszystkich $x \in \mathbb{R}$ spełniony jest warunek

$$r_1 < x < r_2 \wedge x \neq m \Rightarrow f(x) < f(m).$$

Oczywiście, dla każdego $m \in M$ takie liczby r_1 i r_2 istnieją. Dzięki temu, korzystając z przeliczalności produktu $Q \times Q$ można zdefiniować funkcję g przyjmując, że $g(m)$ jest pierwszą w ustalonej numeracji zbioru $Q \times Q$ parą o podanych własnościach.

Teraz wystarczy dowieść, że funkcja g jest różnowartościowa. Przypuśćmy, że mamy dwa różne elementy $m_1, m_2 \in M$ takie, że $g(m_1) = g(m_2)$. Jeżeli $g(m_1) = (r_1, r_2)$, to $m_1, m_2 \in (r_1, r_2)$ i z podanej własności g możemy wywnioskować dwie nierówności:

$$f(m_2) < f(m_1) \text{ oraz } f(m_1) < f(m_2).$$

Z drugiej strony, te nierówności nie mogą być jednocześnie prawdziwe. Uzyskana w ten sposób sprzeczność dowodzi różnowartościowości funkcji g , a to z kolei implikuje przeliczalność zbioru M . ■

Zadanie 534. Pokaż, że zbiory: liczb wymiernych ze zwykłym porządkiem i skończonych niepustych ciągów liczb wymiernych z porządkiem leksykograficznym generowanym przez zwykły porządek na liczbach wymiernych są izomorficzne. Wsk.: skorzystaj z wyników poprzednich zadań.

Rozwiązanie. W tym zadaniu należy skorzystać z twierdzenia, które mówi, że każde dwa przeliczalne porządki liniowe, które są gęste i bez końców, są izomorficzne (zadanie 373). Aby skorzystać z tego twierdzenia, należy pokazać, że:

1. zbiór skończonych, niepustych ciągów o wyrazach wymiernych jest przeliczalny (zadanie 330),
2. porządek leksykograficzny wyznaczony przez porządek liniowy jest porządkiem liniowym (zadanie 360),
3. porządek leksykograficzny w zbiorze skończonych, niepustych ciągów o wyrazach wymiernych jest gęsty,
4. oraz nie ma w nim elementu największego, ani najmniejszego.

Aby dowieść gęstość rozważanego porządku weźmy dwa skończone, niepuste ciągi a i b liczb wymiernych odpowiednio o wyrazach $a_1, a_2, \dots, a_n$ i $b_1, b_2, \dots, b_m$. Załóżmy, że ciąg a jest mniejszy w sensie porządku leksykograficznego od ciągu b . Są możliwe dwa przypadki: albo $n < m$ oraz $a_i = b_i$ dla wszystkich $i = 1, \dots, n$, albo też dla pewnej liczby $k \leq n, m$ zachodzi nierówność $a_k < b_k$ i spełnione są równości $a_i = b_i$ dla $i = 1, \dots, k-1$. Jeżeli zachodzi pierwszy przypadek, to bierzemy ciąg c o wyrazach $b_1, b_2, \dots, b_n, b_{n+1} - 1$. W drugim przypadku bierzemy ciąg c o wyrazach $b_1, b_2, \dots, b_{k-1}, (a_k + b_k)/2$. Bez trudu sprawdzamy, że w obu przypadkach ciąg c jest większy w sensie porządku leksykograficznego od ciągu a i mniejszy od ciągu b .

Jest też oczywiste, że jeżeli a_1 jest pierwszym wyrazem ciągu a , to jednoelementowy ciąg, którego wyrazem jest liczba $a_1 + 1$ jest większy od a , a jednoelementowy

ciąg, którego wyrazem jest liczba $a_1 - 1$ jest mniejszy od a . Tak więc w rozważanym porządku leksykograficznym nie ma elementu największego, ani najmniejszego.

Zadanie 535. Niech $\Sigma = \{+, a\}$ będzie sygnaturą zawierającą dwuargumentowy symbol funkcji $+$ i symbol stałej a . Dla dowolnej dodatniej liczby naturalnej n niech $A_n = \{0, 1, \dots, n-1\}$, $\oplus_n$ oznacza dodawanie modulo n , zaś $a_n = 0$. Rozważmy algebry $\mathcal{A}_n = \langle A_n, \oplus_n, a_n \rangle$. Udowodnij, że jeżeli $k = l \cdot m$, to istnieje homomorfizm h algebry $\mathcal{A}_k$ na algebrę $\mathcal{A}_l$ (surjekcja) taki, że $|h^{-1}(\{0\})| = m$. Podaj przykład takich k, l i m , dla których istnieją co najmniej dwa takie homomorfizmy. Ile jest takich homomorfizmów, jeśli zamiast sygnatury Σ będziemy rozważać sygnaturę $\Sigma' = \{+, a, b\}$ zawierającą dwa symbole stałych a i b oraz algebry $\mathcal{A}'_n = \langle A_n, \oplus_n, a_n, b_n \rangle$, gdzie $b_n = 1$?

Rozwiązanie. Resztę z dzielenia k przez l będę oznaczać także symbolem $k \bmod l$. Zauważmy, że każdy element A_k jest sumą pewnej liczby jedynek (daje się przedstawić w postaci $1 \oplus_k \dots \oplus_k 1$). Wobec tego 1 generuje A_k . Homomorfizm wystarczy zdefiniować na zbiorze generatorów. Przyjmijmy więc, że $h : A_k \rightarrow A_l$ jest homomorfizmem i $h(1) = a$. Wtedy

$$h(n) = h(\underbrace{1 \oplus_k \dots \oplus_k 1}_{n \text{ razy}}) = \underbrace{h(1) \oplus_l \dots \oplus_l h(1)}_{n \text{ razy}} = (a \cdot n) \bmod l.$$

Fakt 199. Jeżeli l dzieli k , to funkcja $h_a : A_k \rightarrow A_l$ zdefiniowana wzorem

$$h_a(x) = (a \cdot x) \bmod l$$

jest homomorfizmem algebr $\mathcal{A}_k$ i $\mathcal{A}_l$.

Dowód. Zauważmy najpierw, że definicja funkcji h_a zależy od k i l , mimo że wprowadzone oznaczenie na to nie wskazuje. Oczywiście, $h_a(0) = 0$. Wystarczy więc dowieść, że dla wszystkich $x, y \in A_k$ zachodzi równość $h_a(x \oplus_k y) = h_a(x) \oplus_l h_a(y)$. Zauważmy, że

$$a \cdot x = p \cdot l + h_a(x) \quad \text{oraz} \quad a \cdot y = q \cdot l + h_a(y)$$

dla pewnych liczb naturalnych p i q . Z tych samych powodów zachodzi równość

$$x + y = r \cdot k + (x \oplus_k y).$$

Łącząc podane równości otrzymujemy

$$a \cdot r \cdot k + a \cdot (x \oplus_k y) = a \cdot (x + y) = (p + q) \cdot l + h_a(x) + h_a(y).$$

Ponieważ l dzieli k , więc

$$h_a(x \oplus_k y) = a \cdot (x \oplus_k y) \bmod l = (h_a(x) + h_a(y)) \bmod l = h_a(x) \oplus_l h_a(y).$$

Część I. Korzystając z podanego faktu można łatwo rozwiązać pierwszą część zadania. Wystarczy zauważyć, że jeżeli $k = l \cdot m$, to $h_1 : A_k \rightarrow A_l$ jest homomorfizmem takim, że $h_1(x) = x$ dla $x = 0, \dots, l-1$, a więc jest homomorfizmem algebry $\mathcal{A}_k$ na algebrę $\mathcal{A}_l$. Mamy także

$$\begin{aligned} h_1^{-1}(0) &= \{x < l \cdot m \mid x \bmod l = 0\} = \{x < l \cdot m \mid l \text{ dzieli } x\} = \\ &= \{i \cdot l \mid i < m\} = g(\{i \mid i < m\}) \end{aligned}$$

dla funkcji $g : \mathbb{N} \rightarrow \mathbb{N}$ takiej, że $g(i) = i \cdot l$. Funkcja g jest oczywiście różnowartościowa. Wobec tego zbiór $h_1^{-1}(0)$ jest równoliczny ze zbiorem $\{i \mid i < m\}$, który oczywiście ma m elementów, i też ma m elementów.

Część II. Aby rozwiązać drugą część zadania wystarczy dodatkowo zauważyć, że jeżeli weźmiemy $k = l = 3$, to odpowiednia funkcja h_2 przekształca A_3 na A_3 ($h_2(1) = 2$ i $h_2(2) = 1$) i — wobec tego — jest homomorfizmem algebry $\mathcal{A}_3$ na algebrę $\mathcal{A}_3$. Funkcje h_1 i h_2 są w tym przypadku różne, ponieważ $1 = h_1(1) \neq h_2(1) = 2$. Podobnie jest w przypadku funkcji $h_2 : A_6 \rightarrow A_3$ (jest to inna funkcja niż poprzednia, mimo że jest tak samo oznaczana!). Można dowieść, że dla dowolnej wielokrotności k liczby l , funkcja h_a przekształca A_k na A_l wtedy i tylko wtedy, gdy a jest względnie pierwsze z l .

Część III. Z definicji homomorfizmu wynika, że homomorfizmy algebry $\mathcal{A}'_k$ w algebrę $\mathcal{A}'_l$ są to dokładnie homomorfizmy algebry $\mathcal{A}_k$ w algebrę $\mathcal{A}_l$ przekształcające 1 na 1. Aby więc odpowiedzieć na ostatnie pytanie wystarczy ustalić, ile jest homomorfizmów przekształcających algebrę $\mathcal{A}_k$ na algebrę $\mathcal{A}_l$ i przeprowadzających 1 na 1. Pokażemy, że jeżeli l dzieli k , to jest dokładnie jeden taki homomorfizm. Oczywiście, jest taki homomorfizm (jest nim h_1). Przypuśćmy, że h też jest takim homomorfizmem. Wtedy

$$h(n) = h(\underbrace{1 \oplus_k \dots \oplus_k 1}_{n \text{ razy}}) = \underbrace{h(1) \oplus_l \dots \oplus_l h(1)}_{n \text{ razy}} = \underbrace{h_1(1) \oplus_l \dots \oplus_l h_1(1)}_{n \text{ razy}} = h_1(n)$$

dla wszystkich $n \in A_k$. Wobec tego, homomorfizmy h i h_1 są identyczne. Bardziej elegancki dowód tego faktu powinien być indukcyjny. ■

Zadanie 536. Niech $A_0, A_1, A_2, \dots$ będzie ciągiem zbiorów takim, że

$$A_{n+1} = \left(\bigcup_{i=0}^n A_i \right) \times \left(\bigcup_{i=0}^n A_i \right)$$

dla wszystkich $n \in \mathbb{N}$. Przyjmijmy, że

$$B = \bigcup_{i=0}^{\infty} A_i.$$

Pokaż, że $B \times B \subseteq B$.

Rozwiązanie. Aby dowieść zawieranie $B \times B \subseteq B$ wystarczy z założenia $X \in B \times B$ wywnioskować, że $X \in B$. Załóżmy więc, że $X \in B \times B$. Elementami iloczynu kartezjańskiego $B \times B$ są pary uporządkowane o współrzędnych należących do B . Przypuśćmy, że X jest parą uporządkowaną $\langle a, b \rangle$ o współrzędnych $a, b \in B$, czyli $X = \langle a, b \rangle$. Zbiór B jest sumą mnogościową wyrazów ciągu $A_0, A_1, A_2, \dots$. Wobec tego, elementy a i b należą do pewnych składników tej sumy. Przyjmijmy, że $a \in A_p$ oraz $b \in A_q$ dla pewnych liczb $p, q \in \mathbb{N}$. Stąd oczywiście wynika, że

$$a, b \in \bigcup_{i=0}^{\max\{p,q\}} A_i.$$

Łatwo zauważyć, że

$$X = \langle a, b \rangle \in \left(\bigcup_{i=0}^{\max\{p,q\}} A_i \right) \times \left(\bigcup_{i=0}^{\max\{p,q\}} A_i \right) = A_{\max\{p,q\}+1}.$$

Zbiór $A_{\max\{p,q\}+1}$ jest jednym ze składników sumy równej B . Ponieważ

$$X \in A_{\max\{p,q\}+1},$$

więc także $X \in B$.

Zadanie 537. Rozważmy formuły zdaniowe ϕ , w których występują jedynie spójniki równoważności i negacji. Niech ϕ^- oznacza formułę, którą otrzymujemy usuwając z ϕ wszystkie znaki negacji. Udowodnij, że

1. jeżeli symbol negacji występuje w ϕ parzystą liczbę razy, to $\phi \Leftrightarrow \phi^-$ jest tautologią,
2. jeżeli symbol negacji występuje w ϕ nieparzystą liczbę razy, to $\phi \Leftrightarrow \neg\phi^-$ jest tautologią.

Zauważ, że operacja $-$ ma następujące własności: $(\neg\phi)^- = \phi^-$ oraz $(\phi \Leftrightarrow \psi)^- = \phi^- \Leftrightarrow \psi^-$.

Przypomnijmy, że formuły zdaniowe ϕ i ψ są równoważne wtedy i tylko wtedy, gdy formuła $\phi \Leftrightarrow \psi$ jest tautologią. Napis $\phi \equiv \psi$ oznacza, że formuły ϕ i ψ są równoważne. Będziemy korzystać z następujących znanych i łatwych do wykazania własności:

1. formuły $\neg\neg\phi$ i ϕ są równoważne,
2. każde dwie z formuł $(\neg\phi) \Leftrightarrow \psi$, $\neg(\phi \Leftrightarrow \psi)$ i $\phi \Leftrightarrow (\neg\psi)$ są równoważne,
3. formuły $(\neg\phi) \Leftrightarrow (\neg\psi)$ i $\phi \Leftrightarrow \psi$ są równoważne.

Niech $\mathcal{F}$ oznacza zbiór wszystkich formuł zdaniowych, w których nie występują spójniki różne od negacji i równoważności. Przyjmijmy też, że symbol $\mathcal{F}_n$ oznacza zbiór tych formuł należących do $\mathcal{F}$, w których występuje najwyżej n spójników.

Rozwiązanie (najbardziej naturalne). Pokażemy przez indukcję ze względu na n , że dla każdej liczby naturalnej n i dla każdej formuły $\phi \in \mathcal{F}_n$ zachodzą następujące implikacje:

1. jeżeli w formule ϕ negacja występuje na parzystej liczbie miejsc, to formuła $\phi \Leftrightarrow \phi^-$ jest tautologią,
2. jeżeli w formule ϕ negacja występuje na nieparzystej liczbie miejsc, to formuła $\phi \Leftrightarrow \neg\phi^-$ jest tautologią.

Z tego pozornie bardziej ogólnego faktu bez trudu można wywnioskować tezę rozwiązywanego zadania.

Pierwsza część dowodu indukcyjnego. Jeżeli $n = 0$, to $\mathcal{F}_n = \mathcal{F}_0$ jest zbiorem zmiennych zdaniowych. Wobec tego, dla formuł $\phi \in \mathcal{F}_0$ zachodzi równość $\phi = \phi^-$. Pierwsza z dowodzonych implikacji jest konsekwencją tego, że formuły postaci $p \Leftrightarrow p$ są tautologiami. Druga zachodzi, ponieważ jej poprzednik jest fałszywy.

Druga część dowodu indukcyjnego. Zakładamy, że formuły ze zbioru $\mathcal{F}_n$ mają obie podane własności i bierzemy formułę $\phi \in \mathcal{F}_{n+1}$. Możemy dodatkowo założyć, że $\phi \notin \mathcal{F}_n$ (dla formuł z $\mathcal{F}_n$ teza zachodzi na mocy założenia indukcyjnego). Oczywiście, wszystkie formuły ze zbioru $\mathcal{F}$ są negacjami, równoważnościami lub zmiennymi i formuła ϕ nie jest zmienną (w przeciwnym razie należałaby do $\mathcal{F}_0 \subseteq \mathcal{F}_n$).

Przypadek 1: formuła ϕ jest negacją. Przyjmijmy, że $\phi = \neg\psi$. W tym przypadku, $\phi^- = \psi^-$. Oczywiście, formuła $\psi \in \mathcal{F}_n$ i dla formuły ψ możemy skorzystać z założenia indukcyjnego. W zależności od liczby wystąpień negacji w formule ψ , tautologią jest albo formuła $\psi \Leftrightarrow \psi^-$ (gdy negacja występuje w ϕ parzystą liczbę razy), albo formuła $\psi \Leftrightarrow \neg\psi^-$ (w przeciwnym przypadku).

Jeżeli w formule ϕ negacja występuje na parzystej liczbie pozycji, to w formule ψ występuje na nieparzystej i tautologią jest formuła $\psi \Leftrightarrow (\neg\psi^-)$. Tautologią jest także formuła $(\neg\psi) \Leftrightarrow \psi^-$, która jest równa formule $\phi \Leftrightarrow \phi^-$.

Jeżeli w formule ϕ negacja występuje w nieparzystej liczbie miejsc, to w formule ψ występuje w parzystej i formuła $\psi \Leftrightarrow \psi^-$ jest tautologią. Wtedy także tautologią jest formuła $(\neg\psi) \Leftrightarrow (\neg\psi^-)$ identyczna z formułą $\phi \Leftrightarrow (\neg\phi^-)$.

Przypadek 2: formuła ϕ jest równoważnością. Przyjmijmy, że $\phi = \psi_1 \Leftrightarrow \psi_2$ dla pewnych formuł $\psi_1, \psi_2 \in \mathcal{F}_n$. Tym razem zachodzi wzór $\phi^- = \psi_1^- \Leftrightarrow \psi_2^-$. Dalej powinniśmy rozważyć cztery przypadki.

Przypadek 2.1: negacja występuje w ϕ nieparzystą, a w ψ_1 parzystą liczbę razy. W tym przypadku negacja występuje w ψ_2 nieparzystą liczbę razy. Dla formuł ψ_1 i ψ_2

możemy skorzystać z założenia indukcyjnego. Wobec tego, formuły ψ_1 i ψ_1^- są równoważne, a także równoważne są ψ_2 i $\neg\psi_2^-$. Wobec tego formuła $\phi = \psi_1 \Leftrightarrow \psi_2$ jest równoważna z $\psi_1^- \Leftrightarrow \neg\psi_2^-$. Korzystając z własności 2), Formuła ϕ jest równoważna z $\neg(\psi_1^- \Leftrightarrow \psi_2^-) = \neg\phi^-$.

Przypadek 2.2: negacja występuje w ϕ i ψ_1 nieparzystą liczbę razy. W tym i kolejnych przypadkach przeprowadzamy rozumowanie podobne do wyżej przedstawionego.

Aby zakończyć rozwiązanie, powinniśmy jeszcze rozważyć następujące przypadki:

Przypadek 2.3: negacja występuje w ϕ parzystą, a w ψ_1 nieparzystą liczbę razy.

Przypadek 2.4: negacja występuje w ϕ i ψ_1 parzystą liczbę razy.

Rozwiązanie (sugerowane przez jedną z prac egzaminacyjnych). Przypuśćmy, że mamy daną formułę $\phi \in \mathcal{F}$ i wartościowanie h (zmiennych występujących w tej formule). Symbolem $\phi[h]$ oznaczamy wartość logiczną formuły ϕ przy wartościowaniu h . Dla danego wartościowania, indeksem $i_h(\phi)$ formuły ϕ nazywamy sumę liczby negacji występujących w ϕ i liczby wystąpień w ϕ zmiennych fałszywych przy wartościowaniu h . Na przykład, jeżeli $h(p) = 1$, $h(q) = 0$ oraz $\phi = (q \Leftrightarrow p) \Leftrightarrow \neg(q \Leftrightarrow (\neg q \Leftrightarrow p))$, to $i_h(\phi) = 5$.

Lemat 200. Przypuśćmy, że mamy formułę $\phi \in \mathcal{F}$ i wartościowanie h zmiennych tej formuły. Formuła ϕ jest spełniona przy wartościowaniu h wtedy i tylko wtedy, gdy $i_h(\phi)$ jest liczbą parzystą.

Dowód. Dowód tego lematu pozostawiamy jako ćwiczenie.

Wniosek. Formuła $\phi \in \mathcal{F}$ jest tautologią wtedy i tylko wtedy, gdy występuje w niej parzysta liczba negacji i każda zmienna zdaniowa występuje parzystą liczbę razy.

Dowód. Weźmy formułę $\phi \in \mathcal{F}$ i najpierw założmy, że jest tautologią. Formuła ϕ jest więc spełniona dla każdego wartościowania. Niech h wartościowaniem, które wszystkim zmiennym z formuły ϕ przyporządkowuje 1 (prawdę). Dla tego wartościowania indeks $i_h(\phi)$ jest liczbą negacji występujących w ϕ . Na podstawie powyższego lematu indeks ten jest liczbą parzystą.

Aby pokazać, że zmienna p występuje w ϕ parzystą liczbę razy weźmy wartościowanie h_p , które zmiennej p przyporządkowuje 0 (fałsz), a pozostałym zmiennym — 1 (prawdę). Dla tego wartościowania indeks $i_{h_p}(\phi)$ jest liczbą parzystą i jest równy sumie liczb wystąpień w ϕ negacji i wystąpień zmiennej p . Odejmując od indeksu liczbę wystąpień negacji otrzymujemy liczbę wystąpień zmiennej p . Liczba ta, jako różnica dwóch liczb parzystych jest parzysta.

Aby dowieść implikację przeciwną do udowodnionej, wystarczy zauważyć, że jeżeli w formule ϕ negacja i każda zmienna występuje parzystą liczbę razy, to dla

dowolnego wartościowania indeks tej formuły jest liczbą parzystą. W tej sytuacji, z powyższego lematu wynika, że formuła ϕ jest spełniona dla dowolnego wartościowania. ■

Korzystając z podanego wniosku bez trudu możemy sprawdzić, czy formuły takie, jak $\phi \Leftrightarrow \phi^-$ lub $\phi \Leftrightarrow \neg\phi^-$ są tautologiami.

Rozwiązanie (też sugerowane). Z lematu podanego w poprzednim rozwiązaniu wynika następujący, oczywisty wniosek:

Wniosek. Przypuśćmy, że formułę ψ otrzymujemy wymazując w formule $\phi \in \mathcal{F}$ jeden znak negacji. Wtedy, dla dowolnego wartościowania h wartości logiczne $\phi[h]$ i $\psi[h]$ są różne. ■

Weźmy teraz formułę $\phi \in \mathcal{F}$ i wymazujemy w niej kolejno symbole negacji tak długo, aż wymażemy wszystkie. Przypuśćmy, że w ten sposób otrzymujemy ciąg formuł

$$\phi = \phi_0, \phi_1, \dots, \phi_n.$$

Oczywiście, $\phi_n = \phi^-$ i n jest liczbą znaków negacji występujących w ϕ . Z powyższego wniosku wynika, że dla dowolnego wartościowania h ciąg wartości logicznych

$$\phi[h] = \phi_0[h], \phi_1[h], \dots, \phi_n[h] = \phi^-[h]$$

zawiera na przemian 0 i 1. Stąd wynika, że jeżeli n jest liczbą parzystą, to $\phi[h] = \phi^-[h]$ dla dowolnego wartościowania h . Podobnie, jeżeli n jest liczbą nieparzystą, to $\phi[h] \neq \phi^-[h]$ dla dowolnego wartościowania h . Teraz teza zadania jest już oczywista.

Rozwiązanie (jeszcze inna wersja). To rozwiązanie też rozpoczniemy od wykazania pomocniczego lematu.

Lemat 201. Jeżeli w formule $\phi \in \mathcal{F}$ występuje dokładnie jeden symbol negacji, to formuła $\phi \Leftrightarrow \neg\phi^-$ jest tautologią.

Dowód. Lemat ten udowodnimy przez indukcję ze względu na liczbę spójników występujących w $\mathcal{F}$. Dla formuł $\phi \in \mathcal{F}_0$ jest on oczywisty, gdyż dla takich formuł nie jest spełnione założenie lematu.

Przypuśćmy, że lemat zachodzi dla formuł ze zbioru $\mathcal{F}_n$ i weźmy formułę $\phi \in \mathcal{F}_{n+1}$. Są możliwe dwa przypadki.

Przypadek 1: formuła ϕ jest negacją. Jeżeli $\phi = \neg\psi$, to $\phi^- = \psi^-$ i dodatkowo — na podstawie założenia — w formule ψ nie występuje negacja, a więc $\psi^- = \psi$. Nietrudno zauważyć, że w tym przypadku w formule $\phi \Leftrightarrow \neg\phi^-$ po obu stronach równoważności znajduje się to samo.

Przypadek 2: formuła ϕ jest równoważnością. Jeżeli $\phi = \psi_1 \Leftrightarrow \psi_2$ i negacja występuje w ϕ w dokładnie jednym miejscu, to występuje w dokładnie jednym miejscu dokładnie jednej z formuł ψ_1 lub ψ_2 . Dla ustalenia uwagi przyjmijmy, że negacja występuje w ψ_1 .

Z założenia indukcyjnego wynika, że formuły ψ_1 i $\neg\psi_1^-$ są równoważne. Jest oczywiste, że $\psi_2^- = \psi_2$. Na podstawie własności 2) podanej na początku mamy, że formuła $\neg\phi^-$, czyli $\neg(\psi_1^- \Leftrightarrow \psi_2^-)$, jest równoważna formule $(\neg\psi_1^-) \Leftrightarrow \psi_2^-$, a ta z kolei — na podstawie założenia indukcyjnego — jest równoważna $\psi_1 \Leftrightarrow \psi_2^-$, czyli formule ϕ . ■

Założmy, że w formule ϕ jest symbol negacji i ten symbol poprzedza formułę δ . Przyjmijmy, że jeżeli wyramyśmy w ϕ tę negację wraz z formułą δ i w to miejsce wstawimy nową zmienną zdaniową q , to otrzymamy formułę ψ . Nietrudno zauważyć, że jeżeli teraz w formule ψ zastąpimy zmienną q formułą $\neg\delta$ to otrzymamy formułę $\psi(\neg\delta)$ identyczną z wyjściową formułą ϕ .

W formułach ψ i δ występuje mniej spójników, niż w ϕ . Z założenia indukcyjnego otrzymujemy, że zależnie od przypadku, formuły $\psi \Leftrightarrow \neg\psi^-$ oraz $\delta \Leftrightarrow \neg\delta^-$ lub podobne formuły bez negacji są tautologiami. Dalej korzystamy z dwóch faktów: zastępując w formułach równoważnych (lub w tautologii) pewną zmienną zdaniową dowolną formułą otrzymujemy formuły równoważne (lub odpowiednio: otrzymujemy tautologię) oraz zastępując w dowolnej formule pewien jej fragment formułą równoważną otrzymujemy formułę równoważną. Na przykład, jeżeli w formule ϕ występuje nieparzysta liczba spójników negacji oraz spójniki te podzieliły się tak, że podane wyżej formuły są tautologiami, to następujące formuły są równoważne:

$$\phi = \psi(\neg\delta), \neg\psi^-(\neg\delta), \neg\psi^-(\delta^-) = \neg\phi^-.$$

Sformułowany wyżej lemat przydaje się w innych przypadkach.

Zadanie 538. Czy prawdziwe jest zdanie: „Dla dowolnych zbiorów A i B , jeśli $A \times B \subseteq B \times A$, to $A = \emptyset \vee B = \emptyset \vee A = B$ ”?

Rozwiązanie. Tak, zdanie powyższe jest prawdziwe dla dowolnych zbiorów A i B . Istotnie, przypuśćmy, że $A \times B \subseteq B \times A$ oraz $A \neq \emptyset$ i $B \neq \emptyset$. Pokażemy, że $A = B$. Skoro $A \neq \emptyset$, to istnieje pewien element $a_0 \in A$. Dla dowolnego $b \in B$ mamy wówczas $\langle a_0, b \rangle \in A \times B$. Skoro $A \times B \subseteq B \times A$, to $\langle a_0, b \rangle \in B \times A$. Zatem $b \in A$. Ponieważ w powyższym rozumowaniu b jest dowolne, więc $B \subseteq A$. Analogicznie skoro $B \neq \emptyset$, to istnieje pewien element $b_0 \in B$. Dla dowolnego $a \in A$ jest wtedy $\langle a, b_0 \rangle \in A \times B$. Skoro $A \times B \subseteq B \times A$, to $\langle a, b_0 \rangle \in B \times A$. Zatem $a \in B$. Pokazaliśmy więc, że $A \subseteq B$. Skoro $B \subseteq A$ oraz $A \subseteq B$, to $A = B$.

Zadanie 539. Pokaż, że $A \setminus (B \setminus (C \setminus D)) = (A \setminus B) \cup ((A \cap C) \setminus D)$ dla dowolnych zbiorów A, B, C i D .

Rozwiązanie. Zauważmy, że równoważne są każde dwie z niżej podanych formuł:

1. $x \in A \setminus (B \setminus (C \setminus D))$,
2. $x \in A \wedge \neg(x \in B \wedge \neg(x \in C \wedge x \notin D))$,
3. $x \in A \wedge (x \notin B \vee (x \in C \wedge x \notin D))$,
4. $(x \in A \wedge x \notin B) \vee (x \in A \wedge (x \in C \wedge x \notin D))$,
5. $(x \in A \wedge x \notin B) \vee ((x \in A \wedge x \in C) \wedge x \notin D)$,
6. $x \in (A \setminus B) \cup ((A \cap C) \setminus D)$.

Równoważność dwóch pierwszych formuł wynika z definicji działań mnogościowych, drugiej i trzeciej – z prawa de Morgana i prawa podwójnej negacji, dwóch kolejnych – z prawa rozdzielności koniunkcji względem alternatywy, następnej pary – z prawa łączności dla koniunkcji, a dwóch ostatnich – znowu z definicji działań mnogościowych. W ten sposób, dla dowolnego x dowiedliśmy równoważność

$$x \in A \setminus (B \setminus (C \setminus D)) \Leftrightarrow x \in (A \setminus B) \cup ((A \cap C) \setminus D).$$

Oznacza to, że

$$\forall x (x \in A \setminus (B \setminus (C \setminus D)) \Leftrightarrow x \in (A \setminus B) \cup ((A \cap C) \setminus D)).$$

W tej sytuacji równość

$$A \setminus (B \setminus (C \setminus D)) = (A \setminus B) \cup ((A \cap C) \setminus D))$$

wynika z zasady ekstensjonalności.

Przedstawione rozwiązanie zawiera elementy sformalizowanego rachunku logicznego. Czytając takie rozwiązanie nie wiadomo, czy osoba, która je przedstawiła rozumie, co robi, czy też nauczyła się tylko mechanicznie wykonywać dziwne i niezrozumiałe przekształcenia. Co więcej, takie rozwiązania są możliwe tylko w prostych przypadkach, a zadań bardziej interesujących nie można rozwiązać w ten sposób. Nie polecałbym tej metody ze względów dydaktycznych, mimo że jej zaletą jest czytelność. Zauważmy także, że czytając podręczniki wyjątkowo spotykamy się z takimi rozumowaniami. Również przekonując siebie i kolegów o słuszności różnych stwierdzeń zwykle robimy to w inny sposób.

Rozwiązanie. Udowodnię teraz dwa zawierania

$$A \setminus (B \setminus (C \setminus D)) \subseteq (A \setminus B) \cup ((A \cap C) \setminus D))$$

oraz

$$(A \setminus B) \cup ((A \cap C) \setminus D)) \subseteq A \setminus (B \setminus (C \setminus D))$$

nie korzystając z formalnego rachunku logicznego (a więc tak naprawdę znowu skorzystam z zasady ekstensjonalności).

Dowód (pierwszego zawierania). Weźmy dowolny $x \in A \setminus (B \setminus (C \setminus D))$. Nietrudno zauważyć, że elementy zbioru $A \setminus B$ należą do $(A \setminus B) \cup ((A \cap C) \setminus D)$. Wobec tego, dalej wystarczy rozważać tylko te elementy x , które nie należą do $A \setminus B$.

Element x należący do $A \setminus (B \setminus (C \setminus D))$ należy również do zbioru A . Jeżeli nie należy do $A \setminus B$, to należy do B . Wiemy też, że $x \notin B \setminus (C \setminus D)$. Jeżeli x należący do B nie znalazł się w tej różnicy, to należy do $C \setminus D$. Otrzymaliśmy więc, że $x \in A$, $x \in C$ oraz $x \notin D$. Teraz łatwo sprawdzić, że x należy do drugiego składnika sumy $(A \setminus B) \cup ((A \cap C) \setminus D)$. To kończy dowód pierwszej inkluzji.

Dowód (drugiego zawierania). Aby dowieść drugą inkluzję, weźmy $x \in (A \setminus B) \cup ((A \cap C) \setminus D)$. Są dwa rodzaje takich elementów x . Taki x może należeć do $A \setminus B$. Wtedy $x \in A$ oraz $x \notin B$. Warunkiem należenia do $B \setminus (C \setminus D)$ jest między innymi należenie do B . Wobec tego, $x \notin B \setminus (C \setminus D)$. Ponieważ $x \in A$, więc także $x \in A \setminus (B \setminus (C \setminus D))$.

Powinniśmy się jeszcze zająć elementami $x \in (A \cap C) \setminus D$. Te elementy należą do A i do $C \setminus D$. Elementy zbioru $C \setminus D$ zostały usunięte ze zbioru $B \setminus (C \setminus D)$, więc $x \notin B \setminus (C \setminus D)$. Oznacza to że x spełnia oba warunki wymagane od elementów $A \setminus (B \setminus (C \setminus D))$, czyli $x \in A \setminus (B \setminus (C \setminus D))$. Udowodniliśmy więc drugie zawieranie i tym samym dowiedliśmy, że

$$A \setminus (B \setminus (C \setminus D)) = (A \setminus B) \cup ((A \cap C) \setminus D).$$

Rozwiązanie. Zamiast wyprowadzać równość z zadania bezpośrednio z definicji działań mnogościowych można skorzystać z własności tych działań. Takie rozwiązanie może być oparte na następującym rachunku:

$$\begin{aligned} A \setminus (B \setminus (C \setminus D)) &= A \cap (B \cap (C \cap D^c)^c)^c = A \cap (B^c \cup (C \cap D^c)) = \\ &= (A \cap B^c) \cup (A \cap C \cap D^c) = (A \setminus B) \cup ((A \cap C) \setminus D). \end{aligned}$$

W powyższych wzorach c oznacza operację dopełnienia. Pierwsza równość wynika ze związku między różnicą i dopełnieniem, czyli z wzoru $X \setminus Y = X \cap Y^c$ zastosowanego trzy razy. Druga równość jest konsekwencją prawa de Morgana $(X \cap Y)^c = X^c \cup Y^c$. Trzecia wynika z prawa rozdzielnosci przekroju względem sumy mnogościowej. Ostatnia jest konsekwencją związku między różnicą a dopełnieniem oraz łączności przekroju.

Przedstawione rozwiązanie może być niezrozumiałe dla osób, które nie słyszały o dopełnieniu. Jest to bardzo naturalne działanie mnogościowe, jeżeli rozważamy podzbiory ustalonego zbioru zwanego wtedy przestrzenią. Z pewną ostrożnością może być wykorzystywane w każdej sytuacji.

Jeżeli P jest przestrzenią, to dopełnieniem zbioru $X \subseteq P$ nazywamy różnicę $P \setminus X$ i oznaczamy ją symbolem X^c . Zauważmy, że dopełnienie to jest właściwie dopełnienie do ustalonego zbioru (w tym przypadku P) i można dopełniać do różnych

zbiorów. Zauważmy również, że dla tak zdefiniowanego dopełnienia i dla $X \subseteq P$ zachodzi wzór

$$X \setminus Y = X \cap (P \setminus Y) = X \cap Y^c$$

oraz podane wyżej prawo de Morgana.

Z treści zadania nie wynika, że zbiory A, B, C i D są zawarte w jakiejś naturalnej przestrzeni. Zawsze jednak możemy przyjąć, że $P = A \cup B \cup C \cup D$ (lub $P = A \cup B \cup C$). Taka definicja P gwarantuje prawdziwość wzoru $X \setminus Y = X \cap Y^c$ w wymaganym zakresie.

Rozwiązanie. Zadanie to można także rozwiązać sprawdzając podaną równość dla konkretnych zbiorów. Spróbuję uzasadnić poprawność tej metody nie zachowując pełnej ogólności. Będziemy teraz dokładnie analizować pierwsze z rozwiązań. Najpierw wprowadźmy kilka oznaczeń. Niech

$$L_{ABCD} = A \setminus (B \setminus (C \setminus D)) \text{ oraz } P_{ABCD} = (A \setminus B) \cup ((A \cap C) \setminus D).$$

Będziemy też rozważać zmienne zdaniowe a, b, c i d (odpowiadają one zbiorom lub zmiennym A, B, C i D), a także formuły zdaniowe z tymi zmiennymi oraz wartościowania takich formuł. Przyjmijmy, że h_{ABCD}^x oznacza wartościowanie zmiennych a, b, c i d takie, że

$$h_{ABCD}^x(a) = T \Leftrightarrow x \in A$$

i spełniające analogiczne warunki dla pozostałych zmiennych, a H_{ABCD} oznacza zbiór wszystkich takich wartościowań. Symbolem $h_{ABCD}^x(\phi)$ będę oznaczać wartość logiczną formuły ϕ przy wartościowaniu h_{ABCD}^x .

Zauważmy, że w rozwiązaniu 1 zostały skonstruowane dwie formuły zdaniowe ϕ i ψ takie, że

$$\forall A, B, C, D \forall x (x \in L_{ABCD} \Leftrightarrow h_{ABCD}^x(\phi) = T)$$

oraz

$$\forall A, B, C, D \forall x (x \in P_{ABCD} \Leftrightarrow h_{ABCD}^x(\psi) = T).$$

Formuły te nie zależą od zbiorów A, B, C i D , a jedynie od wyrażeń występujących po obu stronach równości, np. formuła ϕ jest równa $a \wedge \neg(b \wedge \neg(c \wedge \neg d))$ bez względu na to, co oznaczają symbole A, B, C i D .

Z podanych własności wynika, że

$$\begin{aligned} \forall A, B, C, D (\forall x (x \in L_{ABCD} \Leftrightarrow x \in P_{ABCD}) &\Leftrightarrow \\ &\Leftrightarrow \forall x (h_{ABCD}^x(\phi) = T \Leftrightarrow h_{ABCD}^x(\psi) = T)) \end{aligned}$$

oraz

$$\forall A, B, C, D (L_{ABCD} = P_{ABCD} \Leftrightarrow \forall h \in H_{ABCD} h(\phi \Leftrightarrow \psi) = T). \quad (2)$$

Twierdzenie 202. Jeżeli A', B', C' i D' są jakimikolwiek zbiorami dla których zbiór $H_{A'B'C'D'}$ zawiera wszystkie możliwe wartościowania, oraz zachodzi równość

$$L_{A'B'C'D'} = P_{A'B'C'D'}$$

to

$$\forall A, B, C, D \quad L_{ABCD} = P_{ABCD}$$

(a więc jeżeli równość $L = P$ zachodzi dla jednej (specyficznej) czwórki zbiorów, to zachodzi dla wszystkich możliwych czwórek).

Dowód. Aby dowieść podane twierdzenie skorzystamy z własności (2) dla $A = A', B = B', C = C'$ i $D = D'$. W ten sposób otrzymujemy, że

$$L_{A'B'C'D'} = P_{A'B'C'D'} \Leftrightarrow \forall h \in H_{A'B'C'D'} \quad h(\phi \Leftrightarrow \psi) = T.$$

Na mocy założenia o zbiorze $H_{A'B'C'D'}$ prawa strona tej równoważności stwierdza, że formuła $\phi \Leftrightarrow \psi$ jest tautologią. Zakładamy ponadto lewą stronę tej równoważności. Stąd otrzymujemy, że formuła $\phi \Leftrightarrow \psi$ jest tautologią.

Weźmy cztery dowolne zbiory A, B, C i D . Chcemy teraz z własności (2) wnioskować, że $L_{ABCD} = P_{ABCD}$. Aby to zrobić, wystarczy wykazać, że

$$\forall h \in H_{ABCD} \quad h(\phi \Leftrightarrow \psi) = T.$$

Fakt ten jest oczywistą konsekwencją tego, że $\phi \Leftrightarrow \psi$ jest tautologią (tautologię są spełnione dla wszystkich wartościowań, a więc także dla wartościowań ze zbioru H_{ABCD}). $\square$

Aby wykorzystać to twierdzenie trzeba jeszcze skonstruować zbiory A', B', C' i D' takie, że zbiór $H_{A'B'C'D'}$ zawiera wszystkie możliwe wartościowania zmiennych zdaniowych a, b, c i d . Weźmy dowolne wartościowanie h tych zmiennych. Dla tego wartościowania wybieramy (dowolnie) pewien element x_h . Z wybranych w ten sposób elementów konstruujemy potrzebne nam zbiory w następujący sposób: x_h uznajemy za element zbioru A' wtedy i tylko wtedy, gdy $h(a) = T$. Analogicznie definiujemy pozostałe zbiory.

Dla zdefiniowanych w ten sposób zbiorów sprawdzamy dowodzoną równość. Jeżeli równość ta zachodzi, to z wykazanego twierdzenia otrzymujemy, że zachodzi dla wszystkich możliwych zbiorów.

Zadanie 540. Rodzina zbiorów $\{X_n\}_{n=0}^{\infty}$ jest *zstępująca*, jeżeli $X_{n+1} \subseteq X_n$ dla każdego $n \in \mathbb{N}$. Ciąg liczb naturalnych $(a_n)_{n=0}^{\infty}$ jest *rosnący*, jeżeli $a_n < a_{n+1}$ dla każdego $n \in \mathbb{N}$. Niech $(a_n)_{n=0}^{\infty}$ będzie rosnącym ciągiem liczb naturalnych, a $\{X_n\}_{n=0}^{\infty}$ — zstępującą rodziną zbiorów. Udowodnij, że

$$\bigcap_{n=0}^{\infty} X_n = \bigcap_{n=0}^{\infty} X_{a_n}.$$

Rozwiązanie.

Lemat 203. Jeżeli ciąg $(a_n)_{n \in \mathbb{N}}$ jest rosnący, to $a_n \geq n$ dla każdego $n \in \mathbb{N}$.

Dowód. Przez indukcję względem n . Skoro $a_0 \in \mathbb{N}$, to $a_0 \geq 0$. Przypuśćmy, że $a_n \geq n$. Skoro ciąg jest rosnący, to $a_{n+1} > a_n \geq n$. Zatem $a_{n+1} \geq n+1$.

Lemat 204. Jeżeli rodzina $\{X_n\}_{n \in \mathbb{N}}$ jest zstępująca, to $X_n \subseteq X_m$ dla wszelkich $n, m \in \mathbb{N}$ takich, że $m \leq n$.

Dowód. Przez indukcję względem n . Jeżeli $m \leq 0$, to $m = 0$, więc $X_0 \subseteq X_m$. Przypuśćmy, że $X_n \subseteq X_m$ dla $m \geq n$. Skoro rodzina jest zstępująca, to $X_{n+1} \subseteq X_n \subseteq X_m$ dla $m \geq n$. Ponieważ nadto $X_{n+1} \subseteq X_m$ dla $m = n+1$, to $X_{n+1} \subseteq X_m$ dla dowolnego $m \leq n+1$.

Na mocy zasady ekstensjonalności wystarczy pokazać, że dla dowolnego x spełniona jest równoważność

$$x \in \bigcap_{n \in \mathbb{N}} X_n \Leftrightarrow x \in \bigcap_{m \in \mathbb{N}} X_{a_m}.$$

Z definicji przekroju rodziny zbiorów oznacza to, że dla dowolnego x zachodzi

$$\forall n \in \mathbb{N} \ x \in X_n \Leftrightarrow \forall m \in \mathbb{N} \ x \in X_{a_m}.$$

Aby wykazać żadaną w zadaniu równoważność, uzasadnimy osobno dwie implikacje.

„ $\Rightarrow$ ” Wiemy, że dla dowolnej liczby naturalnej n zachodzi $x \in X_n$. Dla każdego m liczba a_m jest liczbą naturalną, zatem $x \in X_{a_m}$.

„ $\Leftarrow$ ” Przypuśćmy, że $x \in X_{a_m}$ dla dowolnego m . Niech $n \in \mathbb{N}$. Z lematu 203 wiemy, że $a_n \geq n$. Z założenia wynika, że $x \in X_{a_n}$. Z lematu 204 wnioskujemy, że $X_{a_n} \subseteq X_n$. Zatem $x \in X_n$.

Rozwiązanie. Nie jest to rozwiązanie najprostsze, ale zawiera pomysł, który pozwala na odejście od bardzo formalnego rachunku logicznego. Aby uprościć wzory uzupełniamy dany ciąg liczb naturalnych o wyraz $a_{-1} = -1$. Tak uzupełniony ciąg jest nadal rosnący i każda liczba naturalna jest większa od pierwszego wyrazu tego ciągu (czyli od wyrazu o numerze -1).

Główna część rozwiązania wynika z następujących wzorów:

$$\bigcap_{n=0}^{\infty} X_n = \bigcap_{k=0}^{\infty} \bigcap_{n=a_{k-1}+1}^{a_k} X_n = \bigcap_{n=0}^{\infty} X_{a_n}.$$

Dalej wystarczy uzasadnić równości z tego wzoru.

Oczywiście, zaczynamy od dowodu pierwszej równości. Równość ta zachodzi, ponieważ po obu stronach równości mamy właściwie przekroje tej samej rodziny zbiorów. Aby bardziej formalnie wykazać zawieranie

$$\bigcap_{n=0}^{\infty} X_n \subseteq \bigcap_{k=0}^{\infty} \bigcap_{n=a_{k-1}+1}^{a_k} X_n,$$

weźmy dowolny element $x \in \bigcap_{n=0}^{\infty} X_n$. Wystarczy wykazać, że $x \in X_n$ dla dowolnych liczb $k \in \mathbb{N}$ oraz $n \in \mathbb{N}$ takich, że $a_{k-1} < n \leq a_k$. Jest to bezpośrednia konsekwencja wyboru elementu x .

Odwrotne zawieranie wynika z faktu, że każda liczba naturalna znajduje się między dwoma, kolejnymi wyrazami ciągu $\{a_n\}_{n=0}^{\infty}$, a dokładniej

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \ a_{k-1} < n \leq a_k.$$

Jeżeli trzeba to udowodnić, to warto posłużyć się zasadą indukcji.

Aby dowieść to drugie zawieranie, bierzemy $x \in \bigcap_{k=0}^{\infty} \bigcap_{n=a_{k-1}+1}^{a_k} X_n$ i dowolną liczbę $n \in \mathbb{N}$. Będziemy uzasadniać, że $x \in X_n$. Dla liczby n znajdujemy $k \in \mathbb{N}$ takie, że $a_{k-1} < n \leq a_k$. Z założonej własności x wynika najpierw, że $x \in \bigcap_{n=a_{k-1}+1}^{a_k} X_n$, a następnie, że $x \in X_n$. W ten sposób pierwsza równość została udowodniona.

Druga równość jest konsekwencją zstępowania rodziny $\{X_n\}_{n=0}^{\infty}$. Przekrój skończenie wielu zbiorów porównywalnych w sensie inkluzji jest najmniejszym z tych zbiorów, czyli

$$\bigcap_{n=a_{k-1}+1}^{a_k} X_n = X_{a_{k-1}+1} \cap X_{a_{k-1}+2} \cap \dots \cap X_{a_k} = X_{a_k}.$$

Oznacza to, że przekroje po obu stronach drugiej równości są przekrojami tego samego ciągu zbiorów, a więc są równe. Trochę dokładniejsze uzasadnienie powyższej równości może korzystać z zasady indukcji i wzorów

$$\bigcap_{n=p}^{q+1} X_n = \left(\bigcap_{n=p}^q X_n \right) \cap X_{q+1} = X_q \cap X_{q+1} = X_{q+1}.$$

Zadanie 541. Niech A będzie n -elementowym zbiorem uporządkowanym liniowo relacją $\leq$, gdzie $n \geq 5$. Na zbiorze A^2 definiujemy relację $\preceq$ w następujący sposób:

$$\langle a_1, a_2 \rangle \preceq \langle b_1, b_2 \rangle \Leftrightarrow (a_1 = b_1 \wedge a_2 = b_2) \vee (a_1 < b_1 \wedge a_2 < b_2),$$

gdzie $a < b$ oznacza, że $a \leq b$ i $a \neq b$.

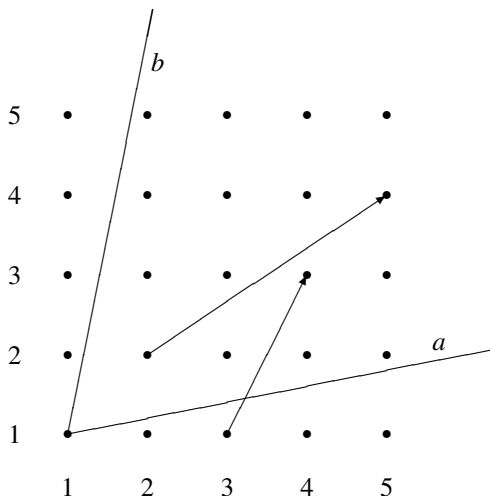
Wśród poniższych zdań wskaż zdania prawdziwe.

1. Porządek $\preceq$ jest regularny.
2. W $\langle A^2, \preceq \rangle$ istnieje element najmniejszy.
3. Liczba elementów maksymalnych w A^2 względem porządku $\preceq$ wynosi
 - n
 - $n - 1$
 - $\lfloor \sqrt{2}n - 1 \rfloor$
 - $2n - 1$
 - $2n + 1$
4. Liczba elementów zbioru A^2 , które są jednocześnie minimalne i maksymalne względem porządku $\preceq$ wynosi
 - $n - 1$
 - 1
 - 0
 - $n + 1$
 - 2
5. Liczba elementów minimalnych w A^2 względem porządku $\preceq$ wynosi
 - n
 - $\lfloor \sqrt{2}n - 1 \rfloor$
 - $n + 1$
 - $2n - 1$
 - n^2
6. W $\langle A^2, \preceq \rangle$ istnieje łańcuch długości
 - n
 - $\lfloor \sqrt{2}n - 1 \rfloor$
 - $\lfloor n/2 \rfloor$
 - $n + 1$
 - 2

Rozwiązanie. Poniższy rysunek przedstawia kwadrat kartezjański zbioru

$$A = \{1, 2, 3, 4, 5\}$$

i pozwala opisać relację $\preceq$. Różne pary z A^2 są w relacji $\preceq$, jeżeli można na tym rysunku poprowadzić strzałkę od pierwszej (mniejszej) pary do drugiej (większej) i strzałka ta jest nachylona do prostej poziomej pod kątem przynajmniej takim, jak prosta a , i najwyżej takim, jak prosta b .



Strzałki znajdujące się na rysunku świadczą o tym, że $(2, 2) \preceq (5, 4)$ oraz $(3, 1) \preceq (4, 3)$. Analizując rysunek łatwo ustalić elementy minimalne w A^2 . Są to pary, w których nie może kończyć się żadna strzałka, a więc pary postaci $(1, i)$ oraz $(i, 1)$ dla $i = 1, 2, 3, 4, 5$. Widać też, że elementami maksymalnymi są pary postaci $(5, i)$ oraz $(i, 5)$ dla $i = 1, 2, 3, 4, 5$. Można także przekonać się, że najdłuższy łańcuch w A^2 ma postać

$$(1, 1) \prec (2, 2) \prec (3, 3) \prec (4, 4) \prec (5, 5).$$

Spostrzeżenia te łatwo uogólnia się i pozwala to rozwiązać zadanie 6.

Niech A oznacza teraz dowolny n elementowy ($n \geq 5$) zbiór liniowo uporządkowany. Przyjmijmy, że m oznacza najmniejszy element zbioru A , a M – element największy. Oczywiście, $m \neq M$.

Część 3. Przypuśćmy, że $(x, y) \in A^2$ oraz $x, y \neq m$. Wtedy $(m, m) \prec (x, y)$. Oznacza to, że pary (x, y) takie, że $x, y \neq m$ nie są elementami minimalnymi. To spostrzeżenie można też wyrazić stwierdzając, że zbiór elementów minimalnych w A^2 zawiera się w zbiorze

$$X = \{(m, x) \in A^2 : x \in A\} \cup \{(x, m) \in A^2 : x \in A\}.$$

Łatwo dowodzi się, że X jest zbiorem wszystkich elementów minimalnych w A^2 , a więc że każda należąca do niego para jest elementem minimalnym. Na przykład, dla każdego $x \in A$ para (m, x) jest elementem minimalnym. W przeciwnym razie musiałaby istnieć inna para (a, b) taka, że $(a, b) \prec (m, x)$. Wtedy zachodziłaby nierówność $a < m$ przecząca definicji m .

Teraz łatwo ustalić liczbę elementów minimalnych. Przekrój zbiorów $\{(m, x) \in A^2 : x \in A\}$ oraz $\{(x, m) \in A^2 : x \in A\}$ jest równy $\{(m, m)\}$. Zbiory te są n elementowe, ponieważ są równoliczne z A . Na przykład, funkcja $f : A \rightarrow \{(m, x) \in A^2 : x \in A\}$ zdefiniowana równością $f(x) = (m, x)$ jest bijekcją. Tak więc liczba elementów minimalnych w A^2 jest równa

$$|X| = |\{(m, x) \in A^2 : x \in A\}| + |\{(x, m) \in A^2 : x \in A\}| - |\{(m, m)\}| = 2n - 1.$$

Część 4. Podobnie, jak w przypadku elementów minimalnych, zbiór elementów maksymalnych jest równy

$$Y = \{(M, x) \in A^2 : x \in A\} \cup \{(x, M) \in A^2 : x \in A\}$$

i ma $2n - 1$ elementów. Wszystkie potrzebne fakty dowodzimy analogicznie.

Część 2. Dla każdego zbioru A o przynajmniej dwóch elementach, w zbiorze A^2 bez trudu znajdujemy trzy elementy minimalne: (M, m) , (m, m) oraz (m, M) . Jeżeli w jakimś zbiorze uporządkowanym są dwa elementy minimalne, to nie ma w nim elementu najmniejszego. Przypuśćmy, że jednak jest element najmniejszy i jest nim para (a, b) . Wtedy zachodzą nierówności $(a, b) \preceq (m, M)$ oraz $(a, b) \preceq (m, m)$. Ponieważ pary (m, M) i (m, m) są różne, więc przynajmniej w jednym przypadku mamy nierówność ostrą. Jeżeli $(a, b) \prec (m, M)$, to $a < m$. Przeczy to definicji m . Podobnie w drugim przypadku. Otrzymana sprzeczność świadczy o nieistnieniu w zbiorze A^2 elementu najmniejszego.

Część 6. Zbiór elementów A^2 , które są jednocześnie minimalne i maksymalne, to przekrój $X \cap Y$. Obliczymy ten zbiór. Zauważmy, że przekrój pierwszych składników z przedstawień zbiorów X i Y jest pusty (należące do nich pary różnią się pierwszą współrzędną). Podobnie jest w przypadku drugich składników. Ponadto,

$$\{(m, x) \in A^2 : x \in A\} \cap \{(x, M) \in A^2 : x \in A\} = \{(m, M)\},$$

a przekrój ostatniej pary składników jest równy $\{(M, m)\}$. Stąd nietrudno wywnioskować, że

$$X \cap Y = \{(m, M), (M, m)\}.$$

Wobec tego, w zbiorze A^2 są dwa takie elementy, które jednocześnie są minimalne i maksymalne, i są to (m, M) oraz (M, m) .

Część 5. Zajmiemy się teraz łańcuchami w A^2 . Jeżeli A jest zbiorem n elementowym, to łatwo zdefiniować łańcuch długości n . Tworzą go pary postaci (x, x) dla wszystkich $x \in A$. Pokażemy, że nie można z elementów A^2 utworzyć łańcucha dłuższego. Rozważmy funkcję $f : A^2 \rightarrow A$ przyporządkowującą parze (x, y) jej pierwszą współrzędną x . Jest to funkcja rosnąca, a więc warunek $(a, b) \prec (x, y)$ implikuje, że $a < x$. Funkcje rosnące są różnowartościowe. Wobec tego, długość dowolnego łańcucha jest równa liczbie elementów zbioru jego pierwszych współrzędnych. Ponieważ pierwsze współrzędne są elementami A , więc długość łańcuchów nie

przekracza $|A| = n$. W A^2 jest łańcuch długości n . Ponieważ fragment łańcucha też jest łańcuchem, więc są też łańcuchy długości 2 oraz $\lfloor n/2 \rfloor$. Nie ma natomiast łańcuchów długości $n+1$, ani $\lfloor \sqrt{2n} - 1 \rfloor$. Nie ma tych ostatnich, gdyż dla $n \geq 5$ zachodzi nierówność $n < \lfloor \sqrt{2n} - 1 \rfloor$.

Część 1. Każdy porządek w zbiorze skończonym jest regularny. Wynika to w sposób oczywisty wprost z definicji porządku regularnego. Wystarczy przypomnieć sobie tę definicję i/lub twierdzenie 141 ze strony 97 niniejszego skryptu.

Udowodnimy jeszcze podane twierdzenie korzystając z zasady indukcji (noetherowskiej dla zwykłego porządku w $\mathbb{N}$, patrz twierdzenie 144 na stronie 100 niniejszego skryptu). Weźmy niepusty zbiór uporządkowany A o n elementach i dowolny element $a \in A$. Może jest to element minimalny. W przeciwnym razie, zbiór

$$X = \{x \in A : x < a\}$$

jest niepusty, ma mniej elementów niż A (brakuje w nim np. a) i jest uporządkowany tą samą relacją, co zbiór A . Korzystając z założenia indukcyjnego znajdujemy element $m \in X$, który jest minimalny w zbiorze X . Element m jest także minimalny w zbiorze A . W przeciwnym razie w zbiorze A istniałby element x taki, że $x < m$. Ponieważ $x < m < a$, więc $x \in X$. Przeczy to jednak założeniu o tym, że m jest minimalny w zbiorze X .

Zadanie 542. Niech $f : \mathbb{N} \rightarrow \mathbb{N}$. Symbol f^n oznacza n -krotne złożenie funkcji f :

$$\begin{aligned} f^0(x) &= x, \\ f^{n+1}(x) &= f(f^n(x)), \end{aligned}$$

dla dowolnych $n, x \in \mathbb{N}$. Rozważmy relację $R \subseteq \mathbb{N} \times \mathbb{N}$ taką, że

$$xRy \Leftrightarrow \exists n, m \in \mathbb{N} \ f^n(x) = f^m(y).$$

Pokaż, że R jest relacją równoważności. Ile klas abstrakcji ma relacja R , jeżeli funkcja f jest zdefiniowana wzorem $f(x) = \lfloor x/2 \rfloor$? Opisz te klasy abstrakcji i uzasadnij odpowiedzi.

Rozwiązanie. Rozwiązanie zadania 2 powinno zawierać między innymi dowód zwrotności i symetryczności relacji R . Ten fragment zadania jest bardzo prosty, prawie oczywisty. Wiele osób miało jednak kłopoty z przedstawieniem rozwiązania. Były one spowodowane koniecznością posługiwania się kwantyfikatorami egzystencjalnymi. Te same problemy występują w dowodzie przechodniości relacji R . Zamiast dowodzić, że R jest relacją równoważności pokażemy tylko przechodniość R i zrobimy to bardzo szczegółowo.

Przechodniość relacji R . Przypuśćmy, że mamy funkcję f i posługując się tą funkcją zdefiniowaliśmy relację R . Weźmy trzy liczby naturalne x, y i z takie, że

xRy i yRz . Z definicji relacji R wynika, że

$$\exists n, m \in \mathbb{N} \ f^n(x) = f^m(y) \wedge \exists n, m \in \mathbb{N} \ f^n(y) = f^m(z).$$

W szczególności, istnieją liczby naturalne n i m takie, że zachodzi równość $f^n(x) = f^m(y)$. Zwrot „istnieją liczby” znaczy, że takie liczby są. Być może nie wiemy jakie to liczby, może ich wyliczenie jest bardzo trudne i tego jeszcze nie zrobiliśmy, a może konkretna wartość tych liczb nie jest dla nas istotna. Ale mamy gwarancję, że one są. Symbole n i m raczej nie oznaczają tych liczb. Pomagają jedynie wyrazić własności, których oczekujemy od tych liczb: jedna z nich powinna pojawić się w równości $f^n(x) = f^m(y)$ w miejscu n , druga – w miejscu m . Jeżeli te liczby są, to albo możemy ustalić ich wartość, albo przynajmniej możemy sobie wyobrażać, że to zrobiliśmy. Wtedy możemy je oznaczyć. Przyjmijmy, że są to liczby a i b . Dokładniej, a jest tą liczbą, która odpowiada symbolowi n , zaś b odpowiada symbolowi m . Liczby a i b zostały więc wybrane tak, aby zachodziła równość $f^a(x) = f^b(y)$.

W podobny sposób z drugiej części założenia możemy wywnioskować, że są liczby c i d takie, że $f^c(y) = f^d(z)$.

Jeżeli $f^a(x) = f^b(y)$, to także $f^{a+1}(x) = f(f^a(x)) = f(f^b(y)) = f^{b+1}(y)$. Nakładając jeszcze raz f na obie strony otrzymanej równości dostajemy równość $f^{a+2}(x) = f^{b+2}(y)$. Łatwo udowodnić przez indukcję, że równość $f^{a+k}(x) = f^{b+k}(y)$ zachodzi dla wszystkich liczb naturalnych k . Wobec tego, zachodzi także równość $f^{a+c}(x) = f^{b+c}(y)$. W ten sam sposób z równości $f^c(y) = f^d(z)$ możemy wywnioskować, że $f^{b+c}(y) = f^{b+d}(z)$. Ponieważ równość jest przechodnia, więc $f^{a+c}(x) = f^{b+d}(z)$. Są więc takie liczby $n = a + c$ i $m = b + d$, że $f^n(x) = f^m(z)$. Tym samym wykazaliśmy istnienie liczb n i m spełniających równość $f^n(x) = f^m(z)$.

Dowiedliśmy więc, że xRz , a przeprowadzone rozumowanie uzasadnia przechodność relacji R .

Klasy abstrakcji R . Łatwo zauważyć, że jeżeli funkcja f jest zdefiniowana wzorem $f(x) = \lfloor x/2 \rfloor$, to dla dowolnego n odpowiednie, wielokrotne złożenie funkcji f przyporządkowuje liczbie n wartość 0. Zgodnie z definicją relacji R fakt ten oznacza, że $0Rn$. Tak więc 0 jest w relacji R z dowolną liczbą naturalną n . Wykażemy to w sposób bardziej precyzyjny korzystając z zasady indukcji. W dowodzie zastosujemy indukcję noetherowską.

Niech n będzie dowolną liczbą naturalną. Jako założenie indukcyjne przyjmujemy, że własność $0Rm$ zachodzi dla wszystkich liczb naturalnych $m < n$. Chcemy wykazać, że także zachodzi własność $0Rn$. Jeżeli $n = 0$, to zwrotność relacji R gwarantuje, że $0Rn$. Dalej możemy więc zakładać, że n jest liczbą dodatnią. Wtedy

$$f(n) = \lfloor n/2 \rfloor \leq n/2 < n.$$

Oznacza to, że dla liczby $f(n)$ możemy skorzystać z założenia indukcyjnego. W ten

sposób otrzymujemy, że $0Rf(n)$. Z definicji relacji R bez trudu wynika, że $f(n)Rn$. Ponieważ relacja R jest przechodnia, więc także $0Rn$.

Klasa abstrakcji $[0]$ relacji R wyznaczona przez 0 jest zawarta w zbiorze liczb naturalnych. Wykazaliśmy też, że zawiera wszystkie liczby naturalne. Wobec tego, $[0] = \mathbb{N}$. Ponieważ klasy abstrakcji relacji R są niepuste i tworzą podział $\mathbb{N}$, więc R nie może mieć innych klas abstrakcji.

Zadanie 543. Czy istnieje relacja równoważności

- (a) w zbiorze $\mathbb{N}$, której wszystkie klasy abstrakcji są nieskończone i jest ich nieskończenie wiele?
- (b) w zbiorze $\mathbb{R}$, której wszystkie klasy abstrakcji są przeliczalne i jest ich przeliczalnie wiele?

Rozwiązanie. Aby rozwiązać to zadanie, dobrze jest przypomnieć sobie zasadę abstrakcji (twierdzenie 68). Zasadę tę przedstawimy teraz nieco nieformalnie. Stwierdza ona, że zamiast zajmować się relacjami równoważności można (w sposób równoważny) zajmować się podziałami na klasy abstrakcji.

Zamiast pytać się o istnienie relacji równoważności, przeformułujemy zadanie i najpierw zapytamy o istnienie odpowiedniego podziału, np. podziału zbioru liczb naturalnych na nieskończenie wiele zbiorów nieskończonych. Na to pytanie odpowiedź jest pozytywna.

Wyobraźmy sobie kwadrat. Jeden z jego boków nazwiemy podstawą, drugi, sąsiadujący z pierwszym – wysokością. Nietrudno zauważyć, że kwadrat można podzielić na odcinki równoległe do podstawy. Każdy z nich ma tyle punktów, co podstawa, i jest ich tyle, co punktów wysokości. Podobnie jest z kwadratem kartezjańskim zbioru liczb naturalnych. Oczywiście,

$$\mathbb{N}^2 = \bigcup_{n \in \mathbb{N}} \{\langle i, n \rangle : i \in \mathbb{N}\} = \bigcup_{n \in \mathbb{N}} L_n$$

dla zbiorów $L_n = \{\langle i, n \rangle : i \in \mathbb{N}\}$. Tak więc zbiór $\mathbb{N}^2$ można podzielić na nieskończenie wiele zbiorów L_n , z których każdy jest nieskończony.

Zbiory L_n tworzą podział (wszystkie razem, dokładniej: podziałem jest rodzina $\{L_n : n \in \mathbb{N}\}$). Oczywiście, zbiory L_n są niepuste. Dla różnych liczb n i m mamy $L_n \cap L_m = \emptyset$. Aby się o tym przekonać wystarczy zauważyć, że w przeciwnym razie, z należenia pewnej pary do przekroju $L_n \cap L_m$ wynika, że pierwsza współrzędna tej pary jest jednocześnie równa n i m , co nie jest możliwe. Ostatnim warunek z definicji podziału został już wcześniej zauważony.

Nieskończoność zbioru L_n (dla każdej, ustalonej liczby n) jest konsekwencją równoliczności zbioru L_n ze zbiorem liczb naturalnych. Równoliczność ustala oczywiście funkcja $k_n : \mathbb{N} \rightarrow L_n \subseteq \mathbb{N}^2$ zdefiniowana wzorem $k_n(i) = \langle i, n \rangle$.

Nieskończoność całej rodziny zbiorów dowodzimy pokazując, że funkcja $l : \mathbb{N} \rightarrow \{L_n : n \in \mathbb{N}\}$ taka, że $l(n) = L_n$, jest bijekcją.

Tak więc udało się nam zdefiniować nieskończony podział zbioru $\mathbb{N}^2$ na nieskończone zbiory. A mieliśmy to zrobić dla zbioru $\mathbb{N}$. Możemy teraz skorzystać z równoliczności $\mathbb{N}$ i $\mathbb{N}^2$.

Niech $f : \mathbb{N} \rightarrow \mathbb{N}^2$ będzie bijekcją. Przyjmijmy, że

$$X_n = \vec{f}^{-1}(L_n) = \{j \in \mathbb{N} : f(j) \in L_n\}.$$

Tak zdefiniowane zbiory, czyli przeciwobrazy zbiorów L_n wyznaczone przez funkcję f , tworzą podział zbioru liczb naturalnych. Pomijam szczegółowy dowód tego faktu, wszystko, co trzeba, wynika z własności przeciwobrazów.

Przedstawione rozwiązanie miało pokazać, jak można znaleźć potrzebny podział zbioru liczb naturalnych. Osoby, które mają już trochę doświadczenia, mogą konstruować podziały zbioru liczb naturalnych na wiele sposobów. Możemy np. przyjąć, że

$$Y_n = \{2^n \cdot i \in \mathbb{N} : i \in \mathbb{N}\},$$

albo, posługując się ciągiem $\langle p_n \rangle_{n \in \mathbb{N}}$ kolejnych liczb pierwszych, zdefiniować zbiory

$$Z_n = \{i \in \mathbb{N} : p_n \text{ dzieli } i \wedge \forall k < n \ p_k \text{ nie dzieli } i\}.$$

Rodziny $\{Y_n : n \in \mathbb{N}\}$ oraz $\{Z_n : n \in \mathbb{N}\}$ też tworzą nieskończone podziały zbioru liczb naturalnych złożone ze zbiorów nieskończonych.

Mając podział $\{X_n : n \in \mathbb{N}\}$ zbioru liczb naturalnych należy jeszcze wskazać relację równoważności R , której klasy równoważności tworzą ten właśnie podział. Odnoszę wrażenie, że powinno teraz wystarczyć powołanie się na zasadę abstrakcji. Niemal równie łatwo jest powtórzyć dowód zasady abstrakcji. Trzeba zdefiniować R i można to zrobić na dwa sposoby: albo pisząc

$$R = \bigcup_{n \in \mathbb{N}} X_n^2,$$

albo, w sposób równoważny,

$$aRb \iff \exists n \in \mathbb{N} \langle a, b \rangle \in X_n^2.$$

Sprawdzenie, że tak zdefiniowana relacja R jest relacją równoważności nie powinno być trudne. Łatwo też wykazać, że klasa abstrakcji $[a]_R$ jest tym zbiorem X_n , do którego należy liczba a .

Drużga część zadania (część (b)) też wynika z zasady abstrakcji, ale w tym przypadku odpowiedź jest negatywna. Nie istnieje relacja równoważności w zbiorze $\mathbb{R}$, która ma przeliczalnie wiele przeliczalnych klas abstrakcji. Zgodnie z zasadą abstrakcji, suma mnogościowa wszystkich klas abstrakcji relacji równoważności jest dziedziną relacji, a więc w rozważanym przypadku — zbiorem liczb rzeczywistych $\mathbb{R}$.

Ze znanego i ważnego twierdzenia o sumowaniu zbiorów przeliczalnych wynika, że jeżeli sumujemy przeliczalną rodzinę takich zbiorów, to otrzymujemy zbiór przeliczalny. Gdyby więc istniała taka relacja, zbiór liczb rzeczywistych byłby przeliczalny. Zbiór liczb rzeczywistych nie jest jednak przeliczalny (jest to twierdzenie Cantora), a uzyskana w ten sposób sprzeczność dowodzi, że nie istnieje interesująca nas relacja równoważności.

Zadanie 544. Udowodnij, że jeśli $\{A_i\}_{i \in \mathbb{N}}$ jest indeksowaną rodziną skończonych zbiorów liczb naturalnych, to uogólniony iloczyn kartezjański $\prod_{i \in \mathbb{N}} A_i$ jest zbiorem skończonym lub ma moc co najmniej continuum.

Rozwiązanie. W tym zadaniu pierwszą trudnością do pokonania jest mnogość sytuacji, jakie mogą wystąpić. Będziemy więc rozważać kilka przypadków. Zrobimy to też w sposób bardziej szczegółowy, niż było to wymagane na egzaminie.

Przypadek 1: dla pewnego $i \in \mathbb{N}$ zbiór A_i jest pusty. Z warunku $\alpha \in \prod_{i \in \mathbb{N}} A_i$ łatwo wyprowadzić sprzeczność, gdyż $\alpha(i) \in A_i$ dla wszystkich i , także dla i takiego, że $A_i = \emptyset$. Wobec tego, zbiór $\prod_{i \in \mathbb{N}} A_i$ jest pusty, a więc skończony.

Przypadek 2: wszystkie zbiory A_i są niepuste. Zdefiniujmy zbiór I wzorem

$$I = \{i \in \mathbb{N} : |A_i| \geq 2\}.$$

Przypadek 2.1: $I = \emptyset$ W tym przypadku równość $|A_i| = 1$ zachodzi dla wszystkich $i \in \mathbb{N}$ i warunek

$$\alpha(i) \in A_i$$

definiuje funkcję α określoną w zbiorze liczb naturalnych $\mathbb{N}$. Przytoczoną definicję można też wyrazić nieco inaczej: $\alpha(i)$ jest tym (jedynym) elementem, który należy do A_i . To, że wszystkie zbiory A_i są jednoelementowe, gwarantuje, że wartości $\alpha(i)$ są dobrze zdefiniowane. Jeżeli zgodzimy się z tym, że funkcja α jest dobrze zdefiniowana, to stwierdzenie, że $\alpha \in \prod_{i \in \mathbb{N}} A_i$ nie budzi wątpliwości. Tak więc interesujący nas zbiór ma przynajmniej jeden element. Pokażemy jeszcze, że nie może mieć dwóch elementów.

Gdyby dwie (różne) funkcje α i β należały do uogólnionego iloczynu $\prod_{i \in \mathbb{N}} A_i$, to musiałyby się różnić dla pewnego argumentu. Przyjmijmy, że $\alpha(i_0) \neq \beta(i_0)$. Wtedy zbiór A_{i_0} musiałby mieć przynajmniej dwa elementy, właśnie $\alpha(i_0)$ oraz $\beta(i_0)$. Uzyskana sprzeczność dowodzi, że produkt $\prod_{i \in \mathbb{N}} A_i$ ma najwyżej jeden element. Ostatecznie otrzymujemy, że w rozważanym przypadku jest to zbiór jednoelementowy, a więc skończony.

Przypadek 2.2: zbiór I jest niepusty i skończony. Najpierw pokażemy, że na moc (liczbę elementów) produktu uogólnionego nie mają wpływu te zbiory A_i , które są jednoelementowe. Zauważmy, że uogólnione produkty

$$\prod_{i \in \mathbb{N}} A_i \text{ oraz } \prod_{i \in I} A_i$$

są równoliczne. Aby to wykazać, definiujemy funkcję

$$f : \prod_{i \in \mathbb{N}} A_i \rightarrow \prod_{i \in I} A_i$$

przyjmując, że

$$f(\alpha) = \alpha|I$$

($\alpha|I$ oznacza obcięcie funkcji α do zbioru I , czyli funkcję określoną na I i przyjmującą dla dowolnego argumentu te same wartości, co α), a następnie pokazujemy, że jest to bijekcja.

Tak więc, aby wykazać skończoność zbioru $\prod_{i \in \mathbb{N}} A_i$, wystarczy wykazać skończoność zbioru $\prod_{i \in I} A_i$. Ten zbiór składa się z funkcji $\alpha : I \rightarrow \bigcup_{i \in I} A_i$, a więc jest podzbiorem $(\bigcup_{i \in I} A_i)^I$. Ten ostatni zbiór jest skończony i wynika to ze znanych twierdzeń: suma skończonej rodziny zbiorów skończonych jest zbiorem skończonym, oraz stwierdzającego, że jest skończenie wiele funkcji określonych na ustalonym, skończonym zbiorze i przyjmujących wartości w ustalonym skończonym zbiorze.

Przypadek 2.3: zbiór I jest nieskończony. Ponieważ $I \subseteq \mathbb{N}$, więc istnieje bijekcja $f : I \rightarrow \mathbb{N}$. Postępując się f zdefiniujemy różnowartościową funkcję

$$F : \{0, 1\}^{\mathbb{N}} \rightarrow \prod_{i \in \mathbb{N}} A_i.$$

Przyjmijmy, że

$$F(\alpha)(i) = \begin{cases} \min A_i & \text{jeżeli } \alpha(f(i)) = 0 \text{ oraz } i \in I \\ \max A_i & \text{jeżeli } \alpha(f(i)) = 1 \text{ oraz } i \in I \\ \min A_i & \text{jeżeli } i \notin I. \end{cases}$$

Jest oczywiste, że $F(\alpha) \in \prod_{i \in \mathbb{N}} A_i$ dla dowolnej funkcji $\alpha \in \{0, 1\}^{\mathbb{N}}$. Aby dowieść różnowartościowość F , weźmy dwie różne funkcje $\alpha, \beta \in \{0, 1\}^{\mathbb{N}}$. Przyjmijmy, że $\alpha(s) \neq \beta(s)$. Możemy dodatkowo założyć, że $\alpha(s) = 0$ i $\beta(s) = 1$. Korzystając z tego, że f jest bijekcją, bierzemy $t \in I$ takie, że $f(t) = s$. Z definicji F otrzymujemy, że $F(\alpha)(t) = \min A_t$ oraz $F(\beta)(t) = \max A_t$. Ponieważ $t \in I$, więc zbiór A_t ma przynajmniej dwa elementy. Tak więc $\min A_t < \max A_t$. Stąd wynika, że $F(\alpha)(t) < F(\beta)(t)$ oraz $F(\alpha) \neq F(\beta)$.

Zbiór $\{0, 1\}^{\mathbb{N}}$ ma moc continuum. Z istnienia różnowartościowej funkcji F wynika, że zbiór $\prod_{i \in \mathbb{N}} A_i$ ma moc nie mniejszą niż continuum. Łatwo też można dowieść, że jest mocy continuum.

Komentarz. Zadanie to pozostaje prawdziwe, jeżeli zamiast $\mathbb{N}$ weźmiemy dowolny, niepusty zbiór indeksów X . Wtedy jednak nie będziemy wiedzieć o zbiorze I , że jest podzbiorem $\mathbb{N}$ i – w przypadku, gdy I jest nieskończony – będziemy musieli

wykazać, że istnieje różnowartościowa funkcja $f: \mathbb{N} \rightarrow I$. Często to się robi w następujący sposób: wybiera się dowolny element $i_0 \in I$ i przyjmuje, że $f(0) = i_0$, a następnie definiuje $f(n)$ jako wybrany element zbioru $I \setminus \{f(0), \dots, f(n-1)\}$ (nieskończoność I gwarantuje niepustość tej różnicy). Wiadomo jednak, że takie rozumowanie nie spełnia rygorystycznie rozumianych zasad logiki. Ale bywa też uznawane za poprawne. Podobne rozumowanie jest potrzebne w dowodzie równoważności dwóch definicji ciągłości funkcji w punkcie, podanych przez Cauchy'ego i Heinego. Proponuje obejrzeć dowód tej równoważności w podręcznikach do analizy matematycznej.

Dowody matematyczne muszą być skończone, dawać się w pełni zapisać i to bez używania trzech kropek $\dots$. Reguła dowodzenia nazywana regułą opuszczania kwantyfikatora egzystencjalnego pozwala wybrać jeden z wielu elementów, których istnienie jest zagwarantowane. Posługując się tą regułą możemy przytoczonym dowodzie zdefiniować $f(0)$, następnie $f(1)$, a nawet wartości funkcji f np. dla miliarda argumentów (w jakimś bardzo długim dowodzie), ale nie możemy tej reguły zastosować nieskończenie wiele razy. Przytoczony schemat definiowania funkcji f nie jest też poprawną definicją rekurencyjną (proszę starannie przeczytać sformułowanie twierdzenia o definiowaniu przez indukcję). Może jednak zostać wyprowadzony z aksjomatu wyboru: ten aksjomat m.in. pozwala nadać mu postać poprawnej definicji indukcyjnej. Aby dowiedzieć się coś więcej o aksjomacie wyboru, proponuję zajrzeć do książek poświęconych teorii mnogości.

Podobne kłopoty wystąpią w zadaniu 12, gdy opuścimy założenie, że A_i są zbiorami liczb naturalnych.

Uwaga. Proponowałbym, aby wzór

$$\left| \prod_{i=1}^n A_i \right| = \prod_{i=1}^n |A_i|$$

– słuszny dla skończonych zbiorów A_i – dowodzić przez indukcję, korzystając znanego wzoru $|A \times B| = |A| \cdot |B|$ (A i B to zbiory skończone, $|A|$ oznacza liczbę elementów zbioru A) i faktu: zbiory

$$\prod_{i=1}^n A_i \quad \text{oraz} \quad \left(\prod_{i=1}^{n-1} A_i \right) \times A_n$$

są równoliczne.

Zadanie 545. (a) Niech $\langle A, \leq \rangle$ będzie skończonym zbiorem częściowo uporządkowanym. Udowodnij, że jeśli A ma element najmniejszy, to $\langle A, \leq \rangle$ jest porządkiem zupełnym.

(b) Niech $\langle A, \leq \rangle$ będzie skończonym porządkiem zupełnym. Udowodnij, że jeśli funkcja $f: A \rightarrow A$ jest monotoniczna, to jest ciągła.

Rozwiązanie (część a). Na mocy założenia w zbiorze A jest element najmniejszy.

Należy jeszcze wykazać, że każdy skierowany podzbiór A ma kres górny. Najpierw wykażę pomocniczy fakt.

Fakt 205. W każdym skończonym, niepustym zbiorze skierowanym jest element największy.

Dowód. W dowodzie skorzystam z indukcji ze względu na liczbę elementów. Oczywiście, w zbiorze jednoelementowym jego jedyny element jest największym.

Założmy, że X jest skierowany i ma $n + 1$ elementów. W każdym niepustym i skończonym zbiorze uporządkowanym jest element minimalny. Przyjmijmy, że x_0 jest elementem minimalnym w X . Zbiór $X \setminus \{x_0\}$ ma n elementów i jest skierowany. Gdyby bowiem usunięcie x_0 spowodowało, że pewna para nie ma ograniczenia, to x_0 byłby niemniejszy od każdego elementu tej pary, i nie mógłby być elementem minimalnym.

Na mocy założenia indukcyjnego, zbiór $X \setminus \{x_0\}$ ma element największy. Niech to będzie element a . Ponieważ X jest zbiorem skierowanym, możemy z X wybrać element b taki, że $a \leq b$ oraz $x_0 \leq b$. Nietrudno zauważyć, że b jest elementem największym w X . Jest on większy od wszystkich elementów $X \setminus \{x_0\}$, ponieważ $a \leq b$ i oczywiście jest większy od jedyne elementu X spoza tego zbioru, czyli x_0 .

Trzeba jeszcze zauważyć, że jeżeli w jakimś zbiorze X jest element największy a , to jest on kresem górnym zbioru X . Element a ogranicza zbiór X z góry, ponieważ jest największy. Jest on też mniejszy lub równy od każdego ograniczenia górnego zbioru X , ponieważ jest jednym z elementów zbioru X .

Rozwiązanie (część b). Przypuśćmy, że $f : A \rightarrow A$ jest funkcją monotoniczną. Należy wykazać, że f zachowuje kresy górne zbiorów skierowanych. Weźmy więc dowolny zbiór skierowany $X \subseteq A$ i niech m będzie jego kresem górnym. Zbiór X jest skończony, ponieważ A jest skończony. W takiej sytuacji, kres górny m jest również elementem największym w zbiorze X i, co najważniejsze, należy do X . Można to wywnioskować np. z jednoznaczności pojęcia kresu i tego, że element największy też jest kresem górnym.

Teraz powinniśmy dowieść, że $f(m)$ jest kresem górnym obrazu $\vec{f}(X)$. Element $f(m)$ jest ograniczeniem górnym obrazu. Dowolny element $\vec{f}(X)$ jest postaci $f(x)$ dla pewnego $x \in X$ i zachodzi $x \leq m$, gdyż m ogranicza zbiór X z góry. Stąd $f(x) \leq f(m)$ na mocy założenia o monotoniczności funkcji f . Element $f(m)$ jest najmniejszym ograniczeniem górnym obrazu, ponieważ $f(m) \in \vec{f}(X)$ i jest również jednym z ograniczanych elementów.

Zadanie 546. W zbiorze Fin wszystkich skończonych podzbiorów zbioru liczb naturalnych określamy relację $\preceq$ w następujący sposób. Dla zbiorów $X, Y \in Fin$ zachodzi

$X \preceq Y$ wtedy i tylko wtedy, gdy

$$X = Y \text{ lub } \max(X \dot{-} Y) \in Y,$$

gdzie $\dot{-}$ oznacza różnicę symetryczną, a $\max(A)$ jest największą w sensie naturalnego porządku liczbą w zbiorze A . Udowodnij, że $\langle \text{Fin}, \preceq \rangle$ jest dobrym porządkiem.

Rozwiązanie. Będziemy sprawdzać po kolei wszystkie warunki z definicji dobrego porządku.

Zwrotność. Ten warunek jest wynikiem z definicji porządku $\preceq$ w sposób oczywisty.

Zauważmy teraz dwa oczywiste fakty.

Fakt 206. Jeżeli X i Y są różnymi zbiorami, to warunki $n \in X$ i $n \in Y$ są równoważne dla wszystkich $n > \max(X \dot{-} Y)$.

Fakt 207. Jeżeli $\max(X \dot{-} Y) \in Y$, to $\max(X \dot{-} Y) \notin X$.

Słaba antysymetryczność. Dowód przeprowadzimy metodą nie wprost. Załóżmy, że mamy dwa zbiory X i Y takie, że $X \preceq Y$ i $Y \preceq X$, które – na mocy założenia dowodu nie wprost – są różne.

Ponieważ $X \neq Y$, więc nierówności między tymi zbiorami implikują, że $\max(X \dot{-} Y) \in Y$ oraz $\max(Y \dot{-} X) = \max(X \dot{-} Y) \in X$. Z drugiego faktu otrzymujemy, że $\max(X \dot{-} Y) \notin X$. Uzyskana w ten sposób sprzeczność dowodzi, że relacja $\preceq$ jest słabo antysymetryczna.

Przechodność. Dość trudno podać ideę dowodu przechodności relacji $\preceq$, ale jest widoczne podobieństwo tego porządku i porządku antyleksykograficznego. Jeżeli ograniczamy się np. do trzech zbiorów skończonych, to możemy je uważać za podzbiory zbioru liczb naturalnych mniejszych od pewnego $n \in \mathbb{N}$ i utożsamiać w zwykły sposób z ciągami zerojedynkowymi długości n . Przy takim utożsamianiu zbiorów i ciągów, porządek $\preceq$ odpowiada właśnie porządkowi antyleksykograficznemu w zbiorze ciągów. Dalej przechodność udowodnimy być może w sposób mało intuicyjny, ale naśladujący dowód przechodności dla porządku (anty)leksykograficznego.

Weźmy trzy zbiory X , Y i Z i załóżmy, że $X \preceq Y$ i $Y \preceq Z$. Symbol $X \prec Y$ będzie oznaczać, że $X \preceq Y$ i $X \neq Y$. Nietrudno zauważyć, że dowód przechodności wystarczy przeprowadzić tylko dla zbiorów parami różnych. Możemy więc założyć, że $X \prec Y$ oraz $Y \prec Z$ i z tego założenia mamy wyprowadzić, że $X \preceq Z$.

Symbolem m oznaczamy $\max(X \dot{-} Y)$. Wiemy (na mocy przyjętych założeń), że $m \in Y$ i $m \notin X$.

Przypadek 1: $\max(Y \dot{-} Z) < m$. W tym przypadku, $\max(X \dot{-} Z) = m$. Wynika to z dwóch spostrzeżeń: Po pierwsze, dla $n > m$ warunki $n \in X$, $n \in Y$ oraz $n \in Z$ są jednocześnie albo prawdziwe, albo fałszywe. W szczególności, dla $n > m$ warunki $n \in X$ oraz $n \in Z$ są równoważne. Z drugiej strony, warunek $m \in X$ jest fałszywy, warunek $m \in Y$ jest prawdziwy i równoważny warunkowi $m \in Z$.

Jeżeli już dowiedliśmy równość $\max(X \dot{-} Z) = m$, to z powyższego rozumowania otrzymujemy jeszcze, że $\max(X \dot{-} Z) \in Z$. Tak więc $X \prec Z$ i, tym bardziej, $X \preceq Z$.

Przypadek 2: $\max(Y \dot{-} Z) = m$. Ta sytuacja prowadzi do sprzeczności i nie może zajść. Liczba $m = \max(Y \dot{-} Z)$ należy bowiem do Z , gdyż $Y \prec Z$. Z faktu 2 otrzymujemy, że $m \notin Y$. Ale m należy także do Y , ponieważ $X \prec Y$.

Przypadek 3: $\max(Y \dot{-} Z) > m$. W tym przypadku, dla $n > \max(Y \dot{-} Z)$ warunki $n \in X$, $n \in Y$ i $n \in Z$ mają tę samą wartość logiczną. Podobnie, warunki $\max(Y \dot{-} Z) \in X$ i $\max(Y \dot{-} Z) \in Y$ są równoważne. Co więcej, wobec nierówności $Y \prec Z$, są fałszywe. Wiemy też, że warunek $\max(Y \dot{-} Z) \in Z$ jest prawdziwy.

Z tych faktów otrzymujemy, że $\max(X \dot{-} Z) = \max(Y \dot{-} Z) \in Z$. Oznacza to, że zarówno $X \prec Z$, jak i $X \preceq Z$.

Liniowość. Aby dowieść liniowość porządku $\preceq$, wystarczy z założenia $X \neq Y$ wywnioskować, że albo $X \prec Y$, albo $Y \prec X$. Jest oczywiste, że jeżeli $X \neq Y$, to różnica symetryczna $X \dot{-} Y$ jest niepusta, liczba $\max(X \dot{-} Y)$ jest dobrze określona (pamiętajmy, że X i Y są skończone) oraz

$$\max(X \dot{-} Y) \in X \dot{-} Y = (X \setminus Y) \cup (Y \setminus X).$$

Stąd wynika, że $\max(X \dot{-} Y) \in X$ (i wtedy $Y \prec X$) lub też $\max(X \dot{-} Y) \in Y$ (czyli $X \prec Y$).

Regularność. Aby dowieść regularność porządku $\prec$, trzeba najpierw zauważyć

Fakt 208. Jeżeli $X \preceq Y$, to $X \subseteq \{i \in \mathbb{N} : i \leq \max(Y)\}$.

Dowód. Zauważmy, że liczba $\max(X \dot{-} Y) \in Y$ i jest mniejsza od $\max(Y)$. Elementy zbioru X dzielą na mniejsze lub równe $\max(X \dot{-} Y)$ i, z tego powodu, mniejsze od $\max(Y)$ oraz na większe od $\max(X \dot{-} Y)$. Te większe – na mocy pierwszego faktu – należą do Y i dlatego nie przekraczają $\max(Y)$.

Załóżmy, że relacja $\preceq$ nie jest regularna. Istnieje więc nieskończony, zstępujący ciąg zbiorów $X_i \in \text{Fin}$. Ten ciąg spełnia więc nierówność

$$X_{n+1} \prec X_n$$

dla wszystkich $n \in \mathbb{N}$. Z przechodniości porządku $\prec$ otrzymujemy, że

$$X_n \prec X_m$$

dla wszystkich liczb liczb spełniających nierówność $n > m$. Stąd wynika, że funkcja $f : \mathbb{N} \rightarrow \text{Fin}$ zdefiniowana wzorem $f(n) = X_n$ jest różnowartościowa. Z nierówności $X_n \prec X_0$ i trzeciego faktu wynika też, że

$$X_n \subseteq [0, \max X_0] = \{i \in \mathbb{N} : i \leq \max X_0\}.$$

Wobec tego, zbiór $[0, \max X_0]$ jest skończony i ma nieskończenie wiele podzbiorów. Jest to niemożliwe, a uzyskana sprzeczność dowodzi regularności $\preceq$.

Zadanie 547. Jeśli φ jest formułą rachunku zdań, to przez $V(\varphi)$ oznaczamy zbiór zmiennych zdaniowych występujących w φ . Niech $\varphi, \varphi_1, \dots, \varphi_n, \psi$ będą formułami rachunku zdań.

- (a) Udowodnij, że $(\bigvee_{i=1}^n \varphi_i) \rightarrow \psi$ jest tautologią wtedy i tylko wtedy, gdy $\varphi_i \rightarrow \psi$ są tautologiami dla wszystkich $i \in \{1, \dots, n\}$.
- (b) Niech p będzie zmienną zdaniową nie występującą w φ ani w ψ . Udowodnij, że $\varphi \wedge p \rightarrow \psi$ jest tautologią wtedy i tylko wtedy, gdy $\varphi \rightarrow \psi$ jest tautologią.
- (c) Udowodnij, że jeśli $\varphi \rightarrow \psi$ jest tautologią, to istnieje taka formuła rachunku zdań ρ , że $V(\rho) = V(\varphi) \cap V(\psi)$ oraz $\varphi \rightarrow \rho$ i $\rho \rightarrow \psi$ są tautologiami.

Rozwiązanie zadania 547 (a). Nietrudno zauważyć, że to zadanie wystarczy rozwiązać dla $n = 2$. Oczywiście, także to spostrzeżenie wymaga jakiegoś uzasadnienia. Zaczniemy od rozwiązania w tym prostym przypadku.

1. Jest wiele metod rozwiązywania tego zadania. Możemy np. zauważyć, że formuła

$$((\varphi_1 \vee \varphi_2) \rightarrow \psi) \longleftrightarrow ((\varphi_1 \rightarrow \psi) \wedge (\varphi_2 \rightarrow \psi))$$

jest tautologią. Fakt ten można sprawdzić metodą zerojedynkową (choć nie polecałbym tej metody). Jeżeli równoważność jest tautologią, to oczywiście lewa strona tej równoważności jest tautologią wtedy i tylko wtedy, gdy prawa jest tautologią.

2. Można też bezpośrednio dowieść implikacje w obie strony. Na przykład założymy, że formuły $\varphi_1 \rightarrow \psi$ oraz $\varphi_2 \rightarrow \psi$ są tautologiami. Spróbujemy dowieść, że także formuła φ

$$(\varphi_1 \vee \varphi_2) \rightarrow \psi$$

jest tautologią. W tym celu bierzemy dowolne wartościowanie zmiennych zdaniowych σ i staramy się wyliczyć wartość logiczną $\hat{\sigma}((\varphi_1 \vee \varphi_2) \rightarrow \psi)$. Możemy założyć, że $\hat{\sigma}(\varphi_1 \vee \varphi_2) = \top$ (w przeciwnym razie, cała implikacja miałaby przy wartościowaniu σ wartość logiczną $\top$). Tak więc jeden z członów alternatywy ma przy wartościowaniu σ wartość logiczną $\top$. Przyjmimy, że $\hat{\sigma}(\varphi_1) = \top$. Założyliśmy jednak, że $\varphi_1 \rightarrow \psi$ jest tautologią, a więc $\hat{\sigma}(\varphi_1 \rightarrow \psi) = \top$. Stąd otrzymujemy, że $\hat{\sigma}(\psi) = \top$ oraz każda implikacja o następniku ψ (także φ) ma przy wartościowaniu σ wartość logiczną $\top$.

Dowiedliśmy, że formuła φ ma wartość logiczną $\top$ przy każdym wartościowaniu. Tak więc jest to tautologia.

3. Implikację odwrotną można dowieść przedstawionymi metodami i proponuję zrobić to jako ćwiczenie. Teraz przedstawię pewien argument świadczący o prawdziwości tej implikacji (można uważać go za mało zrozumiały dowód). Zauważmy, że można uzasadnić każdą formułę o następującym schemacie

$$((\varphi_1 \vee \varphi_2) \rightarrow \psi) \rightarrow (\varphi_1 \rightarrow \psi).$$

Tak jest, ponieważ z każdego członu potrafimy wywnioskować alternatywę. Jeżeli więc z alternatywy potrafimy wywnioskować ψ , to tę formułę potrafimy wywnioskować także dowolnego członu tej alternatywy.

4. Słuszność równoważności z zadania w pełnej ogólności łatwo dowodzi się przez indukcję ze względu na n . Jest oczywiste, że równoważność zachodzi dla $n = 1$. Wtedy obie strony równoważności mówią to samo. Aby przeprowadzić drugi krok dowodu indukcyjnego wystarczy zauważyć, że następujące stwierdzenia są równoważne

(a) $(\bigvee_{i=1}^{n+1} \varphi_i) \rightarrow \psi$ jest tautologią,

(b) $(\bigvee_{i=1}^n \varphi_i) \rightarrow \psi$ oraz $\varphi_{n+1} \rightarrow \psi$ są tautologiami,

(c) formuły $\varphi_i \rightarrow \psi$ są tautologiami dla wszystkich i takich, że $1 \leq i \leq n + 1$.

Równoważność warunków (a) i (b) wynika np. z punktu 1, a warunków (b) i (c) — z założenia dowodu indukcyjnego.

Rozwiązanie zadania 547 (b). To zadanie jest bardzo podobne do poprzedniego, ale tym razem nie da się zastosować metody z punktu 1. Formuły

$$(\varphi \rightarrow \psi) \longleftrightarrow ((\varphi \wedge p) \rightarrow \psi)$$

nie są bowiem tautologiami. Jednak otrzymujemy tautologię, jeżeli znak $\longleftrightarrow$ zastąpimy przez $\rightarrow$. Tylko jedną z implikacji z zadania 547 (b) można dowieść metodami z zadania 547 (a). Dalej przedstawię tylko dowód implikacji odwrotnej.

5. Załóżmy więc, że formuła $(\varphi \wedge p) \rightarrow \psi$ jest tautologią. Pokażę, że tautologią jest też formuła $\varphi \rightarrow \psi$. Zrobię to w zwykły sposób. Wezmę dowolne wartościowanie zmiennych zdaniowych σ takie, że $\hat{\sigma}(\varphi) = \top$ i pokażę, że $\hat{\sigma}(\psi) = \top$.

Mając takie wartościowanie σ tworzę inne wartościowanie δ . Wartościowanie to dla wszystkich zmiennych z wyjątkiem p przyjmuje takie same wartości, jak σ . Ponadto przyjmujemy, że $\delta(p) = \top$ (zmieniłem więc wartościowanie σ dla jednej ze zmiennych lub dodatkowo zdefiniowałem je dla nowej zmiennej). Definicję tę można też zapisać w następującej postaci

$$\delta(x) = \begin{cases} \sigma(x) & \text{jeżeli } x \neq p \\ \top & \text{jeżeli } x = p. \end{cases}$$

Istotne jest to, że formuły takie jak φ i ψ , a więc formuły, w których nie występuje zmienna p , mają te same wartości dla obu wartościowań. Mamy więc

$$\hat{\sigma}(\varphi) = \hat{\delta}(\varphi) \text{ oraz } \hat{\sigma}(\psi) = \hat{\delta}(\psi).$$

Jeżeli ktoś w to nie wierzy, to powinien dowieść przytoczoną własność przez tzw. indukcję ze względu na budowę formuły.

Dalszy dowód jest już prosty. Założyliśmy, że formuła φ jest spełniona przy wartościowaniu σ . Jest więc też spełniona przy wartościowaniu δ . Także formuła $(\varphi \wedge p) \rightarrow \psi$ jest spełniona przy wartościowaniu δ (ponieważ jest to tautologia). Stąd otrzymujemy, że $\hat{\sigma}(\psi) = \hat{\delta}(\psi) = \top$.

Rozwiązanie zadania 547 (c). To zadanie jest dość trudne. Punkty (a) i (b) można jednak uważać za wskazówkę. Fakt z tego zadania jest prostą wersją tzw. lematu Craiga. Będziemy go dowodzić stopniowo, dla coraz bardziej skomplikowanych formuł φ .

6. Najpierw lemat Craiga udowodnimy dla formuł φ , które są koniunkcjami zmiennych zdaniowych i negacji zmiennych zdaniowych. Dodatkowo będziemy zakładać o tych koniunkcjach, że żadna zmienna nie występuje w nich dwukrotnie, a więc nie są postaci $p \wedge p \wedge \dots$ lub $p \wedge \neg p \wedge \dots$. Dowód zostanie przeprowadzony przez indukcję ze względu na liczbę elementów zbioru $V(\varphi) \setminus V(\psi)$.

Jeżeli zbiór $V(\varphi) \setminus V(\psi)$ ma zero elementów (czyli jest pusty), to możemy przyjąć, że $\rho = \varphi$. W tym przypadku wszystkie wymagane własności ρ są oczywiste: $V(\rho) = V(\varphi) = V(\varphi) \cap V(\psi)$, gdyż w rozważanym przypadku $V(\varphi) \subseteq V(\psi)$, formuła $\rho \rightarrow \psi$ jest tautologią na mocy założenia, a formuła $\varphi \rightarrow \rho$ jest tautologią, ponieważ jest to formuła $\varphi \rightarrow \varphi$, która oczywiście jest tautologią.

Jeżeli zbiór $V(\varphi) \setminus V(\psi)$ jest niepusty, to wybieramy z niego dowolną zmienną p i przedstawiamy formułę φ w postaci $\varphi' \wedge p$ lub $\varphi' \wedge \neg p$. Na mocy dodatkowego założenia, w formule φ' nie występuje już zmienna p . Dalszy dowód w obu przypadkach jest taki sam. Zauważmy, że na mocy zadania 547 (b) formuła $\varphi' \rightarrow \psi$ jest tautologią. Dla drugiej formuły korzystamy z oczywistego uogólnienia zadania 547 (b).

W tej sytuacji możemy skorzystać z założenia indukcyjnego dla φ' . Pozwala to znaleźć formułę ρ taką, że

$$V(\rho) = V(\varphi') \cap V(\psi) \text{ oraz } \varphi' \rightarrow \rho \text{ i } \rho \rightarrow \psi \text{ są tautologiami.}$$

Nietrudno zauważyć, że formuła ρ ma też własności wymagane w lemacie Craiga dla formuły φ . Mamy bowiem

$$\begin{aligned} V(\varphi) \cap V(\psi) &= (V(\varphi') \cup \{p\}) \cap V(\psi) = V(\varphi') \cap V(\psi) \cup \{p\} \cap V(\psi) = \\ &= V(\varphi') \cap V(\psi) = V(\rho) \end{aligned}$$

(przedostatnia równość wynika stąd, że $p \notin V(\psi)$). Ponadto, $\varphi \rightarrow \rho$ jest tautologią, ponieważ tautologiami są $\varphi \rightarrow \varphi'$ oraz $\varphi' \rightarrow \rho$.

7. Teraz pokażemy, że jeżeli lemat Craiga jest prawdziwy dla pewnych formuł φ_1 i φ_2 , to jest też prawdziwy dla alternatywy $\varphi_1 \vee \varphi_2$.

Przypuśćmy więc, że $(\varphi_1 \vee \varphi_2) \rightarrow \psi$ jest tautologią oraz istnieją formuły ρ_1 i ρ_2 takie, że

$$V(\rho_1) = V(\varphi_1) \cap V(\psi) \text{ oraz } \varphi_1 \rightarrow \rho_1 \text{ i } \rho_1 \rightarrow \psi \text{ są tautologiami.}$$

oraz

$$V(\rho_2) = V(\varphi_2) \cap V(\psi) \text{ oraz } \varphi_2 \rightarrow \rho_2 \text{ i } \rho_2 \rightarrow \psi \text{ są tautologiami.}$$

Wtedy formuła $\rho_1 \vee \rho_2$ spełnia tezę lematu Craiga dla $\varphi_1 \vee \varphi_2$. Formuła $(\rho_1 \vee \rho_2) \rightarrow \psi$ jest tautologią na mocy zadania 547 (a). Ponieważ formuły $\varphi_1 \rightarrow \rho_1$ oraz $\rho_1 \rightarrow (\rho_1 \vee \rho_2)$ są tautologiami, więc to samo można powiedzieć o $\varphi_1 \rightarrow (\rho_1 \vee \rho_2)$. W tych samych powodów tautologią jest $\varphi_2 \rightarrow (\rho_1 \vee \rho_2)$. Jeżeli teraz skorzystamy z zadania 547 (a), to otrzymamy, że tautologią jest także $(\varphi_1 \vee \varphi_2) \rightarrow (\rho_1 \vee \rho_2)$. Pozostaje jeszcze wyliczyć $V(\varphi_1 \vee \varphi_2)$. Oczywiście zachodzą następujące równości:

$$V(\varphi_1 \vee \varphi_2) \cap V(\psi) = V(\varphi_1) \cap V(\psi) \cup V(\varphi_2) \cap V(\psi) = V(\rho_1) \cup V(\rho_2) = V(\rho_1 \vee \rho_2).$$

8. Z udowodnionych wyżej faktów, stosując bardzo łatwą indukcję, możemy wyprodukować lemat Craiga dla wszystkich formuł φ , które są dane w alternatywnej (dysjunkcyjnej) postaci normalnej (a więc są alternatywami, a każdy z (być może wielu) członów tej alternatywy jest koniunkcją zmiennych zdaniowych i negacji zmiennych zdaniowych). Ponadto, dysjunkty takich formuł powinny spełniać dodatkowy warunek: żadna zmienna nie może wystąpić w nich dwukrotnie.

Dowód lematu Craiga w całej okazałości wymaga jeszcze powołania się na dwa fakty. Po pierwsze trzeba wiedzieć, że dowolna formuła φ jest równoważna formule w alternatywnej postaci normalnej. Co więcej, można żądać od takiej postaci normalnej, aby spełniała wspomniany dodatkowy warunek oraz występowały w niej dokładnie te zmienne, co w φ . Po drugie, jeżeli lemat Craiga jest prawdziwy dla formuły φ , to jest prawdziwy także dla każdej formuły równoważnej z φ , która jest zapisana za pomocą tych samych zmiennych, co φ .

9. Przedstawione uzasadnienie lematu Craiga zawiera drobną usterkę. Dobrym ćwiczeniem byłoby przerwanie w tej chwili czytania dalszej części tego tekstu i podjęcie próby samodzielnego znalezienia tej usterki. Takie usterki często prowadzą do fałszywych wniosków. Tym razem usterka wskazuje tylko na pewne trudności. Podczas egzaminu jedna osoba zwróciła na to uwagę i twierdziła nie do końca słusznie, że lemat Craiga jest fałszywy.

To, czy zadanie 547 (c) jest prawdziwe, zależy od szczegółów z definicji formuły. W „Materiałach do zajęć” przyjmuje się, że formułami są też symbole $\top$ i $\perp$. Klasyczne definicje formuły jednak nie zawierają tego warunku. W mojej ocenie częściej przyjmuje się, że to nie są formuły.

W pewnym miejscu przedstawionego rozumowania, rozważaliśmy m.in. koniunkcję φ (jednej lub więcej) zmiennych, w której jest zmienna p , i stwierdziliśmy, że ta koniunkcja daje się przedstawić w postaci $\varphi' \wedge p$. Powinniśmy rozważać także sytuację, w której $\varphi = p$. Formuły p nie da się tak przedstawić, chyba że symbol φ' może oznaczać $\top$. Jeżeli $\top$ nie jest formułą, to lemat Craiga wymaga ostrożniejszego sformułowania.

10. Przedstawię jeszcze inny dowód lematu Craiga, który wydaje się nieco prostszy. Będziemy się w nim posługiwać pojęciem wartościowania. Aby określić wartość formuły φ dla wartościowania σ musimy założyć, że σ jest określone dla zmiennych występujących w φ . Poza tym, dziedzina σ nie odgrywa zwykle większej roli. W przedstawianym dowodzie będziemy musieli jednak kontrolować dziedziny wartościowań.

Niech φ i ψ spełniają warunki podane w sformułowaniu zadania 547 (c). Przyjmijmy, że X oznacza zbiór

$$\{\sigma : V(\varphi) \cap V(\psi) \rightarrow \{\perp, \top\} : \exists \sigma' : V(\varphi) \rightarrow \{\perp, \top\} \ \sigma'(\varphi) = \top \wedge \sigma \subseteq \sigma'\}$$

(napis $\sigma \subseteq \sigma'$ oznacza, że σ' jest rozszerzeniem σ , albo σ jest obcięciem σ' , czyli spełnia równość $\sigma(p) = \sigma'(p)$ dla wszystkich $p \in V(\varphi) \cap V(\psi)$).

Mając zbiór X konstruujemy formułę ρ , w której występują wszystkie zmienne ze zbioru $V(\varphi) \cap V(\psi)$ i żadne inne, oraz dla dowolnego wartościowania $\sigma : V(\varphi) \cap V(\psi) \rightarrow \{\perp, \top\}$ zachodzi równoważność

$$\hat{\sigma}(\rho) = \top \iff \sigma \in X.$$

Metoda konstrukcji takiej formuły jest znana np. z dowodu twierdzenia o istnieniu alternatywnych postaci normalnych. Proszę zwrócić uwagę, że drobne kłopoty pojawiają się, gdy zbiór $V(\varphi) \cap V(\psi)$ jest pusty.

Pokażemy, że formuła ρ ma żądane własności. W dowodzie wielokrotnie będziemy korzystać z oczywistego faktu: jeżeli mamy dwa wartościowania σ, σ' zmiennych występujących w formule φ spełniające warunek $\sigma \subseteq \sigma'$, to $\sigma(\varphi) = \sigma'(\varphi)$.

Najpierw pokażemy, że $\varphi \rightarrow \rho$ jest tautologią. Weźmy więc dowolne wartościowanie σ' zmiennych z $V(\varphi)$ (tylko takie zmienne występują w tej implikacji). Możemy dodatkowo założyć, że $\hat{\sigma}'(\varphi) = \top$. Pokażemy, że $\hat{\sigma}'(\psi) = \top$. Niech σ będzie obcięciem wartościowania σ' do zmiennych ze zbioru $V(\varphi) \cap V(\psi)$. Oczywiście, $\sigma \in X$. Z definicji ρ otrzymujemy, że $\hat{\sigma}(\rho) = \top$. W końcu, ze przytoczonego faktu o wartościowaniach wnioskujemy, że $\hat{\sigma}'(\rho) = \top$.

Tę samą metodę wykorzystamy do pokania, że implikacja $\rho \rightarrow \psi$ jest tautologią. Niech ν będzie wartościowaniem zmiennych występujących w $\rho \rightarrow \psi$ takim, że $\hat{\nu}(\rho) = \top$. Dziedziną ν jest zbiór $V(\psi)$. Jeżeli obetniemy ν do zmiennych ze zbioru $V(\varphi) \cap V(\psi)$, to otrzymamy wartościowanie, które będziemy oznaczać symbolem σ . Oczywiście, $\hat{\sigma}(\rho) = \top$ oraz $\sigma \in X$. Wartościowanie σ można rozszerzyć do wartościowania σ' spełniającego formułę φ . Wartościowania σ' i ν przypisują te same

wartości zmiennym ze zbioru $V(\varphi) \cap V(\psi)$. Można więc je rozszerzyć do wartościowania v' przypisującemu wartości wszystkim zmiennym ze zbioru $V(\varphi) \cup V(\psi)$. Dla tego wartościowania jest spełniona formuła φ , ponieważ v' jest rozszerzeniem σ' . Spełniona jest także formuła ψ , ponieważ formuła $\varphi \rightarrow \psi$ jest tautologią. Oznacza to, że zachodzi także równość $\hat{v}(\psi) = \top$, gdyż v' jest rozszerzeniem v . Dowiedliśmy więc, że wszystkie wartościowania spełniające ρ spełniają także ψ . Stąd wynika, że $\rho \rightarrow \psi$ jest tautologią.

Zadanie 548. Rozważmy zbiór $\mathbb{N}^{\mathbb{N}}$ wszystkich funkcji z $\mathbb{N}$ w $\mathbb{N}$. Dla danej funkcji f niech $R_f = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N} \ f(m) = n\}$ oznacza zbiór wartości przyjmowanych przez tę funkcję. W $\mathbb{N}^{\mathbb{N}}$ definiujemy relację $\sim$ wzorem

$$f \sim g \stackrel{\text{df}}{\iff} R_f = R_g.$$

Oczywiście $\sim$ jest relacją równoważności.

- Udowodnij, że każda klasa abstrakcji relacji $\sim$ jest albo jednoelementowa, albo ma moc continuum.
- Udowodnij, że zbiór ilorazowy (czyli zbiór wszystkich klas abstrakcji) relacji $\sim$ ma moc continuum.
- Podaj przykład podziału zbioru $\mathbb{N}^{\mathbb{N}}$ na continuum rozłącznych zbiorów mocy continuum.

Rozwiązanie zadania 548 (a). Zbiory wartości funkcji określonych na niepustym zbiorze są niepuste. Tak więc wszystkie rozważane w tym zadaniu zbiory R_f są niepuste. Zbiory te są więc albo jednoelementowe, albo mają przynajmniej dwa elementy.

Niech $f : \mathbb{N} \rightarrow \mathbb{N}$ będzie funkcją taką, że zbiór jej wartości R_f ma dokładnie jeden element i $a \in R_f$. Funkcja f jest ściśle określona. Jej dziedzina jest ustalona, a jej wartością może być tylko a . Jest więc to funkcja stale równa a .

Jeżeli g jest funkcją taką, że $g \sim f$, to g ma ten sam zbiór wartości, co f . Też jest stale równa a , czyli jest identyczna z f . Stąd wynika, że klasa abstrakcji $[f]_{\sim}$ (relacji $\sim$ wyznaczona przez f) ma dokładnie jeden element.

Teraz zajmiemy się funkcjami f , które przyjmują przynajmniej dwie wartości, w tym wartości a i b ($a \neq b$). Oczywiście, $a, b \in R_f$. Posługując się twierdzeniem Cantora-Bernsteina pokażemy, że klasa abstrakcji $[f]_{\sim}$ ma moc continuum. Oczywiście, klasa ta jest zawarta w zbiorze wszystkich funkcji określonych i przyjmujących wartości w zbiorze N . Takich funkcji jest continuum. Wystarczy jeszcze pokazać, że klasa $[f]_{\sim}$ ma moc przynajmniej continuum. W tym celu zdefiniujemy różnowartościową funkcję

$$\varphi : \{a, b\}^N \rightarrow [f]_{\sim}.$$

Przyjmijmy, że $g : N \rightarrow \{a, b\}$ i wartość $\varphi(g)$ jest funkcją definiowaną wzorem

$$\varphi(g)(n) = \begin{cases} f(\frac{n-1}{2}) & \text{jeżeli } n \text{ jest nieparzyste,} \\ g(\frac{n}{2}) & \text{w przeciwnym razie.} \end{cases}$$

Najpierw przekonajmy się, że $\varphi(g) \sim f$. Wyliczmy więc zbiór $R_{\varphi(g)}$ wartości funkcji $\varphi(g)$. Funkcja ta przyjmuje w na zbiorze liczb nieparzystych wszystkie wartości, które przyjmuje funkcja f . Dodatkowo, na zbiorze liczb parzystych przyjmuje wartości a lub b . Tak więc

$$R_f \subseteq R_{\varphi(g)} \subseteq R_f \cup \{a, b\} = R_f.$$

W ten sposób otrzymujemy, że $R_{\varphi(g)} = R_f$, a to oznacza, że $\varphi(g) \sim f$ i ponadto

$$\varphi : \{a, b\}^N \rightarrow [f]_{\sim}.$$

Powinniśmy jeszcze przekonać się, że funkcja φ jest różnowartościowa. Jest to bardzo proste: jeżeli mamy dwa różne argumenty funkcji φ , czyli różne funkcje g_1 i g_2 , to różnią się one wartościami dla pewnego argumentu, powiedzmy dla liczby $k \in \mathbb{N}$. Wtedy (będące funkcjami) wartości $\varphi(g_1)$ i $\varphi(g_2)$ różnią się dla argumentu $2 \cdot k$.

Rozwiązanie zadania 548 (b). Jest to bardzo proste zadanie. Aby je rozwiązać wystarczy powołać się na dwa lub trzy oczywiste fakty.

Pierwszy z nich dotyczy relacji równoważności. Jeżeli mamy funkcję $r : X \rightarrow Y$ i w zbiorze X definiujemy relację równoważności $\sim$ przyjmując, że

$$x \sim y \iff r(x) = r(y).$$

to zbiór klas abstrakcji $X/\sim$ tej relacji jest równoliczny ze zbiorem $r(X)$ wartości funkcji r na zbiorze X . Odpowiednią bijekcję łatwo wskazać. Jest nią funkcja $\rho : X/\sim \rightarrow r(X)$ zdefiniowana wzorem

$$\rho([x]_{\sim}) = r(x).$$

Dalej wystarczy sprawdzić wszystkie wymagane własności ρ , w tym poprawność definicji ρ . Robi się to w sposób standardowy.

Z przytoczonego faktu zastosowanego do relacji $\sim$ z zadania 548 wynika, że zbiór klas abstrakcji tej relacji jest równoliczny ze zbiorem niepustych podzbiorów zbioru liczb naturalnych. Gdyby ktoś czuł potrzebę uzasadnienia czegoś w tym miejscu, to powinien podać konstrukcję funkcji, której zbiór wartości jest danym niepustym zbiorem. Na przykład, jeżeli $a \in A \subseteq \mathbb{N}$, to funkcja f taka, że

$$f(n) = \begin{cases} n & \text{jeżeli } n \in A, \\ a & \text{w przeciwnym razie} \end{cases}$$

spełnia równość $R_f = A$.

W końcu trzeba zauważyć, że zbiór niepustych podzbiorów $\mathbb{N}$ różni się od zbioru $\mathcal{P}(\mathbb{N})$ wszystkich podzbiorów $\mathbb{N}$ jednym elementem. Ten drugi zbiór jest mocy continuum, a więc oba są mocy continuum. Fakt ten wynika z teorii mocy. Można się o tym przekonać np. sprawdzając, że zbiory $\mathcal{P}(N)$, $\mathcal{P}(N \setminus \{0\})$ oraz $\{X \subseteq N : 0 \in X\}$ są równoliczne. Ponieważ zachodzą oczywiste zawierania

$$\{X \subseteq N : 0 \in X\} \subseteq \{X \subseteq N : X \neq \emptyset\} \subseteq \mathcal{P}(N),$$

więc z twierdzenia Cantora-Bernsteina otrzymujemy, że zbiór $\{X \subseteq N : X \neq \emptyset\}$ ma moc continuum.

Rozwiązanie zadania 548 (c). Każda relacja równoważności definiuje podział swojej dziedziny. Także relacja $\sim$ definiuje podział zbioru $\mathbb{N}^{\mathbb{N}}$. Z punktu (b) wynika, że jest to podział na continuum zbiorów, ale niektóre z nich (na mocy punktu (a)) nie mają mocy continuum. Jedną z metod rozwiązania zadania (c) polega na poprawieniu podziału wyznaczonego przez relację $\sim$ tak, aby spełniał warunki zadania. Można to zrobić dołączając małe klasy abstrakcji do dużych.

Niech $S \in \mathbb{N}^{\mathbb{N}}$ oznacza jakąkolwiek funkcję, która nie jest stała, a C_i – funkcję stale równą i (oczywiście, rozważamy tylko funkcje należące do $\mathbb{N}^{\mathbb{N}}$). Utwórzmy sumę

$$U = [S]_{\sim} \cup \bigcup_{i=0}^{\infty} [C_i]_{\sim}.$$

Jest to suma wszystkich jednoelementowych klas abstrakcji relacji $\sim$ i jednej klasy mocy continuum. Oczywiście, jest to zbiór mocy continuum, gdyż jest zawarty w zbiorze $\mathbb{N}^{\mathbb{N}}$ i zawiera zbiór $[S]_{\sim}$ mocy continuum. Jeżeli do tego zbioru dołączymy pozostałe klasy abstrakcji, nie wyznaczone ani przez funkcje stałe, ani przez S , to otrzymamy podział

$$\mathcal{P} = \{U\} \cup \{[f]_{\sim} : f \neq S \wedge f \text{ nie jest stała}\}$$

zbioru $\mathbb{N}^{\mathbb{N}}$ na zbiory mocy continuum. Można mieć wątpliwości, czy w ten sposób otrzymaliśmy podział mocy continuum.

Zdefiniowany podział ma jednak moc continuum. Aby to uzasadnić, można skorzystać z ogólnego i niebanalnego twierdzenia, że odejmując od zbioru mocy continuum zbiór przeliczalny otrzymujemy zbiór mocy continuum. Dobierając odpowiednio S można to też uzasadnić w sposób elementarny: jest continuum podzbiorów zbioru $\mathbb{N} \setminus \{0, 1\}$. Jest więc continuum podzbiorów $\mathbb{N}$, do których należą liczby 0 i 1. W końcu jest continuum klas abstrakcji relacji $\sim$ wyznaczonych przez funkcje przyjmujące wartości 0 i 1, czyli należących do zbioru

$$\{[f]_{\sim} : 0, 1 \in R_f\}.$$

Co więcej, nie ma wśród tych klas abstrakcji klas wyznaczonych przez funkcje stałe (ich wartościami jest najwyżej jedna z liczb 0 i 1) oraz przez funkcję S zdefiniowaną wzorem $S(n) = n + 1$ (nie przyjmuje wartości 0). Tak więc

$$\{[f]_{\sim} : 0, 1 \in R_f\} \subseteq \{[f]_{\sim} : f \neq S \wedge f \text{ nie jest stała}\} \subseteq \mathcal{P}.$$

Stąd podział $\mathcal{P}$ ma continuum elementów.

Zadanie 548 (c) można też rozwiązać inną metodą. Każde dwa zbiory mocy continuum są równoliczne. W szczególności, zbiór X mocy continuum jest równoliczny z X^2 , także ze zbiorem $\mathbb{R}^2$ i z płaszczyzną geometryczną (utożsamianą z $\mathbb{R}^2$). Otóż płaszczyznę bardzo łatwo podzielić na continuum zbiorów mocy continuum. Wystarczy podzielić ją na proste równoległe np. do osi OX . Ponieważ także zbiór X można utożsamiać z płaszczyzną, też można go tak podzielić.

Przedstawię to rozwiązanie jeszcze nieco dokładniej. Weźmy więc zbiór X mocy continuum i bijekcję $f : X \rightarrow X^2$. Rodzina zbiorów

$$\{(x, y) \in X^2 : y \in X\} : x \in X\}$$

jest podziałem zbioru X^2 . Każdy element tego podziału jest równoliczny ze zbiorem X . Także cały ten podział jest równoliczny z X . Nietrudno sprawdzić, że rodzina przeciwbrazów

$$\{f^{-1}(\{(x, y) \in X^2 : y \in X\}) : x \in X\}$$

jest podziałem zbioru X i ma oczekiwane własności. Aby rozwiązać zadanie 548 (c), przedstawione rozumowanie trzeba przeprowadzić dla zbioru $X = \mathbb{N}^{\mathbb{N}}$.

Zadanie 549. Niech A będzie dowolnym zbiorem. *Multizbiorem* nad A nazywamy dowolną funkcję $S : A \rightarrow \mathbb{N}$ (mówimy wtedy, że $S(x)$ jest liczbą wystąpień elementu x w multizbiorze S). Rodzinę wszystkich multizbiorów nad A oznaczamy $\mathcal{M}(A)$. Jeśli S_1 i S_2 są multizbiorami, to ich przekrój $S_1 \cap S_2$, sumę $S_1 \cup S_2$ i różnicę $S_1 \setminus S_2$ definiujemy wzorami

$$\begin{aligned}(S_1 \cap S_2)(x) &= \min(S_1(x), S_2(x)) \\ (S_1 \cup S_2)(x) &= S_1(x) + S_2(x) \\ (S_1 \setminus S_2)(x) &= \max(S_1(x) - S_2(x), 0).\end{aligned}$$

Mówimy, że S_1 jest podzbiorem S_2 i piszemy $S_1 \subseteq S_2$, jeśli istnieje taki multizbiór X , że $S_1 \cup X = S_2$.

(a) Czy dla dowolnych multizbiorów X, Y, Z nad zbiorem A zachodzi równość

$$X \setminus (Y \cup Z) = (X \setminus Y) \setminus Z ?$$

(b) Czy dla dowolnych multizbiorów X, Y, Z nad zbiorem A zachodzi równość

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) ?$$

(c) Czy $\langle \mathcal{M}(A), \subseteq \rangle$ jest porządkiem? Czy jest to porządek zupełny?

Wszystkie odpowiedzi należy uzasadnić.

Rozwiązanie zadania 549 Pozornie wydaje się, że to zadanie dotyczy zbiorów i można je rozwiązać podobnie, jak zadania z rachunku zbiorów. Nic bardziej mylnego. W zadaniach 549 (a) i (b) mamy dowieść równość dwóch funkcji. I trzeba to zrobić tak, jak dowodzi się równość funkcji. Funkcje występujące w tym zadaniu mają tę samą dziedzinę. Trzeba więc rozstrzygać tylko, czy interesujące nas funkcje dla dowolnego argumentu przyjmują te same wartości.

Równość

$$X \setminus (Y \setminus Z) = (X \setminus Y) \setminus Z$$

zachodzi wtedy i tylko wtedy, gdy dla dowolnego $a \in A$ zachodzi równość

$$(X \setminus (Y \setminus Z))(a) = ((X \setminus Y) \setminus Z)(a).$$

Ta ostatnia równość jest na mocy definicji równoważna warunkowi

$$\max(X(a) - \max(Y(a) - Z(a), 0), 0) = \max(\max(X(a) - Y(a), 0) - Z(a), 0).$$

Po odpowiednich podstawieniach z tej ostatniej równości otrzymujemy

$$\max(x - \max(y - z, 0), 0) = \max(\max(x - y, 0) - z, 0).$$

Ta równość jest prawdziwa bez względu na wartości x , y i z . Pomijam jej dowód. Wynika z niej prawdziwość równości z zadania 549 (a).

Równość z zadania 549 (b) jest fałszywa. Jest natomiast równoważna równości

$$\min(x, y + z) = \min(x, y) + \min(x, y).$$

Jest ona fałszywa np. dla $x = 3$, $y = 2$ i $z = 2$. Biorąc trzy funkcję określone w zbiorze A : funkcję X stale równą 3 oraz Y i Z – stale równe 2, możemy wykazać fałszywość równości z zadania 549 (b).

Zdefiniowana w zadaniu 549 relacja $\subseteq$ porządkuje multizbiory z $\mathcal{M}(A)$. Może trochę łatwiej to się dowodzi, jeżeli scharakteryzujemy relację $\subseteq$ w języku funkcji. Dowolne multizbiory X i Y spełniają warunek $X \subseteq Y$ wtedy i tylko wtedy, gdy

$$X(a) \leq Y(a)$$

dla wszystkich $a \in A$. Tak więc relacja zawierania między multizbiorami to jeden z częściej spotykanych porządków w zbiorze funkcji.

Zawieranie w rodzinie multizbiorów nie jest porządkiem zupełnym. Jeżeli przyjmujemy, że X_n jest multizbiorem, do którego wszystkie elementy należą n razy, czyli

jest funkcją stale równą n , to zbiór $\{X_n : n \in N\}$ nie ma kresu górnego. Co więcej, nie ma on ograniczenia górnego. Gdyby bowiem Y ograniczało ten zbiór z góry, $a \in A$ i $Y(a) = m$, to z warunku $X_{m+1} \subseteq Y$ można by wywnioskować, że

$$m + 1 = X_{m+1}(a) \leq Y(a) = m,$$

a to nie powinno się dać zrobić.

Zadanie 550. Niech $\langle A, \leq \rangle$ będzie zbiorem dobrze uporządkowanym (czyli zbiorem liniowo uporządkowanym, w którym każdy niepusty podzbiór ma element najmniejszy). W zbiorze $A \times A$ porządek leksykograficzny jest zdefiniowany wzorem

$$\langle x_1, x_2 \rangle \leq_{lex} \langle y_1, y_2 \rangle \stackrel{\text{df}}{\Leftrightarrow} (x_1 \leq y_1 \wedge x_1 \neq y_1) \vee (x_1 = y_1 \wedge x_2 \leq y_2).$$

W zbiorze $X = (\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0\})$ definiujemy porządek $\preceq$ wzorem

$$\langle x_1, x_2 \rangle \preceq \langle y_1, y_2 \rangle \stackrel{\text{df}}{\Leftrightarrow} \frac{x_1}{x_2} < \frac{y_1}{y_2} \vee \left(\frac{x_1}{x_2} = \frac{y_1}{y_2} \wedge x_1 \leq y_1 \right).$$

- Udowodnij, że $\langle A \times A, \leq_{lex} \rangle$ jest zbiorem dobrze uporządkowanym (nie trzeba dowodzić, że relacja $\leq_{lex}$ jest porządkiem, ani że jest to porządek liniowy).
- Czy $\langle X, \preceq \rangle$ jest izomorficzny z $\langle \mathbb{Q}, \leq \rangle$?
- Czy $\langle X, \preceq \rangle$ jest izomorficzny z $\langle \mathbb{N} \times \mathbb{N}, \leq_{lex} \rangle$?

Uzasadnij odpowiedzi.

Rozwiązanie zadania 550 (a). Porządek leksykograficzny w kwadracie kartezjańskim dobrze uporządkowanego zbioru $\langle A, \leq \rangle$ jest regularny, a więc spełnia zasadę minimum. Weźmy dowolny niepusty zbiór $X \subseteq A \times A$. Przyjmijmy, że

$$Y = \{y \in A : \exists z \in A \langle y, z \rangle \in X\}.$$

Jest to niepusty podzbiór A . Korzystając z zasady minimum w zbiorze A znajdujemy najmniejszy element w zbiorze Y . Niech ntym elementem najmniejszym będzie a . Teraz definiujemy zbiór

$$Z = \{z \in A : \langle a, z \rangle \in X\}.$$

Z definicji a wynika, że zbiór Z jest niepusty. Ponownie korzystamy z zasady minimum i znajdujemy w Z element najmniejszy. Tym razem oznaczamy go symbolem b .

Nietrudno zauważyć, że $\langle a, b \rangle$ jest najmniejszym elementem w zbiorze X . Aby się o tym przekonać weźmy dowolny element $\langle y, z \rangle$ w zbiorze X . Jest oczywiste, że $y \in Y$. Z definicji a otrzymujemy, że $a \leq y$. Gdyby się okazało, że $a \neq y$, to z definicji porządku leksykograficznego wynikałoby, że $\langle a, b \rangle \leq_{lex} \langle y, z \rangle$. Załóżmy

więc, że $a = y$. Wtedy z jest elementem zbioru Z i na mocy definicji b zachodzi nierówność $b \leq z$. Łatwo sprawdzić, że także w tym przypadku zachodzi nierówność $\langle a, b \rangle \leq_{lex} \langle y, z \rangle$.

Rozwiązanie zadania 550 (b) i (c). Najpierw spróbujmy sobie wyobrazić zbiory uporządkowane $\langle X, \prec \rangle$ i $\langle \mathbb{N} \times \mathbb{N}, \leq_{lex} \rangle$.

Pierwszy z tych zbiorów składa się z przedstawień dodatnich liczb wymiernych i rozpada się na fragmenty złożone z przedstawień tej samej liczby. Całe te fragmenty są uporządkowane tak, jak przedstawiane przez nie liczby. Wewnątrz fragmentów porządek jest wyznaczony przez liczniki przedstawień i ma takie własności, jak porządek w zbiorze liczb naturalnych.

Drugi ze zbiorów ma podobną strukturę. Też składa się z fragmentów, tym razem są to zbiory par o ustalonej pierwszej współrzędnej. Poszczególne fragmenty, jak i zbiór fragmentów są uporządkowane, jak zbiór liczb naturalnych.

Porządki $\langle \mathbb{Q}, \leq \rangle$ i $\langle X, \prec \rangle$ nie są izomorficzne. Porządek w zbiorze liczb wymiernych jest gęsty. Natomiast fragmenty drugiego porządku $\langle X, \prec \rangle$ składają się z „kolejnych” wyrazów. Na przykład, między parami $\langle 1, 1 \rangle$ i $\langle 2, 2 \rangle$ (przedstawiającymi liczbę 1) nie ma żadnych innych elementów. Nie jest więc to porządek gęsty. Z drugiej strony, łatwo sprawdzić, że izomorfizm zachowuje gęstość. Gdyby porządek $\langle X, \prec \rangle$ był izomorficzny z $\langle \mathbb{Q}, \leq \rangle$, to byłby gęsty.

Podobnie, nie są izomorficzne porządki $\langle X, \prec \rangle$ i $\langle \mathbb{N} \times \mathbb{N}, \leq_{lex} \rangle$. Pierwszy z nich przypomina porządek w zbiorze dodatnich liczb wymiernych i nie ma elementu najmniejszego. W drugim jest element najmniejszy i jest to para $\langle 0, 0 \rangle$.

Fakt z zadania 550 (c) można też dowieść w inny sposób. Z punktu (a) wynika, że porządek $\langle \mathbb{N} \times \mathbb{N}, \leq_{lex} \rangle$ jest dobry. Porządek izomorficzny z dobrym też jest dobry. Porządek $\langle X, \prec \rangle$ nie jest jednak dobry. Jest w nim ciąg malejący, np. złożony z elementów $\langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 1, 3 \rangle, \dots$

Zadania zgłoszone na ćwiczeniach

W poniższej tabeli proszę notować numery zadań przewidzianych na dane zajęcia, numery zgłoszonych zadań i liczbę otrzymanych punktów. Na następnych stronach są wydrukowane kupony zgłoszenia zadań, które należy wyciąć, wypełnić i przekazać prowadzącym na zajęciach. Pierwsze zajęcia nie są punktowane.

Zaj. 2	Data:												
Zadania:													
Punkty:													
Zaj. 3	Data:											Suma:	
Zadania:													
Punkty:													
Zaj. 4	Data:											Suma:	
Zadania:													
Punkty:													
Zaj. 5	Data:											Suma:	
Zadania:													
Punkty:													
												Suma:	

Zaj. 6	Data:														
Zadania:															
Punkty:															

Zaj. 7	Data:													Suma:	
Zadania:															
Punkty:															

Zaj. 8	Data:													Suma:	
Zadania:															
Punkty:															

Zaj. 9	Data:													Suma:	
Zadania:															
Punkty:															

Zaj. 10	Data:													Suma:	
Zadania:															
Punkty:															

Suma:	
-------	--

Zaj. 11	Data:													
Zadania:														
Punkty:														

Zaj. 12	Data:													Suma:	
Zadania:															
Punkty:															

Zaj. 13	Data:													Suma:	
Zadania:															
Punkty:															

Zaj. 14	Data:													Suma:	
Zadania:															
Punkty:															

Zaj. 15	Data:													Suma:	
Zadania:															
Punkty:															

Suma:	
-------	--

Zadania domowe

1.	Zadane dnia:		na dzień:		Punkty:	
2.	Zadane dnia:		na dzień:		Punkty:	

Kartkówki i inne zdarzenia

Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	

Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	
Dnia:		punkty:	

Ocena końcowa

Liczba punktów zdobytych w semestrze:	
Ocena wyliczona według tablicy C.1:	

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

Logika	Imię i nazwisko:												Sala nr:				
Zadanie:																Data:	
Punkty:																Suma:	

Wypełniać czytelnie i bez skreśleń drukowanymi literami

