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

Leszek Pacholski

Wrocław, 2003

Właściciel tej kopii notatek

Rok akad.

Uwaga: W niejszej książeczce zebrano bez szczegółowej redakcji i korekty listy zadań, notatki do wykładów oraz inne materiały przygotowywane do zajęć z *Logiki dla informatyków* w latach 1997–2002. Mimo iż materiały te posiadają bardziej dopracowaną formę, niż rozpowszechniane dotychczas kserograficzne kopie, jednak nadal zawierają sporo błędów i *nie są ukończonym podręcznikiem do wykładu*.

Podczas redagowania notatek wykorzystano:
- skrypt J. Tiuryna *Wstęp do teorii mnogości i logiki*
- listy zadań M. Zakrzewskiego
- materiały A. Kościelskiego i T. Wierzbickiego

Konsultacja merytoryczna: A. Kościelski, J. Marcinkowski

Data utworzenia dokumentu: 22 września 2003

Strona WWW zajęć: `http://www.ii.uni.wroc.pl/~pacholsk/logika.phtml`

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 powtarzam to, co napisałem 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.

Leszek Pacholski

Spis treści

A

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. 29 i — w wersji elektronicznej — pod adresem:

`http://www.ii.uni.wroc.pl/program/`

A.2. Zapisy na zajęcia

W zajęciach mogą uczestniczyć zarówno studenci studiów magisterskich, jak i licencjackich. 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 jest ogłoszona w *Terminarzu zajęć* na dany rok akademicki, dostępnym pod adresem

`http://www.ii.uni.wroc.pl/~pacholsk/logter.phtml`

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. Poszczególni 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. w *Terminarzu zajęć* i na stronach domowych prowadzących.

Poza prowadzącymi wykład, repetytorium i ćwiczenia, zajęcia obsługuje także *sekretarz 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

Poza niniejszymi notatkami podstawowym podręcznikiem do wykładu jest skrypt:

1. Jerzy Tiuryn, *Wstęp do teorii mnogości i logiki*, który można zakupić w sekretariacie Instytutu, pok. 29 lub 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. 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.

3. Kazimierz Kuratowski, Andrzej Mostowski, *Teoria mnogości*, PWN, Warszawa, 1978. Obszerny wykład teorii mnogości. W bibliotece Instytutu są dwa egzemplarze, sygnatury: II 286, II 8358.

4. 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.

5. 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.

6. 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.

7. 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 ilości. 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 ćwiczenia 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 na wykładzie. Są one także wymienione 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 przeważnie od 10 do 15 zadań. W semestrze zadaje się więc do rozwiązania około 150 zadań. Niniejsze notatki zawierają 342 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 jest ogłaszana (w trakcie wykładu, w gablocie w hallu, na stronie WWW wykładu itp.) 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 przekazuje prowadzącemu ćwiczenia kartkę z numerami zadań z listy, które potrafi rozwiązać.[1] Kartka powinna być wypełniona czytelnie, zawierać datę, jednoznacznie wpisane numery zadań[2] oraz imię i nazwisko studenta. Po rozpoczęciu zajęć dokonywanie jakichkolwiek zmian w treści przekazanych kartek[3] jest niedopuszczalne. Rozwiązanie danego zadania na tablicy przedstawia jedna z osób, wybrana przez prowadzącego, która zgłosiła gotowość rozwiązania tego zadania.[4] Prowadzący ma pra-

[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. prośby o wycofanie lub dopisanie jakiegoś zadania.

[4] Niniejsze 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 ochotnikowi.

wo przerwać osobie referującej w dowolnym momencie i poprosić inne osoby, które zgłosiły gotowość rozwiązania danego zadania, o kontynuowanie.[5]

3. 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 6 i 7.

4. W ciągu semestru student ma obowiązek dostarczyć rozwiązania dwóch zadań domowych. Na każdych zajęciach prowadzący wyznaczają po około trzy osoby w każdej grupie ćwiczeniowej. Te osoby mają obowiązek przynieść na następne ćwiczenia pracę pisemną, napisaną czytelnie na arkuszu papieru formatu A4 lub wydrukowaną na komputerze. Zadania domowe mają rozwinąć u studentów zdolność jasnego, precyzyjnego i czytelnego redagowania rozwiązań zadań. Za pracę można otrzymać od 0 do 5 punktów. Oceniona praca jest zwracana autorom w kolejnym tygodniu. Zadania sprawdza sekretarz dydaktyczny.

5. 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 nieznajomość definicji i/lub podstawowych twierdzeń — czyli za złą odpowiedź na co najmniej jedno pytanie zadane w kartkówce — studentowi odejmuje się 10 punktów.

6. 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.

7. 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] W ten sam sposób jest traktowany student, który nie przyniósł pracy domowej, opisanej w punkcie 4.

---

[5] Niniejsze 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.

[6] Z 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.

punkty	ocena
$-\infty \div 34$	ndst
$35 \div 49$	dst
$50 \div 64$	dst+
$65 \div 79$	db
$80 \div 94$	db+
$95 \div +\infty$	bdb

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

8. Liczba punktów uzyskana przez studenta w ciągu całego semestru jest sumą liczby punktów zadeklarowanych na ćwiczeniach (wraz z otrzymanymi punktami karnymi), 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 120.

9. Ocena końcowa nie podlega poprawianiu po zakończeniu semestru. Nie ma kolokwiów poprawkowych.[7]

10. Studenci po zapisaniu się do grup ćwiczeniowych nie mogą ich zmieniać, mimo iż wszystkie zajęcia odbywają się w tym samym czasie.

11. Podczas referowania zadań przy tablicy student nie może mieć przy sobie notatek.

[7] Student powinien mieć świadomość, że zajęć można nie zaliczyć. W szczególności utrata punktów zgodnie z paragrafem 7 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.

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 (dwuczęściowy), jak i poprawkowy (jednoczęściowy) 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 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: $(C - 35)/10$, gdzie C oznacza całkowitą liczbę punktów uzyskanych na zaliczenie ćwiczeń w semestrze bezpośrednio poprzedzającym egzamin. *Osobom, które zaliczyły ćwiczenia w poprzednich latach 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

punkty	ocena
$-100 \div 32$	ndst
$33 \div 45$	dst
$46 \div 58$	dst+
$59 \div 71$	db
$72 \div 84$	db+
$85 \div +\infty$	bdb

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

egzaminu i otrzymanych ocen studenci powinni wyjaśniać w trakcie konsultacji poegzaminacyjnych. W czasie kosultacji 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.

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.

D.2. Egzamin poprawkowy

W razie otrzymania oceny niedostatecznej z egaminu zasadniczego student przystępuje do egzaminu poprawkowego w sesji poprawkowej.

Nieobecność na egzaminie poprawkowym (niezależnie od przyczyn — usprawiedliwionych bądź nie) jest równoznaczna z uzyskaniem oceny niedostatecznej z tego egzaminu. Ocena z egzaminu poprawkowego nie podlega poprawianiu.

Notacja matematyczna

Na oznaczenie różnych pojęć używa się w matematyce liter pochodzących z różnych krojów pisma i różnych alfabetów. Poniżej są zebrane alfabety użyte w niniejszych notatkach.

Pismo łacińskie, gotyckie, blokowe i kaligraficzne

$$a\ b\ c\ d\ e\ f\ g\ h\ i\ j\ k\ l\ m\ n\ o\ p\ q\ r\ s\ t\ u\ v\ w\ x\ y\ z$$

$$A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z$$

$$\mathfrak{a\ b\ c\ d\ e\ f\ g\ h\ i\ j\ k\ l\ m\ n\ o\ p\ q\ r\ s\ t\ u\ v\ w\ x\ y\ z}$$

$$\mathfrak{A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z}$$

$$\mathbb{A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z}$$

$$\mathcal{A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z}$$

Alfabet grecki

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

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

Alfabet hebrajski

Z alfabetu hebrajskiego używamy pierwszej litery $\aleph$, 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.

Zadanie 1. 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?*

Zadanie 2. Oto przykłady trzech wnioskowań przez indukcję:

1. *Pokażę, że wszystkie liczby naturalne są parzyste. Oczywiście* 0 *jest liczbą parzystą. Niech* n *będzie dowolną liczbą naturalną i załóżmy, że dla wszystkich* $k < n$, k *jest parzyste. Niech* n_1 *i* n_2 *będzie dowolnym rozbiciem 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. *Pokażę, że wszystkie dodatnie liczby naturalne są nieparzyste. Oczywiście* 1 *jest liczbą nieparzystą. Niech* n *będzie dowolną liczbą naturalną i załóżmy, że dla wszystkich* $k < n$, k *jest nieparzyste. Niech* 1, n_1 *i* n_2 *będzie dowolnym rozbiciem 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. *Pokażę, 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.

Celem powyższego zadania jest zwrócenie uwagi na fakt, 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!

W poniższych zadaniach napisz odpowiednie formuły logiczne *nie używając znaku negacji*.

Zadanie 3. Funkcja $f : \mathbb{R} \to \mathbb{R}$ jest *ciągła*, jeśli

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

Zapisz formułę „funkcja f nie jest ciągła.”

Zadanie 4. Liczba $g \in \mathbb{R}$ jest *granicą* (w sensie Cauchy’ego) funkcji $f : \mathbb{R} \to \mathbb{R}$ w punkcie x_0, jeśli

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

Zapisz formułę „liczba g nie jest granicą funkcji f w punkcie x_0.”

Zadanie 5. Liczba $g \in \mathbb{R}$ jest *granicą* (w sensie Heinego) funkcji $f : \mathbb{R} \to \mathbb{R}$ w punkcie x_0, jeśli

$$\forall (x_n)_{n\in\mathbb{N}}\ \big((\lim_{n\to\infty} x_n = x_0 \wedge \forall n\ x_n \neq x_0) \Rightarrow \lim_{n\to\infty} f(x_n) = g\big).$$

Zapisz formułę „liczba g nie jest granicą funkcji f w punkcie x_0.”

1

Rachunek zdań i rachunek kwantyfikatorów

1.1. Składnia rachunku zdań

Definicja 1. *Formuły rachunku zdań* budujemy ze *zmiennych zdaniowych* i *spójników logicznych* (*funktorów zdaniotwórczych*): fałszu $\bot$, prawdy $\top$, negacji $\neg$, koniunkcji $\wedge$, alternatywy $\vee$, implikacji $\Rightarrow$ i równoważności $\Leftrightarrow$ w następujący sposób:

1. Symbole $\bot$ 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 2. Zbiór *wartości logicznych* $\mathcal{B} = \{\mathsf{T}, \mathsf{F}\}$ zawiera dwa elementy: T (prawdziwe) i F (fałszywe).[8] Niech V oznacza zbiór zmiennych zdaniowych. *Wartościowanie zmiennych*, to odwzorowanie $\sigma : V \to \mathcal{B}$. Nadaje ono wartości logiczne zmiennym zdaniowym.

[8] Oznaczenia pochodzą od angielskich słów *true* i *false*.

$\bot$
F

$\top$
T

ϕ	$\neg\phi$
F	T
T	F

ϕ	ψ	$\phi \wedge \psi$
F	F	F
F	T	F
T	F	F
T	T	T

ϕ	ψ	$\phi \vee \psi$
F	F	F
F	T	T
T	F	T
T	T	T

ϕ	ψ	$\phi \Rightarrow \psi$
F	F	T
F	T	T
T	F	F
T	T	T

ϕ	ψ	$\phi \Leftrightarrow \psi$
F	F	T
F	T	F
T	F	F
T	T	T

Rysunek 1. Znaczenie spójników logicznych

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

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

Ponieważ dla danego wartościowania zmiennych wartościowanie formuł jest określone jednoznacznie, znak $\hat{}$ będziemy opuszczać i zarówno wartościowanie zmiennych, jak i wartościowanie formuł będziemy oznaczać tym samym symbolem i nazywać po prostu *wartościowaniem*.

Definicja 3. 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 każdego wartościowania zmiennych.

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

Obecnie zajmiemy się problemem polegającym na sprawdzeniu, 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*. Istotnie, 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 6 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.

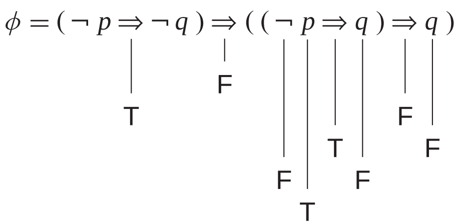
1.2.2. Skrócona metoda zero-jedynkowa

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 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, jej następnik $(\neg p \Rightarrow q) \Rightarrow q$ zaś — fałszywy. Formuła $(\neg p \Rightarrow q) \Rightarrow q$ jest fałszywa tylko wówczas, gdy $\neg p \Rightarrow q$

$$\phi = \neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$$

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

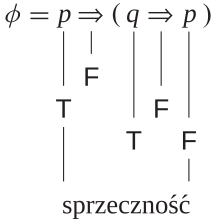
Rysunek 2. Tabelkowa metoda sprawdzenia, że formuła ϕ jest tautologią



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

jest spełniona oraz $\sigma(q) = \mathsf{F}$. Ale $\neg p \Rightarrow q$ jest spełniona dla $\sigma(q) = \mathsf{F}$ tylko wówczas, gdy $\neg p$ nie jest spełniona, tj. gdy $\sigma(p) = \mathsf{T}$. Zauważamy na koniec, że przy wartościowaniu $\sigma(p) = \mathsf{T}$ i $\sigma(q) = \mathsf{F}$ 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 $\sigma(p) = \mathsf{T}$ oraz powinna nie być spełniona formuła $q \Rightarrow p$. Formuła ostatnia nie jest spełniona tylko wówczas, gdy $\sigma(q) = \mathsf{T}$ oraz $\sigma(p) = \mathsf{F}$. Zatem aby ϕ nie była spełniona, musiałoby być jednocześnie $\phi(p) = \mathsf{T}$ i $\phi(p) = \mathsf{F}$, co jest niemożliwe. Formuła ϕ jest zatem tautologią (rysunek 4).



Rysunek 4. Dowód nie wprost, iż formuła ϕ jest tautologią

Przykład 4. Przykładami tautologii są także

$$(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$$
$$(\neg p \Rightarrow \neg q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow p)$$

Definicja 5. Mówimy, że formuły ϕ i ψ są *równoważne*, jeśli przyjmują tę samą wartość logiczną dla każdego wartościowania, tj. gdy formuła $\phi \Leftrightarrow \psi$ jest tautologią.

Przykład 6. Formuły $\neg(p \vee q)$ i $\neg p \wedge \neg q$ są równoważne.

W zadaniach 6–16 sprawdź, które z poniższych formuł są (a) tautologiami, (b) formułami spełnialnymi, (c) formułami sprzecznymi.

Zadanie 6. $(p \vee q \vee r) \Rightarrow (\neg p \Rightarrow ((q \vee r) \wedge \neg p))$

Zadanie 7. $(p \Rightarrow q) \Leftrightarrow ((p \wedge q) \Leftrightarrow p)$

Zadanie 8. $((p \vee q) \Rightarrow r) \Rightarrow ((p \Rightarrow r) \vee (q \Rightarrow r))$

Zadanie 9. $((p \Rightarrow q) \wedge (r \Rightarrow s)) \Rightarrow ((p \wedge s) \Rightarrow (q \vee r))$

Zadanie 10. $p \vee q \vee r \Rightarrow ((p \vee q) \wedge \neg r) \vee (r \wedge p \wedge q)$

Zadanie 11. $((p \vee q) \wedge \neg r) \vee (r \wedge p \wedge q) \Rightarrow p \vee q \vee r$

Zadanie 12. $((p \vee q) \Leftrightarrow (r \vee s)) \Rightarrow ((p \Leftrightarrow r) \vee (q \Leftrightarrow s))$

Zadanie 13. $((p \Leftrightarrow r) \vee (q \Leftrightarrow s)) \Rightarrow ((p \vee q) \Leftrightarrow (r \vee s))$

Zadanie 14. $((p \wedge q) \Leftrightarrow (r \wedge s)) \Rightarrow ((p \Leftrightarrow r) \wedge (q \Leftrightarrow s))$

Zadanie 15. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$

Zadanie 16. $(\neg p \Rightarrow \neg q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow p)$

Zadanie 17–27. Zaneguj formuły z zadań 6–16 i — korzystając z praw de Morgana — przekształć je do postaci, w której negacja występuje jedynie przed zmiennymi zdaniowymi.

1.3. Formalizacja w języku rachunku zdań

Zadanie 28. Sformalizuj zadanie 1, tj. pokaż, jak znaleźć odpowiedzi na postawione w nim pytania korzystając z rachunku zdań.

Zadanie 29. 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 30. 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 31. Zbadaj zasadność poniższych rozumowań:

1. Jeśli stopa procentowa nie ulegnie zmianie, to wzrosną wydatki rządowe lub pojawi się bezrobocie. Jeśli wydatki rządowe nie wrosną, 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

Zadanie 32. 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 33. Dane są formuły $\phi_1, \ldots, \phi_n, \psi$. Czy formuły

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

oraz

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

są równoważne?

Zadanie 34. Dane są formuły $\phi_1, \ldots, \phi_n, \psi$. Czy formuły

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

oraz

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

są równoważne?

Definicja 7. Napis $\bigwedge_{i=1}^n \phi_i$ oznacza $\phi_1 \wedge \cdots \wedge \phi_n$, zaś $\bigvee_{i=1}^n \phi_i$ oznacza $\phi_1 \vee \cdots \vee \phi_n$.

Zadanie 35. Dane są formuły $\phi_1, \ldots, \phi_n, \psi_1, \ldots, \psi_n$. Wykaż, że dla każdego n poniższa formuła zdaniowa jest tautologią:

$$\Big(\bigwedge_{i=1}^{n} \big(\phi_i \Rightarrow \psi_i\big)\Big) \quad \Rightarrow \quad \Big(\Big(\bigvee_{i=1}^{n} \phi_i\Big) \Rightarrow \Big(\bigvee_{i=1}^{n} \psi_i\Big)\Big).$$

Zadanie 36. Dane są formuły $\phi_1, \ldots, \phi_n, \psi$. Wykaż, że dla każdego n poniższa formuła zdaniowa jest tautologią:

$$\Big(\bigvee_{i=1}^{n} \big(\phi_i \Rightarrow \psi\big)\Big) \quad \Rightarrow \quad \Big(\Big(\bigwedge_{i=1}^{n} \phi_i\Big) \Rightarrow \psi\Big).$$

Zadanie 37. 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 38. Wykaż, że formuła $(\ldots((p_1 \Rightarrow p_2) \Rightarrow p_3) \Rightarrow \ldots \Rightarrow p_{n-1}) \Rightarrow p_n$ jest fałszywa dla dokładnie

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

wartościowań zmiennych $p_1, \ldots, p_n$. Dla ilu wartościowań zmiennych $p_1, \ldots, p_n$ prawdziwa jest formuła $p_1 \Rightarrow (p_2 \Rightarrow (p_3 \Rightarrow \ldots \Rightarrow (p_{n-1} \Rightarrow p_n)\ldots)$?

Zadanie 39. Niech V będzie zbiorem zmiennych zdaniowych. V-literałem nazywamy formułę postaci x lub $\neg x$, dla pewnego $x \in V$. 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 40. Pokaż przez indukcję, że dla każdej formuły ϕ zbudowanej ze zmiennych p i q oraz spójnika $\Rightarrow$, można wybrać ze zbioru $\{\top, p, q, (p \Rightarrow q), (q \Rightarrow p), (p \vee q)\}$ taką formułę ψ, że $(\phi \Leftrightarrow \psi)$ jest tautologią.

Zadanie 41. Udowodnij, że jeśli p jest zmienną zdaniową, a ϕ formułą rachunku zdań, taką, że $p \Rightarrow \phi$ i $\neg\phi \Rightarrow p$ są tautologiami, to ϕ jest tautologią.

1.5. Funkcje boolowskie i zupełne zbiory spójników

Definicja 8. Funkcje $f : \mathcal{B}^n \to \mathcal{B}$, gdzie $\mathcal{B} = \{\mathsf{T}, \mathsf{F}\}$ 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 związujemy jego *znaczenie* — funkcję boolowską określającą prawdziwość formuł zbudowanych przy użyciu tego spójnika.

Definicja 9. Formuła ϕ zbudowana ze zmiennych $p_1, \ldots, p_n$ *opisuje* n-argumentową funkcję boolowską f, jeżeli dla każdego wartościowania σ zmiennych $p_1, \ldots, p_n$ zachodzi:

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

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

$$f(p_1, \ldots, p_n) \quad \equiv \quad \phi.$$

Definicja 10. 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 *2-zupełny*, jeżeli każdą *co najwyżej dwuargumentową* funkcję boolowską można opisać za pomocą formuły zdaniowej zawierającej jedynie spójniki z tego zbioru i zmienne.

Innymi słowy zbiór spójników jest zupełny (2-zupełny), jeśli każdą funkcję boolowską (każdą funkcję boolowską co najwyżej dwuargumentową) można przedstawić jako złożenie funkcji boolowskich określających znaczenie spójników z podanego zbioru.

Zadanie 42. Ile jest funkcji boolowskich n-argumentowych?

Zadanie 43. Pokaż, że $\{\vee, \wedge\}$ nie jest zupełny.

Zadanie 44. Pokaż, że $\{\vee, \wedge, \Leftrightarrow, \Rightarrow\}$ nie jest zupełny.

Zadanie 45. Pokaż, że $\{\vee, \wedge, \Leftrightarrow, \bot\}$ nie jest zupełny.

Zadanie 46. Pokaż, że $\{\Leftrightarrow, \bot\}$ nie jest zupełny.

Zadanie 47. Pokaż, że $\{\wedge, \vee, \neg\}$ jest zupełny.

Zadanie 48. Pokaż, że $\{\wedge, \neg\}$ jest zupełny.

Zadanie 49. Pokaż, że $\{\vee, \neg\}$ jest zupełny.

Zadanie 50. Pokaż, że $\{\Rightarrow, \bot\}$ jest zupełny.

Zadanie 51. Pokaż, że $\{\Rightarrow, \neg\}$ jest zupełny.

Zadanie 52. Udowodnij, że każdy 2-zupełny zbiór spójników jest zupełny.

Zadanie 53. Udowodnij, że zbiór $\{\vee, \wedge, \Rightarrow, \neg\}$ jest 2-zupełny.

Zadanie 54. Czy system spójników $\{\oplus, \top\}$ jest zupełny, gdzie $p \oplus q$ jest prawdziwe wtedy i tylko wtedy, gdy $p \wedge \neg q$, zaś $\top$ oznacza prawdę?

Zadanie 55. Pokaż, że istnieje binarny spójnik $\uparrow$, taki, że $\{\uparrow\}$ jest zupełny.

Zadanie 56. Ile jest binarnych spójników logicznych $\oplus$, takich, że $\{\oplus\}$ jest zupełny?

1.6. Składnia rachunku kwantyfikatorów

Definicja 11. W *rachunku kwantyfikatorów* używamy tzw. *zmiennych indywiduowych* pochodzących z nieskończonego zbioru $X = \{x, y, z, x_1, x_2, \ldots\}$, *symboli funkcyjnych* $f, g, f_1, f_2, \ldots$ i *symboli relacji* $p, q, p_1, p_2, \ldots$ Z każdym symbolem funkcyjnym i z każdym symbolem relacji związujemy liczbę naturalną, która określa liczbę jego argumentów (*arność*). Symbole funkcyjne 0-argumentowe nazywamy *symbolami stałych*. Symbole relacji można uważać za uogólnienie zmiennych zdaniowych z rachunku zdań (zmiene zdaniowe, to 0-argumentowe symbole relacji).

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

1. Każda zmienna indywiduowa jest termem.
2. Każdy symbol stałej jest termem.

3. Jeśli $t_1, \ldots, t_n$ są termami, a f jest n-argumentowym ($n > 0$) sybolem funkcyjnym, to $f(t_1, \ldots, t_n)$ jest termem.
4. Wszystkie termy 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 $\bot$ i $\top$ są formułami atomowymi.
2. Każdy 0-argumentowy symbol relacji jest formułą atomową.
3. Jeśli $t_1, \ldots, t_n$ są termami, a p jest n-argumentowym ($n > 0$) sybolem relacji, to $p(t_1, \ldots, t_n)$ jest formułą atomową.
4. Wszystkie formuły atomowe można otrzymać przy pomocy reguł 1–3.

Formuły rachunku kwantyfikatorów (które będziemy oznaczać $\phi, \psi, \ldots$) 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 ϕ jest formułą rachunku kwantyfikatorów, to jest nią też $(\forall x\, \phi)$ i $(\exists x\, \phi)$.
4. Wszystkie formuły rachunku kwantyfikatorów można otrzymać przy pomocy reguł 1–3.

Dla zwiększenia czytelności opuszczamy niektóre nawiasy w podobny sposób, jak w rachunku zdań.

Definicja 12. Mówimy, że w formule $\forall x\, \phi$ kwantyfikator $\forall$ *wiąże* zmienną x. Wystąpienia zmiennej x w formule ϕ są *związane* przez ten kwantyfikator. Zmienne, które nie są związane w danej formule, są *wolne*. Formalnie zbiór $\mathrm{FV}(\phi)$ zmiennych wolnych formuły ϕ definiujemy następująco:

$$\begin{array}{rcl}
\mathrm{FV}(x) & = & \{x\} \\
\mathrm{FV}(f(t_1, \ldots, t_n)) & = & \mathrm{FV}(t_1) \cup \ldots \cup \mathrm{FV}(t_n) \\
\mathrm{FV}(\bot) & = & \emptyset \\
\mathrm{FV}(\top) & = & \emptyset \\
\mathrm{FV}(p(t_1, \ldots, t_n)) & = & \mathrm{FV}(t_1) \cup \ldots \cup \mathrm{FV}(t_n) \\
\mathrm{FV}(\neg\phi) & = & \mathrm{FV}(\phi) \\
\mathrm{FV}(\phi \circ \psi) & = & \mathrm{FV}(\phi) \cup \mathrm{FV}(\psi), \quad \text{gdzie } \circ \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\} \\
\mathrm{FV}(\mathcal{Q}x\, \phi) & = & \mathrm{FV}(\phi) \backslash \{x\}, \quad \text{gdzie } \mathcal{Q} \in \{\forall, \exists\}
\end{array}$$

Podobnie definiujemy zbiór zmiennych związanych.

1.7. 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 $\forall x.\phi$ jest spełniona, gdy formuła ϕ jest spełniona dla każdej możliwej wartości zmiennej x, zaś formuła $\exists x.\phi$ jest spełniona, gdy istnieje pewna wartość zmiennej x, dla której formuła ϕ jest spełniona.

Przykład 13. Prawami rachunku kwantyfikatorów są np. *prawa negowania kwantyfikatorów*:

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

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."

W poniższych zadaniach sprawdź, które z formuł rachunku kwantyfikatorów są prawami rachunku kwantyfikatorów.

Zadanie 57. $(\forall x\, (\Phi(x) \vee \Psi(x))) \Rightarrow (\forall x\, \Phi(x)) \vee (\forall x\, \Psi(x))$

Zadanie 58. $(\forall x\, (\Phi(x) \wedge \Psi(x))) \Rightarrow (\forall x\, \Phi(x)) \wedge (\forall x\, \Psi(x))$

Zadanie 59. $(\exists x\, (\Phi(x) \vee \Psi(x))) \Rightarrow (\exists x\, \Phi(x)) \vee (\exists x\, \Psi(x))$

Zadanie 60. $(\exists x\, \Phi(x)) \wedge (\exists x\, \Psi(x)) \Rightarrow (\exists x\, (\Phi(x) \wedge \Psi(x)))$

Zadanie 61. Czy formuła

$$((\forall x \phi(x)) \Leftrightarrow \neg(\forall x\, \psi(x))) \Rightarrow \exists x (\phi(x)) \Leftrightarrow \neg\psi(x))$$

jest tautologią?

1.8. Formalizacja w języku rachunku kwantyfikatorów

Zadanie 62. Formuła ϕ jest w *postaci normalnej*, jeśli jest postaci $\mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n\, \psi$, gdzie x_i są pewnymi zmiennymi, $\mathcal{Q}_i$ są kwantyfikatorami ($\mathcal{Q}_i \in \{\forall, \exists\}$ dla $i = 1, \ldots, n$), 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.

Funkcja $f : \mathbb{N} \to \mathbb{N}$ jest *słabo rosnąca*, jeśli

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

Funkcja $f : \mathbb{N} \to \mathbb{N}$ jest *słabo malejąca*, jeśli

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

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 63. Przy pomocy symboli $=, \leq, +, \times$, spójników logicznych i kwantyfikatorów zapisz nastepujące 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 64. 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 63 oraz dodatkowo symbolu potęgowania $\uparrow$, zapisz zdanie równoważne zdaniu „dla każdej liczby naturalnej m istnieje n, takie, że $g^n(m) = 1$”, gdzie g^m oznacza funkcję g złożoną ze sobą m razy, na przykład $g^2(3) = 5$. *Wskazówka:* ciąg skończony liczb naturalnych $a_1, a_2, \ldots a_m$ możemy zakodować jako jedną liczbę $2^{a_1} 3^{a_2} \ldots p_m^{a_m}$, gdzie p_i jest i-tą liczbą pierwszą.

Zadanie 65. 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 znajdą 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 $f : \mathbb{N} \to \mathbb{N}$ jest silnie rosnąca (dla większych argumentów ma większe wartości), to jej wartości są nieograniczone.

Zadanie 66. Niech na pewnym skończonym zbiorze X będzie określona binarna relacja R. Mówimy, że zbiór X z relacją R jest *hamiltonowski*, jeśli istnieje ciąg elementów zbioru X, taki, 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) wyraź 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 67. 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

$$\begin{aligned} x \in P &\iff x \text{ jest panią,} \\ x \in D &\iff x \text{ jest dżentelmenem,} \\ Z(x, y) &\iff x \text{ zna } y, \end{aligned}$$

oraz równości $=$ i spójników logicznych oraz kwantyfikatorów.
Niech

$$\begin{aligned} \psi_1 &= \phi_1 \wedge \phi_2 \\ \psi_2 &= \phi_3 \wedge \phi_4 \\ \psi_3 &= \phi_2 \wedge \phi_3 \wedge \phi_4 \\ \psi_4 &= \phi_1 \wedge \phi_2 \wedge \phi_3 \wedge \phi_4 \end{aligned}$$

Używając symboli $+$, $\times$, $:$, $\leq$, liczb naturalnych oraz symboli logicznych, napisz formuły $\delta_i(p, d)$, $i = 1, \ldots, 4$, spełnione dokładnie dla tych liczb naturalnych p i d, dla których istnieją zbiory pań P i dżentelmenów D, oraz relacja „znajomości" $Z \subseteq (P \cup D)^2$, takie, że $p = |P|$, $d = |D|$ i spełniona jest formuła ψ_i. Na przykład formuła

$$\delta_5(p,d) \quad \Leftrightarrow \quad p = 2d$$

zachodzi dla tych liczb naturalnych p i d, dla których istnieją zbiory pań P i dżentelmenów D oraz relacja „znajomości" $Z \subseteq (P \cup D)^2$, takie, że spełniona jest formuła ψ_5, mówiąca, że każdy dżentelmen zna dokładnie dwie panie, a każda pani zna dokładnie jednego dżentelmena.

2

Zbiory

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

Aksjomat 14 (zasada ekstensjonalności). Dwa zbiory są *równe*, jeżeli zawierają dokładnie te same elementy, tj.

$$\forall x\,(x \in A \Leftrightarrow x \in B) \quad \Rightarrow \quad A = B.$$

Definicja 15. *Zbiór pusty* $\emptyset$ jest zbiorem nie zawierającym żadnego elementu:

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

Aksjomat 16 (zbioru pustego). Zbiór pusty istnieje.

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

Definicja 17. Zbiór A jest *podzbiorem* zbioru B, co będziemy zapisywać $A \subseteq B$, jeżeli B zawiera wszystkie elementy zbioru A, tj.

$$A \subseteq B \quad \Leftrightarrow \quad \forall x\,(x \in A \Rightarrow x \in B).$$

Zauważmy, że dwa zbiory są równe wtedy i tylko wtedy, gdy są nawzajem swoimi podzbiorami, tj.

$$A = B \quad \Leftrightarrow \quad A \subseteq B \land B \subseteq A.$$

Definicja 18. Napisy $\{x \mid \phi\}$ i $\{x : \phi\}$ oznaczają zbiór tych elementów x, które spełniają formułę ϕ.

Przykład 19. Napis $\{n \mid \exists m{\in}\mathbb{N}\,(n = 3m)\}$ oznacza zbiór liczb naturalnych podzielnych przez 3.

Definicja 20. Rodzinę wszystkich podzbiorów zbioru A nazywamy *zbiorem potęgowym* zbioru A i oznaczamy $\mathcal{P}(A)$. Formalnie:

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

2.1. Działania na zbiorach

Definicja 21. Na zbiorach wprowadzamy operacje *sumy* $\cup$, *przekroju* $\cap$ i *różnicy* $\setminus$:

$$\begin{aligned} x \in A \cup B &\iff x \in A \vee x \in B \\ x \in A \cap B &\iff x \in A \wedge x \in B \\ x \in A \setminus B &\iff x \in A \wedge x \notin B \end{aligned}$$

Powyższe operacje mają wiele ciekawych własności. Dla przykładu:

Fakt 22 (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

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

Istotnie, z definicji różnicy zbiorów

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

Następnie z definicji sumy zbiorów mamy

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

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

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

Na mocy tautologii $p \Leftrightarrow (p \wedge p)$ możemy do formuły dopisać jeszcze jedno wystąpienie $x \in A$. Ponadto koniunkcja jest łączna i przemienna, możemy zatem dowolnie pogrupować jej czynniki:

$$\begin{aligned} x \in A \wedge (x \notin B \wedge x \notin C) &\iff x \in A \wedge x \in A \wedge (x \notin B \wedge x \notin C) \\ &\iff (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \end{aligned}$$

Korzystając dwukrotnie z definicji różnicy zbiorów mamy

$$(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \iff (x \in A \setminus B) \wedge (x \in A \setminus C)$$

Na mocy definicji przekroju zbiorów mamy ostatecznie

$$(x \in A \setminus B) \wedge (x \in A \setminus C) \iff x \in (A \setminus B) \cap (A \setminus C)$$

Rozpoczęliśmy od formuły $x \in A \setminus (B \cup C)$. Przechodząc przez szereg formuł równoważnych otrzymaliśmy ostatecznie $x \in (A \setminus B) \cap (A \setminus C)$. Twierdzenie jest zatem udowodnione. ■

Zadanie 68. Wykaż, że dla dowolnych zbiorów A, B, C i D zachodzi:

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

Definicja 23. *Różnicę symetryczną* $\dot{-}$ zbiorów A i B definiujemy następująco:

$$x \in A \dot{-} B \quad \Leftrightarrow \quad x \in A \Leftrightarrow x \notin B$$

Zadanie 69. Pokaż, że różnica symetryczna jest operacją *łączną* i *przemienną*, 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 70. Udowodnij, że

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

2.2. Operacje nieskończone na zbiorach

Definicja 24. Dwuargumentowe operacje sumy i przekroju zbiorów można rozszerzyć na dowolne rodziny[9] zbiorów. Suma wszystkich zbiorów z rodziny $\{A_s\}_{s \in S}$, gdzie S jest pewnym zbiorem *indeksów*, 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:

$$x \in \bigcup_{s \in S} A_s \quad \Leftrightarrow \quad \exists s \in S \ (x \in A_s)$$
$$x \in \bigcap_{s \in S} A_s \quad \Leftrightarrow \quad \forall s \in S \ (x \in A_s)$$

W poniższych zadaniach udowodnij, że dla dowolnych rodzin zbiorów $\{A_t\}_{t \in T}$, $\{B_t\}_{t \in T}$ i $\{A_{t,s}\}_{\substack{t \in T \\ s \in S}}$, gdzie T i S są niepustymi zbiorami indeksów, zachodzą odpowiednie relacje. W którym przypadku zachodzi inkluzja odwrotna?

Zadanie 71. $\bigcup_{t \in T} (A_t \cup B_t) = \bigcup_{t \in T} A_t \cup \bigcup_{t \in T} B_t$

Zadanie 72. $\bigcup_{t \in T} (A_t \cap B_t) \subseteq \bigcup_{t \in T} A_t \cap \bigcup_{t \in T} B_t$

[9] Z powodów językowych zbiory zbiorów nazywa się *rodzinami*. Z matematycznego punktu widzenia są to zwykłe zbiory.

Zadanie 73. $\bigcap_{t\in T} A_t \cup \bigcap_{t\in T} B_t \subseteq \bigcap_{t\in T} (A_t \cup B_t)$

Zadanie 74. $\bigcap_{t\in T} A_t \cup \bigcap_{t\in T} B_t \subseteq \bigcup_{t\in T} (A_t \cap B_t)$

Zadanie 75. $\bigcup_{t\in T} \bigcap_{s\in S} A_{t,s} \subseteq \bigcap_{s\in S} \bigcup_{t\in T} A_{t,s}$

Definicja 25. 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 76. Udowodnij, że jeśli $\{A_n\}_{n\in\mathbb{N}}$ jest zstępującą rodziną zbiorów, to

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

Zadanie 77. Udowodnij, że jeśli $\{A_n\}_{n\in\mathbb{N}}$ jest zstępującą rodziną zbiorów, to

$$\bigcup_{n=1}^{\infty} \bigcap_{i=1}^{n} A_i \quad = \quad \bigcap_{n=1}^{\infty} \bigcup_{i=1}^{n} A_i\,.$$

Zadanie 78. Niech $\{A_{n,m}\}_{n,m=1}^{\infty}$ 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

$$\bigcup_{n=1}^{\infty} \bigcup_{m=1}^{\infty} A_{n,m} \quad = \quad \bigcup_{n=1}^{\infty} A_{n,n}\,.$$

W poniższych zadaniach udowodnij podane zawierania. W których wzorach znak zawierania można zastąpić znakiem równości?

Zadanie 79. $\bigcap_{n=0}^{\infty} A_n \subseteq \bigcup_{n=0}^{\infty} \bigcap_{k=n}^{\infty} A_k$

Zadanie 80. $\bigcup_{n=0}^{\infty} \bigcap_{k=n}^{\infty} A_k \subseteq \bigcap_{n=0}^{\infty} \bigcup_{k=n}^{\infty} A_k$

Zadanie 81. $\bigcap_{n=0}^{\infty} \bigcup_{k=n}^{\infty} A_k \subseteq \bigcup_{n=0}^{\infty} A_n$

Zadanie 82. $\bigcup_{n=1}^{\infty} A_n \subseteq \bigcup_{n=1}^{\infty}(A_n \setminus \bigcup_{m=1}^{n-1} A_m)$

Zadanie 83. Dane są ciągi zbiorów $\langle A_i : i \in \mathbb{N}\rangle$ i $\langle B_i : i \in \mathbb{N}\rangle$. 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 84. Niech $\langle A_n : n \in \mathbb{N} \rangle$ będzie ciągiem podzbiorów zbioru X. Niech (A) oznacza, że A_0 jest zbiorem skończonym, oraz (B) oznacza, że dla każdego n zachodzi $\bigcap_{i=0}^{n} A_i \neq \emptyset$. Pokaż, że: a) jeśli zachodzi (A) i (B), to $\bigcap_{i=0}^{\infty} A_i \neq \emptyset$, b) istnieje ciąg $\langle A_n : n \in \mathbb{N} \rangle$ spełniający warunek (B), taki, że $\bigcap_{i=0}^{\infty} A_i = \emptyset$.

Zadanie 85. Niech $\langle A_n : n \in \mathbb{N} \rangle$ będzie ciągiem skończonych podzbiorów zbioru X, takim, że $A_{n_1} \cap \ldots \cap A_{n_k} \neq \emptyset$ dla dowolnych $n_1, \ldots, n_k \in \mathbb{N}$. Pokaż, że $\bigcap_{i=1}^{\infty} A_i \neq \emptyset$.

2.3. Wzór włączeń i wyłączeń

Definicja 26. Mówimy, że zbiór A *ma n elementów* ($n \geq 0$), co zapisujemy $|A| = n$, jeżeli istnieje wzajemnie jednoznaczne przyporządkowanie elementom tego zbioru liczb $1, 2, \ldots, n$, tj. jeśli elementy tego zbioru można ponumerować liczbami od 1 do n. Zbiór pusty ma zatem 0 elementów.

Zadanie 86. 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 87. Liczbę elementów skończonego zbioru A będziemy oznaczać $|A|$. Jeżeli zbiory A i B są rozłączne, to $|A \cup B| = |A| + |B|$. Korzystając z powyższej własności udowodnij, że dla dowolnych zbiorów A, B i C (niekoniecznie rozłącznych):

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B| \\ |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \end{aligned}$$

Zadanie 88. Udowodnij indukcyjnie, że dla dowolnej rodziny zbiorów skończonych $\{A_i\}_{i=1}^{n}$ prawdziwy jest tzw. *wzór włączeń i wyłączeń*:

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

Zadanie 89. Rodzina $\{A_i\}_{i=1}^{n}$ jest rodziną zbiorów *k-rozłącznych*, jeśli dla każdego rosnącego ciągu liczb naturalnych $\langle i_1, i_2, \ldots, i_k \rangle$ takiego, że $i_k \leq n$, mamy

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

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

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

Zadanie 90. 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.

3

Relacje

3.1. Para uporządkowana i iloczyn (produkt) kartezjański

Parę elementów a i b będziemy zapisywać w postaci $\langle a, b\rangle$. Para będzie dla nas pojęciem pierwotnym. Przyjmujemy następujący:

Aksjomat 27. $\langle a, b\rangle = \langle c, d\rangle \iff (a = c \wedge b = d)$.

Specjaliści od podstaw matematyki pragną za pojęcia pierwotne uważać jedynie zbiór i relację należenia do zbioru i wolą *zdefiniować* parę następująco:

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

Para w takim ujęciu składa się ze zbioru dwuelementowego, w którym wyróżniliśmy, który element jest pierwszy. Zauważmy, że tak zdefiniowana para spełnia podany wyżej aksjomat.

Definicja 28. *Iloczynem kartezjańskim* dwóch zbiorów nazywamy zbiór wszystkich par złożonych z elementów tych zbiorów:

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

W poniższych zadaniach uzupełnij i udowodnij podane wzory.

Zadanie 91. $(A \cap B) \times C = (A \times C) \cap (B \times C)$

Zadanie 92. $(A \cup B) \times C = ?$

Zadanie 93. $(A \cup B) \times (C \cup D) = ?$

Zadanie 94. Udowodnij, że

$$A \times B = B \times A \quad \iff \quad A = \emptyset \vee B = \emptyset \vee A = B$$

dla dowolnych zbiorów A i B.

Zadanie 95. Udowodnij, że jeżeli $A \times B = C \times D$, to

$$(A = C \wedge B = D) \vee ((A = \emptyset \vee B = \emptyset) \wedge (C = \emptyset \vee D = \emptyset)).$$

3.2. Relacje

Definicja 29. 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*. Zamiast pisać $\langle a, b\rangle \in R$, piszemy też niekiedy $a R b$. Podzbiory A^2 są *binarnymi relacjami na zbiorze* A.

Przykład 30. Relacjami binarnymi są:

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

Zadanie 96. Podaj intuicyjny sens poniższych relacji dwuargumentowych na zbiorze $\{1, 2, 3, 4, 5, 6\}$:

a)

y\ 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\ 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\ 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.)

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 $\langle a_1, \ldots, a_n \rangle$ jest pojęciem pierwotnym i przyjmujemy:

Aksjomat 31. $\langle a_1, \ldots, a_n \rangle = \langle b_1, \ldots, b_n \rangle \;\Leftrightarrow\; a_1 = b_1 \wedge \ldots \wedge a_n = b_n.$

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:

$$\begin{cases} \langle a_1, a_2 \rangle = \langle a_1, a_2 \rangle & \text{(krotka dwuelementowa jest parą)} \\ \langle a_0, a_1, \ldots, a_n \rangle = \langle a_0, \langle a_1, \ldots, a_n \rangle \rangle & \end{cases}$$

Definicja 32. W oczywisty sposób uogólniamy pojęcie *produktu* na n zbiorów:

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

Relacją n-argumentową nazywamy dowolny podzbiór produktu n zbiorów.

Dla przykładu

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

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

Zadanie 97. Ile jest relacji n-argumentowych na zbiorze 5-elementowym?

3.4. Złożenie relacji. Relacja odwrotna

Definicja 33. Dane są relacje $P \subseteq A \times B$ i $Q \subseteq B \times C$. Relacja

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

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.

Twierdzenie 34. Dla dowolnych relacji $T \subseteq A \times B$, $R \subseteq B \times C$ i $S \subseteq C \times D$:

$$\begin{aligned} T(RS) &= (TR)S \\ (RS)^{-1} &= S^{-1}R^{-1} \end{aligned}$$

Zadanie 98. Oblicz $R^2 = RR$, R^3 i R^4 dla relacji z zadania 96.

Zadanie 99. Uzupełnij i udowodnij wzory:

$$\begin{aligned}
T(RS) &= (TR)S \\
(RS)^{-1} &= S^{-1}R^{-1} \\
(R \cup S)^{-1} &= R^{-1} \cup S^{-1} \\
(R \cap S)^{-1} &= R^{-1} \cap S^{-1} \\
(R^{-1})^{-1} &= R \\
(R \cup S)T &= RT \cup ST \\
(R \cap S)T &\subseteq RT \cap ST \\
((R \cup S)T)^{-1} &= T^{-1}R^{-1} \cup T^{-1}S^{-1} \\
(A \times B)^{-1} &= B \times A \\
(A \times B)(C \times D) &= ?
\end{aligned}$$

4

Funkcje

Definicja 35. Relację $f \subseteq A \times B$ nazywamy *funkcją o dziedzinie* A *i zbiorze wartości (przeciwdziedzinie)* B, jeżeli

1. $\forall a{\in}A\ \exists b{\in}B\ \langle a, b\rangle \in f$
2. $\forall a{\in}A\ \forall b_1{\in}B\ \forall b_2{\in}B\ (\langle a, b_1\rangle \in f \land \langle a, b_2\rangle \in f \Rightarrow b_1 = b_2)$

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

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

Zamiast $f \in B^A$ piszemy zwykle $f : A \to B$. Napis $f(a)$ oznacza element b, taki, 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 36. Ile jest funkcji $f : A \to B$? Ile jest funkcji $f : \emptyset \to B$, a ile $f : A \to \emptyset$?

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

Definicja 37. Funkcja $f : A \to B$ jest *różnowartościowa* (jest *injekcją*), jeżeli

$$\forall a_1, a_2 \in A\ (f(a_1) = f(a_2) \Rightarrow a_1 = a_2).$$

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

$$\forall b{\in}B\ \exists a{\in}A\ \ f(a) = b.$$

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

Zadanie 100. Które spośród relacji z zadania 96 są funkcjami?

4.1. Funkcje odwrotne i złożenie funkcji

Twierdzenie 38. Niech dane będą funkcje $f : A \to B$ i $g : B \to C$. 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 fg też jest różnowartościowa. Jeżeli obie funkcje f i g są „na", to fg też jest „na".

Definicja 39. Niech $f : A \to B$ będzie funkcją. Wtedy funkcja $g : B \to A$ 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 40. Niech $f : A \to B$ 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}.

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

Zadanie 101. Jeżeli gf jest „na", to f jest „na".

Zadanie 102. Jeżeli gf jest „na", to g jest „na".

Zadanie 103. Jeżeli gf jest różnowartościowa, to f jest różnowartościowa.

Zadanie 104. Jeżeli gf jest różnowartościowa, to g jest różnowartościowa.

4.2. Obraz i przeciwobraz zbioru

Definicja 41. Niech $f : A \to B$ będzie funkcją i niech $X \subseteq A$. *Obrazem zbioru X w odwzorowaniu f* nazywamy zbiór

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

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

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

Definicja 42. Niech $\mathcal{X}$ będzie rodziną podzbiorów zbioru A. Wtedy

$$\bigcup \mathcal{X} = \bigcup_{X \in \mathcal{X}} X$$

$$\bigcap \mathcal{X} = \bigcap_{X \in \mathcal{X}} X$$

Twierdzenie 43. Niech $f : A \to B$ będzie funkcją, $\mathcal{X}$ rodziną podzbiorów zbioru A, zaś $\mathcal{Y}$ rodziną podzbiorów zbioru B. Wtedy

$$
\begin{aligned}
& & f(\bigcup \mathcal{X}) &= \bigcup\{f(X) \mid X \in \mathcal{X}\} & (1)\\
&\text{Jeśli } \mathcal{X} \neq \emptyset, \text{ to} & f(\bigcap \mathcal{X}) &\subseteq \bigcap\{f(X) \mid X \in \mathcal{X}\} & (2)\\
& & f^{-1}(\bigcup \mathcal{Y}) &= \bigcup\{f^{-1}(Y) \mid Y \in \mathcal{Y}\} & (3)\\
&\text{Jeśli } \mathcal{Y} \neq \emptyset, \text{ to} & f^{-1}(\bigcap \mathcal{Y}) &= \bigcap\{f^{-1}(Y) \mid Y \in \mathcal{Y}\} & (4)
\end{aligned}
$$

Pytanie 44. Czy symbol „$\subseteq$” we wzorze (2) można zastąpić symbolem „$=$”?

Zadanie 105. Niech $f : X \to Y$, $A, B \subseteq X$. Uzupełnij i udowodnij wzory:

$$
\begin{aligned}
f(A \cup B) &= f(A) \cup f(B)\\
f(A \cap B) &\;?\; f(A) \cap f(B)\\
f^{-1}(f(A)) &\;?\; A
\end{aligned}
$$

Zadanie 106. Niech $f : X \to Y$, $C, D \subseteq Y$. Uzupełnij i udowodnij wzory:

$$
\begin{aligned}
f^{-1}(C \cap D) &= f^{-1}(C) \cap f^{-1}(D)\\
f^{-1}(C \cup D) &= \;?\\
f(f^{-1}(C)) &= \;?
\end{aligned}
$$

Zadanie 107. Niech $f : X \to Y$ będzie bijekcją, a $g : Y \to X$ funkcją odwrotną do f. Udowodnij, że $f^{-1}(C) = g(C)$ dla dowolnego $C \subseteq Y$.

5

Relacje równoważności

Definicja 45. Relacja $R \subseteq A \times A$ jest

- *zwrotna*, jeśli aRa dla każdego $a \in A$,
- *symetryczna*, jeśli $aRb \Rightarrow bRa$ dla każdych $a, b \in A$,
- *przechodnia*, jeśli $aRb \wedge bRc \Rightarrow aRc$ dla wszelkich $a, b, c \in A$.

Relację zwrotną, symetryczną i przechodnią nazywamy *relacją równoważności*.

Definicja 46. *Klasą abstrakcji* elementu $a \in A$ względem relacji równoważności $\sim \subseteq A \times A$ nazywamy zbiór

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

Definicja 47. 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:

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

3. zbiory X_i są parami rozłączne:

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

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

Definicja 48. 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 $Y \in \mathcal{P}_2$, taki, że $X \subseteq Y$.

Lemat 49. Dla dowolnej relacji równoważności $\sim \subseteq A \times A$ i elementów $a, b \in A$

$$a \sim b \quad \Leftrightarrow \quad [a]_\sim = [b]_\sim.$$

Twierdzenie 50 (Zasada Abstrakcji).

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

Przykład 51. Niech $a, b, c, d \in \mathbb{Z}$, $c, d \neq 0$. Definiujemy relację $\sim \subseteq (\mathbb{Z} \times (\mathbb{Z} \backslash \{0\})^2$ wzorem

$$\langle a, b\rangle \sim \langle c, d\rangle \quad \Leftrightarrow \quad a \cdot d = b \cdot c.$$

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

Zadanie 108. 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 109. 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 110. 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 111. Relacja R jest przechodnia. Które z poniższych stwierdzeń są prawdziwe:

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

Zadanie 112. Wykaż, że jeśli R jest relacją zwrotną i przechodnią, to $R^n = R$ dla każdego $n \geq 1$.

Zadanie 113. Relacje R i S są relacjami równoważności na tym samym zbiorze. Czy $R \cup S$, $R \cap S$, $R \backslash S$, $R \dot{-} S$ też są relacjami równoważności?

Zadanie 114. 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 115. Niech A będzie ustalonym niepustym zbiorem. Czy prawdą jest, że dla dowolnej relacji $R \subseteq A^2$

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

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 116. Niech $R \subseteq A^2$ będzie pewną relacją binarną na zbiorze A. Niech $\mathcal{T}$ będzie zbiorem wszystkich relacji przechodnich S na A, takich, że $R \subseteq S$. Oznaczmy przez $\bar{R}$ relację $\bigcap_{S \in \mathcal{T}} S$. Pokaż, że $R \subseteq \bar{R}$. Pokaż, że jeśli S jest relacją przechodnią, taką, że $R \subseteq S$, to $\bar{R} \subseteq S$. Pokaż, że $\bar{R}$ jest relacją przechodnią. Relację $\bar{R}$ nazywamy *tranzytywnym (przechodnim) domknięciem* R.

Zadanie 117. Niech $R \subseteq A^2$ będzię 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 118. Niech $Q \subseteq A^2$ będzię dowolną relacją, $Q^1 = Q$ i niech $Q^{n+1} = Q^n Q$ dla $n \geq 1$. Kładziemy $Q_\infty = \bigcup_{n=1}^{\infty} Q^n$. Wykaż, że Q_∞ jest relacją przechodnią.

Zadanie 119. Wykaż, że Q_∞ jest *przechodnim domknięciem* relacji Q, tj. przekrojem wszystkich relacji przechodnich zawierających Q.

Zadanie 120. Korzystając z zadań poprzednich wykaż, że jeśli R jest dowolną relacją oraz $Q = R \cup R^{-1}$, to Q_∞ jest relacją równoważności.

Zadanie 121. Udowodnij, że Q_∞ jest najmniejszą (w sensie relacji inkluzji) relacją równoważności zawierającą relację R.

Zadanie 122. Przyjmijmy, że R jest relacją w zbiorze A. Udowodnij, że jeżeli przechodnie domknięcie R zawiera R^{-1}, to jest relacją równoważności.

Zadanie 123. Dane jest przekształcenie $f : A \to B$. W zbiorze A definiujemy relację $\sim$ wzorem

$$x \sim y \quad \Leftrightarrow \quad f(x) = f(y).$$

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

Zadanie 124. Dane jest przekształcenie $f : A \to B$ oraz relacja rownoważności R na B. W zbiorze A definiujemy relację $\sim$ wzorem

$$x \sim y \quad \Leftrightarrow \quad \langle f(x), f(y)\rangle \in R.$$

Udowodnij, że $\sim$ jest relacją równoważności.

Zadanie 125. Ile jest różnych relacji równoważności na zbiorze czteroelementowym? Ile jest różnych relacji równoważności na zbiorze sześcioelementowym?

Zadanie 126. 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? Dla każdej z nich, jeśli odpowiedź jest pozytywna, podaj moc zbioru jej klas abstrakcji.

W poniższych zadaniach sprawdź, dla jakich dodatnich liczb naturalnych k podane relacje na zbiorze $\mathbb{N}$ są relacjami równoważności. Opisz ich klasy abstrakcji. Napis $k|m$ oznacza, że m jest podzielne przez k.

Zadanie 127. $x R_1 y \Leftrightarrow k|(x + y)$

Zadanie 128. $x R_2 y \Leftrightarrow k|(x - y)$

Zadanie 129. $x R_3 y \Leftrightarrow x - y = 2$

Zadanie 130. Czy relacja R określona na zbiorze wielomianów jednej zmiennej o współczynnikach naturalnych wzorem

$$pRq \quad \Leftrightarrow \quad \text{wielomian } p - q \text{ ma wszystkie współczynniki parzyste}$$

jest relacją równoważności?

Zadanie 131. Dany jest zbiór X i jego podzbiór $C \subseteq X$. Czy relacja R określona na $\mathcal{P}(X)$ wzorem

$$ARB \quad \Leftrightarrow \quad A \dot{-} B \subseteq C$$

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

Zadanie 132. W zbiorze wszystkich zbieżnych ciągów nieskończonych o wyrazach wymiernych wprowadzamy relację

$$\bar{a} R \bar{b} \quad \Leftrightarrow \quad \lim_{n\to\infty} (a_n - b_n) = 0$$

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

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

Zadanie 134. $X = \mathbb{N} \times \mathbb{N}$,

$$\langle x_1, y_1\rangle R \langle x_2, y_2\rangle \quad \Leftrightarrow \quad x_1 - y_1 = x_2 - y_2.$$

Zadanie 135. $X = \mathbb{R} \times \mathbb{R}$,

$$\langle x_1, y_1\rangle R \langle x_2, y_2\rangle \quad \Leftrightarrow \quad x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Zadanie 136. $X = \mathbb{R} \times \mathbb{R}$,

$$\langle x_1, y_1\rangle R \langle x_2, y_2\rangle \quad \Leftrightarrow \quad |x_1| + |y_1| = |x_2| + |y_2|.$$

6

Teoria mocy

6.1. Równoliczność zbiorów

Definicja 52. Zbiory A i B *są równoliczne*, jeżeli istnieje bijekcja $f : A \to B$. Piszemy wówczas $A \sim B$.

Przykład 53. 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 $(0, 1)$: $(a, b) \sim (0, 1)$.

Twierdzenie 54. Dla dowolnych zbiorów A, B, C

1. $A \sim A$
2. $A \sim B \Leftrightarrow B \sim A$
3. $(A \sim B \wedge B \sim C) \Leftrightarrow A \sim C$

Definicja 55. *Mocą zbioru* (którą oznaczamy $|A|$) nazywamy obiekt spełniający następującą własność: $A \sim B \Leftrightarrow |A| = |B|$.

Zadanie 137. Czy istnieją zbiory A, B, C, D, takie, że $A \not\sim B$ oraz $C \not\sim D$, ale $A^C \sim B^D$?

Zadanie 138. Konstruując odpowiednie bijekcje udowodnij, że następujące trzy zbiory są równoliczne:

- odcinek otwarty $(0, 1) \subseteq \mathbb{R}$;
- odcinek domknięto-otwarty $[0, 1) \subseteq \mathbb{R}$;
- okrąg na płaszczyźnie o środku $(0, 0)$ i promieniu 1.

Zadanie 139. Skonstruuj bijekcję pomiędzy zbiorem liczb naturalnych a zbiorem niemalejących funkcji ze zbioru liczb naturalnych w zbiór $\{1, 2, 3, 4\}$. Możesz skorzystać z faktu, że istnieje bijekcja z $\mathbb{N}$ na $\mathbb{N} \times \mathbb{N}$.

Zadanie 140. Skonstruuj bijekcję pomiędzy zbiorem $\mathbb{Q}$ liczb wymiernych i zbiorem $\mathbb{Q} \setminus [0, 1]$ (napis $[0, 1]$ oznacza odcinek domknięty o końcach 0 i 1).

Zadanie 141. Wykaż, że jeśli $A_1 \sim A_2$, to

$$\begin{gathered} B^{A_1} \sim B^{A_2}, \\ A_1^B \sim A_2^B, \\ A_1 \times B \sim A_2 \times B. \end{gathered}$$

Zadanie 142. Wykaż, że $(A^B)^C \sim A^{(B \times C)}$.

Zadanie 143. 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 144. Udowodnij, że zbiory $\mathbb{R}$ i $\mathbb{R} \setminus \mathbb{N}$ są równoliczne.

Zadanie 145. Wykaż, że $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$.

Zadanie 146. Wykaż, że $\{0, 1\}^{\mathbb{N}} \sim \mathbb{N}^{\mathbb{N}}$.

6.2. Zbiory skończone

Definicja 56. $\underline{n} = \{0, 1, \ldots, n-1\}$ oznacza zbiór liczb naturalnych mniejszych od n.

Definicja 57. Zbiór A jest *zbiorem skończonym*, jeśli istnieje liczba naturalna $n \in \mathbb{N}$, taka, że $A \sim \underline{n}$. Mówimy wówczas, że zbiór A ma n elementów.

Twierdzenie 58.

1. Dla każdego $n \in \mathbb{N}$ 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 $m \in \mathbb{N}$, $\underline{m} \not\sim \mathbb{N}$.

Zadanie 147. Wykaż, że jeśli zbiory A i B są skończone, $|A| = n$ oraz $|B| = m$, to $|A^B| = n^m$.

Zadanie 148. Niech $A^1 = A$ oraz $A^{n+1} = A^n \times A$. Wykaż, że $A^{\underline{n}} \sim A^n$.

Definicja 59. 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.

Zadanie 149. Dany jest zbiór A i dodatnia liczba naturalna k oraz zbiory $X_i \subseteq A$ dla $i = 1, \dots, k$, takie, że dla każdej funkcji $f : \{1, \dots, k\} \to \{0, 1\}$ zbiór $\bigcap_{i=1}^{k} X_i^{f(i)}$ ma co najwyżej 1 element. Wyznacz maksymalną moc zbioru A.

Zadanie 150. Niech $\langle X_n : n \in \mathbb{N}\rangle$ będzie dowolnym ciągiem podzbiorów zbioru $\mathbb{N}$.

1. Czy istnieje taki nieskończony ciąg zerojedynkowy $\langle i_n : n \in \mathbb{N}\rangle$, że
$$\bigcap_{n=0}^{\infty} X_n^{i_n} \neq \emptyset?$$
2. Jaka jest maksymalna moc zbioru wszystkich ciągów $\langle i_n : n \in \mathbb{N}\rangle$ spełniających powyższy wzór?

Definicja 60. Mówimy, że funkcja dwuargumentowa $f : A \times B \to C$ *istotnie zależy od każdego z argumentów*, jeśli istnieją elementy $a \in A$ i $b_1, b_2 \in B$, takie, że $f(a, b_1) \neq f(a, b_2)$ oraz istnieją elementy $a_1, a_2 \in A$ i $b \in B$, takie, że $f(a_1, b) \neq f(a_2, b)$.

Zadanie 151. Ile jest dwuargumentowych funkcji logicznych istotnie zależnych od każdego z argumentów. Ile jest funkcji $f : A \times B \to C$ istotnie zależnych od każdego z argumentów, gdy każdy ze zbiorów A, B, C ma 3 elementy.

Zadanie 152. Ile jest funkcji $f : A \times B \to C$ istotnie zależnych od każdego z argumentów, gdy każdy ze zbiorów A, B ma 4 elementy, a C ma n elementów.

Zadanie 153. Dane są dwie funkcje $f : A \to B$ i $g : B \to A$, 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 154. Udowodnij, że A jest zbiorem nieskończonym wtedy i tylko wtedy, gdy zawiera podzbiór równoliczny ze zbiorem liczb naturalnych, tj. gdy istnieje zbiór $B \subseteq A$, taki, że $B \sim \mathbb{N}$. (Uwaga: zadanie jest trudne, a dowód wymaga skorzystania z pewnika wyboru).

Zadanie 155. Udowodnij, że A jest zbiorem nieskończonym wtedy i tylko wtedy, gdy jest równoliczny ze swoim właściwym podzbiorem, tj. gdy istnieje zbiór $B \subseteq A$, taki, że $B \neq A$ i $A \sim B$. (Uwaga: zadanie jest trudne, a dowód wymaga skorzystania z pewnika wyboru).

Zadanie 156. 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).

6.3. Moce zbiorów nieskończonych

Definicja 61 (wzorce mocy). Mówiąc o liczbach kardynalnych posługujemy się następującymi reprezentantami zbiorów danej mocy:

- zbiory skończone: $\underline{n} = \{0, 1, \ldots, n-1\}$;
- liczby naturalne: $\mathbb{N} = \{0, 1, \ldots\}$;
- liczby rzeczywiste: $\mathbb{R}$.

Definicja 62. Wprowadzamy następujące oznaczenia mocy zbiorów:

- zbiory skończone: $|\underline{n}| = n$;
- liczby naturalne: $|\mathbb{N}| = \aleph_0$ (*alef zero*);
- liczby rzeczywiste: $|\mathbb{R}| = \mathfrak{c}$ (*kontinuum*).

Twierdzenie 63. Zbiór liczb rzeczywistych jest równoliczny ze zbiorem $\{0, 1\}^{\mathbb{N}}$. Zatem zbiór $\{0, 1\}^{\mathbb{N}}$ ma moc kontinuum.

Definicja 64. Mówimy, że moc zbioru A jest nie większa niż moc zbioru B i piszemy $|A| \leq |B|$, jeśli istnieje funkcja różnowartościowa $f : A \to B$.

Twierdzenie 65 (Cantor-Bernstein). Jeśli $|A| \leq |B|$ oraz $|B| \leq |A|$, to $|A| = |B|$.

Definicja 66. Mówimy, że moc zbioru A jest mniejsza niż moc zbioru B i piszemy $|A| < |B|$, jeśli $|A| \leq |B|$ oraz $A \not\sim B$.

Twierdzenie 67.

1. Dla dowolego 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 $|\underline{n}| < \aleph_0$.

Definicja 68. Jeśli $X \subseteq A$, to $f : A \to \{0,1\}$ jest *funkcją charakterystyczną* zbioru X, jeśli

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

dla dowolnego $a \in A$.

Fakt 69. Dla dowolnego zbioru A zachodzi $\underline{2}^A \sim \mathcal{P}(A)$.

Twierdzenie 70. Niech A i B będą zbiorami, przy czym $|B| \geq 2$. Wtedy

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

Twierdzenie 71 (Cantor). Dla żadnego zbioru A nie istnieje funkcja z A *na* zbiór potęgowy $\mathcal{P}(A)$.

Dowód. Przypuśćmy przeciwnie, że pewna funkcja $f : A \to \mathcal{P}(A)$ przekształca A *na* $\mathcal{P}(A)$. Niech

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

Ponieważ $A_0 \subseteq A$ i f odwzorowuje A *na* $\mathcal{P}(A)$, więc istnieje $a_0 \in A$, takie, że $f(a_0) = A$. Mamy wtedy

$$a_0 \in A_0 \quad \Leftrightarrow \quad a_0 \in f(a_0) \quad \Leftrightarrow \quad a_0 \notin A_0.$$

Założenie istnienia funkcji f doprowadziło do sprzeczności. ■

Dowód (twierdzenia Cantora dla przypadku $A = \mathbb{N}$). Przypuśćmy przeciwnie, że pewna funkcja $f : \mathbb{N} \to \underline{2}^{\mathbb{N}}$ przekształca $\mathbb{N}$ *na* $\underline{2}^{\mathbb{N}}$. Tworzymy nieskończoną tablicę

$$\begin{array}{cccccc}
\boxed{\text{(f(0))(0)}} & (f(0))(1) & (f(0))(2) & (f(0))(3) & (f(0))(4) & \cdots \\
(f(1))(0) & \boxed{\text{(f(1))(1)}} & (f(1))(2) & (f(1))(3) & (f(1))(4) & \cdots \\
(f(2))(0) & (f(2))(1) & \boxed{\text{(f(2))(2)}} & (f(2))(3) & (f(2))(4) & \cdots \\
(f(3))(0) & (f(3))(1) & (f(3))(2) & \boxed{\text{(f(3))(3)}} & (f(3))(4) & \cdots \\
(f(4))(0) & (f(4))(1) & (f(4))(2) & (f(4))(3) & \boxed{\text{(f(4))(4)}} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Tworzymy nową funkcję charakterystyczną

$$g(i) \quad = \quad 1 - (f(i))(i)$$

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 72. Dla każdego A jest $|\mathcal{P}(A)| > |A|$. Jeśli $|B| \geq 2$, to $|B^A| > |A|$.

Zadanie 157. Czy $\sim$ zachowuje porządek liczb kardynalnych, tj. 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 158. Udowodnij, że następujące zbiory są równoliczne:

- kwadrat $\{\langle x, y\rangle \mid 0 \leq x, y \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$,
- odcinek domknięty $[0, 1] \subseteq \mathbb{R}$.

Zadanie 159. Udowodnij, że dla każdej dodatniej liczby naturalnej n zbiór $\mathbb{R}^n$, gdzie $\mathbb{R}$ jest zbiorem liczb rzeczywistych, ma moc kontinuum.

Zadanie 160. Jaka jest moc zbioru $\{\langle x, y\rangle \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$?

Zadanie 161. Niech $R_I(x, y)$ oznacza relację

$$\exists p{\in}I \ \ ((\phi(p, x) \wedge \neg\phi(p, y)) \vee (\phi(p, y) \wedge \neg\phi(p, x)))$$

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 162. Dla danej funkcji $f : \mathbb{N} \to \mathbb{N}$ definiujemy zbiór

$$A_f \quad = \quad \{n \in \mathbb{N} \mid f(n) > 1\}.$$

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 163. Dla ciągu nieskończonego $\mathbf{a} = \langle a_1, a_2, a_3, \ldots\rangle$ o wyrazach naturalnych określamy relację $R_{\mathbf{a}}$ w taki sposób, że dla dwóch ciągów nieskończonych o wyrazach naturalnych $\mathbf{b} = \langle b_1, b_2, b_3, \ldots\rangle$ i $\mathbf{c} = \langle c_1, c_2, c_3, \ldots\rangle$ zachodzi $\mathbf{b}R_{\mathbf{a}}\mathbf{c}$, 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 $\mathbf{a}$ relacja $R_{\mathbf{a}}$ jest relacją równoważności.
2. Jaka jest moc zbioru takich ciągów $\mathbf{a}$, dla których wszystkie klasy abstrakcji $R_{\mathbf{a}}$ są przeliczalne?
3. Jaka jest moc zbioru takich ciągów $\mathbf{a}$, dla których relacja $R_{\mathbf{a}}$ ma przeliczalnie wiele klas abstrakcji?

4. Jaka jest moc zbioru takich ciągów $\mathbf{a}$, dla których relacja $R_{\mathbf{a}}$ ma kontinuum klas abstrakcji i każda z tych klas jest mocy kontinuum?
5. Jaka jest moc zbioru takich ciągów $\mathbf{a}$, dla których relacja $R_{\mathbf{a}}$ ma przeliczalnie wiele klas abstrakcji i każda z tych klas jest przeliczalna?
6. Jaka jest moc zbioru takich ciągów $\mathbf{a}$, dla których relacja $R_{\mathbf{a}}$ ma zarówno przeliczalne, jak i nieprzeliczalne klasy abstrakcji?

Zadanie 164. Niech $P \subset \mathbb{R} \times \mathbb{R}$ oznacza relację taką, że

$$P(x, y) \quad \Leftrightarrow \quad (\exists q \in \mathbb{Q})(x = y + q),$$

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 $[\frac{23}{7}]$? Czy wszystkie klasy równoważności mają tę samą moc?
c) Czy rodzina klas równoważności relacji P jest przeliczalna?

6.4. Zbiory przeliczalne

Definicja 73. Zbiór A jest *przeliczalny*, gdy A jest skończony lub jest równoliczny ze zbiorem liczb naturalnych.

Twierdzenie 74. Zbiór A jest przeliczalny wtedy i tylko wtedy, gdy $A = \emptyset$ lub istnieje funkcja z $\mathbb{N}$ *na* A.

Definicja 75. *Ciągiem elementów zbioru* A nazywamy funkcję $f : \mathbb{N} \to A$.

Fakt 76. Zbiór niepusty jest przeliczalny, gdy wszystkie jego elementy można ustawić w ciąg.

Twierdzenie 77.

1. Podzbiór zbioru przeliczalnego jest przeliczalny.
2. Jeśli $f : A \to B$ 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 $\{A_i \mid i \in I\}$ 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 165. Niech $\mathcal{A}$ będzie przeliczalną rodziną zbiorów przeliczalnych. Pokaż, że $\bigcup \mathcal{A}$ i $\bigcap \mathcal{A}$ są zbiorami przeliczalnymi.

Zadanie 166. Niech A będzie nieskończonym zbiorem przeliczalnym i niech $B \subseteq A$ będzie zbiorem nieskończonym. Korzystając z definicji pojęcia przeliczalności zdefiniuj bijekcje $f : B \to A$ i $g : A \to B$.

Zadanie 167. Niech A będzie nieskończonym zbiorem przeliczalnym i niech $f : A \to B$ będzie surjekcją (odwzorowaniem "na"). Zbuduj injekcję (funkcję różnowartościową) $g : B \to A$.

Zadanie 168. Udowodnij, że jeśli $f : \mathbb{R} \to \mathbb{R}$ jest monotoniczna, to zbiór jej punktów nieciągłości jest przeliczalny.

Zadanie 169. 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 170. Udowodnij, że zbiór wszystkich skończonych ciągów o elementach ze skończonego zbioru A jest przeliczalny.

Zadanie 171. Udowodnij, że zbiór liczb wymiernych jest przeliczalny.

Zadanie 172. Wykaż, że zbiór słabo rosnących funkcji $f : \mathbb{N} \to \mathbb{N}$ jest nieprzeliczalny (funkcja $f : \mathbb{N} \to \mathbb{N}$ jest *słabo rosnąca*, jeśli $x > y \Rightarrow f(x) \geq f(y)$ dla wszelkich $x, y \in \mathbb{N}$).

Zadanie 173. Jaka jest moc zbioru nieskończonych ciągów o wyrazach wymiernych?

Zadanie 174. Jaka jest moc zbioru nieskończonych ciągów o wyrazach wymiernych, stałych od pewnego miejsca?

Zadanie 175. Ile jest ciągów liczb wymiernych zbieżnych do 1?

Zadanie 176. Ile jest rosnących ciągów liczb wymiernych zbieżnych do 1?

Zadanie 177. Czy zbiór nierosnących ciągów o wyrazach naturalnych jest przeliczalny? (Ciąg $\langle a_i : i \in \mathbb{N}\rangle$ jest nierosnący, jeśli $a_i \leq a_{i+1}$ dla każdego $i \in \mathbb{N}$).

Zadanie 178. Wykaż, że zbiór słabo malejących funkcji $f : \mathbb{N} \to \mathbb{N}$ jest przeliczalny (funkcja $f : \mathbb{N} \to \mathbb{N}$ jest *słabo malejąca*, jeśli $x > y \Rightarrow f(x) \leq f(y)$ dla wszelkich $x, y \in \mathbb{N}$).

Zadanie 179. 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 180. Ile jest bijekcji $f : A \to A$, gdy zbiór A jest przeliczalny?

Zadanie 181. Liczba rzeczywista x jest *algebraiczna*, jeśli istnieje wielomian jednej zmiennej o współczynnikach wymiernych, taki, że x jest jego pierwiastkiem. Udowodnij, że zbiór liczb algebraicznych jest przeliczalny.

Zadanie 182. 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 $\{0, \ldots, n-1\}$?

Zadanie 183. 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 184. 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 185. Czy zbiór relacji równoważności na zbiorze przeliczalnym jest zbiorem przeliczalnym?

Zadanie 186. Dany jest nieskończony przeliczalny zbiór A i liczba $n \in \mathbb{N}$. Ile jest relacji równoważności $\sim$ na zbiorze A, takich, że dla każdego $a \in A$ klasa abstrakcji $[a]_\sim$ ma dokładnie n elementów?

Zadanie 187. Ile jest relacji równoważności na przeliczalnym zbiorze A, takich, że wszystkie ich klasy abstrakcji są skończone?

Zadanie 188. Niech zbiory $A \cup B$ i $C \cup D$ będą przeliczalne nieskończone. Która z poniższych formuł wynika z tego założenia? Uzasadnij swoje odpowiedzi.

$$A \sim C \vee B \sim D$$
$$A \sim C \vee A \sim D \vee B \sim C \vee B \sim D$$
$$(A \sim C \wedge B \sim D) \vee (A \sim D \wedge B \sim C)$$
$$A \sim C \vee A \sim D$$

Zadanie 189. Mówimy, że ciąg liczb rzeczywistych $(y_n)_{n\in\mathbb{N}}$ *rośnie szybciej* niż ciąg $(x_n)_{n\in\mathbb{N}}$, gdy

$$\lim_{n\to\infty} \frac{x_n}{y_n} = 0.$$

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 190. Udowodnij, że każdy zbiór rozłącznych odcinków na prostej jest przeliczalny. Pokaż, że istnieje nieprzeliczalny zbiór rozłącznych odcinków na płaszczyźnie.

Zadanie 191. 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 192. 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 193. 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 194. 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.

7

Relacje porządku

Definicja 78. Relacja R jest *słabo antysymetryczna*, jeśli dla dowolnych a, b

$$\text{jeśli } aRb \text{ oraz } bRa \text{ to } a = b.$$

Definicja 79. *Częściowym porządkiem* w zbiorze A nazywamy relację „$\leq$" (będącą podzbiorem A^2), która jest *zwrotna*, *przechodnia* i *słabo antysymetryczna*, tzn.

- $\forall a{\in}A\ (a \leq a)$,
- $\forall a, b{\in}A\ (a \leq b \wedge b \leq a \Rightarrow a = b)$,
- $\forall a, b, c{\in}A\ (a \leq b \wedge b \leq c \Rightarrow a \leq c)$.

Definicja 80. Jeśli $\leq$ jest częściowym porządkiem na A, to $a < b$ oznacza

$$a \leq b \wedge a \neq b.$$

Definicja 81. *Zbiór częściowo uporządkowany*, to zbiór A z relacją częściowego porządku $\leq$. Zbiór częściowo uporządkowany oznaczamy czasem $\langle A, \leq\rangle$.

Przykład 82. 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 $a|b \iff \exists x(ax = b)$.

Definicja 83. Porządek częściowy $\leq$ w zbiorze A jest *liniowy*, jeśli

$$\forall a, b{\in}A\ (a \leq b \vee b \leq a).$$

Przykład 84. Porządkiem liniowym jest relacja $\leq$ na zbiorze liczb rzeczywistych. Porządkiem liniowym nie jest relacja inkluzji $\subseteq$ na zbiorze $\mathcal{P}(\mathbb{N})$.

7.1. Przykłady porządków

Zadanie 195. 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 196. Pokaż, że na zbiorze liczb zespolonych $\mathbb{C}$ nie można wprowadzić porządku $\leq$, takiego, 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 197. 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 198. Czy dla danego zbioru X takiego, że $|X| \geq 2$ można określić relację R, taką, by równocześnie:

1. zbiór $\langle X, R\rangle$ był zbiorem liniowo uporządkowanym,
2. R była relacją równoważności w X?

Zadanie 199. 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 antysymetryczna.

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

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. $\neg Z(R_4) \wedge \neg A(R_4) \wedge P(R_4)$.

Zadanie 200. 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 85. Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Na zbiorze A^* skończonych ciągów elementów zbioru A określamy relację $\preceq$ przyjmując, że dla dowolnych $u, w \in A^*$ zachodzi $u \preceq w$ 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 $\preceq$ nazywamy *porządkiem leksykograficznym* na A^* generowanym przez porządek $\leq$.

Zadanie 201. Wykaż, że relacja $\preceq$ jest porządkiem częściowym.

Zadanie 202. Wykaż, jeśli $\langle A, \leq \rangle$ jest porządkiem liniowym, to $\langle A^*, \preceq \rangle$ też jest porządkiem liniowym.

Zadanie 203. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą porządkami liniowymi. Relację $\leq$ na $A \times B$ określamy wzorem

$$\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle \quad \Leftrightarrow \quad a_1 \leq_A a_2 \wedge b_1 \leq_B b_2$$

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 jednoelementowy.

7.2. Izomorfizm porządkowy

Definicja 86. Zbiory uporządkowane $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ są *izomorficzne*, jeżeli istnieje bijekcja $\phi : A \to B$ 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 87. Niech $\langle P, \leq_P \rangle$ oraz $\langle Q, \leq_Q \rangle$ będą zbiorami częściowo uporządkowanymi. Funkcja $f : P \to Q$ jest *monotoniczna*, jeśli

$$\forall x, y \in P \; \big(x \leq_P y \Rightarrow f(x) \leq_Q f(y)\big).$$

Fakt 88. Funkcja ϕ jest izomorfizmem porządkowym, jeśli jest bijekcją oraz ϕ i ϕ^{-1} są monotoniczne.

Zadanie 204. Udowodnij, że następujące zbiory: $\mathbb{Q}$, $\mathbb{Q} \cap (0,1)$, $\mathbb{Q}\backslash\{0\}$, $\mathbb{Q}\backslash[0,1)$ i $\mathbb{Q}\backslash[0,1]$ uporządkowane zwykłą relacją porządku są izomorficzne ($\mathbb{Q}$ oznacza zbiór liczb wymiernych, (a,b) — przedział otwarty o końcach a i b, $[a,b]$ zaś — przedział domknięty).

Definicja 89. Porządek $\leq$ na zbiorze A jest:

- *gęsty*, jeśli pomiędzy każdą parą elementów zbioru A znajduje się trzeci element, tj. gdy dla dowolnych $a, b \in A$, takich, że $a < b$, istnieje $c \in A$, taki, 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 $b, c \in A$, takie, że $b < a < c$.

Dla przykładu zwykły porządek na wszystkich pięciu zbiorach z zadania 204 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 $\mathbb{Q}\backslash(0,1)$ nie jest gęsty, a na zbiorze $\mathbb{Q} \cap [0,1]$ nie jest bez końców.

Zadanie 205. Pokaż, że dowolne dwa zbiory przeliczalne uporządkowane liniowymi, gęstymi relacjami porządku bez końców są izomorficzne.

Zadanie 206. 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 207. 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 208. 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 209. W zbiorze $\mathbb{N}^{\mathbb{N}}$ wprowadzamy relację R_1 wzorem

$$\bar{a} R_1 \bar{b} \quad \Leftrightarrow \quad \forall n\, (a_n \leq b_n),$$

dla $\bar{a} = (a_k)_{k\in\mathbb{N}}$ i $\bar{b} = (b_k)_{k\in\mathbb{N}}$. Udowodnij, że zbiór $\langle \mathbb{N}^{\mathbb{N}}, R_1\rangle$ jest częściowo uporządkowany. Czy R_1 jest liniowym porządkiem? Czy jest gęstym porządkiem? Czy ten porządek jest izomorficzny z $\langle \mathbb{R}, \leq\rangle$?

Zadanie 210. W zbiorze wszystkich ciągów nieskończonych o wyrazach naturalnych wprowadzamy relację

$$\bar{a} R_2 \bar{b} \quad \Leftrightarrow \quad \exists k \ (a_k = b_k \wedge \forall n{<}k \ (a_n < b_n)) \vee \bar{a} = \bar{b},$$

dla $\bar{a} = (a_k)_{k\in\mathbb{N}}$ i $\bar{b} = (b_k)_{k\in\mathbb{N}}$. Czy ta relacja jest liniowym porządkiem? Czy jest gęstym porządkiem? Czy ten porządek jest izomorficzny z $\langle\mathbb{R}, \leq\rangle$?

Zadanie 211. Udowodnij, że $a R_1 b \Rightarrow a R_2 b$ dla wszelkich $a, b \in \mathbb{N}^{\mathbb{N}}$, gdzie R_1 jest relacją rozważaną w zadaniu 209, zaś R_2 — w zadaniu 210.

Zadanie 212. W zbiorze $\mathbb{C}$ liczb zespolonych wprowadzamy porządek

$$x R y \quad \Leftrightarrow \quad \operatorname{Re} x < \operatorname{Re} y \vee (\operatorname{Re} x = \operatorname{Re} y \wedge \operatorname{Im} x < \operatorname{Im} y).$$

Udowodnij, że R jest liniowym gęstym porządkiem bez końców. Czy $\langle\mathbb{C}, R\rangle$ jest izomorficzny z $\langle\mathbb{R}, \leq\rangle$?

Definicja 90. Niech $\langle X, \leq\rangle$ będzie zbiorem częściowo uporządkowanym. *Następnikiem* $x \in X$ nazywamy element $y \in X$, taki, że $x < y$ i dla każdego $z \in X$, takiego, że $x < z < y$ jest $x = z$ lub $z = y$. Podobnie *poprzednikiem* $x \in X$ nazywamy element $y \in X$, taki, że $y < x$ i dla każdego $z \in X$, takiego, że $y < z < x$ jest $y = z$ lub $z = x$.

Zadanie 213. Udowodnij, że każdy zbiór liniowo uporządkowany $\langle X, \preceq\rangle$, taki, że każdy element posiada poprzednik i następnik oraz taki, 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 214. 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 215. W zbiorze liczb rzeczywistych $\mathbb{R}$ wprowadzamy relację $\sim$, taką, że $x \sim y \Leftrightarrow \lfloor x\rfloor = \lfloor y\rfloor$. Udowodnij, że $\sim$ jest relacją równoważności. Opisz jej klasy abstrakcji.

Zadanie 216. W zbiorze $\mathbb{R}/{\sim}$, gdzie $\sim$ jest relacją z zadania 215, definiujemy relację $\preceq$, taką, że

$$[x]_\sim \preceq [y]_\sim \quad \Leftrightarrow \quad x \leq y,$$

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.

Zadanie 217. W zbiorze $\mathbb{R}/\sim$, gdzie $\sim$ jest relacją z zadania 215, 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?

7.3. Zawieranie zbiorów jako relacja porządku

Definicja 91. Rodzina zbiorów $\{A_t\}_{t \in T}$ jest *łańcuchem*, jeśli

$$A_t \subseteq A_s \vee A_s \subseteq A_t,$$

dla wszelkich $s, t \in T$ (tj. gdy $\subseteq$ jest na tej rodzinie porządkiem liniowym).

Definicja 92. Rodzina zbiorów $\{A_t\}_{t \in T}$ jest *antyłańcuchem*, jeśli

$$A_s \subseteq A_t \vee A_t \subseteq A_s \quad \Rightarrow \quad s = t,$$

dla wszelkich $s, t \in T$.

Zadanie 218. Pokaż, że w $\mathcal{P}(\mathbb{N})$ istnieje łańcuch mocy continuum.

Zadanie 219. Pokaż, że w $\mathcal{P}(\mathbb{N})$ istnieje antyłańcuch mocy continuum.

Definicja 93. Rodzina zbiorów $\{A_t\}_{t \in T}$ jest *prawie rozłączna*, jeśli dla wszelkich $s, t \in T$ zbiór $A_t \cap A_s$ jest skończony.

Zadanie 220 (Sierpiński). Pokaż, że w $\mathcal{P}(\mathbb{N})$ istnieje rodzina mocy continuum zbiorów prawie rozłącznych.

Definicja 94. 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 221. Udowodnij, że jeśli $A \subseteq X$ to $\{B \subseteq X \mid A \subseteq B\}$ jest filtrem. Nazywamy go *filtrem głównym wyznaczonym przez* A.

Zadanie 222. Pokaż, że jeśli X jest zbiorem skończonym, to każdy filtr na $\mathcal{P}(X)$ jest główny.

Zadanie 223. Pokaż, że jeśli X jest zbiorem nieskończonym, to istnieje filtr na $\mathcal{P}(X)$, który nie jest główny.

Zadanie 224. 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.

7.4. Liczba relacji porządku

Zadanie 225. Ile jest relacji częściowego porządku w zbiorze n-elementowym?

Zadanie 226. Ile jest relacji porządku liniowego w zbiorze n elementowym?

Zadanie 227. 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 95. 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 $u = u_1u_2 \ldots u_n$ i $w = w_1w_2 \ldots w_m$, to uw oznacza *złożenie* (*konkatenację*) słów u i w, tj. słowo $u_1u_2 \ldots u_n w_1w_2 \ldots w_m$. Słowo u jest *przedrostkiem* (*prefiksem*) słowa w, jeśli istnieje słowo v, takie, że $uv = w$. Podobnie, słowo u jest *przyrostkiem* (*sufiksem*) słowa w, jeśli istnieje słowo v, takie, że $vu = w$.

Fakt 96. 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 97. Niech L będzie zbiorem słów (językiem) nad alfabetem $\{0, 1\}$. Mówimy, że słowa $u, v \in \{0, 1\}^*$ są *równoważne względem języka L*, jeżeli

$$\forall x \in \{0, 1\}^* \ (ux \in L \iff vx \in L).$$

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 $\underbrace{ww \ldots w}_{n \text{ razy}}$.

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 wszelkich naturalnych n, tj. $w^* = \{w^n \mid n \in \mathbb{N}\}$.

Zadanie 228. Wykaż, że $\sim_L$ jest relacją równoważności.

Zbiór klas równoważności relacji $\sim_L$ oznaczamy $\mathcal{Q}(L)$.

Zadanie 229. Pokaż, że jeśli dla pewnych słów $w \in L$ i $v \in \{0, 1\}^*$ zachodzi $wv \in [w]_\sim$, to $wv^n \in L$ dla każdego $n \in \mathbb{N}$.

Zadanie 230. Opisz klasy abstrakcji relacji $\sim_L$ równoważności słów względem następujących języków:

$$\begin{array}{lcl} L_1 & = & \{1^n \mid 1 \le n \le 6\} \\ L_2 & = & (0011)^* \\ L_3 & = & \{0^n 1^n \mid n \in \mathbb{N}\} \end{array}$$

Zadanie 231. Dla języka L nad alfabetem $\{0, 1\}$ określamy funkcje

$$\begin{array}{lcl} f & : & \mathcal{Q}(L) \times \mathcal{Q}(L) \to \mathcal{Q}(L), \\ g & : & \mathcal{Q}(L) \times \{0, 1\} \to \mathcal{Q}(L), \end{array}$$

gdzie $\mathcal{Q}(L)$ jest rodziną klas abstrakcji relacji $\sim_L$ równoważności względem języka L, wzorami:

$$\begin{array}{rcl} f([u]_{\sim_L}, [w]_{\sim_L}) & = & [uw]_{\sim_L}, \\ g([u]_{\sim_L}, a) & = & [ua]_{\sim_L}, \end{array}$$

gdzie $u, w \in \{0, 1\}^*$ oraz $a \in \{0, 1\}$. Która z powyższych definicji jest poprawna?

Zadanie 232. Niech g będzie funkcją zdefiniowaną w poprzednim zadaniu. Kładziemy

$$\begin{array}{rcl} g^*(\epsilon) & = & g([\epsilon]_{\sim_L}, \epsilon), \\ g^*(wa) & = & g(g^*(w), a), \end{array}$$

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 $g^*(w) \subseteq L$.

9

Kresy zbiorów

Definicja 98. 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 oznacza się $\bot$, zaś największy $\top$.

Definicja 99. Element $x \in X$ jest elementem *maksymalnym* (odpowiednio *minimalnym*) w X, jeśli dla każdego $y \in X$, jeśli $x \leq y$ (odpowiednio $y \leq x$), to $x = y$.

Definicja 100. 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 $\mathcal{Q}$ dotyczące porządków, to pojęcie $\mathcal{Q}^{-1}$ dualne do niego otrzymujemy przez zastąpienie w definicji $\mathcal{Q}$ symbolu $\leq$ przez symbol $\leq^{-1}$. Zauważmy, że pojęcia minimalny i maksymalny oraz najmniejszy i największy są dualne.

Twierdzenie 101. Niech $\langle P, \leq \rangle$ będzie częściowym porządkiem i niech $X \subseteq P$. Wtedy element największy w X jest elementem maksymalnym w X.

Twierdzenie 102. Istnieje co najwyżej jeden element największy.

Przykład 103. 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.

Definicja 104. 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 $\{a : a \text{ jest ograniczeniem górnym } X\}$. 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 233. 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 105. Relacja podzielności liczb naturalnych $\mid\ \subset \mathbb{N}^2$ jest określona następująco:

$$x \mid y \quad \Leftrightarrow \quad \exists z{\in}\mathbb{N}\ (xz = y).$$

Zadanie 234. 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 $\sup\{m,n\} = \mathrm{lcm}(m,n)$, gdzie gcd jest największym wspólnym podzielnikiem dwu liczb, a lcm — najmniejszą wspólną wielokrotnością.

Zadanie 235. Rozważmy relację $\mid$ na zbiorze $\mathbb{N} \setminus \{0\}$.

1. Znajdź zbiór elementów minimalnych w zbiorze $\langle \mathbb{N} \setminus \{0\}, \mid \rangle$.
2. Udowodnij, że w zbiorze $\langle \mathbb{N} \setminus \{0\}, \mid \rangle$ nie ma elementów maksymalnych.

Zadanie 236.

1. Znajdź ogólną postać łańcucha w zbiorze $\langle \mathbb{N} \setminus \{0\}, \mid \rangle$,
2. Znajdź ogólną postać antyłańcucha w zbiorze $\langle \mathbb{N} \setminus \{0\}, \mid \rangle$.
3. Udowodnij, że relacja inkluzji w zbiorze łańcuchów zbioru $\langle \mathbb{N} \setminus \{0\}, \mid \rangle$ jest częściowym porządkiem. Znajdź postać łańcuchów minimalnych i maksymalnych względem relacji inkluzji.

Zadanie 237. 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 238. Znajdź elementy minimalne, maksymalne, największy i najmniejszy w zbiorze $\langle \mathbb{N}^{\mathbb{N}}, R_1 \rangle$ z zadania 209.

Zadanie 239. Znajdź elementy minimalne, maksymalne, największy i najmniejszy w zbiorze $\langle \mathbb{N}^{\mathbb{N}}, R_2 \rangle$ z zadania 210.

Definicja 106. Funkcje $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ 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 240. Pokaż, że $\approx$ jest relacją równoważności.

Zadanie 241. Ile jest klas abstrakcji relacji $\approx$? Jaka jest moc każdej z nich?

Definicja 107. Funkcja $f : \mathbb{N} \to \mathbb{N}$ *majoryzuje* funkcję $g : \mathbb{N} \to \mathbb{N}$, 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 $\mathcal{F} = \{[f]_\approx \mid f : \mathbb{N} \to \mathbb{N}\}$ klas abstrakcji relacji $\approx$ wprowadzamy relację $\preceq$ przyjmując, że

$$[f]_\approx \preceq [g]_\approx \quad \Leftrightarrow \quad f \preceq g.$$

Zadanie 242. 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 243. 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 244. Czy istnieje ciąg funkcji $\langle f_i : i \in \mathbb{N}\rangle$ taki, że $f_i \prec f_{i+1}$ dla $i \in \mathbb{N}$, oraz dla każdej funkcji $g : \mathbb{N} \to \mathbb{N}$ istnieje i takie, że $g \prec f_i$?

Zadanie 245. Wykaż, że każdy przeliczalny podzbiór $X \subseteq \mathcal{F}$ posiada w zbiorze $\mathcal{F}$ ograniczenie górne.

Zadanie 246. 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

$$f_j(n) \quad = \quad \begin{cases} 1, & \text{jeżeli } n \in \bigcup_{i=1}^{j} A_i, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Wykaż, że zbiór $\{[f_j]_\approx \mid j \in \mathbb{N}\}$ nie ma kresu górnego w $\langle \mathcal{F}, \preceq\rangle$.

Definicja 108. *Nieskończonym łańcuchem wstępującym* w zbiorze uporządkowanym $\langle A, \leq\rangle$ nazywamy ciąg
$langlea_i : i \in \mathbb{N}\rangle$ 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 247. Wykaż, że żaden przeliczalny nieskończony ściśle wstępujący łańcuch nie posiada w zbiorze $\mathcal{F}$ kresu górnego.

Zadanie 248. Jak jest największa moc ściśle a) wstępującego, b) zstępującego łańcucha w zbiorze $\mathcal{F}$?

Zadanie 249. Wykaż, że jeśli $\langle\{0, 1\}^*, \preceq\rangle$ jest zbiorem uporządkowanym leksykograficznie nad zbiorem $\langle\{0, 1\}, \leq\rangle$, gdzie $0 \leq 1$, to w zbiorze $\langle\{0, 1\}^*, \preceq\rangle$ można znaleźć nieskończony łańcuch wstępujący i nieskończony łańcuch zstępujący. Czy w zbiorze $\langle\{0, 1\}^*, \preceq\rangle$ istnieje element najmniejszy lub największy?

9.1. Kraty

Definicja 109. 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.

Twierdzenie 110. 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 250. Wykaż, że dla każdego zbioru rodzina wszystkich relacji równoważności określonych na tym zbiorze uporządkowana relacją inkluzji jest kratą zupełną. Czy zbiór wszystkich relacji częściowego porządku określonych na tym zbiorze uporządkowany przez relację inkluzji jest kratą?

Zadanie 251. Niech A będzie dowolnym zbiorem niepustym. Wykaż, że rodzina $\mathcal{K} = \{R : R \subseteq A^2\}$ binarnych relacji określonych na zbiorze A uporządkowana relacją inkluzji $\subseteq$ jest kratą zupełną.

Definicja 111. Niech Z oznacza zbiór wszystkich nieskończonych podzbiorów zbioru liczb naturalnych. W zbiorze Z wprowadzamy relację $\sim$ następująco:

$$X \sim Y \quad \text{wtw} \quad |X \dot{-} Y| < \aleph_0.$$

Zadanie 252. Pokaż, że $\sim$ jest relacją równoważności.

Definicja 112. W zbiorze klas abstrakcji $Z/_\sim$ wprowadzamy relację $\leq$, taką że:

$$[X]_\sim \leq [Y]_\sim \quad \text{wtw} \quad |X \setminus Y| < \aleph_0.$$

Zadanie 253. Sprawdź, czy definicja $\leq$ jest poprawna.

Zadanie 254. Sprawdź, czy $\leq$ jest porządkiem częściowym.

Zadanie 255. Znajdź w $\langle Z/_\sim, \leq\rangle$ nieskończony podzbiór liniowo uporządkowany.

Zadanie 256. Znajdź w $\langle Z/_\sim, \leq\rangle$ nieskończony antyłańcuch.

Zadanie 257. Wykaż, że $\langle Z/_\sim, \leq\rangle$ nie jest zupełny.

Zadanie 258. Wykaż, że każdy ściśle malejący ciąg $x_1 > x_2 > x_3 > \ldots$ 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 259. Czy $\langle Z/_\sim, \leq\rangle$ jest kratą?

9.2. Porządki zupełne

Definicja 113. Niech $\langle P, \leq_P \rangle$ będzie zbiorem częściowo uporządkowanym. Wtedy zbiór $\emptyset \neq X \subseteq P$ jest zbiorem *skierowanym*, jeśli

$$\forall x, y{\in}X\ \exists z{\in}X\ (x \leq z \wedge y \leq z).$$

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 114. Niech $\langle P, \leq_P \rangle$ oraz $\langle Q, \leq_Q \rangle$ będą porządkami zupełnymi. Funkcja $f : P \to Q$ 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 115.

1. Każda funkcja ciągła jest monotoniczna.
2. Złożenie funkcji ciągłych jest funkcją ciągłą.

Zadanie 260. Pokaż, że relacja inkluzji na rodzinie skończonych podzbiorów zbioru liczb naturalnych nie jest porządkiem zupełnym.

Zadanie 261. 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 262. 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 263. 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 264. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą porządkami zupełnymi. Pokaż, że funkcja $\phi : [A, B] \times A \to B$, gdzie $[A, B]$ jest zbiorem funkcji ciągłych z A w B, zdefiniowana wzorem $\phi(f, a) = f(a)$ jest ciągła.

Zadanie 265. 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 266. 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.

9.3. Twierdzenia o punkcie stałym

Twierdzenie 116 (Knaster, Tarski). Niech $\langle P, \leq\rangle$ będzie kratą zupełną i niech funkcja $f : P \to P$ 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 nazywamy *najmniejszym punktem stałym* funkcji f. Element spełniający tylko warunek 1 nazywamy *punktem stałym*.

Twierdzenie 117. Niech $\langle P, \leq_P\rangle$ będzie porządkiem zupełnym oraz niech funkcja $f : P \to P$ będzie ciągła. Wtedy element $a = \bigvee\{f^n(\perp) \mid n \in N\}$ jest najmniejszym punktem stałym funkcji f.

Zadanie 267. Niech $A \neq \emptyset$ i niech $f : A \to A$. 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 268. Niech $\mathcal{K} = \mathcal{P}(A^2)$ będzie zbiorem uporządkowanym relacją inkluzji $\subseteq$, $R \in \mathcal{K}$ i niech funkcja $\phi_R : \mathcal{K} \to \mathcal{K}$ będzie zdefiniowana wzorem

$$\phi_R(X) \quad = \quad X \cup X^{-1} \cup XX \cup E_A \cup R,$$

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 269. Niech, że R^+ będzie najmniejszym punktem stałym funkcji ϕ_R. Wykaż, że R^+ jest najmniejszą (względem relacji inkluzji $\subseteq$) relacją równoważności zawierającą relację R.

Zadanie 270. Na rodzinie $\mathcal{L} = \mathcal{P}(\{0, 1\}^*)$ wszystkich języków nad alfabetem $\{0, 1\}$ określamy funkcję

$$f(X) \quad = \quad X \cup \{w01 \mid w \in X\}.$$

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 $g(X) = \{w01 \mid x \in X\}$?

9.4. Relacje w zbiorze formuł zdaniowych

Definicja 118. 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:

$$\alpha \sim \beta \text{ wtedy i tylko wtedy, gdy formuła } (\alpha \Leftrightarrow \beta) \text{ jest tautologią.}$$

Zadanie 271. Wykaż, że $\sim$ jest relacją równoważności.

Zadanie 272. Ile jest klas abstrakcji relacji $\sim$, gdy zbiór zmiennych V

1. ma trzy elementy,
2. ma n elementów,
3. ma moc $\aleph_0$?

Zadanie 273. 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.

Która z tych relacji jest relacją równoważności?

Definicja 119. 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

$$\phi_1 \sim_{\phi_a} \phi_2 \text{ wtedy i tylko wtedy, gdy formuła } (\phi_a \Rightarrow (\phi_1 \Leftrightarrow \phi_2)) \text{ jest tautologią.}$$

Zadanie 274. Udowodnij, że $\sim_{\phi_a}$ jest relacją równoważności. Opisz klasy równoważności formuł $p \vee \neg p$ i $p \wedge \neg p$.

Definicja 120. 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 275. Sprawdź, że powyższa definicja relacji $\leq$ jest poprawna (nie zależy od wyboru reprezentanta klasy abstrakcji) i że definiuje porządek częściowy.

Zadanie 276. Czy $\langle \mathcal{F}(V)/_\sim, \leq \rangle$ jest kratą?

Zadanie 277. Czy $\langle \mathcal{F}(V)/_\sim, \leq \rangle$ jest kratą zupełną?

Zadanie 278. Przyjmijmy, że zbiór zmiennych V jest przeliczalny nieskończony. Znajdź w zbiorze $\langle \mathcal{F}(V)/_\sim, \leq \rangle$ nieskończony podzbiór liniowo uporządkowany (łańcuch).

Zadanie 279. Przyjmijmy, że zbiór zmiennych V jest przeliczalny nieskończony. Czy można w zbiorze $\langle \mathcal{F}(V)/_\sim, \leq \rangle$ znaleźć nieskończony *antyłańcuch*, to znaczy zbiór X taki, że jeśli $x \neq y$, to $\neg(x \leq y)$ dla wszelkich $x, y \in X$?

Zadanie 280. 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 281. Wypisz najkrótszych reprezentantów wszystkich klas abstrakcji relacji $\sim$ gdy zbiór V ma dwa elementy. Narysuj diagram porządku $\leq$ dla tego przypadku.

Zadanie 282. Wyznacz zbiór elementów minimalnych i kres dolny zbioru $F_1 = \mathcal{F}(V)/_\sim \setminus \{[\bot]_\sim\}$, gdy zbiór zmiennych V jest (a) skończony i (b) nieskończony.

Zadanie 283. Niech $V = \{p_n\}_{n=1}^{\infty}$ będzie zbiorem zmiennych. Wyznacz kresy (dolny i górny) zbiorów $F_2 = \{[\alpha_n]_\sim\}_{n=1}^{\infty}$ i $F_3 = \{[\beta_n]_\sim\}_{n=1}^{\infty}$, gdzie $\alpha_n = \bigwedge_{i=1}^{n} p_i = p_1 \wedge \ldots \wedge p_n$ i $\beta_n = \bigvee_{i=1}^{n} p_i = p_1 \vee \ldots \vee p_n$.

Zadanie 284. Niech $V = \{p_n\}_{n=1}^{\infty}$ będzie zbiorem zmiennych. Wyznacz kresy (dolny i górny) zbioru $F_4 = \{[\gamma_n]_\sim\}_{n=1}^{\infty}$, gdzie $\gamma_n = \bigvee_{i=0}^{n}(p_{2i} \vee \neg p_{2i+1})$.

Zadanie 285. W zbiorze $\mathcal{F}(V)$, gdzie $V = \{p_1, \ldots, p_5\}$, definiujemy relacje R_1, R_2 oraz R_3 w następujący sposób:

$$\begin{array}{lcl} \phi R_1 \psi & \Leftrightarrow & \phi \text{ i } \psi \text{ mają tyle samo wystąpień spójników logicznych} \\ \phi R_2 \psi & \Leftrightarrow & (\phi \Leftrightarrow \psi) \text{ jest tautologią} \\ \phi R_3 \psi & \Leftrightarrow & (\phi \Leftrightarrow \psi) \text{ jest formułą spełnialną} \end{array}$$

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 286. Niech $\mathcal{F}$ będzie zbiorem formuł zadaniowych zbudowanych ze zmiennych ze zbioru $V = \{p, q, r, \ldots\}$ i spójników implikacji $\Rightarrow$ i fałszu $\bot$. Binarna relacja R na zbiorze $\mathcal{F}$ jest *monotoniczna*, jeśli

1. $\bot\, R\, \phi$,
2. 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 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 121. Porządek częściowy $\langle P, \leq \rangle$ jest *regularny* (*dobrze ufundowany*), jeśli nie istnieje nieskończony ciąg $a_0, a_1, a_2, \ldots$ taki, że $\forall i{\in}\mathbb{N}\ a_{i+1} < a_i$. Mówimy, że porządek jest *dobry*, jeśli jest liniowy i regularny.

Twierdzenie 122. Porządek częściowy $\langle P, \leq \rangle$ jest *regularny*, jeśli w każdym niepustym zbiorze $X \subseteq P$ istnieje element minimalny.

Zadanie 287. 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 288. 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 289. Udowodnij, że jeśli $f : A \to B$ 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?

Zadanie 290. W zbiorze $\mathbb{N} \setminus \{0\}$ wprowadzamy relację R wzorem

$$xRy \quad \Leftrightarrow \quad (2|x \wedge 2|y \wedge y \leq x) \vee (2|x \wedge \neg(2|y)) \vee (\neg(2|x) \wedge \neg(2|y) \wedge x \leq y).$$

Udowodnij, że zbiór $\langle \mathbb{N} \setminus \{0\}, R \rangle$ jest liniowo uporządkowany. Czy jest to dobry porządek?

Zadanie 291. 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 292. Dany jest zbiór

$$A = \left\{ n + \frac{m}{m+1} \;\middle|\; n, m \in \mathbb{N} \right\}.$$

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 293. 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. kratą,
2. kratą zupełną,
3. porządkiem zupełnym,
4. porządkiem regularnym?

Zadanie 294. Niech $\mathcal{F} = \{ f \in 2^{\mathbb{N}} \mid \{n \in \mathbb{N} \mid f(n) = 1\}$ jest skończony$\}$. W zbiorze $\mathcal{F}$ wprowadzamy relacje $\leq_F$ i $\leq_L$ kładąc

$$\begin{array}{lcl} f \leq_F g & \Leftrightarrow & (\forall n \in \mathbb{N})(f(n) \leq g(n)) \quad \text{oraz} \\ f \leq_L g & \Leftrightarrow & f = g \vee \exists m{\in}\mathbb{N}\, (f(m) < g(m) \wedge \forall n{\in}\mathbb{N}\, (n < m \Rightarrow f(n) = g(n))). \end{array}$$

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 295. Czy porządek zadany definicją 112 jest regularny?

Zadanie 296. Czy na zbiorze A o mocy większej niż 1 można zdefiniować porządek jednocześnie dobry i gęsty?

Definicja 123. Relacja R 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 297. Pokaż, że istnieje relacja R słabo konfluentna, która nie jest konfluentna.

Zadanie 298. Pokaż, że istnieje relacja R słabo konfluentna, której graf jest acykliczny i która nie jest konfluentna.

Zadanie 299. Pokaż, że jeśli relacja R jest ufundowana i słabo konfluentna, to jest konfluentna.

10.2. Indukcja

Twierdzenie 124. 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 $X = P$.

Twierdzenie 125 (o definiowaniu przez indukcję). Niech A i B będą dowolnymi zbiorami. Niech $g : A \to B$ oraz $h : B \times A \times \mathbb{N} \to B$ będą dowolnymi funkcjami. Wtedy istnieje dokładnie jedna funkcja $f : A \times \mathbb{N} \to B$ 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 126 (drugie twierdzenie o definiowaniu przez indukcję).
Niech A i B będą dowolnymi zbiorami. Niech $g : A \to B$ oraz $h : B^* \times A \times \mathbb{N} \to B$ będą dowolnymi funkcjami. Wtedy istnieje dokładnie jedna funkcja $f : A \times \mathbb{N} \to B$ spełniająca warunki:

1. $\forall a{\in}A\ \ f(a, 0) = g(a)$,
2. $\forall a{\in}A\ \forall n{\in}\mathbb{N}\ \ f(a, n+1) = h((f(a, 0), \ldots, f(a, n)), a, n)$.

Twierdzenie 127 (O definiowaniu funkcji przez indukcję noetherowską).
Niech $B^{\subseteq A}$ oznacza zbiór funkcji częściowych z A w B. Niech $\langle A, \leq \rangle$ będzie zbiorem regularnym i niech B, C będą dowolnymi zbiorami. Dla dowolnej funkcji funkcji $h : B^{\subseteq A \times C} \times A \times C \to B$ 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 300. 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 301. Skończony zbiór liniowo uporządkowany $\langle A, \leq_A \rangle$ ma n elementów, a zbiór uporządkowany $\langle B, \leq_B \rangle$ ma 2 elementy. Na ile sposobów można porządek liniowy na A rozszerzyć o elementy zbioru B (to znaczy znaleźć porządek liniowy $\langle A \cup B, \leq \rangle$, taki, 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 302. Udowodnij, że jeśli wyrazy ciągu spełniają warunki $a_0 = 2$, $a_1 = 3$ i $a_{n+1} = 3a_n - 2a_{n-1}$, to $a_n = 2^n + 1$.

Zadanie 303. Dany jest ciąg a_n taki, że $a_0 = 0$, $a_1 = 1$ oraz $a_{n+1} = a_n + a_{n-1}$. Udowodnij, że jeśli $n > 0$, to $a_{n+1} = 1 + \sum_{i=0}^{n-1} a_i$.

Zadanie 304. Dany jest ciąg a_n taki, że $a_0 = 0$, $a_1 = 1$ oraz $a_{n+1} = a_n + a_{n-1}$. Udowodnij, że jeśli $n > 0$, to $a_n^2 = (-1)^{n+1} + a_{n-1}a_{n+1}$.

Zadanie 305. Dany jest ciąg a_n, taki, że $a_0 = 0$, $a_1 = 1$ oraz $a_{n+1} = a_n + a_{n-1}$. Udowodnij, że jeśli $n > 0$, to $a_{2n+1} = a_n^2 + a_{n+1}^2$.

Zadanie 306. 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 307. Wykaż indukcyjnie, że $2^n \geq n^2$ dla każdego $n \geq 5$.

Zadanie 308. 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 zbiorów wypukłych, takich, 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 309. Niech $X \subseteq \mathbb{N}$ będzie zbiorem, takim, 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 310. 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 311. 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 312. Wykaż, że n prostych przecina się na płaszczyźnie w co najwyżej $\frac{n(n-1)}{2}$ punktach.

Zadanie 313. 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 314. Pokaż przez indukcję, że dla każdego zbioru A mocy $n \in \mathbb{N}$ istnieje $n!$ bijekcji $f : A \to A$.

11

Elementy algebry uniwersalnej

Definicja 128. *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 129. *Algebrą nad* Σ (lub Σ-*algebrą*) nazywamy niepusty zbiór A wraz z interpretacją $\cdot^{\mathcal{A}}$, czyli przyporządkowaniem, które każdemu symbolowi $f \in \Sigma_n$ przyporządkowuje funkcję $f^{\mathcal{A}} : A^n \to A$. Tak opisaną algebrę oznaczamy przez $\mathcal{A}$ lub $\langle A, f^{\mathcal{A}} \mid f \in \Sigma \rangle$. Zbiór A nazywamy *nośnikiem* algebry $\mathcal{A}$.

11.1. Algebra termów

Definicja 130. 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 $f \in \Sigma_n, t_1, \ldots, t_n \in T(\Sigma, V)$, to $f(t_1, \ldots, t_n) \in T(\Sigma, V)$).

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 $f \in \Sigma_n, t_1, \ldots, t_n \in T(\Sigma)$, to $f(t_1, \ldots, t_n) \in T(\Sigma)$).

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 $f^{\mathcal{F}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$ dla $f \in \Sigma_n, t_1, \ldots, t_n \in T(\Sigma, V)$. 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 131. Niech $t, t' \in T(\Sigma, V)$. Mówimy, że t' jest *podtermem* t, jeśli $t = t'$ lub $t = f(t_1, \ldots, t_n)$ 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 132. 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 ścieżka jest skończona, to zawiera dokładnie jeden liść. *Stopniem* wierzchołka w w drzewie T nazywamy ilość 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 133. 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 *ukorzenionym w* w. Drzewo U jest poddrzewem T, jeśli $U = T_w$ dla pewnego $w \in T$.

Definicja 134. *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 $n \in N$, oraz $m < n$, to $wm \in T$.

Definicja 135. Niech Σ będzie sygnaturą. *Termem* nad Σ nazywamy dowolną parę $t = \langle T, e\rangle$, gdzie T jest drzewem adresów, $e : T \to \Sigma$ zaś funkcją, taką, że jeśli $w \in T$, $e(w) \in \Sigma_n$, to w ma stopień n.

Definicja 136. 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 $w \in T$.

Definicja 137. 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 $\sigma : X \to A$. *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 interpretacje w $\mathcal{A}$ oraz obliczenie tak otrzymanego wyrażenia w $\mathcal{A}$.

Formalnie, wartościowanie σ rozszerza się do funkcji $\sigma^* : T(\Sigma, X) \to A$ zdefiniowanej w następujący sposób:

$$\begin{aligned} \sigma^*(x) &= \sigma(x), \text{ dla } x \in X \text{ oraz} \\ \sigma^*(f(t_1, \ldots, t_n)) &= f^{\mathcal{A}}(\sigma(t_1), \ldots, \sigma(t_n)), \text{ dla } f \in \Sigma_n, t_1, \ldots, t_n \in T(\Sigma, X) \end{aligned}$$

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 $\sigma(x)$.

11.2. Homomorfizmy

Definicja 138. Niech $\mathcal{A}$ i $\mathcal{B}$ będą algebrami nad sygnaturą Σ. Funkcja $h : A \to B$ jest homomorfizmem algebry $\mathcal{A}$ w algebrę $\mathcal{B}$, jeśli dla każdego $f \in \Sigma_n$ i dowolnych $a_1, \ldots, a_n \in A$ zachodzi równość

$$h(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(h(a_1), \ldots, h(a_n)).$$

Przykład 139. Wartościowanie termów w algebrze $\mathcal{A}$ jest homomorfizmem algebry termów w algebrę $\mathcal{A}$.

Definicja 140. Niech Σ będzie sygnaturą. Podstawienie σ w algebrze termów $\mathcal{F} = \langle T(\Sigma, X), f : f \in \Sigma\rangle$ jest funkcją przyporządkowująca zmiennym ze zbioru $X \subseteq V$ elementy $T(\Sigma, V)$. Jest to więc wartościowanie w algebrze termów. Jak poprzednio wartościowanie σ rozszerzamy do $\sigma^* : T(\Sigma, V) \to T(\Sigma, V)$ kładąc $\sigma(y) = y$ dla $y \in V \setminus X$. Oczywiście, tak jak poprzednio $\sigma^*(x) = \sigma(x)$ dla $x \in X$ oraz $\sigma^*(f(t_1, \ldots, t_n) = f(\sigma^*(t_1), \ldots, \sigma^*(t_n))$. 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 $\sigma(x)$.

Zadanie 315. 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 316. Udowodnij, że pierścień $\mathbb{Z}_p = (\{0, \ldots, p-1\}, +, \cdot, 0, 1)$ dla dowolnej liczby pierwszej p spełnia formułę $\forall x (x \neq 0 \Rightarrow \exists y (x \cdot y = 1))$.

Zadanie 317. 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 318. Niech $\langle \{a, b\}^*, \cdot \rangle$ będzie algebrą słów nad alfabetem $\{a, b\}$ z konkatenacją „$\cdot$". Jaka jest moc zbioru wszystkich homomorfizmów $h : \{a, b\}^* \to \{a, b\}^*$ algebry $\langle \{a, b\}^*, \cdot \rangle$ w siebie?

Zadanie 319. Niech $\mathbb{Z}_n$ oznacza algebrę $\langle \{0, 1, \ldots, n-1\}, + \rangle$, gdzie $+$ oznacza dodawanie modulo n. Ile jest homomorfizmów

1. $h : \mathbb{Z}_5 \to \mathbb{Z}_3$,
2. $h : \mathbb{Z}_3 \to \mathbb{Z}_5$?

Zadanie 320. Ile jest homomorfizmów $h : \mathbb{Z}_{2^n} \to \mathbb{Z}_k$, dla $k \leq 2^n$.

Zadanie 321. Niech $\mathfrak{B}_n$ oznacza algebrę $\langle \mathcal{P}(\{0, \ldots, n-1\}), \cup, \cap, \setminus \rangle$. Ile jest homomorfizmów:

1. $h : \mathfrak{B}_5 \to \mathfrak{B}_3$?
2. $h : \mathfrak{B}_3 \to \mathfrak{B}_5$?

Zadanie 322. Niech $\mathfrak{B}_n$ oznacza algebrę $\langle \mathcal{P}(\{0, \ldots, n-1\}), \cup, \cap, {}^C \rangle$, gdzie ^{C} oznacza dopełnienie zbioru. Ile jest homomorfizmów:

1. $h : \mathfrak{B}_5 \to \mathfrak{B}_3$?
2. $h : \mathfrak{B}_3 \to \mathfrak{B}_5$?

Zadanie 323. Niech $\mathfrak{B}_n$ oznacza algebrę $\langle \mathcal{P}(\{0, \ldots, n-1\}), \cup, \cap \rangle$. Ile jest homomorfizmów:

1. $h : \mathfrak{B}_5 \to \mathfrak{B}_3$?
2. $h : \mathfrak{B}_3 \to \mathfrak{B}_5$?

Zadanie 324. Niech $\mathfrak{B}_n$ oznacza algebrę $\langle \mathcal{P}(\{0, \ldots, n-1\}), \cup \rangle$. Ile jest homomorfizmów:

1. $h : \mathfrak{B}_5 \to \mathfrak{B}_3$?
2. $h : \mathfrak{B}_3 \to \mathfrak{B}_5$?

Zadanie 325. Przyjmijmy, że $[0, 1) = \{r \in \mathbb{R} : 0 \leq r < 1\}$, funkcja $f : \mathbb{R} \to [0, 1)$ 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 $g : [0, 1) \to \mathbb{R}$ 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

$$
\begin{aligned}
\mathcal{R}_1 &= \langle \mathbb{R}, + \rangle \\
\mathcal{R}_2 &= \langle \mathbb{R}, +, \times \rangle \\
\mathcal{R}_3 &= \langle [0, 1), \oplus \rangle \\
\mathcal{R}_4 &= \langle [0, 1), \oplus, \times \rangle
\end{aligned}
$$

a) Czy f jest homomorfizmem algebry $\mathcal{R}_1$ w $\mathcal{R}_3$?

b) Czy f jest homomorfizmem algebry $\mathcal{R}_2$ w $\mathcal{R}_4$?

c) Czy g jest homomorfizmem algebry $\mathcal{R}_3$ w $\mathcal{R}_1$?

d) Czy g jest homomorfizmem algebry $\mathcal{R}_4$ w $\mathcal{R}_2$?

Zadanie 326. 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 133). W zbiorze $\mathcal{P}(\mathbb{N})/\sim$ definiujemy działania

$$
\begin{aligned}
[X]_\sim \cup [Y]_\sim &= [X \cup Y]_\sim \\
[X]_\sim \cap [Y]_\sim &= [X \cap Y]_\sim \\
[X]_\sim \setminus [Y]_\sim &= [X \setminus Y]_\sim
\end{aligned}
$$

Czy powyższe definicje są poprawne? Czy funkcja $h : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})/\sim$ określona wzorem $h(X) = [X]_\sim$ jest homomorfizmem algebry $\langle \mathcal{P}(\mathbb{N}), \cup, \cap, \setminus \rangle$ w algebrę $\langle \mathcal{P}(\mathbb{N})/\sim, \cup, \cap, \setminus \rangle$.

Definicja 141. W zbiorze $\mathcal{P}(\mathbb{N})/\sim$ definiujemy porządek $\preceq$ kładąc $[X]_\sim \preceq [Y]_\sim$, jeśli $X \cup Y \in [Y]_\sim$.

Zadanie 327. Sprawdź, czy powyższa definicja jest poprawna. Czy $\langle \mathcal{P}(\mathbb{N})/\sim, \preceq \rangle$ jest kratą?

Zadanie 328. Czy zbiór $\{[X]_\sim \mid n \in \mathbb{N}\}$, gdzie $X_n = \{2^n k \mid k \in \mathbb{N}\}$ ma kres dolny?

Zadanie 329. Czy w $\langle \mathcal{P}(\mathbb{N})/\sim, \preceq \rangle$ istnieje nieskończony antyłańcuch?

11.3. Problem unifikacji

Definicja 142. Niech Σ będzie sygnaturą. *Problemem unifikacji* nazywamy następujące zadanie: „mając dany zbiór $\{(t_1, u_1), \ldots, (t_n, u_n)\}$, 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 $t_1, u_1, \ldots, t_n, u_n$, żeby po podstawieniu tych termów za odpowiednie zmienne uzyskać termy równe. Podstawienie σ nazywamy *unifikatorem* zbioru $\{(t_1, u_1), \ldots, (t_n, u_n)\}$. Często ten zbiór (nazywany czasem *instancją problemu unifikacji*) zapisujemy jako

$$\{t_1 \stackrel{?}{=} u_1, \ldots, t_n \stackrel{?}{=} u_n\}.$$

Definicja 143. Jeśli σ i τ są unifikatorami zbioru $\{(t_1, u_1), \ldots, (t_n, u_n)\}$, to mówimy, że σ jest *ogólniejsze* od τ, (co oznaczamy $\tau \leq \sigma$) jeśli istnieje podstawienie ϱ, takie, że $\tau = \varrho(\sigma)$, gdzie $(\varrho(\sigma))(x) = \varrho(\sigma(x))$. Podstawienie σ nazywamy *najogólniejszym unifikatorem* zbioru

$$PU \quad = \quad \{t_1 \stackrel{?}{=} u_1, \ldots, t_n \stackrel{?}{=} u_n\},$$

jeśli σ jest unifikatorem PU oraz σ jest ogólniejsze od każdego innego unifikatora PU.

Twierdzenie 144. Istnieje algorytm, który dla zadanej instancji

$$\{t_1 \stackrel{?}{=} u_1, \ldots, t_n \stackrel{?}{=} u_n\}$$

problemu unifikacji znajduje jego najogóniejszy unifikator lub odpowiada „nie ma unifikatora”.

Zadanie 330. 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 $\mathcal{X} = \{x, y, z, u, v, \ldots\}$.

Zadanie 331. $\{f(x,\ f(x, c, g(z)),\ f(g(g(z)), x, g(c))) \stackrel{?}{=} f(f(u, v, v), y, y)\}$

Zadanie 332. $\{f(f(d, y),\ f(z, x)) \stackrel{?}{=} f(f(y, z),\ f(x, c))\}$

Zadanie 333. $\{f(f(x,y),\ f(z,u)) \stackrel{?}{=}$
$f(f(f(f(u,u),\ f(u,u)),\ f(f(x,x),\ f(x,x))),$
$f(f(f(y,y),\ f(y,y)),\ f(f(u,u),\ f(u,u))))\}$

Zadanie 334. $\{f(x_1,x_1) \stackrel{?}{=} x_2,\ f(x_2,x_2) \stackrel{?}{=} x_3,\ \ldots,\ f(x_{n-1},x_{n-1}) \stackrel{?}{=} x_n\}$

12

Elementy logiki formalnej

12.1. System Hilberta dla rachunku zdań ze spójnikami implikacji i fałszu

Definicja 145. 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 $\alpha \to \bot$.

Wyrażenie postaci $\Delta \vdash \alpha$ nazywamy *sekwentem*. Wyrażenie $\vdash \alpha$ oznacza $\emptyset \vdash \alpha$. Wyrażenie Δ, α oznacza $\Delta \cup \{\alpha\}$.

Aksjomaty systemu Hilberta

$$\begin{aligned} \Delta, \alpha &\vdash \alpha \\ \Delta &\vdash \alpha \to (\beta \to \alpha) \\ \Delta &\vdash (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to \alpha \to \gamma)) \\ \Delta &\vdash \neg\neg\alpha \to \alpha \end{aligned}$$

Reguła dowodzenia (reguła odrywania)

$$\frac{\Delta \vdash \alpha \quad \Delta \vdash \alpha \to \beta}{\Delta \vdash \beta}$$

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. Piszemy, że $\Delta \vdash \alpha$, jeśli sekwent $\Delta \vdash \alpha$ jest wyprowadzalny w systemie Hilbertowskim.

Twierdzenie 146 (O dedukcji). Dla dowolnego zbioru formuł Δ oraz dowolnych formuł α i β, jeśli $\Delta, \alpha \vdash \beta$, to $\Delta \vdash \alpha \to \beta$.

Twierdzenie 147 (O adekwatności). Jeśli $\Delta \vdash \alpha$, to dla każdego wartościowania zmiennych zdaniowych, jeśli spełnia ono wszystkie formuły z Δ, to spełnia także formułę α. W szczególności, jeśli $\vdash \alpha$, to α jest tautologią.

Twierdzenie 148. Dla dowolnych formuł α i β zbudowanych ze zmiennych zdaniowych przy użyciu spójników $\bot$ i $\to$, następujące sekwenty są wyprowadzalne w systemie Hilbertowskim:

$$\begin{array}{ll} \vdash & \alpha \to (\neg\beta \to \neg(\alpha \to \beta)) \\ \vdash & \bot \to \alpha \\ \vdash & (\alpha \to \beta) \to ((\neg\alpha \to \beta) \to \beta) \end{array}$$

Twierdzenie 149 (Kalmar). Niech α będzie formułą zbudowaną ze zmiennych q_1, $q_2, \ldots, q_n$ przy użyciu spójników $\bot$ i $\to$, i niech $v : V \to \{0,1\}$ będzie dowolnym wartościowaniem. Dla $i = 1, \ldots, n$ definiujemy formuły:

$$q_i' = \begin{cases} q_i & \text{jeśli } v(q_i) = 1, \\ \neg q_i & \text{jeśli } v(q_i) = 0. \end{cases}$$

Niech α' będzie formuła identyczną z α, jeśli wartościowanie v spełnia formułę α. Jeśli natomiast wartościowanie v nie spełnia formuły α, to jako α' bierzemy $\neg\alpha$. Wówczas $\{q_1', \ldots, q_n'\} \vdash \alpha'$.

Twierdzenie 150. Dla dowolnego zbioru formuł Δ i dowolnych formuł α i β, jeśli $\Delta, \alpha \vdash \beta$ i $\Delta, \neg\alpha \vdash \beta$, to $\Delta \vdash \beta$.

Twierdzenie 151 (O pełności). Jeśli α jest tautologią zbudowaną ze zmiennych zdaniowych przy użyciu spójników $\to$ i $\bot$, to $\vdash \alpha$.

12.2. System Hilberta dla rachunku zdań ze spójnikami alternatywy i koniunkcji

Pozwalamy, by formuły zawierały spójniki $\vee$ i $\wedge$ i rozszerzamy system Hilberta o następujące aksjomaty:

$$\begin{array}{lll} \Delta & \vdash & (\alpha \wedge \beta) \to \neg(\alpha \to \neg\beta) \\ \Delta & \vdash & \neg(\alpha \to \neg\beta) \to (\alpha \wedge \beta) \\ \Delta & \vdash & (\alpha \vee \beta) \to (\neg\alpha \to \beta) \\ \Delta & \vdash & (\neg\alpha \to \beta) \to (\alpha \vee \beta) \end{array}$$

Aby odróżnić ten system od poprzedniego, jego sekwenty będziemy oznaczać $\Delta \vdash_{H^+} \alpha$.

Twierdzenie 152. Dla dowolnej formuły zdaniowej α istnieje formuła $\tilde{\alpha}$ zbudowana ze zmiennych zdaniowych jedynie przy użyciu spójników $\bot$ i $\rightarrow$, taka, że

$$\vdash_{H^+} \alpha \rightarrow \tilde{\alpha} \text{ oraz } \vdash_{H^+} \tilde{\alpha} \rightarrow \alpha.$$

Dla rozszerzonego systemu również są prawdziwe twierdzenia o adekwatności i pełności.

Podaj formalne wyprowadzenia w systemie hilbertowskim sekwentów wymienionych w poniższych zadaniach.

Zadanie 335. $\vdash p \wedge q \Rightarrow \neg(\neg p \vee \neg q)$

Zadanie 336. $\{p, \neg p\} \vdash q$

Zadanie 337. $\{p \Rightarrow q, p, q \Rightarrow r\} \vdash r$

Zadanie 338. Niech $\hat{\alpha}$ oznacza *dualizację formuły* α, tzn. formułę powstałą przez zastąpienie każdego wystąpienia symbolu $\vee$ przez $\wedge$, i każdego wystąpienia $\wedge$ przez $\vee$. Udowodnij, że

- α jest tautologią wtedy i tylko wtedy, gdy tautologią jest $\neg\hat{\alpha}$;
- $\alpha \Leftrightarrow \beta$ jest tautologią wtedy i tylko wtedy, gdy tautologią jest $\hat{\alpha} \Leftrightarrow \hat{\beta}$.

Zadanie 339. Niech $\vdash_{H_1}$ oznacza hilbertowski system dowodzenia $\vdash_H$, w którym aksjomat $\Delta \vdash \neg\neg\alpha \Rightarrow \alpha$ jest zastąpiony przez

$$\Delta \vdash (\neg\alpha \Rightarrow \neg\beta) \Rightarrow ((\neg\alpha \Rightarrow \beta) \Rightarrow \alpha).$$

Udowodnij, że obydwa systemy są równoważne, tzn., że dla dowolnego sekwentu $\Delta \vdash \alpha$ zachodzi $\Delta \vdash_H \alpha$ wtedy i tylko wtedy, gdy $\Delta \vdash_{H_1} \alpha$.

Zadanie 340. Udowodnij, że aksjomatu $\Delta \vdash (\neg\alpha \Rightarrow \neg\beta) \Rightarrow ((\neg\alpha \Rightarrow \beta) \Rightarrow \alpha)$ hilbertowskiego systemu dowodzenia nie można wyprowadzić z pozostałych aksjomatów za pomocą reguły odrywania.

Zadanie 341. Udowodnij $\vdash_H \neg p \Rightarrow (p \Rightarrow q)$ używając twierdzenia o dedukcji oraz bez użycia tego twierdzenia.

Zadanie 342. Pokaż, że w systemie $\vdash_H$ wyprowadzalna jest reguła

$$\frac{\Delta \vdash \alpha \Rightarrow \beta \quad \Delta \vdash \neg\beta}{\Delta \vdash \neg\alpha}$$

12.3. Składnia języka pierwszego rzędu

Definicja 153. *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 154. 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 $t_1, \ldots, t_n$ są termami, zaś $f \in \Sigma_n^F$, to $f(t_1, \ldots, t_n)$ też jest termem.

Definicja 155. Zbiór formuł atomowych jest zbiorem napisów postaci $R(t_1, \ldots, t_n)$, gdzie $R \in \Sigma_n^R$, zaś $t_1, \ldots, t_n$ są termami.

Definicja 156. Zbiór *formuł języka pierwszego rzędu* jest najmniejszym zbiorem napisów zawierającym formuły atomowe, zamkniętym ze względu na spójniki zdaniowe $\vee$, $\wedge$, $\neg$, $\bot$, $\Rightarrow$, $\Leftrightarrow$, oraz kwantyfikatory $\forall$ i $\exists$, tzn. jeśli α i β są formułami, zaś x jest zmienną (z V), to formułami są także $\bot, \neg\alpha, \alpha \vee \beta, \alpha \wedge \beta, \alpha \Rightarrow \beta, \alpha \Leftrightarrow \beta$, $\forall x\, \alpha, \exists x\, \alpha$.

Definicja 157. Zbiór zmiennych *wolnych* $\mathrm{FV}(\alpha)$ formuły α definiujemy indukcyjnie:

$$\begin{array}{rcl}
\mathrm{FV}(\bot) & = & \emptyset \\
\mathrm{FV}(R(t_1, \ldots, t_n)) & = & \mathrm{FV}(t_1) \cup \ldots \cup \mathrm{FV}(t_n) \\
\mathrm{FV}(\alpha \vee \beta) = \mathrm{FV}(\alpha \wedge \beta) = \mathrm{FV}(\alpha \Rightarrow \beta) = \mathrm{FV}(\alpha \Leftrightarrow \beta) & = & \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta) \\
\mathrm{FV}(\forall x\, \alpha) = \mathrm{FV}(\exists x\, \alpha) & = & \mathrm{FV}(\alpha) \setminus \{x\}
\end{array}$$

gdzie dla termów $\mathrm{FV}(t_i)$ oznacza zbiór wszystkich zmiennych występujących w t_i.

Definicja 158. Wszystkie wolne wystąpienia zmiennej x w formule α stają się *związanie* w formule $\forall x\, \alpha$ i $\exists x\, \alpha$. Mówimy że kwantyfikator *wiąże* te wystąpienia.

Definicja 159. Formuła bez zmiennych wolnych nazywa się *zdaniem*.

12.4. Semantyka języka pierwszego rzędu

Definicja 160. *Struktura* $\mathfrak{A}$ *sygnatury* Σ to niepusty zbiór A zwany jej *uniwersum* i *interpretacja*, czyli funkcja $\cdot^{\mathfrak{A}}$, która każdemu symbolowi funkcji $f \in \Sigma_n^F$ przyporządkowuje funkcję $f^{\mathfrak{A}} : A^n \to A$ i każdemu symbolowi relacji $R \in \Sigma_n^R$ przyporządkowuje relację $R^{\mathfrak{A}} \subseteq A^n$.

Definicja 161. *Wartościowaniem* w strukturze $\mathfrak{A}$ nazywamy dowolną funkcję $v : V \to A$. Ponadto niech

$$(v_x^a)(y) \quad = \quad \begin{cases} v(y), & \text{gdy } x \neq y, \\ a, & \text{gdy } x = y, \end{cases}$$

dla dowolnego wartościowania $v : V \to A$, zmiennej $x \in V$ i elementu $a \in A$.

Definicja 162. Dla dowolnego termu z $\mathcal{T}(\Sigma^F, V)$ definiujemy indukcyjnie jego *interpretację* $t^{\mathfrak{A}}[v]$ przy zadanym wartościowaniu zmiennych $v : V \to A$:

$$\begin{aligned} x^{\mathfrak{A}}[v] &= v(x) \\ (f(t_1, \ldots, t_n))^{\mathfrak{A}}[v] &= f^{\mathfrak{A}}(t_1^{\mathfrak{A}}[v], \ldots, t_n^{\mathfrak{A}}[v]) \end{aligned}$$

Definicja 163. 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 $\mathfrak{A} \models \bot[v]$.
2. $\mathfrak{A} \models R(t_1, \ldots, t_n)[v]$ wtw $(t_1^{\mathfrak{A}}[v], \ldots, t_n^{\mathfrak{A}}[v]) \in R^{\mathfrak{A}}$.
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 164. Formuła α jest *spełnialna w* $\mathfrak{A}$, jeśli istnieje wartościowanie $v : V \to A$ 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 $v : V \to A$ zachodzi $\mathfrak{A} \models \alpha[v]$. Formuła α jest *prawdziwa* (jest *tautologią*), jeśli dla każdej struktury $\mathfrak{A}$, formuła α jest prawdziwa w $\mathfrak{A}$.

12.5. Podstawienia

Definicja 165. 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 166 (o podstawianiu). Dla dowolnych termów s i t i zmiennej x zachodzi

$$(t[x/s])^{\mathfrak{A}}[v] \quad = \quad t^{\mathfrak{A}}[v_x^{s^{\mathfrak{A}}[v]}].$$

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 167. 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.

12.6. Hilbertowski system dowodzenia dla rachunku I rzędu

Aksjomaty

$$\begin{array}{rcl}
\Delta, \alpha & \vdash & \alpha \\
\Delta & \vdash & \alpha \Rightarrow (\beta \Rightarrow \alpha) \\
\Delta & \vdash & (\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)) \\
\Delta & \vdash & \neg\neg\alpha \Rightarrow \alpha \\
\Delta & \vdash & (\alpha \wedge \beta) \Rightarrow \neg(\alpha \Rightarrow \neg\beta) \\
\Delta & \vdash & \neg(\alpha \Rightarrow \neg\beta) \Rightarrow (\alpha \wedge \beta) \\
\Delta & \vdash & (\alpha \vee \beta) \Rightarrow (\neg\alpha \Rightarrow \beta) \\
\Delta & \vdash & (\neg\alpha \Rightarrow \beta) \Rightarrow (\alpha \vee \beta) \\
\Delta & \vdash & (\alpha \Leftrightarrow \beta) \Rightarrow ((\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)) \\
\Delta & \vdash & ((\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)) \Rightarrow (\alpha \Leftrightarrow \beta) \\
\Delta & \vdash & (\forall x.(\alpha \Rightarrow \beta)) \Rightarrow ((\forall x.\alpha) \Rightarrow (\forall x.\beta)) \\
\Delta & \vdash & \alpha \Rightarrow (\forall x.\alpha), \quad \text{jeśli } x \notin \mathrm{FV}(\alpha) \\
\Delta & \vdash & (\forall x.\alpha) \Rightarrow \alpha[x/t], \quad \text{jeśli } [x/t] \text{ jest dopuszczalne w } \alpha \\
\Delta & \vdash & x = x \\
\Delta & \vdash & x_1 = y_1 \Rightarrow (\ldots \Rightarrow (x_n = y_n \Rightarrow (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)))), \\
& & \quad \text{gdzie } f \in \Sigma_n^F \\
\Delta & \vdash & x_1 = y_1 \Rightarrow (\ldots \Rightarrow (x_n = y_n \Rightarrow (R(x_1, \ldots, x_n) \Rightarrow R(y_1, \ldots, y_n)))), \\
& & \quad \text{gdzie } R \in \Sigma_n^R
\end{array}$$

Reguła dowodzenia

$$\frac{\Delta \vdash \alpha \Rightarrow \beta \quad \Delta \vdash \alpha}{\Delta \vdash \beta}$$

Zbiór formuł Δ jest *sprzeczny*, jeśli $\Delta \vdash \bot$. Zbiór, który nie jest sprzeczny, jest *niesprzeczny*.

Twierdzenie 168 (O dedukcji). Dla dowolnego zbioru formuł Δ oraz dowolnych formuł α i β, jeśli $\Delta, \alpha \vdash \beta$, to $\Delta \vdash \alpha \to \beta$.

Definicja 169. Napis $\Delta \models \alpha$ oznacza, że dla każdej struktury $\mathfrak{A}$ i każdego wartościowania v, jeśli dla każdej formuły $\beta \in \Delta$ zachodzi $\mathfrak{A} \models \beta[v]$, to również $\mathfrak{A} \models \alpha$.

Twierdzenie 170 (O adekwatności). Jeśli $\Delta \vdash \alpha$, to $\Delta \models \alpha$. W szczególności, jeśli $\vdash \alpha$, to α jest tautologią.

Twierdzenie 171 (O istnieniu modelu). Dla dowolnej sygnatury Σ, każdy niesprzeczny zbiór zdań nad Σ ma model.

Twierdzenie 172 (Silne twierdzenie o pełności). Dla dowolnego zbioru formuł Δ oraz dowolnej formuły α, jeśli $\Delta \models \alpha$, to $\Delta \vdash \alpha$. W szczególności, jeśli α jest tautologią, to $\vdash \alpha$.

Twierdzenie 173 (O α-konwersji). Jeśli $\Delta \vdash \forall x.\beta$ oraz podstawienie $[x/y]$ jest dopuszczalne w β, oraz $y \notin \mathrm{FV}(\forall x.\beta)$, to $\Delta \vdash \forall y.(\beta[x/y])$.

Twierdzenie 174 (O generalizacji). Jeśli $\Delta \vdash \alpha$, to dla dowolnej zmiennej x, jeśli $x \notin \mathrm{FV}(\Delta)$, to $\Delta \vdash \forall x.\alpha$.

13

Zadania egzaminacyjne z rozwiązaniami

Zadanie 343. 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. Bierzemy 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 wartość logiczną pewnej formuły przy wartościowaniu wyznaczonym przez ten układ. Dokładniej, bierzemy n zmiennych zdaniowych $p_1, \ldots, p_n$ i tworzymy formuły będące koniunkcją tych zmiennych bądź ich negacji (np. $\neg p_1 \wedge p_2 \wedge \ldots \wedge p_n$). 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 175. Jeżeli w formule ϕ występuje n zmiennych, to $|W(\neg\phi)| = 2^n - |W(\phi)|$.

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 176. Jeżeli żadna zmienna nie występuje jednocześnie w formulach 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 177. 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 jest 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 178. 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 jest 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 179. 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 344. 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 $\psi_1 \vee \psi_2 \vee \ldots \vee \psi_n$, 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 180. 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 181. Formuła

$$(\phi_1 \vee \ldots \vee \phi_n) \wedge \psi \Leftrightarrow (\phi_1 \wedge \psi) \vee \ldots \vee (\phi_n \wedge \psi)$$

jest tautologią. Tautologią jest także formuła

$$\psi \wedge (\phi_1 \vee \ldots \vee \phi_n) \Leftrightarrow (\psi \wedge \phi_1) \vee \ldots \vee (\psi \wedge \phi_n).$$

Fakt 182. Formuła

$$\begin{gathered}(\phi_1 \vee \ldots \vee \phi_n) \wedge (\phi'_1 \vee \ldots \vee \phi'_m) \Leftrightarrow \\ (\phi_1 \wedge \phi'_1) \vee \ldots \vee (\phi_n \wedge \phi'_1) \vee \ldots \vee (\phi_1 \wedge \phi'_m) \vee \ldots \vee (\phi_n \wedge \phi'_m)\end{gathered}$$

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 wykażemy, 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 załóżmy, 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. Załóżmy, 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 345. Używając jedynie zmiennych, kwantyfikatorów, spójników logicznych, nawiasów i symboli $\in$, $\mathbb{N}$, $+$, $\times$, $=$ napisz formuły mówiące, że:

a) nie ma największej liczby pierwszej,
b) istnieje taka liczba naturalna, że każda liczba naturalna większa od niej jest sumą nie więcej niż czterech kwadratów liczb pierwszych,
c) 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

$$\neg\exists a \in \mathbb{N}\exists b \in \mathbb{N}\exists r \in \mathbb{N}\exists s \in \mathbb{N}(\neg x = a \wedge \neg x = b \wedge x = a+r \wedge x = b+s \wedge x = a \cdot b)$$

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

$$\begin{aligned}&\exists x \in \mathbb{N}\ \forall y \in \mathbb{N}\ \exists a \in \mathbb{N}\ \exists b \in \mathbb{N}\ \exists c \in \mathbb{N}\ \exists d \in \mathbb{N}\\ &\qquad((P(a) \vee a + a = a) \wedge (P(b) \vee b + b = b) \wedge (P(c) \vee c + c = c)\\ &\qquad\ \wedge(P(d) \vee d + d = d) \wedge x + y = a \times a + b \times b + c \times c + d \times d)\end{aligned}$$

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

$$\begin{aligned}&\forall x \in \mathbb{N}\ \exists y \in \mathbb{N}\ \exists d \in \mathbb{N}\ \exists r \in \mathbb{N}\\ &\qquad ((\neg(d + d = d) \wedge d \times d = d + d) \wedge y = x + r \wedge P(y) \wedge P(y + d)).\end{aligned}$$

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 $\{y \in \mathbb{N} : \phi(y)\}$ jest nieskończony wtedy i tylko wtedy, gdy $\forall x \in \mathbb{N}\ \exists y \in \mathbb{N}\ (x \leq y \wedge \phi(y))$. ■

Zadanie 346. Pokaż, że

$$(A_1 \cup A_2) \dot{-} (B_1 \cup B_2) \subseteq (A_1 \dot{-} B_1) \cup (A_2 \dot{-} B_2). \tag{5}$$

Czy zawieranie

$$(A_1 \cap A_2) \dot{-} (B_1 \cap B_2) \subseteq (A_1 \dot{-} B_1) \cup (A_2 \dot{-} B_2) \tag{6}$$

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 $x \in (A_1 \cup A_2) \dot{-} (B_1 \cup B_2)$. Z definicji różnicy symetrycznej wiemy, że element ten spełnia równoważność

$$x \in (A_1 \cup A_2) \Leftrightarrow x \notin (B_1 \cup B_2). \tag{7}$$

Na podstawie tej równoważności niewiele potrafimy rozstrzygnąć. Załóżmy więc dodatkowo, że zachodzi

Przypadek 1: $x \in (A_1 \cup A_2)$. Z równoważności (7) 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

$$x \in A_1 \Leftrightarrow x \notin B_1, \tag{8}$$

np. dlatego, że w rozważany 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 (8) oznacza, że $x \in (A_1 \dot{-} B_1)$, i tym bardziej, x należy do prawej strony wzoru (5).

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 (5).

Przypadek 2: $x \notin (A_1 \cup A_2)$. Z równoważności (7) 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 (6) 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 (5) w dowód inkluzji (6). 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:

$$\begin{aligned} X \mathbin{\dot{-}} Y &= (X \setminus X) \cup (Y \setminus X), \\ (X \cup Y) \setminus Z &= (X \setminus Z) \cup (Y \setminus Z), \\ X \setminus (Y \cup Z) &\subseteq X \setminus Y. \end{aligned}$$

Posługując się tymi prawami oraz monotonicznością sumy mnogościowej można wykazać, że

$$\begin{aligned} &(A_1 \cup A_2) \mathbin{\dot{-}} (B_1 \cup B_2) = ((A_1 \cup A_2) \setminus (B_1 \cup B_2)) \cup ((B_1 \cup B_2) \setminus (A_1 \cup A_2)) \\ &= (A_1 \setminus (B_1 \cup B_2)) \cup (A_2 \setminus (B_1 \cup B_2)) \cup (B_1 \setminus (A_1 \cup A_2)) \cup (B_2 \setminus (A_1 \cup A_2) \\ &\subseteq (A_1 \setminus B_1) \cup (A_2 \setminus B_2) \cup (B_1 \setminus A_1) \cup (B_2 \setminus A_2) = (A_1 \mathbin{\dot{-}} B_1) \cup (A_2 \mathbin{\dot{-}} B_2). \end{aligned}$$

Jeżeli wprowadzimy pojęcie dopełnienia zbioru, to w dowodzie zawierania (6) możemy wykorzystać wzór

$$X \mathbin{\dot{-}} Y = X^c \mathbin{\dot{-}} Y^c.$$

Zauważmy, że

$$\begin{aligned} &(A_1 \cap A_2) \mathbin{\dot{-}} (B_1 \cap B_2) = (A_1 \cap A_2)^c \mathbin{\dot{-}} (B_1 \cap B_2)^c = (A_1^c \cup A_2^c) \mathbin{\dot{-}} (B_1^c \cup B_2^c) \\ &\subseteq (A_1^c \mathbin{\dot{-}} B_1^c) \cup (A_2^c \mathbin{\dot{-}} B_2^c) = (A_1 \mathbin{\dot{-}} B_1) \cup (A_2 \mathbin{\dot{-}} B_2). \end{aligned}$$

Zadanie 347. Pokaż, że

1. $A_1 \mathbin{\dot{-}} \ldots \mathbin{\dot{-}} A_n$ zawiera te i tylko te elementy, które należą do nieparzystej liczby zbiorów A_i, gdzie $i = 1, \ldots, n$;

2. jeśli zbiory $A_1, \ldots, A_n$ są skończone, to

$$|A_1 \mathbin{\dot{-}} \ldots \mathbin{\dot{-}} A_n| = \sum_{i=1}^{n} (-2)^{i-1} \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=i}} \left| \bigcap_{j \in I} A_j \right|$$

Rozwiązanie. *Część 1.* Tak naprawdę rozwiążemy ogólniejsze zadanie, a mianowicie pokażemy, że dla dowolnych zbiorów $A_1, \ldots, A_n$, dla dowolnego wyrażenia $A_1 \dot{-} \ldots \dot{-} A_n$ (z dowolnym rozmieszczeniem nawiasów) i dla dowolnego x zachodzi następująca równoważność:

$x \in A_1 \dot{-} \ldots \dot{-} A_n \Leftrightarrow x$ należy do nieparzystej liczby zbiorów spośród $A_1, \ldots, A_n$.

Najpierw musimy nieco uściślić sformułowanie zadania, które nie jest precyzyjne np. w przypadku, gdy $A_1 = \cdots = A_n$. Przypuśćmy, że rozważamy rodzinę zbiorów $(A_i)_{i \in I}$ indeksowanych zbiorem I. Tak więc, jeżeli rozważamy rodzinę $A_1, \ldots, A_n$, to $I = \{1, \ldots, n\}$. Dla takiej rodziny i dla dowolnego elementu x definiujemy zbiór

$$I(x) = \{i \in I : x \in A_i\}.$$

Posługując się wprowadzonym oznaczeniem równoważność z treści zadania możemy zapisać w postaci

$$x \in A_1 \dot{-} \ldots \dot{-} A_n \Leftrightarrow |I(x)| \text{ jest nieparzysta.}$$

Zauważmy od razu, że dla $n = 1$ ta równoważność jest oczywista.

Dowód będziemy prowadzić przez indukcję. Musimy więc przeformułować zadanie tak, aby było możliwe zastosowanie zasady indukcji. Będziemy dowodzić, że dla każdej liczby naturalnej $n \geq 1$, dla dowolnej rodziny zbiorów $A_1, \ldots, A_n$ indeksowanej zbiorem $\{1, \ldots, n\}$ zachodzi teza zadania. Fakt, że dla dowolnej rodziny zbiorów $A_1, \ldots, A_n$ 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

$$A_1 \dot{-} \ldots \dot{-} A_n = (A_1 \dot{-} \ldots \dot{-} A_k) \dot{-} (A_{k+1} \dot{-} \ldots \dot{-} A_n).$$

Weźmy dowolny element x. Będziemy rozważać dwa przypadki: $x \in A_{k+1} \dot{-} \ldots \dot{-} A_n$ oraz $x \notin A_{k+1} \dot{-} \ldots \dot{-} A_n$.

W pierwszym przypadku, z założenia indukcyjnego wynika, że x należy do nieparzystej liczby zbiorów spośród $A_{k+1}, \ldots, A_n$. Zauważmy także, że następujące warunki są równoważne:

1. $x \in A_1 \dot{-} \ldots \dot{-} A_n$,
2. $x \notin A_1 \dot{-} \ldots \dot{-} A_k$,
3. x należy do parzystej liczby zbiorów spośród $A_1, \ldots, A_k$

4. x należy do nieparzystej liczby zbiorów spośród $A_1, \ldots, A_n$

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, $A \dot{-} B \subseteq A \cup B$. Stąd przez łatwą indukcję otrzymujemy, że $A_1 \dot{-} \ldots \dot{-} A_n \subseteq A_1 \cup \ldots \cup A_n$. Z tego wzoru wynika, że elementy nie należące do żadnego ze zbiorów $A_1, \ldots, A_n$ nie należą także do różnicy $A_1 \dot{-} \ldots \dot{-} A_n$.

Przypuśćmy, że element x należy do parzystej liczby zbiorów spośród $A_1, \ldots, A_n$. Przestawmy zbiory $A_1, \ldots, A_n$ tak, aby te zbiory, do których należy x, znalazły się na pierwszych miejscach. Jeżeli po takim przestawieniu zbiory znalazły się w porządku $A_{i_1}, \ldots, A_{i_n}$ i x należy do $2 \cdot k$ tych zbiorów, to z łączności i przemienności różnicy symetrycznej otrzymujemy, że

$$A_1 \dot{-} \ldots \dot{-} A_n = (A_{i_1} \dot{-} A_{i_2}) \dot{-} \ldots \dot{-} (A_{i_{2k-1}} \dot{-} A_{i_{2k}}) \dot{-} A_{i_{2k+1}} \dot{-} \ldots \dot{-} A_{i_n}.$$

Zauważmy, że x nie należy do zbiorów

$$(A_{i_1} \dot{-} A_{i_2}), \ldots, (A_{i_{2k-1}} \dot{-} A_{i_{2k}}), A_{i_{2k+1}}, \ldots, A_{i_n}.$$

Stąd wynika, że x nie należy także do różnicy $A_1 \dot{-} \ldots \dot{-} A_n$.

Udowodniliśmy więc, że elementy należące do parzystej liczby zbiorów spośród $A_1, \ldots, A_n$ nie należą do różnicy $A_1 \dot{-} \ldots \dot{-} A_n$. Oznacza to, że elementy należące do różnicy $A_1 \dot{-} \ldots \dot{-} A_n$ należą do nieparzystej liczby zbiorów spośród $A_1, \ldots, A_n$.

Udowodnimy jeszcze implikację odwrotną. Załóżmy więc, że element x należy do nieparzystej liczby zbiorów spośród $A_1, \ldots, A_n$, w tym do zbioru A_1. Element ten należy do parzystej liczby zbiorów spośród $A_2, \ldots, A_n$. Wobec tego nie należy do różnicy $A_2 \dot{-} \ldots \dot{-} A_n$. Tym samym należy do różnicy

$$A_1 \dot{-} (A_2 \dot{-} \ldots \dot{-} A_n) = A_1 \dot{-} \ldots \dot{-} A_n.$$

Część 2. Jeśli zbiory $A_1, \ldots, A_n$ są skończone, to

$$|A_1 \dot{-} \ldots \dot{-} A_n| = \sum_{i=1}^{n} (-2)^{i-1} \sum_{|I|=i} \Big| \bigcap_{j \in I} A_j \Big|.$$

Weźmy skończony zbiór X zawierający zbiory $A_1, \ldots, A_n$. 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

$$\sum_{x \in X} \mathrm{Ch}_A(x) = |A|.$$

Będziemy przekształcać prawą stronę dowodzonego wzoru. Mamy więc

$$\sum_{i=1}^{n}(-2)^{i-1}\sum_{|I|=i}\left|\bigcap_{j\in I}A_j\right| = \sum_{i=1}^{n}(-2)^{i-1}\sum_{|I|=i}\sum_{x\in X}\mathrm{Ch}_{\bigcap_{j\in I}A_j}(x)$$

$$= \sum_{x\in X}\sum_{i=1}^{n}(-2)^{i-1}\sum_{|I|=i}\mathrm{Ch}_{\bigcap_{j\in I}A_j}(x).$$

Przyjmijmy, że $I(x) = \{i \leq n : x \in A_i\}$. Nietrudno zauważyć, że warunek

$$\mathrm{Ch}_{\bigcap_{j\in I}A_j}(x) = 1$$

jest równoważny ze stwierdzeniem $I \subseteq I(x)$. Wobec tego (po rozbiciu sumy na składniki równe 0 i równe 1) otrzymujemy, że dla $i \leq |I(x)|$

$$\sum_{|I|=i}\mathrm{Ch}_{\bigcap_{j\in I}A_j}(x) = \sum_{\substack{|I|=i \\ \mathrm{Ch}_{\bigcap_{j\in I}A_j}(x)=1}} 1 = \sum_{\substack{|I|=i \\ I\subseteq I(x)}} 1 = \binom{|I(x)|}{i}.$$

Ponadto, dla $i > |I(x)|$ suma ta jest równa 0. Wróćmy do przerwanych przekształceń:

$$\sum_{x\in X}\sum_{i=1}^{n}(-2)^{i-1}\sum_{|I|=i}\mathrm{Ch}_{\bigcap_{j\in I}A_j}(x) = \sum_{x\in X}\sum_{i=1}^{|I(x)|}(-2)^{i-1}\sum_{|I|=i}\mathrm{Ch}_{\bigcap_{j\in I}A_j}(x)$$

$$= \sum_{x\in X}\sum_{i=1}^{|I(x)|}(-2)^{i-1}\binom{|I(x)|}{i} = \sum_{x\in X}(-2)^{-1}\Big(\sum_{i=0}^{|I(x)|}(-2)^{i}\binom{|I(x)|}{i} - 1\Big)$$

$$= \sum_{x\in X}(-2)^{-1}((1-2)^{|I(x)|} - 1) = \sum_{x\in X}2^{-1}(1-(-1)^{|I(x)|}).$$

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

$$\sum_{x\in X}2^{-1}(1-(-1)^{|I(x)|}) = |\{x \in X : |I(x)| \text{ jest nieparzysta}\}| = |A_1 \dot{-} \ldots \dot{-} A_n|,$$

i to kończy dowód. ■

Zadanie 348. Dla jakich zbiorów C prawdziwe jest zdanie stwierdzające, że dla dowolnych zbiorów A i B zachodzi

$$A \times C \subseteq B \times C \Rightarrow A \subseteq B \tag{9}$$

Rozwiązanie. Najpierw spróbujemy dowieść implikację (9). 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 (9), 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 (9) jest prawdziwy dla dowolnych zbiorów A i B. Jeżeli przyjmiemy, że A jest dowolnym zbiorem niepustym (np. zbiorem liczb naturalnych), a B jest zbiorem pustym, to następnik implikacji (9) 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 349. Inwolucją nazywamy odwzorowanie $f : A \to A$ takie, że ff jest identycznością na A. Czy inwolucja jest bijekcją na A? Pokaż, że każdą bijekcję można przedstawić jako złożenie dwóch inwolucji.

Rozwiązanie. *Część 1: każda inwolucja jest bijekcją.* Przypuśćmy, że $f : A \to A$ jest inwolucją. 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 inwolucją, 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 inwolucji. 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 inwolucji, weźmy funkcje $f, g : \mathbb{Z} \to \mathbb{Z}$ zdefiniowane wzorami $f(n) = -n$ oraz $g(n) = -(n + 1)$. Funkcje te są inwolucjami. 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 $S_m : \{i \in \mathbb{N} : i < m\} \to \{i \in \mathbb{N} : i < m\}$ 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 $f_m : \{i \in \mathbb{N} : i < m\} \to \{i \in \mathbb{N} : i < m\}$ 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 $g_m : \{i \in \mathbb{N} : i < m\} \to \{i \in \mathbb{N} : i < m\}$ 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 $s : A \to A$ 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 $s^{(1)} : A_1 \to A_1$ 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 $f, g : A \to A$ 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 $s : A \to A$ 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

$$xRy \Leftrightarrow \exists n \in \mathbb{Z}\; y = s^n(x)$$

dla dowolnych $x, y \in A$. Relacja R jest relacją równoważności. Rozbija więc zbiór A na klasy abstrakcji, czyli na zbiory postaci $\{y \in A : xRy\}$. Różne klasy abstrakcji są rozłączne. Jest też oczywiste, że jeżeli $z \in \{y \in A : xRy\}$, to także $s(z) \in \{y \in A : xRy\}$. 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 $s : X \to X$ mamy bijekcje $t : Y \to Y$ i $\phi : Y \to X$ 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 $f, g : Y \to Y$, 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 $A_0 = \{y \in A : a_0 Ry\}$. Zdefiniujmy pomocniczą funkcję $\phi : \mathbb{Z} \to A_0$ 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 załóżmy, 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 $\{x \in \mathbb{N} : x < m_0\}$ 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 350. Przypuśćmy, że $f : X \to Y$, $A \subseteq X$ oraz $B \subseteq Y$. Udowodnij, że

$$f(A \cap f^{-1}(B)) \quad = \quad f(A) \cap B$$

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 $y \in B$, wiec 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 zawierań i zasady ekstensjonalności.

Rozwiązanie (inny dowód jednego z zawierań). Skorzystamy teraz z dwóch własności pojęcia obrazu: monotoniczności

$$C \subseteq D \Rightarrow f(C) \subseteq f(D)$$

oraz zawierania

$$f(f^{-1}(B)) \subseteq B,$$

a także z dwóch znanych własności przekroju:

$$E \subseteq C \wedge E \subseteq D \Rightarrow E \subseteq C \cap D$$

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 351. 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 załóżmy, 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 spełniają 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 przechodniość relacji R jest równoważna zawieraniu $RR \subseteq R$.

Załóżmy, 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 przechodniości 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 przechodniości relacji R.

Część 4. Z części 1, 2 i 3 wynika równoważność z częsci 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 $\varphi_1 \wedge \varphi_2 \wedge \varphi_3$ jest równoważna koniunkcji $\psi_1 \wedge \psi_2 \wedge \psi_3$.■

Zadanie 352. Niech f będzie bijekcją przekształcającą zbiór A w A. Zdefiniujmy relację $R \subseteq A^2$ przyjmując, że

$$xRy \iff f(x) = y.$$

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

$$\langle x, y\rangle \in R \Leftrightarrow xRy \Leftrightarrow f(x) = y \Leftrightarrow \langle x, y\rangle \in f,$$

czyli 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 $f : \mathbb{Z} \to \mathbb{Z}$ 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 $I : \mathbb{N} \to A$ 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 f była różnowartościowa, to zbiór A byłby nieskończony. Dla skończonego zbioru A funkcja f 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, $f^p(x) = f^q(x) = f^p(f^{q-p}(x))$. Różnowartościowości 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

$$f^r(x) = x. \tag{10}$$

Udowodniona własność oznacza, że relacja R_∞ jest zwrotna. Aby się o tym przekonać, bierzemy $x \in A$ i liczbę $r > 0$ spełniającą (10). Z równości (10) 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 (10) implikuje także, że jeżeli iterujemy obliczanie wartości funkcji f zaczynając od argumentu x, to otrzymujemy w kółko te same wartości

$$f(x),\ f^2(x), \ldots,\ f^r(x) = x,\ f(x),\ f^2(x), \ldots,\ f^r(x) = x,\ f(x), \ldots$$

Spostrzeżenie to pozwala dowieść symetryczność relacji R_∞. Najpierw jednak zauważmy, że równość (10) 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. Przypuśćmy, 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 118.

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 równoważnością. ■

Zadanie 353. 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 impikacje $p \Rightarrow q$ 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 354. 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 $f : K \to A$ będzie funkcją, która dla klasy $Y \in K$ przyjmuje wartość $f(Y) \in Y \cap A$. Punkt 3) ze sformułowania zadania gwaratuje poprawność tej definicji.

Pokażemy, że funkcja f jest bijekcją. Jeżeli $f(Y) = f(Z)$ dla pewnych klas 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 $g : A \to K$, 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

$$|A| = |\bigcup_{Y \in K} A \cap Y| = \sum_{Y \in K} |A \cap Y| = \sum_{Y \in K} 1 = |K|.$$

■

Zadanie 355. 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 $A \not\subseteq B$.

Załóżmy, 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 definiujmy 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 2 i 3. 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 356. Niech $\alpha : \mathbb{N} \to \{0, 1\}$ będzie ciągiem zero-jedynkowym. Symbolem $\sim_\alpha$ oznaczamy relację w zbiorze $\{0, 1\}^{\mathbb{N}}$ nieskończonych ciągów zero-jedynkowych zdefiniowaną formułą

$$\beta \sim_\alpha \gamma \quad \Leftrightarrow \quad (\forall n \in \mathbb{N})\ \alpha(n)\beta(n) = \alpha(n)\gamma(n).$$

Czy istnieje taki ciąg α, dla którego:

a) relacja $\sim_\alpha$ ma przeliczalnie i nieskończenie wiele klas równoważności?

b) wszystkie klasy równoważności relacji $\sim_\alpha$ są przeliczalne i nieskończone?

c) istnieje przeliczalna i nieskończona klasa równoważności relacji $\sim_\alpha$?

Rozwiązanie. Ustalmy α i przyjmijmy, że $A = \{n \in \mathbb{N} : \alpha(n) = 1\}$. 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 183. Zbiór N_α i zbiór $\{0, 1\}^A$ są równoliczne.

Dowód. Dla funkcji $\xi : A \to \{0, 1\}$ definiujemy funkcję $\bar{\xi} : \mathbb{N} \to \{0, 1\}$ przyjmując, że

$$\bar{\xi}(n) \quad = \quad \begin{cases} \xi(n), & \text{jeżeli } n \in A, \\ 0, & \text{w przeciwnym razie.} \end{cases}$$

Zdefiniujmy jeszcze wzorem

$$f(\xi) \quad = \quad [\bar{\xi}]_\alpha$$

funkcję $f : \{0, 1\}^A \to N_\alpha$. 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 $\delta : A \to \{0,1\}$ 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 $g : \{0,1\}^{\mathbb{N}} \to \{0,1\}^A$ 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 $g(\bar{\xi}) = \xi$.

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 $G : N_\alpha \to \{0,1\}^A$ i – co więcej – funkcja ta jest różnowartościowa. Ponieważ g jest typu „na”, więc także G jest typu „na”.

Fakt 184. 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 $f : [\beta]_\alpha \to \{0,1\}^{\mathbb{N}\setminus A}$. 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 obcięcia 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 185. 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 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 357. Niech $f : \mathbb{R} \to \mathbb{R}$. Mówimy, że $x \in \mathbb{R}$ jest lokalnym maksimum funkcji f, jeżeli istnieje taka dodatnia liczba rzeczywista r, że dla każdego $y \in \mathbb{R}$

$$(x - r < y < x + r \land x \neq y) \Rightarrow f(x) > f(y)$$

Udowodnij, że dla każdej funkcji $f : \mathbb{R} \to \mathbb{R}$ 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 przedział zawierający x, taki, 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 przeliczany.

Niestety nie zadbaliśmy 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 rodziny parami rozłącznych przedziałów zawierających wszystkie maksima lokalne, takiej, że w każdym przedziale jest najwyżej jedno maksimum.

Rozważmy funkcję $f_1 : \mathbb{R} \to \mathbb{R}$ zdefiniowaną wzorem

$$f_1(x) = \begin{cases} \sin\left(\dfrac{1}{x}\right) & \text{dla } x \neq 0, \\ 2 & \text{dla } x = 0. \end{cases}$$

Łatwo sprawdzić, że funkcja f_1 przyjmuje maksimum lokalne dla $x = 0$ i dla wszystkich $x = \frac{1}{2k\pi}$ dla $k \in Z$.

Podobnie jest w przypadku funkcji f_2 zdefiniowanej wzorem

$$f_2(x) = \begin{cases} x^2\left(\sin\left(\dfrac{1}{x}\right) - 2\right) & \text{dla } x \neq 0, \\ 0 & \text{dla } x = 0, \end{cases}$$

która dodatkowo jest ciągła, a nawet różniczkowalna.

Weźmy teraz funkcję $f : \mathbb{R} \to \mathbb{R}$ przyjmującą wartości

$$f(x) = \begin{cases} \frac{1}{n}, & \text{jeżeli } x = \frac{m}{n}, \text{ gdzie } n \text{ i } m \text{ są liczbami względnie pierwszymi i } n > 0 \\ 1, & \text{jeżeli } x = 0 \\ 0, & \text{jeżeli } x \notin Q. \end{cases}$$

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

$$a_k = \max\{a \in Z : \frac{a}{k} < \frac{m}{n}\}.$$

Oczywiście, $\frac{a_k}{k} < \frac{m}{n} \leq \frac{a_k+1}{k}$. Jeżeli $0 < k < n$, to także $\frac{m}{n} < \frac{a_k+1}{k}$, 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

$$p = \max\{a_1, \ldots, a_n\} \text{ oraz } q = \min\{a_1 + 1, \ldots, a_{n-1} + 1, a_n + 2\}.$$

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 $f : \mathbb{R} \to \mathbb{R}$, która ma maksima lokalne dokładnie w punktach należących do X.

Dowód (poprawny). Weźmy funkcję $f : \mathbb{R} \to \mathbb{R}$ i zdefiniujmy zbiór

$$M = \{x \in \mathbb{R} : x \text{ jest maksimum lokalnym funkcji } f\}.$$

Aby rozwiązać zadanie wystarczy dowieść, że M jest przeliczalny. Przeliczalność zbioru M wykażemy dowodząc, że istnieje różnowartościowa funkcja

$$g : M \to Q \times Q.$$

Od funkcji g będzie 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 358. 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 205). Aby skorzystać z tego twierdzenia, należy pokazać, że:

1. zbiór skończonych, niepustych ciągów o wyrazach wymiernych jest przeliczalny (zadanie 173),
2. porządek leksykograficzny wyznaczony przez porządek liniowy jest porządkiem liniowym (zadanie 202),
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 $a_1, a_2, \ldots, a_n$ i $b_1, b_2, \ldots, b_m$. 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 $i = 1, \ldots, n$, albo też dla pewnej liczby $k \leq n, m$ zachodzi nierówność $a_k < b_k$ i spełnione są równości $a_i = b_i$ dla $i = 1, \ldots, k-1$. Jeżeli zachodzi pierwszy przypadek, to bierzemy ciąg c o wyrazach $b_1, b_2, \ldots, b_n, b_{n+1} - 1$. W drugim przypadku bierzemy ciąg c o wyrazach $b_1, b_2, \ldots, b_{k-1}, (a_k + b_k)/2$. 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 359. Niech $\Sigma = \{+, a\}$ będzie sygnaturą zawierającą dwuargumentowy symbol funkcji $+$ i symbol stałej a. Dla dowolnej dodatniej liczby naturalnej n niech $A_n = \{0, 1, \ldots, n-1\}$, $\oplus_n$ 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 conajmniej 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 $1 \oplus_k \ldots \oplus_k 1$). Wobec tego 1 generuje A_k. Homomorfizm wystarczy zdefiniować na zbiorze generatorów. Przyjmijmy więc, że $h : A_k \to A_l$ jest homomorfizmem i $h(1) = a$. Wtedy

$$h(n) = h(\underbrace{1 \oplus_k \ldots \oplus_k 1}_{n \text{ razy}}) = \underbrace{h(1) \oplus_l \ldots \oplus_l h(1)}_{n \text{ razy}} = (a \cdot n) \bmod l.$$

Fakt 186. Jeżeli l dzieli k, to funkcja $h_a : A_k \to A_l$ 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 1. Korzystając z podanego faktu można łatwo rozwiązać pierwszą część zadania. Wystarczy zauważyć, że jeżeli $k = l \cdot m$, to $h_1 : A_k \to A_l$ jest homomorfizmem takim, że $h_1(x) = x$ dla $x = 0, \ldots, l-1$, a więc jest homomorfizmem algebry $\mathcal{A}_k$ na algebrę $\mathcal{A}_l$. Mamy także

$$\begin{aligned} h_1^{-1}(0) &= \{x < l \cdot m : x \bmod l = 0\} = \{x < l \cdot m : l \text{ dzieli } x\} = \\ &= \{i \cdot l : i < m\} = g(\{i : i < m\}) \end{aligned}$$

dla funkcji $g : \mathbb{N} \to \mathbb{N}$ takiej, że $g(i) = i \cdot l$. Funkcja g jest oczywiście różnowartościowa. Wobec tego zbiór $h_1^{-1}(0)$ jest równoliczny ze zbiorem $\{i : i < m\}$, 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 $h_2 : A_6 \to A_3$ (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 algebrą $\mathcal{A}_k$ 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

$$h(n) = h(\underbrace{1 \oplus_k \ldots \oplus_k 1}_{n \text{ razy}}) = \underbrace{h(1) \oplus_l \ldots \oplus_l h(1)}_{n \text{ razy}} = \underbrace{h_1(1) \oplus_l \ldots \oplus_l h_1(1)}_{n \text{ razy}} = h_1(n)$$

dla wszystkich $n \in A_k$. Wobec tego, homomorfizmy h i h_1 są identyczne. Bardziej elegancki dowód tego faktu powinien być indukcyjny. ■

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:															
											Suma:				

Zaj. 3	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 4	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 5	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 6	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 7	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 8	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 9	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 10	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 11	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 12	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 13	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 14	Data:														
Zadania:															
Punkty:															
											Suma:				

Zaj. 15	Data:														
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