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

Logika dla informatyków

Materiały do zajęć

Wrocław, 2020

Właściciel tej kopii notatek	Rok akad. 2020/21

Uwaga: W niniejszej książeczce zebrano listy zadań, notatki do wykładów oraz inne materiały przygotowywane do zajęć z *Logiki dla informatyków* w latach 1997–2020. Mimo iż materiały te posiadają bardziej dopracowaną formę, niż przygotowywane do innych zajęć kserograficzne kopie oraz zostały oddane do druku i oprawy, jednak nie były poddane — jak to ma miejsce w przypadku podręczników — solidnej korekcie i zawierają sporo błędów. Nie zamieszczono w nich także szczegółowych wyjaśnień i komentarzy. Dlatego notatki te *nie są podręcznikiem do wykładu*. Mają jedynie służyć jako wykaz zagadnień obowiązujących do egzaminu i lista zadań przerabianych na ćwiczeniach. Przegląd zalecanych do zajęć podręczników jest zamieszczony na stronie xi.

Podczas redagowania notatek wykorzystano:
– skrypt J. Tiuryna *Wstęp do teorii mnogości i logiki*
– listy zadań M. Zakrzewskiego
– materiały K. Apta, A. Kościelskiego, P. Urzyczyna i T. Wierzbickiego
– podręczniki wymienione w bibliografii na stronie xi

Manuskrypt: W. Charatonik i L. Pacholski
Redakcja i skład: W. Charatonik i T. Wierzbicki
Konsultacja merytoryczna: A. Kościelski

Wydanie osiemnaste, poprawione

Data utworzenia dokumentu: 14 września 2020

Szanowni Państwo,

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

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

Od wielu lat wszystkim studentom zaczynającym studia powtarzamy to, co napisaliśmy w poprzednim paragrafie. Niestety z marnym skutkiem. Co roku w drugiej połowie semestru okazuje się, że znaczna część studentów nie rozumie wykładu, bo nie pamięta wcześniej wprowadzonych definicji i nie zna treści udowodnionych wcześniej twierdzeń. Co roku około połowy studentów nie zalicza tego przedmiotu. 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, kolokwia itd.). Ich celem nie jest uprzykrzenie Wam życia, ale zwiększenie szansy na to, że zdacie egzamin.

Wykładowcy

Spis treści

A
Informacje ogólne

Logika dla Informatyków jest przedmiotem obowiązkowym na pierwszym semestrze studiów informatycznych I stopnia na Uniwersytecie Wrocławskim. W roku akademickim 2019/20 logika uzyskała szczególny status: jest to jedyny przedmiot, którego nie można na tych studiach powtarzać.

A.1. Zapisy na zajęcia

Na zajęcia należy się zapisać w internetowym systemie *Zapisy*, dostępnym pod adresem `https://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.

Mimo że w systemie *Zapisy* prowadzący są dla porządku przypisani do poszczególnych grup ćwiczeniowych, jednak w kolejnych tygodniach mogą mieć zajęcia z różnymi grupami. Dlatego przy wyborze grupy nie należy się kierować nazwiskiem prowadzącego.

Oprócz systemu *Zapisy* w trakcie zajęć będziemy korzystać z *Systemu Komunikacji ze Studentami (Skos)* pod adresem `https://skos.ii.uni.wroc.pl`, gdzie będą ogłaszane listy zadań i inne materiały dla studentów (w tym informacje o sprawdzianach, egzaminach, konsultacjach itp) oraz z *Uczelnianego Systemu Obsługi Studiów (Usosweb)* pod adresem `https://usosweb.uni.wroc.pl`, gdzie będzie prowadzona punktacja ćwiczeń.

A.2. Obsada zajęć i konsultacje

Obsada zajęć dydaktycznych w danym roku akademickim jest dostępna w systemie *Zapisy*.

Każdy student ma niepodważalne prawo do bezpośredniej rozmowy z prowadzącymi na temat zajęć, w których uczestniczy. Uważamy, że z takich spotkań, tj. *konsultacji*, studenci korzystają nawet zbyt mało. Serdecznie zapraszając na konsultacje mamy jednak prośbę, by przestrzegać ustalonych przez prowadzących zasad. Każdy pracownik dydaktyczny wyznacza dwie godziny w tygodniu, w czasie których jest do dyspozycji studentów. 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. Studentów zapisanych na przedmiot jest ponad stu, a prowadzący — jeden. Nie chcemy, żeby studenci odnieśli wrażenie, że prowadzący starają się od nich izolować. Chodzi tylko o to, by nasze kontakty z dużą liczbą studentów przebiegały sprawnie i nie dezorganizowały naszej pracy w Instytucie.

Godziny konsultacji można znaleźć m. in. na stronach domowych prowadzących oraz w systemie *Zapisy*.

Po zajęciach prowadzący będą uzupełniać w systemie *Usosweb* punktację ćwiczeń służącą do wyliczenia ocen końcowych. Problemy techniczne dotyczące punktacji za zadania, sprawdziany i kartkówki należy wyjaśniać z osobą, która danego dnia prowadziła ćwiczenia, osobiście w czasie jej konsultacji lub za pośrednictwem poczty elektronicznej, nie później niż trzy tygodnie po ćwiczeniach. W początkowym okresie (mniej więcej pierwsze dwa tygodnie semestru) system *Usosweb* nie ma jeszcze wystarczających informacji o studentach zapisanych na przedmiot; w tym czasie punktacja nie jest dostępna.

B

Literatura

Spośród licznych podręczników dostępnych w bibliotekach i księgarniach warto wymienić (wszystkie wymienione książki są dostępne w bibliotece wydziałowej):

1. Jerzy Tiuryn, *Wstęp do teorii mnogości i logiki*. Skrypt można wypożyczyć w bibliotece wydziałowej. Wersja elektroniczna jest dostępna na stronie wykładu.

2. Wojciech Guzicki, Piotr Zakrzewski, *Wykłady ze wstępu do matematyki. Wprowadzenie do teorii mnogości* oraz *Wstęp do matematyki. Zbiór zadań*, PWN, Warszawa, 2005.

3. Kazimierz Kuratowski, *Wstęp do teorii mnogości i topologii*, PWN, Warszawa, 1982. Krótkie wprowadzenie do teorii mnogości.

4. Kazimierz Kuratowski, Andrzej Mostowski, *Teoria mnogości*, PWN, Warszawa, 1978. Obszerny wykład teorii mnogości.

5. Wiktor Marek, Janusz Onyszkiewicz, *Elementy logiki i teorii mnogości w zadaniach*, PWN, Warszawa, 2000. Obszerny zbiór prostych, typowych zadań.

6. Helena Rasiowa, *Wstęp do matematyki współczesnej*, PWN, Warszawa, 1999. Klasyczny podręcznik podstaw logiki i teorii mnogości.

7. Kenneth A. Ross, Charles R. B. Wright, *Matematyka dyskretna*, PWN, Warszawa, 1986. Wbrew tytułowi książka zawiera sporo elementarnie wyłożonego materiału z logiki i teorii mnogości. Oryginał angielski: (*Discrete Mathematics*, Prentice Hall, 1988).

8. Jerzy Słupecki, Ludwik Borkowski, *Elementy logiki matematycznej i teorii mnogości*, PWN, Warszawa, 1963.

9. Michael Huth, Mark Ryan, *Logic in computer science*, Cambridge University Press, 2004.

10. Susanna S. Epp, *Discrete mathematics with applications*, Brooks/Cole, 2011.
11. Keith Devlin, *Myślenie matematyczne. Twój nowy sposób pojmowania świata*, Helion, 2019.

C

Zasady prowadzenia i zaliczania ćwiczeń

Poniższy regulamin zakłada, że zajęcia będą się odbywać w formie stacjonarnej; w przypadku zmian reżimu sanitarnego zasady prowadzenia zajęć i progi punktowe mogą się zmienić. O szczegółach tych zmian będziemy informować na bieżąco w systemie Skos. W chwili drukowania skryptu przewidujemy jedynie, że w przypadku konieczności przejścia na zdalne nauczanie przeniesiemy nacisk z prezentacji ustnych przy tablicy na pisemne prace domowe.

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. Mimo że zachęcamy studentów do wspólnej nauki, stanowczo odradzamy metodę polegającą na słuchaniu rozwiązań prezentowanych przez innych (np. starszych kolegów) lub szukaniu ich w internecie i uczeniu się ich na pamięć. Metoda taka nie może dać dobrych rezultatów, podobnie jak nie można nauczyć się grać na fortepianie tylko słuchając koncertów.

Podstawą do wystawienia oceny jest liczba zadań, które student rozwiązał w trakcie całego semestru i, pomijając wyjątkowe przypadki, ocena zależy w sposób liniowy od tej liczby. Prowadzący spotyka się ze studentami regularnie na ćwiczeniach, aby ustalić faktyczną liczbę zadań rozwiązanych przez każdego studenta. Dlatego pomimo iż na zajęciach powinna panować swobodna atmosfera, nie należy zapominać, że każde 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 powinni prezentować jedynie studenci dobrze przygotowani). Trzeba przy tym pamiętać, że rozwiązania powinny być prezentowane przez *studentów*. O ile dopuszcza się możliwość prezentowania pojedynczych rozwiązań przez prowadzącego, zajęcia zdominowane przez taką formę przyjmowane są z niechęcią.

Numery zadań obowiązujących na następny tydzień są ogłaszane w systemie Skos. Począwszy od około trzeciego tygodnia semestru w systemie Usosweb jest prowadzona punktacja ćwiczeń zawierająca zestawienie aktualnie zdobytej liczby punktów przez każdego studenta i prognozę oceny końcowej. Po zakończeniu semestru zawiera ona ostateczne wyniki ćwiczeń. We wszelkich sprawach dotyczących liczby zdobytych punktów studenci winni zgłaszać się do osoby prowadzącej zajęcia w danym dniu.

Na każdą z około 28 godzin zajęć zadaje się przeciętnie 3 zadania, zatem w ciągu całego semestru będzie ich około 84. Niniejsze notatki zawierają o kilkaset zadań więcej, a więc spory nadmiar. Bardzo zachęcamy studentów do rozwiązywania także pozostałych zadań.

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

C.2. Szczegółowe zasady prowadzenia zajęć

1. Co najmniej na trzy dni (zwykle na tydzień) przed zajęciami na stronie WWW wykładu jest ogłaszana lista numerów zadań z niniejszego zbioru. Część zadań jest oznaczona gwiazdką. Na ćwiczeniach są rozwiązywane wybrane zadania z tej listy. Prowadzącemu pozostawia się decyzję odnośnie wyboru zadań do rozwiązania.

2. Przed rozpoczęciem zajęć student wypełnia kupon wpisując numery zadań z listy, które potrafi rozwiązać.[1] Kartka powinna być wypełniona czytelnie, zawierać datę, jednoznacznie wpisane numery zadań[2], liczby punktów za poszczególne zadania, sumę punktów oraz imię i nazwisko studenta. Bezpośrednio po wejściu do sali ćwiczeniowej prowadzący zajęcia zbiera kupony. *Gdy prowadzący przychodzi do sali ćwiczeniowej, kupony powinny być już wypeł-*

[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.

nione przez studentów tak, by mogły być natychmiast zebrane i by prowadzący nie musiał opóźniać rozpoczęcia zajęć oczekując na wypełnienie kuponów.

3. Po rozpoczęciu zajęć dokonywanie jakichkolwiek zmian w treści złożonych deklaracji[3] jest niemożliwe.
4. Na każdych zajęciach student zdobywa liczbę punktów równą liczbie zadań, które zgłosił do rozwiązania z listy przewidzianej na dane zajęcia, z wyjątkiem przypadków opisanych w punktach 10–12.
5. Student nieobecny na zajęciach nie otrzymuje punktów. Poza przypadkami długotrwałej (trwającej co najmniej trzy tygodnie) choroby poświadczonej zwolnieniem lekarskim nie można odzyskać utraconych w ten sposób punktów.
6. Rozwiązanie danego zadania na tablicy przedstawia jedna z osób, wybrana przez prowadzącego, która zgłosiła gotowość rozwiązania tego zadania.[4] Prowadzący ma prawo przerwać osobie referującej w dowolnym momencie i poprosić inne osoby, które zgłosiły gotowość rozwiązania danego zadania, o kontynuowanie.[5]
7. Osoba przedstawiająca rozwiązanie musi znać i rozumieć definicje wszystkich pojęć, których używa w rozwiązaniu; nieznajomość lub niezrozumienie definicji jakiegokolwiek używanego pojęcia są traktowane jak błąd w rozwiązaniu. Osoba ta musi być także przygotowana na niewielkie zmiany w treści zadania.[6]
8. W ciągu semestru odbędą się trzy kolokwia punktowane od 0 do 25 punktów. Każdy student otrzyma punkty za dwa najlepiej napisane z tych trzech kolokwiów. Nie będzie kolokwiów poprawkowych. Również w przypadku usprawiedliwionej nieobecności na którymś z kolokwiów nie będzie możliwości poprawienia wyniku.
9. 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

[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.

[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] Ma to na celu zapobieganie dość powszechnym wśród studentów praktykom uczenia się na pamięć rozwiązań bez ich zrozumienia. W świetle tej regulacji np zadania 39 i 40 są tym samym zadaniem i wobec studenta, który zgłasza jedno z nich a nie umie rozwiązać drugiego, mogą być zastosowane sankcje z punktów 10 lub 12.

materiał. Aby ułatwić studentom systematyczne powtarzanie wcześniej poznanego materiału, ćwiczenia mogą rozpoczynać się od krótkiej kartkówki sprawdzającej znajomość pojęć wprowadzanych na wykładzie oraz podstawowych faktów (według niniejszych notatek do wykładu) lub rozwiązywanych wcześniej zadań. Za poprawną odpowiedź na wszystkie pytania zadane w kartkówce można otrzymać 5 punktów, z tym że w semestrze odbędzie się około siedmiu kartkówek a punkty otrzymuje się tylko za sześć najlepiej napisanych.

10. 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 punkty. W ciągu tygodnia od tego zdarzenia student może dostarczyć prowadzącemu, z którym miał w tym dniu zajęcia, pisemne rozwiązanie[7] tego samego zadania, za które będzie mógł otrzymać od zera do trzech punktów.

11. Student rozwiązujący zadanie przy tablicy otrzymuje za nie dodatkowo od 0 do 2 punktów. Standardowo jest to 1 punkt; eleganckie i zrozumiałe dla słuchaczy rozwiązania nagradzane są 2 punktami; rozwiązania częściowe lub niezrozumiałe mogą nie być nagradzane. O liczbie przyznanych punktów decyduje prowadzący zajęcia.

12. 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 5 punktów.[8]

13. W ciągu semestru do rozwiązania zostaną przedstawione zadania o łącznej liczbie punktów nie mniejszej niż 84. Ponadto będzie można uzyskać 80 punktów za prace pisemne: 50 za kolokwia i 30 za kartkówki. Oznacza to, że łącznie można uzyskać co najmniej 164 punkty oraz kilka do kilkunastu punktów za rozwiązywanie zadań przy tablicy.

14. Ocena końcowa z ćwiczeń jest wystawiana na podstawie uzyskanych punktów, według zasad opisanych w następnym rozdziale i podsumowanych w tabeli C.1.

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

---

[7] Rozwiązanie musi być napisane odręcznie, w szczególności nie może być wydrukowane. Ma to na celu zapobieganie kopiowaniu gotowych rozwiązań od innych studentów.

[8] Z punktu widzenia interesów studenta okazuje się krytyczne rozróżnienie między tym punktem i punktem 10. Niestety, mimo jasnego sformułowania, chodzi tu o kwestię merytoryczną co do której podanie ścisłego algorytmu postępowania jest niemożliwe. Rozróżnienie to pozostaje do decyzji prowadzącego.

[9] Student powinien mieć świadomość, że zajęć można nie zaliczyć. W szczególności utrata punktów zgodnie z paragrafem 12 może jednoznacznie i nieodwołalnie skazać studenta na niezaliczenie zajęć i konieczność powtarzania przedmiotu w następnym roku lub skreślenie z listy studentów.

16. Studenci po zapisaniu się do grup ćwiczeniowych nie mogą ich zmieniać, nawet jeśli zajęcia odbywają się w tym samym czasie.
17. Podczas referowania zadań przy tablicy student nie może mieć przy sobie notatek.

punkty	ocena
$\geq 70^{*}$	dst
$\geq 86^{*}$	dst+
$\geq 102^{*\dagger}$	db
$\geq 118^{*\dagger}$	db+
$\geq 134^{*\ddagger}$	bdb

* w tym 25 punktów za prace pisemne, 30 za ustne, 30 przed końcem roku
† w tym rozwiązanie przy tablicy co najmniej jednego zadania z gwiazdką
‡ w tym rozwiązanie przy tablicy co najmniej trzech zadań z gwiazdką

Tablica C.1: Sposób przeliczania liczby punktów na ocenę z ćwiczeń. Punkty bonusowe: patrz rozdział D.

C.3. Szczegółowe zasady zaliczania ćwiczeń

Ocena z ćwiczeń wystawiana jest na podstawie sumy uzyskanych w ciągu semestru punktów według tabeli C.1. Aby zaliczyć ćwiczenia należy spełnić dodatkowe warunki:

1. uzyskać co najmniej 30 punktów przed końcem roku kalendarzowego,
2. uzyskać co najmniej 25 punktów za prace pisemne,
3. uzyskać co najmniej 30 punktów za zgłoszone zadania

Dodatkowo, aby otrzymać ocenę dobrą lub dobrą plus należy rozwiązać przy tablicy co najmniej jedno zadanie oznaczone gwiazdką. Do otrzymania oceny bardzo dobrej konieczne jest rozwiązanie przy tablicy co najmniej trzech takich zadań.

D

Egzaminy

Oceną, jaką student otrzymuje z przedmiotu, jest wynik egzaminu zasadniczego. W razie otrzymania oceny niedostatecznej student ma prawo przystąpić do egzaminu poprawkowego. Każdy z tych egzaminów (końcowy i poprawkowy) składa się z dwóch części.

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 itp). 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, jak i poprawkowy można otrzymać od minus kilkunastu do 100 punktów. Punkty ujemne będą przyznawane za rozpoczęcie rozwiązywania zadania[1] oraz za umieszczenie w rozwiązaniu odpowiedzi kompromitująco fałszywych. Za brak rozwiązania zadania otrzymuje się 0 punktów. Liczba punktów możliwych do zdobycia na egzaminie może zostać zwiększona poprzez dodanie zadań bonusowych.

Do wyników egzaminu zasadniczego i poprawkowego dolicza się punkty bonusowe za zaliczenie ćwiczeń. Liczba punktów bonusowych jest częścią całkowitą ilorazu: $(C - 62)/16$, 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.

---

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

punkty	ocena
$[-100 \div 18)$	ndst
$[18 \div 34)^*$	dst
$[34 \div 50)^*$	dst+
$[50 \div 66)^*$	db
$[66 \div 82)^*$	db+
$[82 \div +\infty)^*$	bdb

*Co najmniej 18 punktów należy uzyskać z pierwszej części.

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

Terminy egzaminów, miejsca ich przeprowadzenia, przydział studentów do sal, terminy ogłoszenia wyników oraz miejsca i terminy konsultacji poegzaminacyjnych są podane na stronie wykładu. Wszelkie wątpliwości dotyczące sposobu oceniania egzaminu i otrzymanych ocen studenci powinni wyjaśniać w trakcie konsultacji poegzaminacyjnych. Konsultacje dotyczące wyników egzaminów w innych terminach nie będą dokonywane.

Treść zadań egzaminacyjnych oraz wyniki egzaminów są ogłaszane na stronie wykładu po zakończeniu egzaminu.

D.1. Egzamin końcowy

Ocena z egzaminu końcowego jest wystawiana na podstawie sumy punktów uzyskanych na egzaminie i punktów bonusowych. Zakres materiału na egzaminie końcowym obejmuje cały semestr.

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.

Egzamin składa się z dwóch części oddzielonych od siebie krótką przerwą. Pierwsza część sprawdza podstawowe opanowanie materiału, natomiast druga sprawdza umiejętność twórczego posługiwania się nabytą wiedzą.

W razie nieobecności na egzaminie spowodowanej chorobą student ma obowiązek dostarczyć egzaminatorowi (osobiście, pocztą lub przez osoby trzecie) zwolnienie lekarskie w ciągu siedmiu dni licząc od dnia egzaminu. W szczególnych przypadkach decyzję o usprawiedliwieniu nieobecności na egzaminie może podjąć Dziekan lub Dyrektor Instytutu. W razie usprawiedliwionej nieobecności na egzaminie końcowym egzaminator ustali dla danej osoby inny termin egzaminu w sesji zimowej (zwykle jest to pierwszy dzień roboczy po ustaniu przyczyny nieobecności).

Na pierwszej części egzaminu można zdobyć do 40 punktów. Osoby, które zdobędą co najmniej 18 punktów, będą mogły otrzymać (bez względu na wynik drugiej części) ocenę dostateczną z egzaminu końcowego. Ponadto osoby te będą mogły na pełnych prawach wziąć udział w drugiej części. Studenci, którzy w pierwszej części uzyskają mniej niż 18 punktów, otrzymają ocenę niedostateczną a ich prace z drugiej części egzaminu końcowego nie będą sprawdzane.

D.2. Egzamin poprawkowy

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

Notacja matematyczna

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

Pismo łacińskie, gotyckie, blokowe i kaligraficzne

$$
\begin{array}{cccccccccccccccccccccccccc}
a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\
A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\
\mathfrak{a} & \mathfrak{b} & \mathfrak{c} & \mathfrak{d} & \mathfrak{e} & \mathfrak{f} & \mathfrak{g} & \mathfrak{h} & \mathfrak{i} & \mathfrak{j} & \mathfrak{k} & \mathfrak{l} & \mathfrak{m} & \mathfrak{n} & \mathfrak{o} & \mathfrak{p} & \mathfrak{q} & \mathfrak{r} & \mathfrak{s} & \mathfrak{t} & \mathfrak{u} & \mathfrak{v} & \mathfrak{w} & \mathfrak{x} & \mathfrak{y} & \mathfrak{z} \\
\mathfrak{A} & \mathfrak{B} & \mathfrak{C} & \mathfrak{D} & \mathfrak{E} & \mathfrak{F} & \mathfrak{G} & \mathfrak{H} & \mathfrak{I} & \mathfrak{J} & \mathfrak{K} & \mathfrak{L} & \mathfrak{M} & \mathfrak{N} & \mathfrak{O} & \mathfrak{P} & \mathfrak{Q} & \mathfrak{R} & \mathfrak{S} & \mathfrak{T} & \mathfrak{U} & \mathfrak{V} & \mathfrak{W} & \mathfrak{X} & \mathfrak{Y} & \mathfrak{Z} \\
\mathbb{A} & \mathbb{B} & \mathbb{C} & \mathbb{D} & \mathbb{E} & \mathbb{F} & \mathbb{G} & \mathbb{H} & \mathbb{I} & \mathbb{J} & \mathbb{K} & \mathbb{L} & \mathbb{M} & \mathbb{N} & \mathbb{O} & \mathbb{P} & \mathbb{Q} & \mathbb{R} & \mathbb{S} & \mathbb{T} & \mathbb{U} & \mathbb{V} & \mathbb{W} & \mathbb{X} & \mathbb{Y} & \mathbb{Z} \\
\mathcal{A} & \mathcal{B} & \mathcal{C} & \mathcal{D} & \mathcal{E} & \mathcal{F} & \mathcal{G} & \mathcal{H} & \mathcal{I} & \mathcal{J} & \mathcal{K} & \mathcal{L} & \mathcal{M} & \mathcal{N} & \mathcal{O} & \mathcal{P} & \mathcal{Q} & \mathcal{R} & \mathcal{S} & \mathcal{T} & \mathcal{U} & \mathcal{V} & \mathcal{W} & \mathcal{X} & \mathcal{Y} & \mathcal{Z}
\end{array}
$$

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	rho
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	ipsilon
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	theta	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. Pan Hilary zgubił swoje okulary i w ich poszukiwaniu stwierdza następujące fakty:

- Jeśli czytałem gazetę w kuchni to okulary są na stole kuchennym.
- Jeśli okulary są na stole kuchennym, to widziałem je podczas śniadania.
- Nie widziałem okularów podczas śniadania.
- Czytałem gazetę w kuchni lub w sypialni.
- Jeśli czytałem gazetę w sypialni to okulary są na łóżku.

Czy z tych faktów można wywnioskować gdzie są okulary?

Zadanie 2. 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 3. Udowodnij, że istnieją takie liczby całkowite m i n, że $m > 1$, $n > 1$ oraz $\frac{1}{m} + \frac{1}{n}$ jest liczbą całkowitą.

Zadanie 4. Udowodnij, że stwierdzenie *dla dowolnych nieujemnych liczb rzeczywistych a i b zachodzi równość $\sqrt{a} + \sqrt{b} = \sqrt{a+b}$* jest fałszywe.

Definicja 1. Mówimy, że liczba całkowita d jest *dzielnikiem* liczby całkowitej n jeśli istnieje taka liczba całkowita k, że $n = dk$. Mówimy, że liczba naturalna n jest *pierwsza* jeśli $n > 1$ oraz n nie ma innych niż 1 i n dzielników naturalnych; w przeciwnym przypadku, gdy n ma inne niż 1 i n dzielniki naturalne, mówimy że jest to liczba *złożona*.

Zadanie 5. Udowodnij, że dla wszystkich większych od 1 liczb całkowitych n liczba $n^2 + 2n$ jest złożona.

Zadanie 6. Udowodnij, że nie istnieje taka dodatnia liczba naturalna n, że n^2+3n+2 jest liczbą pierwszą.

Zadanie 7. Udowodnij, że dla dowolnych liczb rzeczywistych a, b, c, d równość

$$(a + b)(c + d) = (a + c)(b + d)$$

zachodzi wtedy i tylko wtedy, gdy $a = d$ lub $b = c$.

Zadanie 8. Wskaż błąd w następujących „dowodach" twierdzenia, że dla wszystkich dodatnich liczb naturalnych k liczba $k^2 + 2k + 1$ jest złożona.

„Dowód" 1 Weźmy $k = 2$. Wtedy $k^2+2k+1 = 2^2+2\cdot2+1 = 9$, ale liczba 9 dzieli się przez 3, więc 9 jest liczbą złożoną. Zatem twierdzenie jest prawdziwe.

„Dowód" 2 Weźmy dowolną dodatnią liczbę naturalną k. Jeśli k^2+2k+1 jest liczbą złożoną to $k^2 + 2k + 1 = pq$ dla pewnych dodatnich liczb naturalnych p i q takich, że

$$1 < p < k^2 + 2k + 1$$

oraz

$$1 < q < k^2 + 2k + 1.$$

Skoro $k^2 + 2k + 1 = pq$ i obie liczby p i q są ściśle pomiędzy 1 i $k^2 + 2k + 1$ to znaczy że p i q są innymi niż 1 i k^2+2k+1 dzielnikami liczby k^2+2k+1, a zatem liczba $k^2 + 2k + 1$ jest złożona.

Definicja 2. Mówimy, że liczba całkowita n jest *parzysta* jeśli istnieje taka liczba całkowita k, że $n = 2k$. Mówimy, że n jest *nieparzysta* jeśli istnieje taka liczba całkowita k, że $n = 2k + 1$.

Zadanie 9. Wskaż błąd w następującym „dowodzie" twierdzenia, że różnica pomiędzy dowolną liczbą parzystą a dowolną nieparzystą jest nieparzysta.

„Dowód" Weźmy dowolną liczbę parzystą m i dowolną liczbę nieparzystą n. Z definicji parzystości wiemy, że $m = 2k$ dla pewnego k oraz $n = 2k + 1$ dla pewnego k. Wtedy $n - m = (2k + 1) - 2k = 1$. Skoro 1 jest liczbą nieparzystą, pokazaliśmy że różnica pomiędzy dowolną liczbą parzystą a dowolną nieparzystą jest nieparzysta.

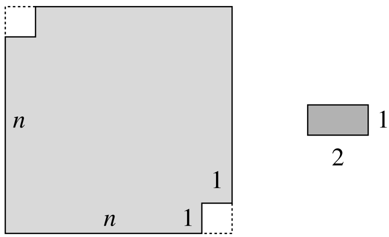
Zadanie 10. Wskaż błąd w następującym „dowodzie” twierdzenia, że iloczyn liczby parzystej przez nieparzystą jest parzysty.

„Dowód” Weźmy dowolną liczbę parzystą m i dowolną liczbę nieparzystą n. Jeśli mn jest parzysta, to z definicji parzystości istnieje taka liczba r, że $mn = 2r$. Z parzystości m wiemy, że istnieje taka liczba p, że $m = 2p$, a z nieparzystości n wiemy, że istnieje taka liczba q, że $n = 2q + 1$. Wtedy

$$mn = (2p)(2q + 1) = 2r.$$

Z definicji parzystości otrzymujemy, że mn jest parzysta, co kończy dowód.

Zadanie 11. Rozważmy kwadrat o boku n, gdzie $n \geq 3$, z którego usunięto dwa naprzeciwległe narożniki o wymiarach 1×1, jak na poniższym rysunku:



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

1

Indukcja matematyczna

Twierdzenie 3 (zasada indukcji). Niech X będzie takim podzbiorem zbioru liczb naturalnych $\mathbb{N}$, że

1. $0 \in X$, oraz
2. dla wszystkich liczb naturalnych n spełniona jest implikacja: jeśli $n \in X$ to $n + 1 \in X$.

Wtedy $X = \mathbb{N}$.

Dowolny zbiór spełniający warunki 1 i 2 powyższego twierdzenia nazywamy *induktywnym*. Innymi słowami, zbiór induktywny to zbiór zawierający 0 i zamknięty na dodawanie jedynki. Zasada indukcji w tej postaci mówi po prostu, że każdy zbiór induktywny zawiera zbiór liczb naturalnych. Zasada ta wynika wprost z definicji zbioru liczb naturalnych (formalnie jest to najmniejszy zbiór induktywny), ale głębsze rozważania na ten temat wybiegają poza ramy tego wykładu. Jeśli oprzemy się na wiedzy wyniesionej ze szkoły średniej, możemy do uzasadnienia zasady indukcji użyć zasady minimum mówiącej, że każdy niepusty podzbiór zbioru liczb naturalnych ma element najmniejszy.

Dowód (twierdzenia 3, oparty na zasadzie minimum). Przeprowadzimy dowód nie wprost. Gdyby $X \neq \mathbb{N}$ to zbiór $\mathbb{N} - X$ byłby niepusty, więc z zasady minimum miałby element najmniejszy. Niech k będzie najmniejszą liczbą naturalną w zbiorze $\mathbb{N} - X$. Oczywiście $k \neq 0$, bo $0 \in X$. Z faktu, że k jest najmniejszą liczbą naturalną nienależącą do X wnioskujemy, że $k - 1 \in X$. Wtedy z drugiego warunku otrzymujemy $k \in X$, co przeczy założeniu, że $k \notin X$. ■

Przykład 4. Rozważmy funkcję $f : \mathbb{N} \to \mathbb{N}$ zdefiniowaną rekurencyjnie wzorami $f(0) = 0$ oraz $f(n + 1) = f(n) + 2$. Pokażemy indukcyjnie, że $f(n) = 2n$ dla wszystkich $n \in \mathbb{N}$.

Niech $X = \{n \in \mathbb{N} \mid f(n) = 2n\}$. Z wzoru $f(0) = 0$ wynika, że $0 \in X$. Weźmy teraz dowolną liczbę naturalną n i załóżmy, że $n \in X$. Wtedy z tego założenia wynika, że $f(n) = 2n$ a z wzoru $f(n+1) = f(n)+2$ otrzymujemy $f(n+1) = 2n+2$, czyli $f(n+1) = 2(n+1)$, a stąd $n+1 \in X$. Na mocy zasady indukcji otrzymujemy, że $X = \mathbb{N}$, czyli warunek $f(n) = 2n$ zachodzi dla wszystkich liczb naturalnych. ∎

Typowy dowód indukcyjny składa się z dwóch części: dowodu, że $0 \in X$ (warunek ten oraz jego dowód są nazywane *podstawą indukcji*) oraz dowodu implikacji $n \in X \Rightarrow (n+1) \in X$ dla wszystkich liczb naturalnych n (zarówno ta implikacja jak i jej dowód są nazywane *krokiem indukcyjnym*). Warunek $n \in X$ w kroku indukcyjnym nazywamy *założeniem indukcyjnym* a warunek $(n+1) \in X$ *tezą indukcyjną*. Czasem tezą indukcyjną nazywa się także dowodzone twierdzenie, czyli warunek $\forall n{\in}\mathbb{N}\ n \in X$.

W literaturze spotyka się wiele różnych wersji zasady indukcji. Chyba najczęściej spotykaną jest wersja następująca.

Twierdzenie 5. Niech W będzie własnością liczb naturalnych spełniającą następujące dwa warunki.

- $W(0)$ jest prawdą, oraz
- dla wszystkich liczb naturalnych n, jeśli $W(n)$ jest prawdą to także $W(n+1)$ jest prawdą.

Wtedy wszystkie liczby naturalne mają własność W.

W tym miejscu należałoby się zastanowić, czym właściwie jest „własność". Najwygodniej myśleć o niej jako o funkcji $W : \mathbb{N} \to \{\mathit{prawda}, \mathit{fałsz}\}$. Jeśli np. $W(n)$ zdefiniujemy jako „$2^n \leq n!$", to $W(4) = \mathit{prawda}$ (bo $2^4 = 16 \leq 24 = 4!$), natomiast $W(2) = \mathit{fałsz}$ (bo $2^2 = 4 \not\leq 2 = 2!$), czyli liczba 4 ma własność W a liczba 2 jej nie ma.

Twierdzenia 3 i 5 są w istocie rzeczy tym samym twierdzeniem (zasadą indukcji), różnią się tylko sformułowaniem. Formalnie oba twierdzenia wynikają z siebie nawzajem. Żeby uzasadnić, że twierdzenie 5 wynika z twierdzenia 3 wystarczy użyć zbioru $\{n \in \mathbb{N} \mid W(n)\}$ i zauważyć jego induktywność. Żeby zobaczyć, że twierdzenie 3 wynika z twierdzenia 5 wystarczy zdefiniować własność $W(n)$ jako „$n \in X$".

Czasem chcemy wykazać prawdziwość pewnej własności dla wszystkich liczb naturalnych większych od zadanej liczby początkowej. Można w tym celu skorzystać z następującej wersji zasady indukcji.

Twierdzenie 6 (zasada indukcji, wersja 3). Niech $a \in \mathbb{N}$ i niech W będzie własnością liczb naturalnych spełniającą następujące dwa warunki.

- $W(a)$ jest prawdą, oraz
- dla wszystkich liczb naturalnych $n \geq a$, jeśli $W(n)$ jest prawdą to $W(n+1)$ też jest prawdą.

Wtedy dla wszystkich liczb naturalnych $n \geq a$ zachodzi $W(n)$.

Prawdziwość tej wersji zasady indukcji można uzasadnić korzystając z twierdzenia 3 i zauważając, że zbiór

$$\{n \in \mathbb{N} \mid \text{jeśli } n \geq a \text{ to } W(n)\}$$

jest induktywny.

Przykład 7. Pokażemy indukcyjnie, że $2^n \leq n!$ dla każdego $n \geq 4$. Skorzystamy z twierdzenia 6 dla własności $W(n)$ zdefiniowanej jako $2^n \leq n!$ oraz dla $a = 4$.

W tym przypadku podstawa indukcji to warunek $W(4)$. Warunek ten jest prawdziwy, bo $2^4 = 16$, $4! = 24$ oraz $16 < 24$.

Dla uzasadnienia kroku indukcyjnego weźmy dowolne $n \geq 4$ i załóżmy, że $2^n < n!$. Pokażemy, że $2^{n+1} < (n+1)!$. Wiemy, że $2^{n+1} = 2 \cdot 2^n$, zatem z założenia indukcyjnego wynika, że $2^{n+1} < 2 \cdot n!$. Ponieważ $n \geq 4$, więc $2 < (n+1)$ a zatem $2^{n+1} < (n+1) \cdot n!$. Czyli $2^{n+1} < (n+1)!$, co należało pokazać.

Z zasady indukcji wnioskujemy, że $2^n \leq n!$ dla wszystkich liczb naturalnych $n \geq 4$. ■

Często w dowodach indukcyjnych zamiast założenia indukcyjnego, że liczba n ma własność W potrzebujemy silniejszego założenia, że wszystkie liczby naturalne od a do n mają własność W. Używając bardziej zwięzłej notacji matematycznej, odpowiednią zasadę indukcji możemy zapisać następująco.

Twierdzenie 8 (zasada indukcji, wersja 4). Niech $a \in \mathbb{N}$ i niech X będzie takim podzbiorem zbioru liczb naturalnych $\mathbb{N}$, że

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

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

Wtedy dla wszystkich $n \geq a$ zachodzi $n \in X$.

Prawdziwość takiej zasady indukcji dowodzi się wykazując że zbiór

$$\{n \in \mathbb{N} \mid \text{jeśli } n \geq a \text{ to } \forall a \leq i \leq n \; i \in X\}$$

jest induktywny.

W szczególnym przypadku, gdy $a = 0$, powyższe warunki się upraszczają i całe twierdzenie można zapisać w następującej postaci. Zakładamy tutaj, że zmienne i, n przebiegają zbiór liczb naturalnych (w szczególności nie mogą być ujemne).

Twierdzenie 9 (zasada indukcji, wersja 5). Jeśli $X \subseteq \mathbb{N}$ spełnia warunek

$$\forall n\big((\forall i\!<\!n\ i\!\in\!X) \Rightarrow n\!\in\!X\big)$$

to $X = \mathbb{N}$.

W tej wersji podstawa indukcji jest szczególnym przypadkiem kroku indukcyjnego: dla $n = 0$ wszystkie liczby mniejsze od n (a jest tych liczb dokładnie zero) są już w zbiorze X, więc warunek z treści twierdzenia wymusza $0 \in X$.

Przykład 10. Rozważmy układankę puzzle złożoną z n kawałków obrazka. Ułożenie obrazka zaczyna się od połączenia ze sobą dwóch pasujących do siebie kawałków, a w kolejnych ruchach łączy się ze sobą dwa pasujące do siebie fragmenty obrazka (złożone z jednego lub więcej kawałków). Pokażemy indukcyjnie, że dla każdego obrazka złożonego z n kawałków każde jego ułożenie wymaga wykonania dokładnie $n - 1$ ruchów. Skorzystamy w tym celu z twierdzenia 8 dla $a = 1$.

Niech X będzie zbiorem takich liczb naturalnych $n \geq 1$, że dla każdego obrazka złożonego z n kawałków każde jego ułożenie wymaga wykonania dokładnie $n - 1$ ruchów.

Podstawa indukcji: Oczywiście liczba 1 należy do zbioru X, bo ułożenie dowolnego obrazka złożonego z 1 kawałka wymaga dokładnie 0 ruchów.

Krok indukcyjny: Weźmy teraz dowolną liczbę naturalną $n \geq 1$ i załóżmy, że dla wszystkich takich liczb naturalnych i, że $i \geq 1$ i $i \leq n$ zachodzi $i \in X$. Pokażemy, że $n + 1 \in X$. W tym celu weźmy dowolny obrazek złożony z $n + 1$ kawałków i rozważmy dowolny sposób jego ułożenia, nazwijmy ten sposób s. W ostatnim ruchu ułożenia s połączono ze sobą dwa fragmenty obrazka. Niech i będzie liczbą kawałków pierwszego fragmentu. Wtedy drugi fragment składa się z $(n + 1) - i$ kawałków. Obie liczby i oraz $(n + 1) - i$ są nie mniejsze niż 1 i nie większe niż n, zatem z założenia indukcyjnego obie należą do zbioru X. Oba fragmenty naszego obrazka są obrazkami złożonymi odpowiednio z i oraz $(n+1)-i$ kawałków, zatem każde ich ułożenie wymagało odpowiednio dokładnie $i - 1$ oraz $(n + 1) - i - 1$ ruchów. Ułożenie s składało się zatem z $(i - 1) + (n + 1) - i - 1 + 1 = n$ ruchów: ułożenia pierwszego i drugiego fragmentu oraz połączenia tych fragmentów. Z dowolności wyboru obrazka i sposobu jego ułożenia wnioskujemy, że ułożenie dowolnego obrazka złożonego z $n + 1$ kawałków wymaga dokładnie n ruchów. Zatem $n + 1 \in X$.

Na mocy zasady indukcji wnioskujemy, że dla każdej liczby naturalnej $n \geq 1$ ułożenie dowolnego obrazka puzzle złożonego z n kawałków wymaga wykonania dokładnie $n - 1$ ruchów. ■

Zadanie 12. Udowodnij, że dla wszystkich liczb naturalnych $n \geq 1$ liczba 6^n w zapisie dziesiętnym kończy się cyfrą 6.

Zadanie 13. Udowodnij indukcyjnie, że suma pierwszych n liczb nieparzystych wynosi n^2.

Zadanie 14. Firma kateringowa pakuje kanapki wyłącznie w pudełka po 3 lub 5 sztuk. Udowodnij indukcyjnie, że każdą liczącą co najmniej 8 sztuk liczbę kanapek da się zapakować w takie pudełka tak, aby wszystkie pudełka były pełne.

Definicja 11. *Liczby Fibonacciego* $F_0, F_1, F_2, \ldots$ definiuje się równaniami

- $F_0 = 0$, $F_1 = 1$,
- $F_n = F_{n-2} + F_{n-1}$ dla $n \geq 2$.

Zadanie 15. Udowodnij indukcyjnie, że dla każdego $n \in \mathbb{N}$ zachodzi $F_n \leq F_{n+1}$,

Zadanie 16. Udowodnij, że jeśli $n > 3$, to $F_{n+1} < 2F_n$.

Zadanie 17. Udowodnij, że dla wszystkich $n \geq 1, n \in \mathbb{N}$ zachodzi równość

$$F_{n+1} = 1 + \sum_{i=0}^{n-1} F_i .$$

Zadanie 18. Udowodnij, że dla wszystkich $n \geq 1, n \in \mathbb{N}$ zachodzi równość

$$F_n^2 = (-1)^{n+1} + F_{n-1}F_{n+1}.$$

Zadanie 19. Udowodnij, że dla wszystkich $n \in \mathbb{N}$ zachodzi równość

$$F_{2n+1} = F_n^2 + F_{n+1}^2.$$

Zadanie 20. Udowodnij, że dla wszystkich $n \geq 3, n \in \mathbb{N}$ liczby F_n i F_{n+1} są względnie pierwsze (tzn. nie mają wspólnych dzielników pierwszych).

Zadanie 21. 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 większą od* 1 *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.

Zadanie 22. 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 23. Udowodnij, że jeśli wyrazy ciągu spełniają warunki $a_0 = 2$, $a_1 = 3$ i $a_{n+1} = 3a_n - 2a_{n-1}$ dla $n \geq 1$, to $a_n = 2^n + 1$.

Zadanie 24. Znajdź błąd w następującym rozumowaniu. *Pokażę, że dla wszystkich liczb rzeczywistych r i wszystkich liczb naturalnych n zachodzi równość $r^n = 1$. Oczywiście dla $n = 0$ mamy $r^n = 1$. Niech n będzie dowolną liczbą naturalną i załóżmy, że dla wszystkich $k \leq n$ zachodzi równość $r^k = 1$. Wtedy $r^{n+1} = r^{n+n-(n-1)} = \frac{r^n \cdot r^n}{r^{n-1}}$. Ponieważ liczby n oraz $n-1$ są nie większe niż n, więc z założenia indukcyjnego mamy $r^n = r^{n-1} = 1$. Zatem $r^{n+1} = \frac{1 \cdot 1}{1} = 1$, co kończy dowód.*

Zadanie 25. 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 26. Niech $X \subseteq \mathbb{N}$ będzie takim zbiorem, że spełniona jest koniunkcja warunków

1. $0, 1 \in X$
2. $\forall n\ (n \in X \Rightarrow 2n \in X)$
3. $\forall n\ (n + 1 \in X \Rightarrow n \in X)$

Udowodnij, że $X = \mathbb{N}$.

Zadanie 27. Wykaż indukcyjnie, że $2^n \geq n^2$ dla każdego $n \geq 5$.

Zadanie 28. 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 29. Rozważmy grę, w której ruchy wykonują na zmianę gracze A i 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 30. Wykaż, że n prostych przecina się na płaszczyźnie w co najwyżej $\frac{n(n-1)}{2}$ punktach.

Zadanie 31. Wykaż indukcyjnie, że dla wszystkich liczb rzeczywistych $x > -1$ oraz wszystkich liczb naturalnych n zachodzi nierówność $(1 + x)^n \geq 1 + nx$.

Zadanie 32. Na stole znajdują się trzy szklanki, każda wypełniona dokładnie w połowie. W pierwszej z nich znajduje się martini, w dwóch pozostałych woda sodowa. Nie mamy żadnej miarki do odmierzania płynów; jedyną operacją, jaką możemy wykonać, jest przelanie zawartości z jednej szklanki do drugiej aż do wypełnienia tej drugiej (lub opróżnienia pierwszej) szklanki. Zakładamy przy tym, że podczas przelewania nic się nie rozlewa oraz że po przelaniu płyn zostaje dokładnie wymieszany. Czy można w skończonej liczbie kroków dokładnie wymieszać martini z wodą sodową tak, aby otrzymać roztwór, którego 1/3 objętości stanowi martini?

Zadanie 33. Iloczyn liczb x_1, x_2 i x_3 można obliczyć mnożąc najpierw x_1 przez x_2 a potem mnożąc wynik przez x_3, ale można też najpierw wymnożyć x_1 przez x_3 i potem wynik wymnożyć przez x_2. Udowodnij, że dla każdej liczby naturalnej $n \geq 1$ obliczenie iloczynu n liczb wymaga zawsze, bez względu na kolejność tych liczb i rozstawienie nawiasów, wykonania $n - 1$ mnożeń.

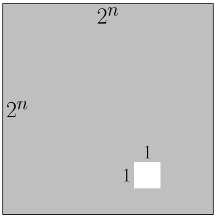
Zadanie 34. Wiadomo, że Chiny powstały około roku 1700 p.n.e. Przyjmijmy dla uproszczenia, że w roku 1700 p.n.e. o każdym żyjącym wtedy człowieku na ziemi można było jednoznacznie powiedzieć, czy jest Chińczykiem. Osoby, które były wtedy Chińczykami nazwiemy 1-Chińczykami, wszystkie pozostałe żyjące wtedy osoby osoby nazwiemy 0-Chińczykami. Osobę, której ojciec jest c_1-Chińczykiem a matka c_2-Chińczykiem, nazwiemy $\frac{c_1+c_2}{2}$-Chińczykiem. Udowodnij, że nikt z żyjących obecnie na świecie ludzi nie jest $\frac{1}{3}$-Chińczykiem.

Wskazówka: udowodnij indukcyjnie, że każda żyjąca po roku 1700 p.n.e. osoba jest $\frac{k}{2^l}$-Chińczykiem dla pewnych liczb naturalnych k i l.

W kolejnych zadaniach *triomino* () to kwadrat o boku 2, z którego usunięto jeden narożnik o wymiarach 1×1.

Zadanie 35. Udowodnij, że dla wszystkich liczb naturalnych $n \geq 1$ prostokąt o wymiarach $2 \times 3n$ można pokryć triominami.

Zadanie 36. Rozważmy kwadrat o boku 2^n, gdzie $n \geq 1$, z usuniętym dowolnym kwadratem o boku 1, tak jak na rysunku:



Udowodnij, że każdy taki kwadrat można pokryć triominami.

2

Rachunek zdań

2.1. Składnia rachunku zdań

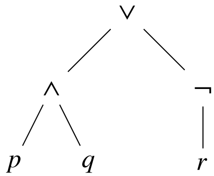
Definicja 12. *Formuły rachunku zdań* nad zbiorem zmiennych zdaniowych V budujemy ze *zmiennych zdaniowych* z V i *spójników logicznych*: fałszu $\bot$, prawdy $\top$, negacji $\neg$, koniunkcji $\wedge$, alternatywy $\vee$, implikacji $\Rightarrow$ i równoważności $\Leftrightarrow$ w następujący sposób:

1. Symbole $\bot$ i $\top$ są formułami rachunku zdań.
2. Każda zmienna zdaniowa ze zbioru V 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.

Innymi słowy, zbiór formuł rachunku zdań jest to najmniejszy zbiór zawierający stałe $\bot$ i $\top$, zmienne zdaniowe, i zamknięty na spójniki $\neg$, $\wedge$, $\vee$, $\Rightarrow$ i $\Leftrightarrow$. Zbiór wszystkich formuł nad zbiorem zmiennych zdaniowych V będziemy oznaczać przez $\mathcal{F}(V)$. 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.

Będziemy używać składni w dwóch wersjach: *konkretnej* i *abstrakcyjnej*. W składni konkretnej formuła jest ciągiem znaków (napisem), natomiast w składni abstrakcyjnej drzewem (algebraicznym typem danych) ze spójnikami logicznymi w węzłach wewnętrznych oraz stałymi i zmiennymi w liściach (por. rysunek 1). Proces tłumaczenia składni konkretnej na abstrakcyjną nazywa się *parsowaniem*; odwrotny proces tłumaczenia składni abstrakcyjnej na konkretną to *wypisywanie* formuły (ang. *pretty printing*). Mówiąc „formuła” zwykle mamy na myśli składnię abstrakcyjną, dlatego np. przyjmujemy, że w formułach nie występują nawiasy.

Składnia abstrakcyjna w jednoznaczny sposób podaje kolejność użytych spójników logicznych, jednak niewygodnie się jej używa do zapisywania formuł na tablicy



Rysunek 1. Formuła $p \wedge q \vee \neg r$ w składni abstrakcyjnej

$\bot$
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 2. Znaczenie spójników logicznych

czy papierze. Zapisując formuły w składni konkretnej spłaszczamy ich drzewiastą strukturę, i żeby tej struktury całkowicie nie stracić, używamy nawiasów. Dla większej czytelności będziemy niektóre nawiasy opuszczać, 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 $(p \vee q) \vee (r \wedge s)$.

2.2. Wartości logiczne i znaczenie formuł zdaniowych

Definicja 13. Zbiór *wartości logicznych* $\mathcal{B} = \{\mathsf{T}, \mathsf{F}\}$ zawiera dwa elementy: T (prawda) i F (fałsz).[1] Niech V oznacza zbiór zmiennych zdaniowych. *Wartościowanie zmiennych*, to odwzorowanie $\sigma : V \to \mathcal{B}$. Nadaje ono wartości logiczne zmiennym zdaniowym.

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

Wartość logiczna dowolnej formuły zdaniowej zależy jedynie od wartościowania występujących w niej zmiennych i można ją wyznaczyć korzystając z tabelek z rysunku 2. Dlatego mówimy, że wartościowanie zmiennych nadaje wartość logiczną formułom. Formalnie, wartościowanie zmiennych σ wyznacza *wartościowanie formuł* $\hat{\sigma}$, które przypisuje wartości logiczne dowolnym formułom w następujący sposób:

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

Wartość logiczną $\hat{\sigma}(\phi) \in \mathcal{B}$ nazywamy *wartością logiczną formuły ϕ przy wartościowaniu σ*. Ponieważ dla danego wartościowania zmiennych wartościowanie formuł jest określone jednoznacznie, znak ˆ będziemy opuszczać i zarówno wartościowanie zmiennych, jak i wartościowanie formuł będziemy oznaczać tym samym symbolem i nazywać po prostu *wartościowaniem*.

Definicja 14. Formuła jest:

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

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

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

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 3. Tabelkowa metoda sprawdzenia, że formuła ϕ jest tautologią

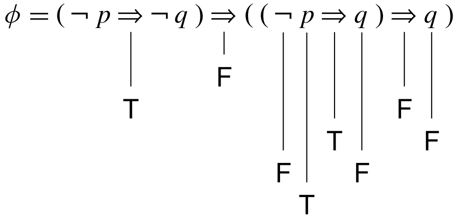
Obecnie zajmiemy się sposobami sprawdzania, czy dana formuła jest tautologią.

2.2.1. Metoda zero-jedynkowa

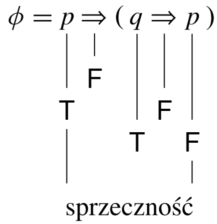
Przykładami tautologii są formuły $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ oraz $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ zwane *prawami De Morgana*. Aby się o tym przekonać rysujemy tabelkę (rysunek 3) umieszczając w kolumnach 1 i 2 wartości zmiennych zdaniowych p i q. W kolumnie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

2.2.2. 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 przy pewnym wartościowaniu, jej następnik $(\neg p \Rightarrow q) \Rightarrow q$ zaś fałszywy przy tym wartościowaniu. Formuła $(\neg p \Rightarrow q) \Rightarrow q$ jest fałszywa tylko wówczas, gdy $\neg p \Rightarrow q$ jest spełniona oraz $\sigma(q) = \mathsf{F}$. 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



Rysunek 4. Wartościowanie, dla którego formuła ϕ nie jest spełniona



Rysunek 5. Ilustracja dowodu nie wprost, iż formuła ϕ jest tautologią

$\sigma(p) = \mathsf{T}$ i $\sigma(q) = \mathsf{F}$ nasza wyjściowa formuła istotnie nie jest spełniona, nie jest więc tautologią (rysunek 4).

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 $q \Rightarrow p$. Ostatnia formuła nie jest spełniona tylko wówczas, gdy $\sigma(q) = \mathsf{T}$ oraz $\sigma(p) = \mathsf{F}$. Zatem aby ϕ nie była spełniona, musiałoby być jednocześnie $\sigma(p) = \mathsf{T}$ i $\sigma(p) = \mathsf{F}$, co jest niemożliwe. Formuła ϕ jest zatem tautologią (rysunek 5).

Zadanie 37. Udowodnij, że podane formuły są tautologiami.

1. **(modus ponens)** $(p \Rightarrow q) \wedge p \Rightarrow q$
2. **(modus tollens)** $(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$
3. **(prawo kompozycji)** $(p \vee q \Rightarrow r) \Rightarrow p \Rightarrow r$
4. **(prawo kompozycji)** $(p \vee q \Rightarrow r) \Rightarrow q \Rightarrow r$
5. **(prawo symplifikacji)** $p \wedge q \Rightarrow p$
6. **(prawo symplifikacji)** $q \Rightarrow p \vee q$
7. **(prawo symplifikacji)** $p \Rightarrow q \Rightarrow p$
8. **(prawo Dunsa Szkota)** $\neg p \Rightarrow p \Rightarrow q$
9. **(prawo dylematu konstrukcyjnego)** $(p \Rightarrow r) \wedge (q \Rightarrow r) \wedge (p \vee q) \Rightarrow r$

10. **(prawo eksportacji)** $(p \wedge q \Rightarrow r) \Rightarrow p \Rightarrow q \Rightarrow r$
11. **(prawo importacji)** $(p \Rightarrow q \Rightarrow r) \Rightarrow p \wedge q \Rightarrow r$
12. **(prawo redukcji do absurdu)** $(p \Rightarrow \neg p) \Rightarrow \neg p$
13. **(prawo sprzeczności)** $\neg(p \wedge \neg p)$
14. **(prawo wyłączonego środka)** $p \vee \neg p$
15. **(prawo sylogizmu hipotetycznego)** $(p \Rightarrow q) \Rightarrow (q \Rightarrow r) \Rightarrow p \Rightarrow r$
16. **(prawo Peirce'a)** $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$
17. **(Prawo Claviusa)** $(\neg p \Rightarrow p) \Rightarrow p$
18. **(prawo tożsamości)** $p \Leftrightarrow p$

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

Zadanie 38. Sprawdź, które z podanych formuł są (a) tautologiami, (b) formułami spełnialnymi, (c) formułami sprzecznymi.

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

18. $(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow p \vee q$
19. $(p \vee q \Rightarrow p \vee \neg q) \Rightarrow \neg p \vee q$
20. $(p \wedge q) \vee (p \Rightarrow q) \Rightarrow p \Rightarrow q$
21. $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
22. $(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow p \vee r \Rightarrow q \vee s$
23. $(p \wedge q \Rightarrow r) \Rightarrow (p \Rightarrow r) \wedge (q \Rightarrow r)$
24. $(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow p \wedge r \Rightarrow q \wedge s$
25. $(p \wedge q \Rightarrow r) \wedge (p \vee q \Rightarrow \neg r) \Rightarrow p \wedge q \wedge r$
26. $\neg(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow p \wedge \neg q$
27. $((p \Rightarrow q) \Rightarrow q \Rightarrow r) \Rightarrow (r \Rightarrow p) \Rightarrow q \Rightarrow p$
28. $(p \Rightarrow q) \vee (p \Rightarrow r) \vee (p \Rightarrow s) \Rightarrow p \Rightarrow q \vee r \vee s$
29. $(p \Rightarrow q) \wedge (r \Rightarrow q) \wedge (s \Rightarrow q) \Rightarrow p \wedge r \wedge s \Rightarrow q$
30. $(p \Rightarrow q) \wedge (r \Rightarrow q) \wedge (s \Rightarrow q) \Rightarrow p \wedge r \wedge \neg s \Rightarrow q$
31. $(p \wedge q \Rightarrow r) \wedge (p \wedge q \Rightarrow \neg r) \Rightarrow \neg p \wedge \neg q \wedge \neg r$
32. $(\neg p \wedge q) \vee (p \vee \neg q) \Rightarrow (p \Rightarrow q \vee r) \Rightarrow p \Rightarrow r$
33. $(p \vee q) \wedge (r \vee s) \Rightarrow ((p \Rightarrow q) \vee (p \Rightarrow r)) \wedge ((q \Rightarrow s) \vee (q \Rightarrow p))$
34. $(p \Rightarrow q) \wedge (r \Rightarrow s) \wedge (t \Rightarrow u) \Rightarrow p \wedge r \wedge t \Rightarrow q \wedge s \wedge u$
35. $(p \Leftrightarrow q) \wedge p \Rightarrow q$
36. $(\neg p \Rightarrow \neg q) \Rightarrow (\neg p \Rightarrow q) \Rightarrow p$

Użycie metody zero-jedynkowej wymaga znajomości wszystkich zmiennych zdaniowych występujących w formule. W poniższych przykładach mówimy o dowolnych formułach, nie wiemy więc jakie zmienne w nich występują i nie możemy użyć metody zero-jedynkowej.

Przykład 15. Pokażemy, że dla dowolnych formuł zdaniowych ϕ i ψ, jeśli ϕ i ψ są tautologiami to $\phi \wedge \psi$ jest tautologią.

Weźmy dowolne formuły ϕ i ψ i załóżmy, że są one tautologiami. Weźmy dowolne wartościowanie σ. Ponieważ ϕ i ψ są tautologiami, mamy $\hat{\sigma}(\phi) = \mathsf{T}$ oraz $\hat{\sigma}(\psi) = \mathsf{T}$, a stąd $\hat{\sigma}(\phi \wedge \psi) = \mathsf{T}$. Zatem $\phi \wedge \psi$ jest spełniona przy każdym wartościowaniu, czyli jest tautologią.

Pokazaliśmy, że tautologie są zamknięte na koniunkcje (tzn., że koniunkcja dwóch tautologii jest tautologią). Następny przykład pokazuje, że formuły spełnialne nie mają tej własności.

Przykład 16. Istnieją takie spełnialne formuły zdaniowe ϕ i ψ, że $\phi \wedge \psi$ nie jest spełnialna.

Tutaj wystarczy po prostu wskazać takie dwie formuły. Niech $\phi = p$ i niech $\psi = \neg p$. Rozważmy takie wartościowania σ_1 i σ_2, że $\sigma_1(p) = \mathsf{T}$ i $\sigma_2(p) = \mathsf{F}$. Wtedy $\hat{\sigma}_1(\phi) = \mathsf{T}$, zatem ϕ jest spełnialna. Podobnie $\hat{\sigma}_2(\psi) = \mathsf{T}$, zatem ψ jest spełnialna. Natomiast $\phi \wedge \psi = p \wedge \neg p$ nie jest spełnialna.

Zauważmy, że przykład 15 ma uniwersalny charakter (mówimy w nim o wszystkich formułach i wszystkich wartościowaniach), natomiast przykład 16 ma charakter egzystencjalny (mówimy w nim o istnieniu formuł i istnieniu wartościowań). W kolejnym przykładzie sytuacja jest odrobinę bardziej skomplikowana.

Przykład 17. Pokażemy, że dla dowolnych formuł zdaniowych ϕ i ψ, jeśli $\phi \Rightarrow \psi$ jest spełnialna, to $\phi \wedge \neg\psi$ nie jest tautologią.

Weźmy dowolne formuły ϕ i ψ i załóżmy, że $\phi \Rightarrow \psi$ jest spełnialna. Weźmy takie wartościowanie σ, że $\hat{\sigma}(\phi \Rightarrow \psi) = \mathsf{T}$ i rozważmy dwa przypadki. Jeśli $\hat{\sigma}(\phi) = \mathsf{F}$ to oczywiście $\hat{\sigma}(\phi \wedge \neg\psi) = \mathsf{F}$. Jeśli natomiast $\hat{\sigma}(\phi) = \mathsf{T}$ to z faktu, że $\hat{\sigma}(\phi \Rightarrow \psi) = \mathsf{T}$ wnioskujemy, że $\hat{\sigma}(\psi) = \mathsf{T}$, a stąd $\hat{\sigma}(\neg\psi) = \mathsf{F}$ i $\hat{\sigma}(\phi \wedge \neg\psi) = \mathsf{F}$. W obu przypadkach $\hat{\sigma}(\phi \wedge \neg\psi) = \mathsf{F}$, co oznacza, że $\phi \wedge \neg\psi$ nie jest tautologią.

Zadanie 39. Niech symbole ϕ i ψ oznaczają formuły zdaniowe. Udowodnij poniższe stwierdzenia lub podaj przykłady świadczące o ich fałszywości:

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

Zadanie 40. Które z poniższych zdań są prawdziwe dla dowolnych formuł zdaniowych φ i ψ?

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

Podaj dowody ich prawdziwości. W pozostałych przypadkach wskaż kontrprzykłady.

2.2.3. Równoważność formuł

Definicja 18. Mówimy, że formuły ϕ i ψ są *równoważne*, jeśli dla każdego wartościowania przyjmują tę samą wartość logiczną (tj. gdy formuła $\phi \Leftrightarrow \psi$ jest tautologią).

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

Przykład 19. Formuły $\neg(p \vee q)$ i $\neg p \wedge \neg q$ są równoważne.

Zadanie 41. Udowodnij, że a) dowolne dwie tautologie, b) dowolne dwie formuły sprzeczne są równoważne. Czy dowolne dwie formuły spełnialne są równoważne?

Zadanie 42. Udowodnij, że podane formuły są równoważne.

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

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

Zadanie 43. Sprawdź, czy podane formuły są równoważne.

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

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

Zadanie 44. Sprawdź, czy podane formuły są równoważne.

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

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

Zadanie 45. Sprawdź, czy podane formuły są równoważne.

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

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

Zadanie 46. Sprawdź, czy podane formuły są równoważne.

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

Zadanie 47. Sprawdź, czy podane formuły są równoważne.

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

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

Zadanie 48. Spójnik logiczny $\oplus$ jest *prawostronnie rozdzielny* względem spójnika $\otimes$, jeżeli formuły $(p \otimes q) \oplus r$ i $(p \oplus r) \otimes (q \oplus r)$ są równoważne. Które spośród spójników logicznych $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$ są prawostronnie rozdzielne względem których?

2.2.4. Lemat o podstawianiu

Definicja 20. *Podstawieniem* formuły ψ w miejsce zmiennej zdaniowej p nazywamy przekształcenie, które formule ϕ przyporządkowuje formułę powstałą przez wstawienie formuły ψ w miejsce każdego wystąpienia zmiennej p w formule ϕ. Formalnie:

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

Przykład 21. $(p \Rightarrow p \vee q)[p/q \Rightarrow p] = (q \Rightarrow p) \Rightarrow (q \Rightarrow p) \vee q.$

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

Lemat 22 (o podstawianiu). Niech ϕ i ψ będą formułami, niech p będzie zmienną zdaniową i niech σ będzie wartościowaniem. Niech σ' będzie wartościowaniem zdefiniowanym wzorem

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

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

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

Wniosek ten pozwala dowodzić, że skomplikowane formuły są tautologiami. Dla przykładu formuła $(q \Rightarrow p) \Rightarrow (q \Rightarrow p) \vee q$ z przykładu 21 jest tautologią, gdyż jest wynikiem podstawienia formuły $q \Rightarrow p$ w miejsce zmiennej p w tautologii $p \Rightarrow p \vee q$.

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

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

W zadaniach 49–52 zbadaj, czy podane formuły są tautologiami.

Zadanie 49. $(s \wedge u \wedge t \wedge (p \vee q \vee r)) \Rightarrow (x \Rightarrow y \wedge \neg z) \Leftrightarrow$
$((p \vee q \vee r) \Rightarrow (s \wedge u \wedge t) \Rightarrow (x \Rightarrow y \wedge \neg z))$

Zadanie 50. $((p \Rightarrow q \wedge (r \vee s \Leftrightarrow \neg p)) \wedge \neg((p \Rightarrow q \wedge (r \vee s \Leftrightarrow \neg p))))$

Zadanie 51. $(p \wedge \neg q) \wedge ((r \Rightarrow s) \vee (p \Rightarrow q \Rightarrow r \vee \neg s)) \Rightarrow \neg(q \vee \neg p)$

Zadanie 52. $((p \Rightarrow q \vee r) \vee s \vee t) \wedge \neg(p \Rightarrow q \vee r) \Rightarrow s \vee t$

Zadanie 53. Wskaż podstawienie $[p/\phi_1, q/\phi_2, r/\phi_3]$, dla którego formuła

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

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

2.3. Formalizacja rozumowań w języku rachunku zdań

Zadanie 54. Sformalizuj zadanie 2, tj. pokaż, jak znaleźć odpowiedzi na postawione w nim pytania korzystając z rachunku zdań.

Zadanie 55. 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 56. 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 57. Zbadaj zasadność poniższych rozumowań:

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

Zadanie 58. Rozważmy następujący fragment kodu

$$
\begin{array}{l}
\textbf{while}\ \ ((i < n) \land \neg \mathit{found}) \lor \neg \mathit{interrupted}\ \ \textbf{do} \\
\quad A \\
\quad \textbf{if}\ \mathit{found} \\
\qquad \textbf{then} \\
\qquad\quad B \\
\qquad\quad \textbf{if}\ \ \mathit{interrupted} \\
\qquad\qquad \textbf{then}\ C \\
\qquad\qquad \textbf{else}\ D \\
\qquad \textbf{else}\ E \\
\quad F \\
G
\end{array}
$$

Mamy w nim siedem interesujących nas miejsc (od A do G), przy czym sam kod w tych miejscach nie jest dla nas interesujący i został pominięty. Zakładamy tylko, że zmienne i, n, *found* i *interrupted* mogą być zmieniane wyłącznie w miejscu F. Dla każdego z tych miejsc podaj

- warunek na dojście sterowania programu do tego miejsca, oraz
- przykład początkowych wartości zmiennych, dla których sterowanie dochodzi do tego miejsca.

Warunek powinien być napisany w postaci formuły rachunku zdań nad zbiorem zmiennych $\{(i < n), \mathit{found}, \mathit{interrupted}\}$. Na przykład dla punktu A szukany warunek to $(i < n) \land \neg \mathit{found} \lor \neg \mathit{interrupted}$ a wartości początkowe to np. $i = 5$, $n = 7$, $\mathit{found} = \mathit{false}$, $\mathit{interrupted} = \mathit{false}$.

Czy można na tej podstawie wskazać oczywiste błędy w tym fragmencie kodu?

2.4. Własności formuł zdaniowych

Definicja 23. Intuicyjnie, napis $\bigwedge_{i=1}^{n} \phi_i$ oznacza $\phi_1 \wedge \cdots \wedge \phi_n$, zaś $\bigvee_{i=1}^{n} \phi_i$ oznacza $\phi_1 \vee \cdots \vee \phi_n$. Bardziej formalnie, napisy te są zdefiniowane indukcyjnie: $\bigwedge_{i=1}^{1} \phi_i = \phi_1$, $\bigwedge_{i=1}^{n+1} \phi_i = (\bigwedge_{i=1}^{n} \phi_i) \wedge \phi_{n+1}$ oraz $\bigvee_{i=1}^{1} \phi_i = \phi_1$, $\bigvee_{i=1}^{n+1} \phi_i = (\bigvee_{i=1}^{n} \phi_i) \vee \phi_{n+1}$.

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

Definicja 24. Niech V będzie zbiorem zmiennych zdaniowych. *V-literałem* nazywamy formułę postaci p lub $\neg p$, gdzie $p \in V$. Jeżeli zbiór zmiennych zdaniowych jest ustalony, to formułę takiej postaci nazywamy po prostu *literałem*. Niekiedy do zbioru literałów zaliczamy też stałe logiczne $\top$ i $\bot$.

Zadanie 59. Dane są formuły $\phi_1, \phi_2, \ldots, \psi_1, \psi_2, \ldots$. 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 60. Dane są formuły $\phi_1, \phi_2, \ldots, \psi$. 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 61. 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 62. Czy istnieje taki nieskończony ciąg formuł $\{\phi_i\}_{i=1}^{\infty}$ rachunku zdań, że wszystkie formuły $\phi_i \Rightarrow \phi_{i+1}$ są tautologiami rachunku zdań, zaś żadna z formuł $\phi_{i+1} \Rightarrow \phi_i$ nie jest tautologią?

Zadanie 63. 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 64. Udowodnij, że jeśli p jest zmienną zdaniową, a ϕ taką formułą rachunku zdań, że $p \Rightarrow \phi$ i $\neg\phi \Rightarrow p$ są tautologiami, to ϕ jest tautologią.

Zadanie 65. Niech $\phi_1, \ldots, \phi_n$ będą formułami zdaniowymi, w których nie występują zmienne zdaniowe $p_1, \ldots, p_{n+1}$. Udowodnij, że formuła

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

jest tautologią wtedy i tylko wtedy, gdy tautologią jest formuła

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

Zadanie 66. Udowodnij, że jeżeli formuła ϕ jest tautologią, to dla dowolnych formuł $\psi_1, \ldots, \psi_n$ formuła

$$\psi_1 \Rightarrow \ldots \Rightarrow \psi_n \Rightarrow \phi$$

jest tautologią.

Zadanie 67. Udowodnij, że jeżeli ϕ jest formułą sprzeczną, to dla dowolnych formuł $\psi_1, \ldots, \psi_n$ formuła

$$\phi \Rightarrow \psi_1 \Rightarrow \ldots \Rightarrow \psi_n$$

jest tautologią.

Zadanie 68. Dla jakich $n \geq 1$ formuła

$$(\ldots((p \Rightarrow p) \Rightarrow p) \Rightarrow \ldots) \Rightarrow p,$$

w której zmienna p występuje n razy jest tautologią?

Zadanie 69. Niech p^0 oznacza $\neg p$ oraz niech p^1 oznacza p. Dla jakich ciągów $(i_1, \ldots, i_n) \in \{0, 1\}^n$ formuła

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

jest tautologią?

Zadanie 70. Niech $p_1, \ldots, p_n$ będą wszystkimi zmiennymi zdaniowymi występującymi w formule ϕ. Udowodnij, że formuła ϕ jest spełnialna wtedy i tylko wtedy, gdy istnieje podstawienie $[p_1/\phi_1,...,p_n/\phi_n]$ takie, że formuła $\phi[p_1/\phi_1,...,p_n/\phi_n]$ jest tautologią. Udowodnij, że formuła ϕ nie jest tautologią wtedy i tylko wtedy, gdy istnieje podstawienie $[p_1/\phi_1,...,p_n/\phi_n]$ takie, że formuła $\phi[p_1/\phi_1,...,p_n/\phi_n]$ jest sprzeczna.

Zadanie 71. 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 72. 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 formuł rachunku zdań (Definicja 12) prowadzi w dość oczywisty sposób do następującej zasady indukcji.

Twierdzenie 25 (zasada indukcji strukturalnej dla rachunku zdań). Niech X będzie takim zbiorem, że

1. formuły $\perp$ i $\top$ należą do zbioru X,
2. każda zmienna zdaniowa ze zbioru V należy do zbioru X,
3. dla wszystkich formul ϕ, ϕ_1 i ϕ_2, jeżeli ϕ, ϕ_1 i ϕ_2 należą do zbioru X, to także $(\neg\phi)$, $(\phi_1 \wedge \phi_2)$, $(\phi_1 \vee \phi_2)$, $(\phi_1 \Rightarrow \phi_2)$ oraz $(\phi_1 \Leftrightarrow \phi_2)$ należą do zbioru X.

Wtedy X jest zawiera zbiór $\mathcal{F}(V)$.

W dalszej części będziemy się czasem posługiwać formułami rachunku zdań zbudowanymi w określony sposób, np. z użyciem tylko spójników $\neg$, $\wedge$ i $\vee$. Takie formuły często mają proste definicje indukcyjne, i co za tym idzie, własne zasady indukcji strukturalnej. W przykładzie poniżej, zbiór formuł zbudowanych ze zmiennych zdaniowych i spójników $\neg$, $\wedge$ i $\vee$ moglibyśmy zdefiniować jako zbiór tych formuł rachunku zdań, w których nie występują symbole $\perp$, $\top$, $\Rightarrow$, $\Leftrightarrow$. Jednak definicja tego zbioru jako najmniejszego zbioru zawierającego zmienne zdaniowe i zamkniętego na spójniki $\neg$, $\wedge$ i $\vee$ prowadzi do prostszej zasady indukcji: *Jeśli zbiór X spełnia warunki*

- *każda zmienna zdaniowa ze zbioru V należy do X, oraz*
- *dla wszystkich formuł ϕ, ϕ_1 i ϕ_2, jeżeli ϕ, ϕ_1 i ϕ_2 należą do zbioru X, to także $\neg\phi$, $\phi_1 \wedge \phi_2$ i $\phi_1 \vee \phi_2$, należą do zbioru X,*

to X zawiera wszystkie formuły zbudowane ze zmiennych zdaniowych z V i spójników $\neg$, $\wedge$ i $\vee$. Dowody oparte na takiej zasadzie indukcji są prostsze od dowodów opartych na twierdzeniu 25, bo trzeba w nich rozpatrzyć mniej przypadków (nie trzeba rozpatrywać symboli $\bot$, $\top$ w podstawie indukcji ani symboli $\Rightarrow$, $\Leftrightarrow$ w kroku indukcyjnym).

Przykład 26. Rozważmy odwzorowanie $\mathcal{T}$ przyporządkowujące formułom zbudowanym ze zmiennych zdaniowych oraz spójników $\vee, \wedge, \neg$ formuły zbudowane ze zmiennych, spójników $\Rightarrow$, $\bot$ w następujący sposób.

$$
\begin{aligned}
\mathcal{T}(p) &= p, \quad \text{dla wszystkich zmiennych } p \in V \\
\mathcal{T}(\phi_1 \vee \phi_2) &= (\mathcal{T}(\phi_1) \Rightarrow \bot) \Rightarrow \mathcal{T}(\phi_2) \\
\mathcal{T}(\phi_1 \wedge \phi_2) &= (\mathcal{T}(\phi_1) \Rightarrow (\mathcal{T}(\phi_2) \Rightarrow \bot)) \Rightarrow \bot \\
\mathcal{T}(\neg\phi) &= \mathcal{T}(\phi) \Rightarrow \bot
\end{aligned}
$$

Pokażemy, że dla wszystkich formuł ϕ zbudowanych ze zmiennych zdaniowych z V oraz spójników $\vee, \wedge, \neg$ formuły ϕ i $\mathcal{T}(\phi)$ są równoważne.

Dowód. Przeprowadzimy dowód indukcyjny względem struktury formuły ϕ. Niech $\mathcal{F}$ oznacza zbiór wszystkich formuł zbudowanych ze zmiennych zdaniowych z V oraz spójników $\vee, \wedge, \neg$ i niech

$$X = \{\phi \in \mathcal{F} \mid \phi \equiv \mathcal{T}(\phi)\}.$$

Musimy pokazać, że X zawiera zmienne zdaniowe (to jest podstawa indukcji) oraz że jest zamknięty na spójniki $\vee, \wedge, \neg$ (krok indukcyjny).

Podstawa indukcji: Weźmy dowolną zmienną zdaniową $p \in V$. Ponieważ $\mathcal{T}(p) = p$, formuły $\mathcal{T}(p)$ oraz p są równoważne, a stąd $p \in X$.

Krok indukcyjny: Weźmy dowolne formuły ϕ, ϕ_1 i ϕ_2 i załóżmy, że $\phi, \phi_1, \phi_2 \in X$ (to jest założenie indukcyjne). Pokażemy, że także $\phi_1 \vee \phi_2$, $\phi_1 \wedge \phi_2$ oraz $\neg\phi$ należą do zbioru X. Z założenia indukcyjnego wiemy, że $\phi \equiv \mathcal{T}(\phi)$, $\phi_1 \equiv \mathcal{T}(\phi_1)$ oraz $\phi_2 \equiv \mathcal{T}(\phi_2)$.

- $\mathcal{T}(\phi_1 \vee \phi_2) = (\mathcal{T}(\phi_1) \Rightarrow \bot) \Rightarrow \mathcal{T}(\phi_2)$, a zatem z założenia indukcyjnego jest to formuła równoważna $(\phi_1 \Rightarrow \bot) \Rightarrow \phi_2)$. Korzystając z równoważności $p \Rightarrow q \equiv \neg p \vee q$ otrzymujemy równoważną formułę $\neg(\neg\phi_1 \vee \bot) \vee \phi_2$, która uprasza się do $\phi_1 \vee \phi_2$. Zatem $\mathcal{T}(\phi_1 \vee \phi_2) \equiv \phi_1 \vee \phi_2$, co pokazuje że $\phi_1 \vee \phi_2 \in X$.

- Przypadek $\phi_1 \wedge \phi_2$ jest podobny:

$$\mathcal{T}(\phi_1 \wedge \phi_2) \quad = \quad (\mathcal{T}(\phi_1) \Rightarrow (\mathcal{T}(\phi_2) \Rightarrow \bot)) \Rightarrow \bot$$

$$
\begin{aligned}
&\equiv (\phi_1 \Rightarrow (\phi_2 \Rightarrow \bot)) \Rightarrow \bot \\
&\equiv \neg(\phi_1 \Rightarrow (\phi_2 \Rightarrow \bot)) \vee \bot \\
&\equiv \phi_1 \wedge \neg(\phi_2 \Rightarrow \bot) \\
&\equiv \phi_1 \wedge (\phi_2 \wedge \neg\bot) \\
&\equiv \phi_1 \wedge \phi_2.
\end{aligned}
$$

Zatem $\mathcal{T}(\phi_1 \wedge \phi_2) \equiv \phi_1 \wedge \phi_2$, co pokazuje, że $\phi_1 \wedge \phi_2 \in X$.

- $\mathcal{T}(\neg\phi_1) = \mathcal{T}(\phi) \Rightarrow \bot \equiv \phi \Rightarrow \bot \equiv \neg\phi \vee \bot \equiv \neg\phi$. Zatem $\neg\phi \in X$.

Na mocy zasady indukcji zbiór X zawiera wszystkie formuły z $\mathcal{F}$, a to oznacza, że dla wszystkich formuł ϕ zbudowanych ze zmiennych zdaniowych oraz spójników $\vee, \wedge, \neg$ formuły ϕ i $\mathcal{T}(\phi)$ są równoważne. ■

Dowody indukcyjne w literaturze zwykle nie definiują explicite ani zasady indukcji, z której korzystają, ani zbioru X. W przyszłości (na wyższych latach studiów) też będziemy te definicje pomijać, musimy jednak umieć je rozpoznać i sformułować. Poniżej przykład takiego dowodu.

Przykład 27. Rozważmy formuły zbudowane ze zmiennej p i spójnika $\Leftrightarrow$. Pokażemy, że jeśli w takiej formule zmienna p występuje parzystą liczbę razy, to formuła ta jest tautologią.

Dowód. Rozważmy dwa wartościowania σ_{F} i σ_{T} zdefiniowane tak, że $\sigma_{\mathsf{F}}(p) = \mathsf{F}$ oraz $\sigma_{\mathsf{T}}(p) = \mathsf{T}$. Pokażemy przez indukcję, że dla każdej formuły ϕ zbudowanej ze zmiennej p i spójnika $\Leftrightarrow$ zachodzą następujące trzy warunki.

(a) $\hat{\sigma}_{\mathsf{T}}(\phi) = \mathsf{T}$,

(b) jeśli p występuje w ϕ parzystą liczbę razy, to $\hat{\sigma}_{\mathsf{F}}(\phi) = \mathsf{T}$, oraz

(c) jeśli p występuje w ϕ nieparzystą liczbę razy, to $\hat{\sigma}_{\mathsf{F}}(\phi) = \mathsf{F}$.

Oczywiście teza przykładu wynika bezpośrednio z punktów (a) i (b).

Podstawa indukcji: $\phi = p$. Wtedy zmienna p występuje w ϕ nieparzystą liczbę razy, $\hat{\sigma}_{\mathsf{F}}(\phi) = \mathsf{F}$, $\hat{\sigma}_{\mathsf{T}}(\phi) = \mathsf{T}$, a zatem wszystkie trzy warunki są spełnione.

Krok indukcyjny: $\phi = \phi_1 \Leftrightarrow \phi_2$, gdzie warunki (a), (b) i (c) są spełnione dla formuł ϕ_1 i ϕ_2. Pokażemy, że są one również spełnione dla formuły ϕ.

Warunek (a) dla ϕ jest spełniony, bo z założenia indukcyjnego $\hat{\sigma}_{\mathsf{T}}(\phi_1) = \mathsf{T}$ oraz $\hat{\sigma}_{\mathsf{T}}(\phi_2) = \mathsf{T}$, więc $\hat{\sigma}_{\mathsf{T}}(\phi_1 \Leftrightarrow \phi_2) = \mathsf{T}$.

Dla dowodu warunków (b) i (c) rozważmy dwa przypadki.

1. p występuje w ϕ parzystą liczbę razy. Mamy dwie możliwości

(i) p występuje w ϕ_1 parzystą liczbę razy. Wtedy p występuje w ϕ_2 parzystą liczbę razy; z założenia indukcyjnego $\hat{\sigma}_{\mathsf{F}}(\phi_1) = \mathsf{T}$ oraz $\hat{\sigma}_{\mathsf{F}}(\phi_2) = \mathsf{T}$, więc $\hat{\sigma}_{\mathsf{F}}(\phi_1 \Leftrightarrow \phi_2) = \mathsf{T}$.

(ii) p występuje w ϕ_1 nieparzystą liczbę razy. Wtedy p występuje w ϕ_2 nieparzystą liczbę razy; z założenia indukcyjnego mamy $\hat{\sigma}_{\mathsf{F}}(\phi_1) = \mathsf{F}$ oraz $\hat{\sigma}_{\mathsf{F}}(\phi_2) = \mathsf{F}$, więc $\hat{\sigma}_{\mathsf{F}}(\phi_1 \Leftrightarrow \phi_2) = \mathsf{T}$.

Zatem w obu przypadkach warunki (b) i (c) są spełnione.

2. p występuje w ϕ nieparzystą liczbę razy. Wtedy parzystość liczby wystąpień zmiennej p w ϕ_1 jest inna niż parzystość tych wystąpień w ϕ_2, czyli z założenia indukcyjnego $\hat{\sigma}_{\mathsf{F}}(\phi_1) \neq \hat{\sigma}_{\mathsf{F}}(\phi_2)$, a więc $\hat{\sigma}_{\mathsf{F}}(\phi_1 \Leftrightarrow \phi_2) = \mathsf{F}$.

Zatem we wszystkich możliwych przypadkach wszystkie trzy warunki są spełnione, co kończy dowód. ■

Aby sformułować zasadę indukcji użytą w tym dowodzie, musimy najpierw zdefiniować zbiór formuł zbudowanych ze zmiennej p i spójnika $\Leftrightarrow$: jest to najmniejszy zbiór zawierający p i zamknięty na spójnik $\Leftrightarrow$. Definicja ta daje następującą zasadę indukcji: *Jeśli zbiór X spełnia warunki*

- *zmienna p należy do X, oraz*
- *dla wszystkich formuł ϕ_1 i ϕ_2, jeżeli ϕ_1 i ϕ_2 należą do zbioru X, to także $\phi_1 \Leftrightarrow \phi_2$ należy do zbioru X,*

to X zawiera wszystkie formuły zbudowane ze zmiennej p i spójnika $\Leftrightarrow$. Ukryty w dowodzie zbiór X to zbiór wszystkich formuł ϕ spełniających warunki (a), (b) i (c).

Zadanie 73. Pokaż przez indukcję, że każda formuła ϕ zbudowana ze zmiennych p i q oraz spójnika $\Rightarrow$ jest równoważna dokładnie jednej z formuł z poniższego zbioru:

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

Wskazówka: W przypadku formuł zbudowanych ze zmiennych p i q oraz spójnika $\Rightarrow$ zasada indukcji strukturalnej upraszcza się do następującego twierdzenia: *Jeśli X jest takim zbiorem formuł, że*

- *zmienne p i q należą do X, oraz*
- *dla wszystkich formuł ϕ_1 i ϕ_2, jeżeli ϕ_1 i ϕ_2 należą do zbioru X, to także formuła $(\phi_1 \Rightarrow \phi_2)$ należy do X,*

to X zawiera zbiór wszystkich formuł zbudowanych ze zmiennych p i q oraz spójnika $\Rightarrow$.

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

Zadanie 74. Udowodnij, że jeżeli formuły ϕ_1 i ϕ_2 są równoważne, to równoważne są także formuły ϕ_1^n i ϕ_2^n.

Zadanie 75. Udowodnij, że dla dowolnej formuły ϕ formuły $\neg\phi^d$ oraz ϕ^n są równoważne.

Zadanie 76. Udowodnij, że jeżeli formuły ϕ_1 i ϕ_2 są równoważne, to równoważne są także formuły ϕ_1^d i ϕ_2^d.

Zadanie 77. 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 78 (lemat interpolacyjny Craiga dla rachunku zdań). Niech $V(\phi)$ oznacza zbiór zmiennych zdaniowych występujących w formule ϕ. Przypuśćmy, że ϕ i ψ są takimi formułami rachunku zdań, że $\phi \Rightarrow \psi$ jest tautologią. Udowodnij, że istnieje taka formuła ρ, że $\phi \Rightarrow \rho$ oraz $\rho \Rightarrow \psi$ są tautologiami i $V(\rho) \subseteq V(\phi) \cap V(\psi)$.

Zadanie 79 (o zamkniętym układzie twierdzeń). Niech n będzie ustaloną liczbą naturalną. Przypuśćmy, że dla pewnego wartościowania są spełnione formuły:

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

Udowodnij, że wartościowanie to spełnia także formuły

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

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

Zadanie 80. 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 tej formuły. Dla ilu wartościowań jest fałszywa formuła

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

Zadanie 81. Niech ϕ oraz ψ będą formułami rachunku zdań zbudowanymi wyłącznie ze zmiennych zdaniowych oraz spójników $\vee$ oraz $\wedge$ (oczywiście w składni konkretnej można używać nawiasów). Pokaż, że formuła $\phi \Leftrightarrow \psi$ jest spełniona przez co najmniej dwa wartościowania. Podaj przykład formuł ϕ i ψ takich, że formuła $\phi \Leftrightarrow \psi$ jest spełniona przez dokładnie dwa wartościowania.

Zadanie 82. Niech n będzie dodatnią liczbą naturalną i niech $V_n = \{p_0, \ldots, p_{n-1}\}$ będzie zbiorem zmiennych zdaniowych. Przyjmijmy, że dla formuły ϕ nie zawierającej zmiennych spoza zbioru V_n napis $nv_n(\phi)$ oznacza liczbę wartościowań $\sigma : V_n \to \{\mathsf{T}, \mathsf{F}\}$ spełniających tę formułę. Pokaż, że dla dowolnych formuł zdaniowych ϕ oraz ψ, które nie zawierają zmiennych spoza zbioru V_n, równość

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

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

Zadanie 83. Niech V będzie niepustym i skończonym zbiorem zmiennych zdaniowych. Znajdź zbiór wszystkich wartościowań spełniających formułę

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

2.5. Postaci normalne formuł zdaniowych

2.5.1. Usuwanie symbolu negacji

Formuły w których symbol negacji występuje przed formułą złożoną są często trudne do zrozumienia (wyrażenie „nieprawda, że liczba n dzieli się przez 2 lub przez 3” jest bardziej skomplikowane, niż równoważne mu wyrażenie „liczba n nie dzieli się przez 2 i nie dzieli się przez 3”). *Prawa negowania formuł zdaniowych* (punkty 5–12 z zadania 42) pozwalają znaleźć dla danej formuły formułę jej równoważną, w której negacja występuje jedynie przed zmiennymi zdaniowymi. Formuły tej postaci (tzn. takie, w których negacja występuje jedynie przed zmiennymi zdaniowymi) będziemy nazywać formulami w *negacyjnej postaci normalnej* (NNF, ang. *Negation Normal Form*). Dla dowolnej formuły ϕ na mocy lematu o podstawianiu i prawa podwójnego przeczenia formuły $\neg\neg\phi$ oraz ϕ są równoważne. Na mocy lematu o podstawianiu i prawa De Morgana dla dowolnych formuł ϕ_1 i ϕ_2 formuły $\neg(\phi_1 \wedge \phi_2)$ oraz $\neg\phi_1 \vee \neg\phi_2$ są równoważne. Podobnie postępujemy dla formuł dowolnej innej postaci. Możemy zatem zdefiniować odwzorowanie T przyporządkowujące dowolnym formułom równoważne formuły, w których negacja występuje jedynie przed zmiennymi zdaniowymi:

$$
\begin{array}{rcl}
T(p) & = & p, \quad \text{dla } p \in V \\
T(\bot) & = & \bot \\
T(\top) & = & \top \\
T(\phi_1 \vee \phi_2) & = & T(\phi_1) \vee T(\phi_2) \\
T(\phi_1 \wedge \phi_2) & = & T(\phi_1) \wedge T(\phi_2) \\
T(\phi_1 \Rightarrow \phi_2) & = & T(\phi_1) \Rightarrow T(\phi_2) \\
T(\phi_1 \Leftrightarrow \phi_2) & = & T(\phi_1) \Leftrightarrow T(\phi_2) \\
T(\neg p) & = & \neg p, \quad \text{dla } p \in V \\
T(\neg\bot) & = & \top \\
T(\neg\top) & = & \bot \\
T(\neg(\phi_1 \vee \phi_2)) & = & T(\neg\phi_1) \wedge T(\neg\phi_2) \\
T(\neg(\phi_1 \wedge \phi_2)) & = & T(\neg\phi_1) \vee T(\neg\phi_2) \\
T(\neg(\phi_1 \Rightarrow \phi_2)) & = & T(\phi_1) \wedge T(\neg\phi_2) \\
T(\neg(\phi_1 \Leftrightarrow \phi_2)) & = & T(\neg\phi_1) \Leftrightarrow T(\phi_2) \\
T(\neg\neg\phi) & = & T(\phi)
\end{array}
$$

Fakt 28. Dla dowolnej formuły ϕ, formuły ϕ oraz $T(\phi)$ są równoważne i w formule $T(\phi)$ negacja występuje jedynie przed zmiennymi zdaniowymi.

Bezpośredni dowód Faktu 28 okazuje się zaskakująco skomplikowany i niezgrabny, z dwóch powodów. Po pierwsze, definicja odwzorowania T nie pasuje do schematu indukcji strukturalnej. W dowodach indukcyjnych chcemy dowodzić własności formuł korzystając tylko z założeń o podformułach, np. żeby dowieść czegoś o formule $\phi_1 \vee \phi_2$ chcemy korzystać tylko z własności formuł ϕ_1 i ϕ_2; tymczasem wartość T dla $\neg(\phi_1 \vee \phi_2)$ zależy od wartości T dla $\neg\phi_1$, która nie jest podformułą $\neg(\phi_1 \vee \phi_2)$. Żeby obejść ten problem, możemy zdefiniować T w inny, równoważny, sposób, używając dodatkowego odwzorowania F. Na rysunku 6 odwzorowania T i F definiujemy jednocześnie, przez wzajemną rekursję. W tej definicji odwołujemy się rekurencyjnie wyłącznie do podformuł, dzięki czemu łatwiej będzie użyć schematu indukcji strukturalnej. Tak zdefiniowaną funkcję łatwiej również zaimplementować.

Drugi powód trudności dowodu jest następujący: mimo że interesuje nas własność odwzorowania T, w dowodzie musimy skorzystać także z własności odwzorowania F. Mamy tu do czynienia z dość typową w matematyce sytuacją, w której

$$
\begin{array}{rcll}
T(p) & = & p, & \text{dla } p \in V \\
T(\bot) & = & \bot & \\
T(\top) & = & \top & \\
T(\phi_1 \vee \phi_2) & = & T(\phi_1) \vee T(\phi_2) & \\
T(\phi_1 \wedge \phi_2) & = & T(\phi_1) \wedge T(\phi_2) & \\
T(\phi_1 \Rightarrow \phi_2) & = & T(\phi_1) \Rightarrow T(\phi_2) & \\
T(\phi_1 \Leftrightarrow \phi_2) & = & T(\phi_1) \Leftrightarrow T(\phi_2) & \\
T(\neg\phi) & = & F(\phi) &
\end{array}
\qquad
\begin{array}{rcll}
F(p) & = & \neg p, & \text{dla } p \in V \\
F(\bot) & = & \top & \\
F(\top) & = & \bot & \\
F(\phi_1 \vee \phi_2) & = & F(\phi_1) \wedge F(\phi_2) & \\
F(\phi_1 \wedge \phi_2) & = & F(\phi_1) \vee F(\phi_2) & \\
F(\phi_1 \Rightarrow \phi_2) & = & T(\phi_1) \wedge F(\phi_2) & \\
F(\phi_1 \Leftrightarrow \phi_2) & = & F(\phi_1) \Leftrightarrow T(\phi_2) & \\
F(\neg\phi) & = & T(\phi) &
\end{array}
$$

Rysunek 6. Sprowadzanie formuły do NNF

żeby udało się przeprowadzić dowód, musimy wzmocnić dowodzone twierdzenie. Intuicyjnie: żeby dowód był łatwiejszy, trzeba udowodnić trudniejsze twierdzenie.

Fakt 29. Dla dowolnej formuły ϕ, (1) formuły ϕ oraz $T(\phi)$ są równoważne, (2) formuły $\neg\phi$ oraz $F(\phi)$ są równoważne, oraz (3) w formułach $T(\phi)$ i $F(\phi)$ negacja występuje jedynie przed zmiennymi zdaniowymi.

Zadanie 84. Udowodnij Fakt 29. *Wskazówka:* Pomocny może się okazać zbiór

$$X = \{\phi \in \mathcal{F}(V) \mid T(\phi) \equiv \phi \text{ oraz } F(\phi) \equiv \neg\phi\}.$$

Zadanie 85. Zaneguj formuły z zadania 38 i — korzystając z praw negowania formuł logicznych — znajdź formuły im równoważne, w których negacja występuje jedynie przed zmiennymi zdaniowymi.

Formuły w negacyjnej postaci normalnej możemy określić jako formuły zbudowane z literałów przy pomocy spójników logicznych alternatywy, koniunkcji, implikacji i równoważności. Zauważmy, że na mocy lematu o podstawianiu i punktów 13–15 zadania 42 każda formuła jest równoważna pewnej formule nie zawierającej spójników implikacji i równoważności. Możemy więc rozpatrywać formuły zbudowane z literałów jedynie przy pomocy spójników alternatywy i koniunkcji. Jeszcze węższe klasy formuł rozważamy w następnych paragrafach.

2.5.2. Dysjunkcyjna postać normalna

Definicja 30. Formuła ma *dysjunkcyjną postać normalną* (DNF, ang. *Disjunctive Normal Form*), jeśli ma postać

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

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

Zadanie 86. Udowodnij, że dla każdej formuły zdaniowej ϕ istnieje formuła ψ równoważna z ϕ i mająca dysjunkcyjną postać normalną.

Zadanie 87. Znajdź formuły zdaniowe ϕ_1, ϕ_2, ϕ_3 mające dysjunkcyjną postać normalną, zawierające zmienne p, q i r i spełnione dla podanych niżej wartościowań:

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

Zadanie 88. Znajdź formuły mające dysjunkcyjną postać normalną równoważne formułom z zadania 47.

Definicja 31. Formuła ma postać k-DNF, gdzie k jest liczbą naturalną, jeżeli ma postać

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

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

Zadanie 89. Wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci 1-DNF.

Zadanie 90. Dla każdego $k \geq 1$ wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci k-DNF.

Definicja 32. Formuła ma postać DNF_j, gdzie j jest liczbą naturalną, jeżeli ma postać DNF i każda zmienna występuje w niej co najwyżej j razy.

Zadanie 91. Wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci DNF_1.

Zadanie 92. Dla każdego $k \geq 1$ wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci DNF_k.

2.5.3. Koniunkcyjna postać normalna

Definicja 33. *Klauzulą* nazywamy formułę postaci

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

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

Definicja 34. Formuła ma *koniunkcyjną postać normalną* (CNF, ang. *Conjunctive Normal Form*), jeśli ma postać

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

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

Zadanie 93. Udowodnij, że dla każdej formuły zdaniowej ϕ istnieje formuła ψ równoważna z ϕ i mająca koniunkcyjną postać normalną.

Zadanie 94. Znajdź formuły mające koniunkcyjną postać normalną równoważne formułom z zadania 87.

Zadanie 95. Znajdź formuły mające koniunkcyjną postać normalną równoważne formułom z zadania 38.

Definicja 35. Formuła ma postać k-CNF, gdzie k jest liczbą naturalną, jeżeli ma postać

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

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

Zadanie 96. Wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci 1-CNF.

Zadanie 97. Dla każdego $k \geq 1$ wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci k-CNF.

Definicja 36. Formuła ma postać CNF_j, gdzie j jest liczbą naturalną, jeżeli ma postać CNF i każda zmienna występuje w niej co najwyżej j razy. Formuła ma postać k-CNF_j, gdzie k i j są liczbami naturalnymi, jeżeli ma postać k-CNF i każda zmienna występuje w niej co najwyżej j razy.

Zadanie 98. Wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci CNF_1.

Zadanie 99. Dla każdego $k \geq 1$ wskaż przykład formuły, która nie jest równoważna z żadną formułą postaci CNF_k.

Definicja 37. Literał l jest *pozytywny*, jeżeli $l = p$ dla pewnej zmiennej $p \in V$. Literał l jest *negatywny*, jeżeli $l = \neg p$ dla pewnej zmiennej $p \in V$.

Definicja 38. Operację negowania literału definiujemy następująco:

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

dla dowolnego $p \in V$.

Zadanie 100. Niech $C = \bigvee_{j=1}^{m} l_j$ będzie dowolną klauzulą i niech

$$\begin{array}{rcl} P & = & \{j \in \{1, \ldots, m\} \mid \text{literał } l_j \text{ jest pozytywny}\}, \\ N & = & \{j \in \{1, \ldots, m\} \mid \text{literał } l_j \text{ jest negatywny}\} \end{array}$$

oraz

$$C' \quad = \quad \bigwedge_{j \in N} \overline{l_j} \Rightarrow \bigvee_{j \in P} l_j.$$

Udowodnij, że formuły C oraz C' są równoważne.

Na mocy powyższego zadania klauzule można zapisywać w postaci

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

gdzie p_j i q_j są zmiennymi zdaniowymi.

Definicja 39. Klauzula $\bigvee_{j=1}^{m} l_j$ jest *klauzulą hornowską*, jeżeli co najwyżej jeden spośród literałów $l_1, \ldots, l_m$ jest pozytywny. Formuła ma *postać hornowską*, jeżeli jest koniunkcją klauzul hornowskich.

Klauzule hornowskie można więc zapisać w postaci

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

gdzie p_j oraz q są zmiennymi zdaniowymi.

Zadanie 101. Wskaż przykład formuły, która nie jest równoważna z żadną formułą w postaci hornowskiej.

Zadanie 102. Które spośród formuł z zadania 37 można przedstawić w postaci hornowskiej? Tam, gdzie to możliwe, podaj tę postać.

Zadanie 103. Które spośród formuł z zadania 38 można przedstawić w postaci hornowskiej? Tam, gdzie to możliwe, podaj tę postać.

2.6. Funkcje boolowskie i zupełne zbiory spójników

Definicja 40. 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 ($\bot$, $\top$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$). 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. Tabelki funkcji boolowskich określających prawdziwość spójników $\bot$, $\top$, $\neg$, $\vee$, $\wedge$, $\Rightarrow$ i $\Leftrightarrow$ zostały przedstawione na rysunku 2.

Definicja 41. 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 42. Zbiór spójników logicznych jest *zupełny*, jeżeli dla wszystkich $n \geq 1$ dowolną n-argumentową funkcję boolowską można opisać za pomocą formuły zdaniowej zawierającej jedynie spójniki z tego zbioru i zmienne. Zbiór spójników jest *k-zupełny*, jeżeli każdą *co najwyżej k-argumentową* funkcję boolowską można opisać za pomocą formuły zdaniowej zawierającej jedynie spójniki z tego zbioru i zmienne.

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

Zadanie 104. Ile jest funkcji boolowskich n-argumentowych?

Zadanie 105. Pokaż, że $\{\vee, \wedge\}$ nie jest zupełny.

Zadanie 106. Pokaż, że $\{\vee, \wedge, \Leftrightarrow, \Rightarrow\}$ nie jest zupełny.

Zadanie 107. Pokaż, że $\{\Leftrightarrow, \bot\}$ nie jest zupełny oraz że jest 1-zupełny.

Zadanie 108. Pokaż, że $\{\wedge, \vee, \neg\}$ jest zupełny.

Zadanie 109. Pokaż, że $\{\wedge, \neg\}$ jest zupełny.

Zadanie 110. Pokaż, że $\{\vee, \neg\}$ jest zupełny.

Zadanie 111. Pokaż, że $\{\Rightarrow, \bot\}$ jest zupełny.

Zadanie 112. Pokaż, że $\{\Rightarrow, \neg\}$ jest zupełny.

Zadanie 113. Pokaż, że $\{\vee, \Leftrightarrow, \bot\}$ jest zupełny.

Zadanie 114. Udowodnij, że każdy 2-zupełny zbiór spójników jest zupełny.

Zadanie 115. Udowodnij, że zbiór $\{\vee, \wedge, \Rightarrow, \neg\}$ jest 2-zupełny.

Zadanie 116. Rozważmy unarną funkcję boolowską f_1 opisaną formułą $\neg p_1$ i binarną funkcję f_2 opisaną formułą $p_1 \wedge p_2$. Udowodnij, że jeśli funkcje f_1 i f_2 można opisać za pomocą formuł zawierających jedynie spójniki ze zbioru S i zmienne, to zbiór S jest zupełny.

Zadanie 117. Czy system spójników $\{\oplus, \top\}$ jest zupełny, gdzie $p \oplus q$ jest prawdziwe wtedy i tylko wtedy, gdy $p \wedge \neg q$ jest prawdą, zaś $\top$ oznacza prawdę?

Zadanie 118. Pokaż, że istnieje taki dwuargumentowy spójnik $\uparrow$, że $\{\uparrow\}$ jest zupełny.

Zadanie 119. Ile jest takich dwuargumentowych spójników logicznych $\oplus$, że $\{\oplus\}$ jest zupełny?

Zadanie 120. Niech s będzie takim spójnikiem logicznym, że $s(\mathsf{T}, \mathsf{T}) = \mathsf{F}$. Udowodnij, że zbiór $\{s, \Rightarrow\}$ jest zupełny.

2.7. Rezolucja dla rachunku zdań

Definicja 43. *Literał* w rachunku zdań to zmienna zdaniowa lub negacja zmiennej zdaniowej. *Klauzulą* nazywamy alternatywę skończenie wielu literałów. Alternatywę zera literałów nazywamy klauzulą pustą i oznaczamy $\perp$.

W tym rozdziale przyjmujemy konwencję utożsamiającą klauzulę ze zbiorem jej literałów. W szczególności klauzule $p \vee q$ i $q \vee p$, podobnie jak $p \vee p$ i p będziemy uważać za identyczne.

Definicja 44. Mówimy, że zbiór formuł $\mathcal{F}$ jest spełnialny jeśli istnieje takie wartościowanie σ, że $\hat{\sigma}(\phi) = \mathsf{T}$ dla wszystkich $\phi \in \mathcal{F}$; w przeciwnym przypadku mówimy że $\mathcal{F}$ jest *sprzeczny*. Formułę ϕ nazywamy *logiczną konsekwencją* zbioru formuł $\mathcal{F}$ jeśli dla każdego wartościowania σ spełniającego $\mathcal{F}$ zachodzi $\hat{\sigma}(\phi) = \mathsf{T}$.

Definicja 45. Jeśli C i D są klauzulami a p jest zmienną zdaniową to klauzulę $C \vee D$ nazywamy *rezolwentą* klauzul $C \vee p$ i $D \vee \neg p$. Rezolucyjnym dowodem sprzeczności zbioru $\mathcal{F}$ nazywamy ciąg klauzul $C_0, \ldots C_n$ spełniający warunki

- dla wszystkich $i \in \{0, \ldots, n\}$ zachodzi $C_i \in \mathcal{F}$ lub istnieją takie $j, k < i$, że C_i jest rezolwentą C_j i C_k.
- $C_n = \perp$.

W rożnych systemach formalnych reguły dowodzenia często zapisywane są w następującej postaci:

$$\frac{\alpha_1 \quad \ldots \quad \alpha_n}{\beta}$$

Formuły $\alpha_1, \ldots, \alpha_n$ nad poziomą kreską nazywamy *przesłankami*, a formułę β pod kreską nazywamy *konkluzją*. Wtedy dowód formuły ϕ można sobie wyobrazić jako skończone drzewo etykietowane formułami, którego korzeń ma etykietę ϕ, liście są etykietowane aksjomatami (w naszym przypadku elementami zbioru $\mathcal{F}$) oraz dla każdego wierzchołka, który nie jest liściem, jego etykieta jest konkluzją reguły wnioskowania, której przesłankami są etykiety następników tego wierzchołka.

Regułę rezolucji możemy zapisać w takiej postaci jako

$$\frac{C \vee p \quad D \vee \neg p}{C \vee D}$$

a rezolucyjny dowód sprzeczności zbioru formuł $\{p \vee q, \neg p \vee q, p \vee \neg q, \neg p \vee \neg q\}$ można narysować tak:

$$\frac{\dfrac{p \vee q \quad \neg p \vee q}{q} \quad \dfrac{p \vee \neg q \quad \neg p \vee \neg q}{\neg q}}{\perp}$$

W systemie rezolucji dość łatwo dowodzi się twierdzenie o poprawności (*jeśli istnieje rezolucyjny dowód sprzeczności zbioru $\mathcal{F}$, to zbiór $\mathcal{F}$ jest sprzeczny*). Natomiast dowód twierdzenia o zupełności (*jeśli zbiór $\mathcal{F}$ jest sprzeczny, to istnieje rezolucyjny dowód jego sprzeczności*) jest trudniejszy i wybiega poza ramy tego wykładu.

Zadanie 121. Udowodnij, że formuła ϕ jest logiczną konsekwencją zbioru formuł $\mathcal{F}$ wtedy i tylko wtedy, gdy zbiór $\mathcal{F} \cup \{\neg\phi\}$ jest sprzeczny.

Zadanie 122. Udowodnij, że dla dowolnych klauzul C i D oraz dowolnej zmiennej zdaniowej p rezolwenta $C \vee D$ jest logiczną konsekwencją zbioru $\{C \vee p,\ D \vee \neg p\}$.

Zadanie 123. Udowodnij, że jeśli istnieje rezolucyjny dowód sprzeczności zbioru $\mathcal{F}$, to zbiór $\mathcal{F}$ jest sprzeczny.

Zadanie 124. Podaj rezolucyjny dowód sprzeczności dla zbioru klauzul $\{\neg p \vee q, \neg p \vee \neg r \vee s, \neg q \vee r,\ \ p,\ \ \neg s\}$.

Zadanie 125. Podaj rezolucyjny dowód sprzeczności dla zbioru klauzul

$$\begin{array}{lccl} \{ & p \vee r, & \neg r \vee \neg s, & \\ & q \vee s, & q \vee r, & \\ & \neg p \vee \neg q, & s \vee p & \}. \end{array}$$

Zadanie 126. Sprawdź, czy zbiór klauzul

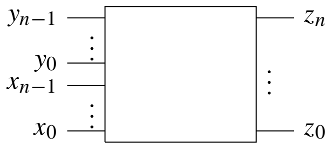
$$\{p \vee q \vee r,\quad \neg r \vee \neg q \vee \neg p,\quad \neg q \vee r,\quad \neg r \vee p\}$$

jest sprzeczny. Jeśli jest sprzeczny, podaj dla niego rezolucyjny dowód sprzeczności. Jeśli nie jest, podaj wartościowanie spełniające ten zbiór.

2.8. Funkcje boolowskie i układy elektroniczne

Na przykładzie sumatora n-bitowego pokażemy jak funkcje boolowskie są wykorzystywane w konstrukcji układów elektronicznych. Sumator n-bitowy jest prostym układem elektronicznym o $2n$ wejściach i $n+1$ wyjściach, który dla podanych na wejściu dwóch ciągów n-bitowych $\vec{x} = \langle x_{n-1}, \ldots, x_0\rangle$ oraz $\vec{y} = \langle y_{n-1}, \ldots, y_0\rangle$ podaje na wyjściu ciąg $\vec{z} = \langle z_n, \ldots, z_0\rangle$ będący binarną reprezentacją sumy liczb reprezentowanych przez $\vec{x}$ i $\vec{y}$. Np 4-bitowy sumator dla danych na wejściu ciągów $\langle 1, 1, 0, 1\rangle$ (liczba 13 w systemie dwójkowym) oraz $\langle 1, 1, 0, 0\rangle$ (liczba 12 w systemie dwójkowym) powinien wyliczyć na wyjściu ciąg $\langle 1, 1, 0, 0, 1\rangle$ (liczba 25 w systemie dwójkowym).

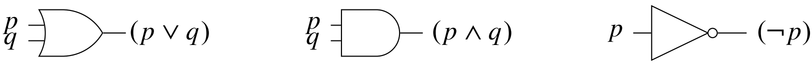
Takie układy elektroniczne można budować z tzw *bramek logicznych*, czyli jeszcze prostszych układów elektronicznych implementujących najprostsze spójniki logiczne, np. bramek or, and i not



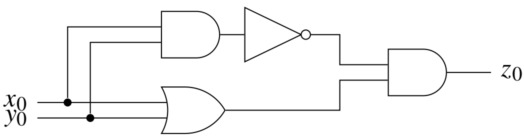
Rysunek 7. Sumator n-bitowy

x_0	y_0	z_1	z_0
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

Rysunek 8. Tabelka zero-jedynkowa dla sumatora 1-bitowego



Oczywiście sumator 1-bitowy powinien realizować tabelkę zero-jedynkową z rysunku 8. Łatwo zauważyć, że wyjście z_0 sumatora można opisać formułą $(x_0 \vee y_0) \wedge \neg(x_0 \wedge y_0)$, odpowiedni fragment układu mamy na rysunku 9.



Rysunek 9. Fragment sumatora 1-bitowego obliczający bit z_0

Zadanie 127. Jeden ze studentów zaproponował realizację wyjścia z_1 sumatora 1-bitowego za pomocą formuły $x_0 \wedge y_0 \wedge \neg((x_0 \wedge \neg y_0) \vee (\neg x_0 \wedge y_0))$.

1. Sprawdź czy jest to poprawna definicja. Formalnie, sprawdź, czy formuła $\phi = x_0 \wedge y_0 \wedge \neg((x_0 \wedge \neg y_0) \vee (\neg x_0 \wedge y_0))$ ma następującą tabelkę zero-jedynkową.

x_0	y_0	ϕ
F	F	F
F	T	F
T	F	F
T	T	T

2. Przed przystąpieniem do masowej produkcji sumatorów chcielibyśmy ograniczyć niepotrzebne koszty i tu pojawia się pytanie czy da się zbudować moduł obliczający z_1 z mniejszej liczby bramek logicznych. Formalnie, sprawdź czy istnieje formuła o takiej tabelce zero-jedynkowej jak w poprzednim punkcie, w której występuje mniej niż 8 spójników logicznych.

Najprostszy schemat sumatora otrzymuje się z prostszych modułów odpowiedzialnych za obliczanie kolejnych bitów wyniku, tak jak w algorytmie dodawania pisemnego: do obliczenia bitu z_k trzeba zsumować bity x_k, y_k oraz bit przeniesienia p_k wynikający z sumowania poprzednich bitów (por. rysunek 10). W naszym przykładzie sumowania liczb 12 i 13 bity przeniesienia to $p_1 = 0$, $p_2 = 0$, $p_3 = 1$ i $p_4 = 1$. W następnym zadaniu mamy zaprojektować właśnie taki moduł sumujący trzy bity.

$$
\begin{array}{rccccccc}
p: & & \boxed{1} & \boxed{1} & \boxed{0} & \boxed{0} & \\
x: & & & 1 & 1 & 0 & 1 \\
y: & + & & 1 & 1 & 0 & 0 \\
\hline
z: & & 1 & 1 & 0 & 0 & 1
\end{array}
$$

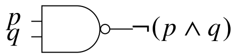
Rysunek 10: Dodawanie pisemne liczb 12 i 13 w systemie dwójkowym. W pierwszym wierszu bity przeniesienia.

Zadanie 128. Zaprojektuj z bramek logicznych or, and i not układ elektroniczny sumujący trzy bity. Formalnie, używając tylko zmiennych zdaniowych x, y i p oraz spójników $\vee$, $\wedge$, $\neg$ skonstruuj formuły ϕ_1, ϕ_2 o następujących tabelkach zero-jedynkowych.

p	x	y	ϕ_1	ϕ_2
F	F	F	F	F
F	F	T	F	T
F	T	F	F	T
F	T	T	T	F
T	F	F	F	T
T	F	T	T	F
T	T	F	T	F
T	T	T	T	T

W zadaniu 105 pokazaliśmy, że zbiór $\{\vee, \wedge\}$ jest niezupełny. Rozwiązanie opierało się na obserwacji, że każda formuła zbudowana z tych spójników i zmiennych zdaniowych jest spełniona przy wartościowaniu przyporządkowującym wszystkim zmiennym prawdę. Można stąd wywnioskować, że każdy obwód elektroniczny zbudowany z bramek and i or po otrzymaniu na wejściu samych jedynek zwróci również same jedynki na wyjściu. Dlatego, mając do dyspozycji tylko bramki and oraz or, nie da się zbudować sumatora: sumator otrzymaniu jedynek na wejściach x_0 i y_0 musiałby zwrócić zero na wyjściu z_0.

W konstrukcji układów elektronicznych często korzysta się z bramek nand realizujących negację koniunkcji



W zadaniu 119 pokazaliśmy, że {nand} jest zupełnym zbiorem spójników. Wynika stąd, że każdą funkcję boolowską można obliczyć układem elektronicznym zbudowanym wyłącznie z bramek nand. A zatem można zbudować wyłącznie z takich bramek sumator 1024-bitowy.

2.9. System dedukcji naturalnej dla rachunku zdań

System rezolucji pozwalał na dowodzenie sprzeczności dla zbiorów klauzul. Równoważnie można powiedzieć, że służy on do dowodzenia, że dana formuła w dysjunkcyjnej postaci normalnej jest tautologią. Poniżej prezentujemy system, którego można użyć dla wszystkich formuł (a nie tylko tych w określonej postaci normalnej).

System dedukcji naturalnej jest formalnym systemem dowodzenia, którego intencją jest zachowanie jak największej zgodności struktury dowodów z naturalnym sposobem rozumowania w matematyce. Reguły dowodzenia podzielone są na dwie grupy: reguły wprowadzania spójników logicznych, mówiące jak dowodzi się zdań z użyciem danego spójnika, oraz reguły eliminacji spójników logicznych mówiące jakie wnioski można wyciągnąć ze zdań używających danego spójnika. Poniżej, przy każdej regule na wysokości kreski wpisujemy nazwę spójnika oraz literę i dla reguł wprowadzania (od angielskiego słowa *introduction*) lub literę e dla reguł eliminacji (od angielskiego słowa *elimination*).

Reguły dowodzenia systemu dedukcji naturalnej

Reguły wprowadzania:

$$\frac{\alpha \quad \beta}{\alpha \wedge \beta}\ (\wedge\mathrm{i}) \qquad \frac{\alpha}{\alpha \vee \beta}\ (\vee\mathrm{i}_1) \qquad \frac{\beta}{\alpha \vee \beta}\ (\vee\mathrm{i}_2) \qquad \frac{}{\top}\ (\top\mathrm{i})$$

$$\frac{\boxed{\begin{array}{c} \alpha \\ \vdots \\ \beta \end{array}}}{\alpha \Rightarrow \beta}\ (\Rightarrow \mathrm{i}) \qquad\qquad \frac{\boxed{\begin{array}{c} \alpha \\ \vdots \\ \bot \end{array}}}{\neg\alpha}\ (\neg\mathrm{i})$$

Pierwsze trzy reguły to reguły wprowadzania koniunkcji i alternatywy. Intuicyjnie są one oczywiste: aby udowodnić prawdziwość koniunkcji $\alpha \wedge \beta$ należy udowodnić prawdziwość obu formuł α oraz β, natomiast do udowodnienia prawdziwości alternatywy $\alpha \vee \beta$ wystarczy udowodnienie prawdziwości jednej z tych formuł. Reguła wprowadzania prawdy jest trywialna: formuła $\top$ jest prawdziwa i jej dowód nie wymaga żadnych przesłanek. Nie ma reguły wprowadzania fałszu.

Więcej wyjaśnień wymagają reguły wprowadzania implikacji i negacji. W tych regułach przesłanki zamknięte w prostokątach (zwyczajowo zwanych oknami) nie są formułami tylko dowodami, a pierwsza formuła w oknie (czyli α) jest *założeniem*. Reguła wprowadzania implikacji mówi, że aby udowodnić implikację $\alpha \Rightarrow \beta$ należy założyć prawdziwość α i korzystając z tego założenia udowodnić prawdziwość β. Podobnie, aby udowodnić prawdziwość $\neg\alpha$ należy założyć prawdziwość α i korzystając z tego założenia dojść do sprzeczności. Bardzo ważna przy tym jest zasada, że założeń można używać tylko wewnątrz odpowiednich okien (założenia są lokalne, podobnie jak zmienne w programach; podobnie jak zmiennych lokalnych, nie wolno ich używać poza zasięgiem ich deklaracji). W dowolnym miejscu dowodu wolno przyjąć nowe założenie i utworzyć nowe okno; w dowolnym miejscu wewnątrz tego okna można użyć tego założenia jak aksjomatu, ale każde założenie musi być zamknięte przez zamknięcie odpowiedniego okna.
Reguły eliminacji:

$$\frac{\alpha \wedge \beta}{\alpha}\ (\wedge e_1) \qquad \frac{\alpha \wedge \beta}{\beta}\ (\wedge e_2) \qquad \frac{\alpha \vee \beta \quad \boxed{\begin{array}{c}\alpha\\ \vdots\\ \gamma\end{array}} \quad \boxed{\begin{array}{c}\beta\\ \vdots\\ \gamma\end{array}}}{\gamma}\ (\vee e)$$

$$\frac{\alpha \quad \alpha \Rightarrow \beta}{\beta}\ (\Rightarrow e) \qquad \frac{\alpha \quad \neg\alpha}{\bot}\ (\neg e) \qquad \frac{\bot}{\alpha}\ (\bot e)$$

Reguły eliminacji koniunkcji i implikacji są dość intuicyjne. Reguła eliminacji alternatywy odpowiada dowodom przez rozpatrywanie przypadków: jeśli wiemy, że zachodzi któryś z przypadków α lub β i w każdym z tych przypadków umiemy udowodnić γ, to mamy dowód prawdziwości γ. Regułę eliminacji negacji można także potraktować jako regułę wprowadzania sprzeczności: aby otrzymać sprzeczność należy udowodnić prawdziwość jednocześnie jakiejś formuły i jej negacji. Reguła eliminacji sprzeczności mówi, że z fałszu można wszystko wywnioskować — intuicyjnie odpowiada to faktowi, że dla dowolnej formuły α formuła $\bot \Rightarrow \alpha$ jest tautologią. Nie ma reguły eliminacji prawdy.

Ostatnia reguła to reguła eliminacji podwójnej negacji

$$\frac{\neg\neg\alpha}{\alpha}\ (\neg\neg e)$$

Jest ona konieczna np. do udowodnienia prawa wyłączonego środka mówiącego, że dla dowolnej formuły α zachodzi $\alpha \lor \neg\alpha$. Osoby zainteresowane funkcyjnymi językami programowania dowiedzą się na dalszych latach studiów, że reguła ta jest pomijana w logice intuicjonistycznej.

W literaturze można znaleźć także reguły dla równoważności, są one jednak mniej naturalne i tutaj celowo je pomijamy. Możemy myśleć o równoważności jako o skrócie notacyjnym oznaczającym dwie implikacje, tzn. dla potrzeb tego rozdziału możemy uznać, że formuła $\phi \Leftrightarrow \psi$ jest skrótem notacyjnym oznaczającym formułę $(\phi \Rightarrow \psi) \land (\psi \Rightarrow \phi)$.

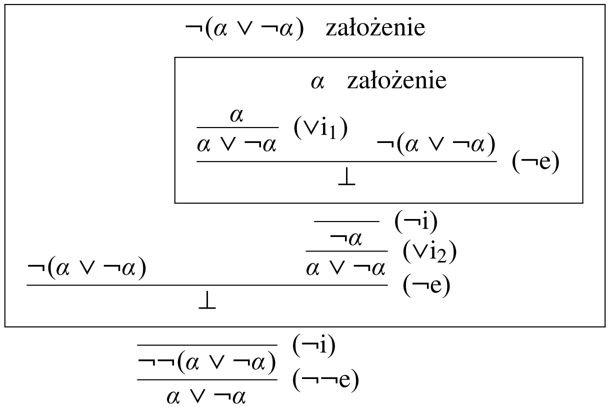
Można udowodnić, że system dedukcji naturalnej dla rachunku zdań jest poprawny (jeśli formuła ma dowód w systemie naturalnej dedukcji to jest tautologią rachunku zdań) i zupełny (czyli każda tautologia ma dowód w tym systemie).

Przykład 46. Pokażemy w systemie naturalnej dedukcji dowód jednej implikacji z praw De Morgana: $\neg(p \lor q) \Rightarrow \neg p \land \neg q$.

$$\dfrac{\boxed{\begin{array}{c} \neg(p \lor q) \quad \text{założenie} \\ \boxed{\begin{array}{c} p \quad \text{założenie} \\ \dfrac{\dfrac{p}{p \lor q}\,(\lor\mathrm{i}_1) \qquad \neg(p \lor q)}{\bot}\,(\neg\mathrm{e}) \end{array}} \quad \boxed{\begin{array}{c} q \quad \text{założenie} \\ \dfrac{\dfrac{q}{p \lor q}\,(\lor\mathrm{i}_2) \qquad \neg(p \lor q)}{\bot}\,(\neg\mathrm{e}) \end{array}} \\ \dfrac{\dfrac{\qquad}{\neg p}\,(\neg\mathrm{i}) \qquad\qquad \dfrac{\qquad}{\neg q}\,(\neg\mathrm{i})}{\neg p \land \neg q}\,(\land\mathrm{i}) \end{array}}}{\neg(p \lor q) \Rightarrow \neg p \land \neg q}\,(\Rightarrow \mathrm{i})$$

Powyższy dowód formalny dość łatwo tłumaczy się na dowód w języku naturalnym: *Załóżmy, że formuła $\neg(p \lor q)$ jest prawdziwa. Gdyby p było prawdą, to oczywiście $p \lor q$ także byłoby prawdą, co przeczy założeniu $\neg(p \lor q)$. Zatem $\neg p$ jest prawdą. Podobnie gdyby q było prawdą, to oczywiście $p \lor q$ także byłoby prawdą, co przeczy założeniu $\neg(p \lor q)$. Zatem $\neg q$ jest prawdą. Czyli $\neg p \land \neg q$ jest prawdą, co kończy dowód implikacji $\neg(p \lor q) \Rightarrow \neg p \land \neg q$.*

Przykład 47. Pokażemy w systemie naturalnej dedukcji schemat dowodu prawa wyłączonego środka. Tutaj α jest zmienną oznaczającą dowolną formułę, a podany schemat reprezentuje nieskończenie wiele różnych dowodów (po jednym dla każdej wartości zmiennej α; aby otrzymać konkretny dowód należy zastąpić α konkretną formułą).



Zadanie 129. Podaj w systemie dedukcji naturalnej dowód implikacji $\neg(p \wedge q) \Rightarrow \neg p \vee \neg q$. *Wskazówka:* możesz skorzystać z prawa wyłączonego środka. Tej implikacji nie da się udowodnić konstruktywnie (tzn. bez użycia reguły eliminacji podwójnej negacji).

Zadanie 130. Podaj w systemie dedukcji naturalnej dowody wszystkich, z wyjątkiem $p \Leftrightarrow p$ oraz prawa Peirce'a, tautologii z zadania 37.

Zadanie 131. Podaj w systemie dedukcji naturalnej dowód prawa Peirce'a.
Wskazówka: Tego nie da się zrobić konstruktywnie; trzeba użyć reguły eliminacji podwójnej negacji lub prawa wyłączonego środka.

Zadanie 132. Podaj w systemie dedukcji naturalnej schemat dowodu reguły wnioskowania przez kontrapozycję, czyli implikacji

$$(\neg\psi \Rightarrow \neg\phi) \Rightarrow (\phi \Rightarrow \psi)$$

dla dowolnych formuł rachunku zdań ϕ i ψ.
Wskazówka: Tego również nie da się zrobić konstruktywnie.

Zadanie 133. Pan Hilary zgubił swoje okulary i w ich poszukiwaniu stwierdza następujące fakty:

- Jeśli czytałem gazetę w kuchni (α) to okulary są na stole kuchennym (β).
- Jeśli okulary są na stole kuchennym (β), to widziałem je podczas śniadania (γ).
- Nie widziałem okularów podczas śniadania ($\neg\gamma$).

- Czytałem gazetę w kuchni (α) lub w sypialni (δ).
- Jeśli czytałem gazetę w sypialni (δ) to okulary są na łóżku (ϵ).

Pomóż panu Hilaremu i udowodnij w systemie naturalnej dedukcji, że okulary są na łóżku, czyli że

$$(\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \gamma) \wedge \neg\gamma \wedge (\alpha \vee \delta) \wedge (\delta \Rightarrow \epsilon) \Rightarrow \epsilon$$

jest tautologią.

Zadanie 134. Podaj w systemie dedukcji naturalnej dowód rozdzielności alternatywy względem koniunkcji, czyli dwóch implikacji

$$\alpha \vee (\beta \wedge \gamma) \Rightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$$

oraz

$$(\alpha \vee \beta) \wedge (\alpha \vee \gamma) \Rightarrow \alpha \vee (\beta \wedge \gamma).$$

Zadanie 135. Rozważmy fragment systemu dedukcji naturalnej zawierający wyłącznie reguły wprowadzania i eliminacji implikacji. Udowodnij, że każda formuła dowodliwa w tym fragmencie jest tautologią.[3]

Wskazówka. Powiemy, że założenie jest aktywne w pewnym węźle drzewa dowodu jeśli ten węzeł znajduje się wewnątrz prostokąta, w którym założenie zostało przyjęte. Rozważmy drzewo T dowodu pewnej formuły. Udowodnij przez indukcję strukturalną względem drzewa dowodu, że dla każdego poddrzewa drzewa T o korzeniu etykietowanym formułą α i dla każdego wartościowania σ spełniającego wszystkie założenia aktywne w korzeniu tego poddrzewa zachodzi $\hat{\sigma}(\alpha) = \mathsf{T}$.

[3] Właściwie w tym miejscu spodziewalibyśmy się zadania polegającego na udowodnieniu twierdzenia, że każda formuła dowodliwa w systemie dedukcji naturalnej jest tautologią. Wydaje się jednak, że takie zadanie nie byłoby ani ciekawsze ani trudniejsze, a tylko bardziej nużące.

3

Rachunek kwantyfikatorów

3.1. Składnia rachunku kwantyfikatorów

Definicja 48. 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 relacyjnych* $p, q, p_1, p_2, \ldots$ Z każdym symbolem funkcyjnym i z każdym symbolem relacyjnym związujemy liczbę naturalną, która określa liczbę jego argumentów (*arność*). Symbole funkcyjne 0-argumentowe nazywamy *symbolami stałych*. Symbole relacyjne można uważać za uogólnienie zmiennych zdaniowych z rachunku zdań (zmienne zdaniowe, to 0-argumentowe symbole relacyjne).

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

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

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

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

Formuły rachunku kwantyfikatorów (które będziemy oznaczać ϕ, $\psi, \ldots$) 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 x jest zmienną indywiduową, a ϕ — formułą rachunku kwantyfikatorów, to formułami rachunku kwantyfikatorów są też $(\forall x\, \phi)$ i $(\exists x\, \phi)$.
4. Każdą formułę rachunku kwantyfikatorów można otrzymać przy pomocy reguł 1–3.

Dla zwiększenia czytelności w składni konkretnej opuszczamy niektóre nawiasy w podobny sposób, jak w rachunku zdań, a niektóre symbole funkcyjne lub relacyjne piszemy infiksowo. Niestety w literaturze można spotkać różne konwencje dotyczące priorytetu kwantyfikatorów; nawet w naszym instytucie nie ma zgody, czy napis „$\forall x\phi(x) \Rightarrow \psi(y)$” oznacza $(\forall x\phi(x)) \Rightarrow \psi(y)$ czy $\forall x(\phi(x) \Rightarrow \psi(y))$, a nie są to formuły równoważne. Dlatego będziemy się starali używać nawiasów tam, gdzie mogą wystąpić wątpliwości. Czasem będziemy korzystać także z innej konwencji, w której po kwantyfikatorze można napisać kropkę zastępującą nawias — wtedy kwantyfikator wiąże słabiej niż wszystkie pozostałe spójniki i w szczególności zapis $\forall x.\phi(x) \Rightarrow \psi(y)$ oznacza $\forall x(\phi(x) \Rightarrow \psi(y))$.

Definicja 49. Mówimy, że w formule $\forall x\, \phi$ (lub $\exists x\, \phi$) kwantyfikator $\forall$ (lub $\exists$) *wiąże* wystąpienia zmiennej x w formule ϕ, oraz że wystąpienia zmiennej x w formule ϕ są *związane* przez ten kwantyfikator. Wystąpienie zmiennej pod kwantyfikatorem nazywamy *wiążącym*. Wystąpienia zmiennych, które w danej formule nie są związane ani wiążące, są w niej *wolne*. Formalnie zbiór $\mathrm{FV}(\phi)$ zmiennych, które występują jako wolne w formule ϕ definiujemy następująco:

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

Podobnie definiujemy zbiór zmiennych występujących w formule jako związane.

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

Definicja 50. 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. żadne wolne wystąpienie x w α nie znajduje się w zasięgu żadnego kwantyfikatora wiążącego zmienną występującą w t.

Dla przykładu, podstawienie $[x/y]$ jest niedopuszczalne w formule $\exists y\ x < y$. Formuła ta jest prawdziwa w zbiorze liczb rzeczywistych dla dowolnego ustalonego x, natomiast wynikiem podstawienia w niej y w miejsce x byłaby fałszywa formuła $\exists y\ y < y$.

Zadanie 136. Wskaż wolne, wiążące i związane wystąpienia zmiennych w formułach z zadania 172. Narysuj w tych formułach strzałki od wystąpień zmiennych związanych do wystąpień wiążących te zmienne.

3.2. 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 13. Tutaj powiemy jedynie, że formuła ϕ jest tautologią, jeżeli jest spełniona w każdym niepustym zbiorze przy każdej interpretacji symboli funkcyjnych i relacyjnych. Przy danej interpretacji symboli funkcyjnych i relacyjnych formuła $\forall x\ \phi$ jest spełniona, gdy jest spełniona formuła ϕ dla każdej wartości zmiennej x, zaś formuła $\exists x\ \phi$ jest spełniona, gdy istnieje pewna wartość zmiennej x, dla której formuła ϕ jest spełniona.

Przykład 51. Prawami rachunku kwantyfikatorów są np. *prawa negowania kwantyfikatorów*:

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

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

Przykład 52. Niech ϕ i ψ oznaczają formuły rachunku kwantyfikatorów być może zawierające wolne wystąpienia zmiennej x. Wtedy

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

są prawami rachunku kwantyfikatorów.

Przykład 53. Niech ϕ i ψ oznaczają takie formuły rachunku kwantyfikatorów, że zmienna x nie ma wolnych wystąpień w formule ϕ (lecz może mieć w ψ). Wtedy

$$\begin{array}{ccc}
(\forall x\ (\phi \lor \psi)) & \Leftrightarrow & (\phi \lor \forall x\ \psi) \\
(\forall x\ (\phi \land \psi)) & \Leftrightarrow & (\phi \land \forall x\ \psi) \\
(\exists x\ (\phi \lor \psi)) & \Leftrightarrow & (\phi \lor \exists x\ \psi) \\
(\exists x\ (\phi \land \psi)) & \Leftrightarrow & (\phi \land \exists x\ \psi)
\end{array}$$

są prawami rachunku kwantyfikatorów.

3.3. System dedukcji naturalnej dla rachunku kwantyfikatorów

System dedukcji naturalnej, który poznaliśmy w poprzednim rozdziale, daje się rozszerzyć na rachunek kwantyfikatorów. Nowe reguły dowodzenia to reguły wprowadzania i eliminacji dla obu kwantyfikatorów. Napis $\alpha[x/t]$ oznacza formułę, w której wszystkie wolne wystąpienia zmiennej x zostały zastąpione przez wystąpienia termu t.

Reguły wprowadzania:

$$\frac{\alpha[x/t]}{\exists x\ \alpha}\ (\exists\mathrm{i}) \qquad\qquad \frac{\boxed{\begin{array}{c} x_0 \\ \vdots \\ \alpha[x/x_0] \end{array}}}{\forall x\ \alpha}\ (\forall\mathrm{i})$$

Reguła wprowadzania kwantyfikatora egzystencjalnego jest intuicyjna: aby udowodnić prawdziwość $\exists x\ \alpha$ wystarczy wskazać takie t, dla którego α zachodzi; t może być tutaj dowolnym termem (pod warunkiem, że podstawienie $[x/t]$ jest dopuszczalne w α). W regule wprowadzania kwantyfikatora ogólnego potrzebujemy dodatkowego założenia, że x_0 jest świeżą zmienną — zmienną lokalną, widoczną tylko wewnątrz okna, w którym została zadeklarowana. Reguła ta odpowiada następującej technice dowodzenia: *Weźmy dowolne x_0 i pokażmy, że α zachodzi dla tego x_0. Z dowolności wyboru x_0 wnioskujemy, że α zachodzi dla wszystkich x.*

Reguły eliminacji:

$$\frac{\exists x\ \alpha \qquad \boxed{\begin{array}{c} x_0 \quad \alpha[x/x_0] \\ \vdots \\ \beta \end{array}}}{\beta}\ (\exists\mathrm{e}) \qquad\qquad \frac{\forall x\ \alpha}{\alpha[x/t]}\ (\forall\mathrm{e})$$

W regule eliminacji kwantyfikatora egzystencjalnego znowu mamy założenie, że x_0 jest świeżą zmienną. Odpowiada to takiemu argumentowi: *Skoro wiemy, że zachodzi $\exists x\ \alpha$, to niech x_0 będzie takim elementem, dla którego zachodzi α.* Reguła eliminacji kwantyfikatora ogólnego mówi natomiast, że *skoro α zachodzi dla wszystkich x, to w szczególności zachodzi dla t.* Trzeba przy tym podkreślić, że zmienna x_0 może występować tylko wewnątrz okna, w którym została zadeklarowana (nie może występować np. wcześniej w dowodzie), natomiast t może być dowolnym termem (pod warunkiem, że podstawienie $[x/t]$ jest dopuszczalne, tzn. t nie zawiera zmiennych związanych w α) i zwykle występuje w innych miejscach dowodu.

Przykład 54. Poniżej prezentujemy schemat dowodu implikacji $(\forall x\ (\phi \land \psi)) \Rightarrow (\forall x\ \phi) \land (\forall x\ \psi)$ w systemie naturalnej dedukcji.

$$
\dfrac{\boxed{\begin{array}{c}
\forall x\ (\phi \land \psi) \quad \text{założenie}\\[4pt]
\boxed{\begin{array}{c} x_0 \quad \text{świeża zmienna}\\ \dfrac{\dfrac{\forall x\ (\phi\land\psi)}{\phi[x/x_0]\land\psi[x/x_0]}\ (\forall \mathrm{e})}{\phi[x/x_0]}\ (\land \mathrm{e}_1)\end{array}}
\quad
\boxed{\begin{array}{c} x_1 \quad \text{świeża zmienna}\\ \dfrac{\dfrac{\forall x\ (\phi\land\psi)}{\phi[x/x_1]\land\psi[x/x_1]}\ (\forall \mathrm{e})}{\psi[x/x_1]}\ (\land \mathrm{e}_2)\end{array}}
\\[4pt]
\dfrac{\dfrac{}{\forall x\ \phi}\ (\forall \mathrm{i}) \qquad \dfrac{}{\forall x\ \psi}\ (\forall \mathrm{i})}{(\forall x\ \phi)\land(\forall x\ \psi)}\ (\land \mathrm{i})
\end{array}}}{(\forall x\ (\phi \land \psi)) \Rightarrow (\forall x\ \phi) \land (\forall x\ \psi)}\ (\Rightarrow \mathrm{i})
$$

Kolejny przykład to schemat dowodu jednej implikacji z praw De Morgana: $\neg\exists x\ \phi \Rightarrow \forall x\ \neg\phi$.

$$
\dfrac{\boxed{\begin{array}{c}
\neg\exists x\ \phi \quad \text{założenie}\\[4pt]
\boxed{\begin{array}{c}
x_0 \quad \text{świeża zmienna}\\[4pt]
\boxed{\begin{array}{c}
\phi[x/x_0] \quad \text{założenie}\\
\dfrac{\dfrac{\phi[x/x_0]}{\exists x\ \phi}\ (\exists \mathrm{i}) \qquad \neg\exists x\ \phi}{\bot}\ (\neg \mathrm{e})
\end{array}}\\
\dfrac{}{\neg\phi[x/x_0]}\ (\neg \mathrm{i})
\end{array}}\\
\dfrac{}{\forall x\ \neg\phi}\ (\forall \mathrm{i})
\end{array}}}{\neg\exists x\ \phi \Rightarrow \forall x\ \neg\phi}\ (\Rightarrow \mathrm{i})
$$

W języku naturalnym ten dowód można przeczytać tak: *Załóżmy, że* $\neg\exists x\ \phi$ *jest prawdą i weźmy dowolne* x_0*. Gdyby* $\phi(x_0)$ *było prawdą, to istniałby taki* x*, dla którego* $\phi(x)$ *zachodzi, co przeczy prawdziwości* $\neg\exists x\ \phi$*. Zatem* $\neg\phi(x_0)$ *jest prawdą. Z dowolności wyboru* x_0 *wnioskujemy, że* $\forall x\ \neg\phi$ *jest prawdą, co kończy dowód.*

W powyższych przykładach ϕ i ψ były zmiennymi oznaczającymi dowolne formuły. W następnym przykładzie p jest symbolem relacyjnym, co trochę upraszcza notację, bo zamiast $p(x)[x/x_0]$ możemy po prostu napisać $p(x_0)$.

Przykład 55. Pokażemy dowód formuły $(\exists x\ p(x)) \Rightarrow \neg\forall x.\neg p(x)$ w systemie naturalnej dedukcji.

$$\dfrac{\boxed{\begin{array}{c} \exists x\ p(x) \quad \text{założenie} \\ \boxed{\begin{array}{c} \forall x\ \neg p(x) \quad \text{założenie} \\ \dfrac{\exists x\ p(x) \qquad \boxed{\begin{array}{c} x_0 \text{ świeża zmienna; } p(x_0) \text{ założenie} \\ \dfrac{\dfrac{\forall x\ \neg p(x)}{\neg p(x_0)}\,(\forall \mathrm{e}) \qquad p(x_0)}{\bot}\,(\neg \mathrm{e}) \end{array}}}{\bot}\,(\exists \mathrm{e}) \end{array}} \\ \dfrac{}{\neg\forall x\ \neg p(x)}\,(\neg \mathrm{i}) \end{array}}}{(\exists x\ p(x)) \Rightarrow \neg\forall x.\neg p(x)}\,(\Rightarrow \mathrm{i})$$

Zadanie 137. Podaj w systemie dedukcji naturalnej schemat dowodu drugiej implikacji powyższego prawa De Morgana, czyli implikacji $(\forall x\ \neg\phi) \Rightarrow \neg\exists x\ \phi$.

Zadanie 138. Podaj w systemie dedukcji naturalnej schemat dowodu implikacji $(\exists x \neg\phi) \Rightarrow \neg\forall x \phi$.

Zadanie 139. Podaj w systemie dedukcji naturalnej schemat dowodu implikacji $\neg(\forall x \phi) \Rightarrow \exists x \neg\phi$.

Wskazówka: Tego się nie da zrobić w sposób konstruktywny. Trzeba skorzystać z prawa wyłączonego środka lub z eliminacji podwójnej negacji.

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

Zadanie 140. $(\forall x\ (\phi \vee \psi)) \Rightarrow (\forall x\ \phi) \vee (\forall x\ \psi)$

Zadanie 141. $(\forall x\, \phi) \vee (\forall x\, \psi) \Rightarrow (\forall x\, (\phi \vee \psi))$

Zadanie 142. $(\forall x\, (\phi \wedge \psi)) \Rightarrow (\forall x\, \phi) \wedge (\forall x\, \psi)$

Zadanie 143. $((\forall x\, \phi) \Rightarrow (\forall x\, \psi)) \Rightarrow (\forall x\, (\phi \Rightarrow \psi))$

Zadanie 144. $(\forall x\, (\phi \Rightarrow \psi)) \Rightarrow (\exists x\, \phi) \Rightarrow (\forall x\, \psi)$

Zadanie 145. $((\exists x\, \phi) \Rightarrow (\forall x\, \psi)) \Rightarrow (\forall x\, (\phi \Rightarrow \psi))$

Zadanie 146. $(\exists x\, \phi) \wedge (\exists x\, \psi) \Rightarrow (\exists x\, (\phi \wedge \psi))$

Zadanie 147. $(\exists x\, (\phi \wedge \psi)) \Rightarrow (\exists x\, \phi) \wedge (\exists x\, \psi)$

Zadanie 148. $((\exists x\, \phi) \Rightarrow (\exists x\, \psi)) \Rightarrow (\exists x\, (\phi \Rightarrow \psi))$

Zadanie 149. $(\exists x\, (\phi \Rightarrow \psi)) \Rightarrow (\exists x\, \phi) \Rightarrow (\exists x\, \psi)$

Zadanie 150. $(\forall x\, \phi) \Rightarrow ((\exists x\, \psi) \Rightarrow (\exists x\, (\phi \Rightarrow \psi)))$

Zadanie 151. $(\exists x\, (\phi \Rightarrow \psi)) \Rightarrow (\forall x\, \phi) \Rightarrow (\exists x\, \psi)$

Zadanie 152. $((\forall x\, \phi) \Leftrightarrow \neg(\forall x\, \psi)) \Rightarrow \exists x\, (\phi \Leftrightarrow \neg\psi)$

Zadanie 153. $(\exists x\, (\phi \Leftrightarrow \neg\psi)) \Rightarrow ((\forall x\, \phi) \Leftrightarrow \neg(\forall x\, \psi))$

Zadanie 154. $(\forall x\, \phi) \Rightarrow \exists x\, \phi$

Zadanie 155. $(\exists x\, \phi) \Rightarrow \forall x\, \phi$

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

Zadanie 156. $(\forall x\, \exists y\, \phi) \Rightarrow (\exists y\, \forall x\, \phi)$

Zadanie 157. $(\exists y\, \forall x\, \phi) \Rightarrow (\forall x\, \exists y\, \phi)$

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

Zadanie 158. $\forall x\, (\phi \Rightarrow \psi)$ oraz $\phi \Rightarrow (\forall x\, \psi)$

Zadanie 159. $\forall x\, (\phi \Rightarrow \psi)$ oraz $\phi \Rightarrow (\exists x\, \psi)$

Zadanie 160. $\forall x\, (\psi \Rightarrow \phi)$ oraz $(\forall x\, \psi) \Rightarrow \phi$

Zadanie 161. $\forall x\, (\psi \Rightarrow \phi)$ oraz $(\exists x\, \psi) \Rightarrow \phi$

Zadanie 162. $\forall x\, (\phi \Leftrightarrow \psi)$ oraz $\phi \Leftrightarrow (\forall x\, \psi)$

Zadanie 163. $\forall x\, (\phi \Leftrightarrow \psi)$ oraz $\phi \Leftrightarrow (\exists x\, \psi)$

Zadanie 164. $\exists x\, (\phi \Rightarrow \psi)$ oraz $\phi \Rightarrow (\exists x\, \psi)$

Zadanie 165. $\exists x\, (\phi \Rightarrow \psi)$ oraz $\phi \Rightarrow (\forall x\, \psi)$

Zadanie 166. $\exists x\, (\psi \Rightarrow \phi)$ oraz $(\exists x\, \psi) \Rightarrow \phi$

Zadanie 167. $\exists x\, (\psi \Rightarrow \phi)$ oraz $(\forall x\, \psi) \Rightarrow \phi$

Zadanie 168. $\exists x\, (\phi \Leftrightarrow \psi)$ oraz $\phi \Leftrightarrow (\exists x\, \psi)$

Zadanie 169. $\exists x\, (\phi \Leftrightarrow \psi)$ oraz $\phi \Leftrightarrow (\forall x\, \psi)$

3.4. Formalizacja wypowiedzi w języku rachunku kwantyfikatorów

Zadanie 170. Następująca formuła mówi, że funkcja $f : \mathbb{R} \to \mathbb{R}$ jest *ciągła*.

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

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

Zadanie 171. Następująca formuła mówi, że liczba $g \in \mathbb{R}$ jest *granicą* (w sensie Cauchy'ego) funkcji $f : \mathbb{R} \to \mathbb{R}$ w punkcie x_0.

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

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

Formuła ϕ jest w *postaci normalnej*[1], 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, podobnie jak $\forall x{>}0\ \exists y\ x = y$.

[1] W literaturze mówi się o formułach, w których wszystkie kwantyfikatory są na początku, że są w *preneksowej* postaci normalnej. Tutaj dodatkowo wymagamy, aby formuła ψ była w negacyjnej postaci normalnej.

Zadanie 172. Dla każdej z formuł poniżej podaj równoważną formułę w postaci normalnej

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

Zadanie 173. Funkcja $f : \mathbb{N} \to \mathbb{N}$ jest *słabo rosnąca*, jeśli prawdziwa jest formuła

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

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

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

Zapisz poniższe zdania jako formuły w postaci normalnej:

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

Zadanie 174. Przy pomocy zmiennych, stałych 0 i 1, symboli $=, \leq, +, \times$, spójników logicznych i kwantyfikatorów zapisz następujące formuły dotyczące liczb naturalnych:

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

Wskaż zmienne wolne i związane w tych formułach.
Wskazówka: Możesz definiować makra podobne do makr z języka C. Np. możesz zdefiniować makro $\mathit{dzielnik}(x, y)$ jako $\exists d.\ x \times d = y$. Wtedy formułę „$x$ jest wspólnym dzielnikiem y i z” zapiszemy jako $\mathit{dzielnik}(x, y) \wedge \mathit{dzielnik}(x, z)$.

Zadanie 175. 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 174 oraz dodatkowo symbolu potęgowania $\uparrow$, zapisz zdanie równoważne zdaniu „dla każdej liczby naturalnej m istnieje taka liczba n, że $g^n(m) = 1$”, gdzie g^n oznacza funkcję g złożoną ze sobą n razy, na przykład $g^2(3) = 5$. *Wskazówka:* ciąg skończony liczb naturalnych $a_1, a_2, \ldots a_m$ 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 176. Używając tylko kwantyfikatorów, zmiennych, nawiasów, spójników logicznych oraz symboli $0, 1, 2, \in, \mathbb{N}, +, \times, =$ 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 177. Liczbę naturalną q nazywamy *liczbą bliźniaczą*, jeżeli liczby q oraz $q + 2$ są pierwsze. Używając symboli $+, \times, 0, 1, 2, =$ oraz nawiasów, zmiennych, kwantyfikatorów i spójników logicznych zapisz formalnie zdanie: „Istnieje największa liczba bliźniacza taka, że pomiędzy nią a poprzednią liczbą bliźniaczą jest co najwyżej jedna liczba pierwsza.”

Zadanie 178. Niech na pewnym skończonym zbiorze X będzie określona binarna relacja R. Mówimy, że zbiór X z relacją R jest *hamiltonowski*, jeśli istnieje taki ciąg elementów zbioru X, że każdy element zbioru X występuje w tym ciągu dokładnie raz, każde dwa kolejne elementy ciągu są ze sobą w relacji R, oraz ostatni element ciągu jest w relacji z pierwszym elementem ciągu. Używając jedynie poniższych słów i zwrotów (z odpowiednią odmianą) 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 179. 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 P, D oraz Z, gdzie

$$\begin{array}{rl} P(x) & \text{oznacza, że } x \text{ jest panią,} \\ D(x) & \text{oznacza, że } x \text{ jest dżentelmenem,} \\ Z(x, y) & \text{oznacza, że } x \text{ zna } y, \end{array}$$

oraz równości $=$ i spójników logicznych oraz kwantyfikatorów.

4

Zbiory

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

Aksjomat 56 (zasada ekstensjonalności). Dwa zbiory są *równe*, jeżeli zawierają dokładnie te same elementy, tj. $A = B$ wtedy i tylko wtedy, gdy prawdziwa jest formuła

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

Definicja 57. *Zbiór pusty* $\emptyset$ jest zbiorem nie zawierającym żadnego elementu. Prawdziwa jest formuła

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

Aksjomat 58 (zbioru pustego). Zbiór pusty istnieje.

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

Nie będziemy tu wymieniać wszystkich aksjomatów teorii mnogości. Aksjomaty gwarantują między innymi istnienie zbioru potęgowego (Definicja 63), sumy zbiorów (Definicje 64 i 69) czy zbioru liczb naturalnych, ale nie będziemy wchodzić w szczegółowe rozważania na ten temat. Zainteresowanych czytelników odsyłamy do podręczników do teorii mnogości wymienionych w rozdziale B.

Definicja 59. Zbiór A jest *podzbiorem* zbioru B, co będziemy zapisywać $A \subseteq B$, jeżeli B zawiera wszystkie elementy zbioru A, tj. zachodzi

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

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

Przykład 60. Pokażemy, że dla dowolnego zbioru A zachodzi inkluzja $\emptyset \subseteq A$.

Dowód. Niech A będzie dowolnym zbiorem. Z definicji zawierania wystarczy pokazać, że dla wszystkich x, jeśli $x \in \emptyset$, to $x \in A$. Weźmy więc dowolne x. Przez kontrapozycję wystarczy pokazać, że jeśli $x \notin A$ to $x \notin \emptyset$. Załóżmy więc, że $x \notin A$. Z definicji zbioru pustego mamy $x \notin \emptyset$, co kończy dowód. ■

W powyższym dowodzie skorzystaliśmy z niekonstruktywnej reguły wnioskowania przez kontrapozycję (porównaj Zad. 132): zamiast dowodzić implikacji $x \in \emptyset \Rightarrow x \in A$ udowodniliśmy $x \notin A \Rightarrow x \notin \emptyset$. Implikację $x \in \emptyset \Rightarrow x \in A$ można także udowodnić konstruktywnie, choć dowód jest mniej intuicyjny: Załóżmy, że $x \in \emptyset$. Z definicji zbioru pustego mamy $x \notin \emptyset$, co daje sprzeczność, a z niej wynika, że $x \in A$.

Definicja 61. Napisy $\{x \mid \phi\}$ i $\{x : \phi\}$ oznaczają zbiór tych elementów x, które spełniają formułę ϕ. Będziemy również pisać $x \in A \stackrel{\text{df}}{\Leftrightarrow} \phi$ zamiast $A = \{x \mid \phi\}$ oraz $\{f(x) \mid \phi\}$ zamiast $\{y \mid \exists x\, \phi \wedge (y = f(x))\}$.

W ogólnym przypadku zbiór $\{x \mid \phi\}$ wcale nie musi istnieć, jednak w niniejszej książeczce nie spotkamy się z taką sytuacją i nie będziemy wchodzić w szczegółowe rozważania na ten temat. Zainteresowanych czytelników zachęcamy do zapoznania się z antynomią Russella i jej konsekwencjami.

Przykład 62. Napis $\{n \mid \exists m{\in}\mathbb{N}\, (n = 3m)\}$ oznacza zbiór liczb naturalnych podzielnych przez 3. Ten sam zbiór możemy krócej zapisać jako $\{3m \mid m \in \mathbb{N}\}$.

Definicja 63. Zbiór, którego elementy są zbiorami, nazywamy *rodziną zbiorów*. Rodzinę wszystkich podzbiorów zbioru A nazywamy *zbiorem potęgowym* zbioru A i oznaczamy $\mathcal{P}(A)$. Możemy napisać:

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

4.1. Działania na zbiorach

Definicja 64. Na zbiorach wprowadzamy operacje *sumy* $\cup$, *przekroju* $\cap$ i *różnicy* $\setminus$:

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

Powyższe operacje mają wiele ciekawych własności. Dla przykładu:

Fakt 65 (prawa rozdzielności).

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

Udowodnimy pierwsze z nich.

Dowód. Na mocy prawa ekstensjonalności wystarczy pokazać, że dla każdego x zachodzi

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

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

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

jest równoważna formule

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

Następnie korzystając z definicji sumy zbiorów otrzymujemy równoważną formułę

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

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

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

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

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

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

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

Korzystając dwukrotnie z definicji różnicy zbiorów dostajemy

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

Na mocy definicji przekroju zbiorów mamy ostatecznie

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

Twierdzenie jest zatem udowodnione. ∎

Czysto syntaktyczne przekształcanie formuł (czyli mechaniczne rachunki na formułach bez zastanawiania się, co te formuły oznaczają) takie jak w powyższym dowodzie czasem okazuje się kłopotliwe. Rozumowanie semantyczne, oparte na znaczeniu formuł, często jest wygodniejsze i mniej podatne na błędy. Następujący przykład ilustruje tę metodę.

Przykład 66. Pokażemy, że dla dowolnych zbiorów A, B i C zachodzi inkluzja

$$(A \cup B) \setminus C \subseteq A \cup (B \setminus C).$$

Dowód. Rozważmy dowolne zbiory A, B i C oraz dowolny element x i załóżmy, że $x \in (A \cup B) \setminus C$. Z definicji sumy i różnicy zbiorów otrzymujemy wtedy, że $x \in A$ lub $x \in B$, oraz że $x \notin C$. Rozważmy teraz dwa przypadki.

Przypadek 1: $x \in A$. W tym przypadku oczywiście $x \in A \cup (B \setminus C)$.

Przypadek 2: $x \in B$. W tym przypadku z warunku $x \notin C$ wnioskujemy, że $x \in (B \setminus C)$, a stąd $x \in A \cup (B \setminus C)$.

W obu (czyli we wszystkich możliwych) przypadkach otrzymaliśmy, że $x \in A \cup (B \setminus C)$, a to kończy dowód naszej inkluzji. ∎

Przykład 67. Pokażemy, że dla dowolnych zbiorów A, B i C zachodzi implikacja *jeśli* $A \cap B = A \cap C$ *oraz* $A \cup B = A \cup C$ *to* $B = C$.

Dowód. Załóżmy, że $A \cap B = A \cap C$ oraz $A \cup B = A \cup C$. Do dowodu, że $B = C$ wystarczy pokazać dwie inkluzje: $B \subseteq C$ oraz $C \subseteq B$. Pokażemy najpierw, że $B \subseteq C$. Weźmy więc dowolne $x \in B$ i rozważmy dwa przypadki:

1: $x \in A$. W tym przypadku $x \in A \cap B$, z równości $A \cap B = A \cap C$ otrzymujemy $x \in A \cap C$, a stąd $x \in C$.

2: $x \notin A$. W tym przypadku $x \in A \cup B$, z równości $A \cup B = A \cup C$ otrzymujemy $x \in A \cup C$ i z faktu, że $x \notin A$ wnioskujemy, że $x \in C$.

W obu przypadkach otrzymaliśmy $x \in C$, co kończy dowód inkluzji $B \subseteq C$.

Dowód inkluzji $C \subseteq B$ jest symetryczny: wystarczy w dowodzie inkluzji $B \subseteq C$ zamienić miejscami wszystkie wystąpienia B i C. ∎

Zadanie 180. Pokaż, że dla dowolnych zbiorów A, B i C zachodzą podane równości.

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

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

Zadanie 181. Pokaż, że dla dowolnych zbiorów A, B, C i D zachodzą podane równości.

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

Zadanie 182. Czy dla dowolnych zbiorów A, B i C zachodzą podane równości?

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

Zadanie 183. Pokaż, że dla dowolnych takich zbiorów A, B, C i D, że $A \subseteq B$ i $C \subseteq D$ zachodzą podane inkluzje.

$$A \cup C \subseteq B \cup D$$

$$\begin{array}{rcl} A \cap C & \subseteq & B \cap D \\ A \setminus D & \subseteq & B \setminus C \end{array}$$

Zadanie 184. Wykaż, że dla dowolnych zbiorów A, B, C i D zachodzi:

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

Zadanie 185. Czy dla dowolnych zbiorów A, B i C zachodzą poniższe inkluzje?

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

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

Zadanie 186. $(A \cup B) \setminus C = (A \setminus C) \cup B$

Zadanie 187. $(A \cup B) \setminus (B \cap C) = A \cap C$

Zadanie 188. $((A \cap B) \cup C) \setminus A = (A \cap B) \setminus C$

Zadanie 189. $(A \setminus C) \cup B = A \cup B$

Zadanie 190. $(A \cap B) \cup (C \cap B) = B$

Zadanie 191. $(A \cup B) \cap (C \cup B) = B$

Zadanie 192. Pokaż, że jeżeli dla pewnych zbiorów A i B jest $A \setminus B = B \setminus A$, to $A = B$.

Zadanie 193. Udowodnij, że dla dowolnych zbiorów A i B następujące formuły są równoważne

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

Zadanie 194. Niech A, B i C będą dowolnymi zbiorami. Udowodnij, że $A \subseteq A \cup B$ i $B \subseteq A \cup B$. Udowodnij, że jeśli $A \subseteq C$ oraz $B \subseteq C$, to $A \cup B \subseteq C$. Innymi słowy suma zbiorów A i B jest najmniejszym (w sensie inkluzji) zbiorem zawierającym zbiory A i B.

Zadanie 195. Niech A, B i C będą dowolnymi zbiorami. Udowodnij, że $A \cap B \subseteq A$ i $A \cap B \subseteq B$. Udowodnij, że jeśli $C \subseteq A$ oraz $C \subseteq B$, to $C \subseteq A \cap B$. Innymi słowy przekrój zbiorów A i B jest największym (w sensie inkluzji) zbiorem zawartym w zbiorach A i B.

Zadanie 196. Niech A, B i C będą dowolnymi zbiorami. Udowodnij, że $A \setminus B \subseteq A$ i $(A \setminus B) \cap B = \emptyset$. Udowodnij, że jeśli $C \subseteq A$ oraz $C \cap B = \emptyset$, to $C \subseteq A \setminus B$. Innymi słowy różnica zbiorów A i B jest największym (w sensie inkluzji) zbiorem zawartym w A i rozłącznym z B.

Definicja 68. *Różnicę symetryczną* $\dot{-}$ zbiorów A i B definiujemy następująco:

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

Zadanie 197. 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 198. Udowodnij, że

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

Zadanie 199. Wśród poniższych zdań wskaż zdania prawdziwe i udowodnij je. Dla pozostałych zdań podaj kontrprzykłady dowodzące, że zdania te nie są prawdziwe.

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

Zadanie 200. Czy istnieją niepuste zbiory A i B takie, że

$$A \subseteq A \dot{-} B \subseteq A \setminus B?$$

Zadanie 201. Czy dla dowolnych zbiorów A i B zachodzą równości:

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

4.2. Operacje nieskończone na zbiorach

Dwuargumentowe operacje sumy i przekroju zbiorów można rozszerzyć na dowolne rodziny zbiorów.

Definicja 69. Suma wszystkich zbiorów z rodziny $\mathcal{A}$ jest zbiorem zawierającym elementy występujące w którymkolwiek ze zbiorów rodziny $\mathcal{A}$. Podobnie przekrój tej rodziny jest zbiorem zawierającym elementy występujące w każdym zbiorze rodziny $\mathcal{A}$. Formalnie:

$$\begin{aligned} \bigcup \mathcal{A} &= \{x \mid \exists X \in \mathcal{A}\ (x \in X)\}, \\ \bigcap \mathcal{A} &= \{x \mid \forall X \in \mathcal{A}\ (x \in X)\}. \end{aligned}$$

Czasem chcielibyśmy nazwać zbiory należące do rodziny zbiorów tak, aby móc wykonywać na nich pewne operacje. Służą do tego *indeksowane rodziny zbiorów*.

Definicja 70. Rodziną zbiorów indeksowaną elementami zbioru S nazywamy odwzorowanie, które każdemu elementowi $s \in S$ przyporządkowuje pewien zbiór A_s. Taką rodzinę oznaczamy $\{A_s\}_{s\in S}$ lub $\{A_s \mid s \in S\}$. Rodziną zbiorów $\{A_{s,t}\}_{\substack{t\in T\\ s\in S}}$ indeksowaną elementami dwóch zbiorów S i T nazywamy odwzorowanie, które każdej parze $\langle s, t\rangle$, gdzie $s \in S$ oraz $t \in T$ przyporządkowuje pewien zbiór $A_{s,t}$. Jeżeli $S = \{i{\in}\mathbb{N} \mid i{\geq}n\}$, to zamiast $\{A_i\}_{i\in S}$ piszemy też $\{A_i\}_{i=n}^{\infty}$. Jeżeli $S = \{n, \dots, m\}$, to zamiast $\{A_i\}_{i\in S}$ piszemy też $\{A_i\}_{i=n}^{m}$.

Operacje sumy i przekroju w oczywisty sposób uogólniają się na indeksowane rodziny zbiorów. Suma wszystkich zbiorów z rodziny $\{A_s\}_{s\in S}$ jest zbiorem zawierającym elementy występujące w którymkolwiek ze zbiorów A_s. Podobnie przekrój tej rodziny jest zbiorem zawierającym elementy występujące w każdym ze zbiorów A_s. Formalnie:

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

Zadanie 202. Rozważmy zbiór $A_{s,t} = \{x \in \mathbb{R} \mid s{\leq}x \wedge x{\leq}t\}$, gdzie $s, t \in \mathbb{R}$ są dowolnymi liczbami. Dla każdego ze zbiorów poniżej wylicz jego wartość.

1. $\bigcup\limits_{t\geq 2} A_{0,t}$
2. $\bigcap\limits_{t\geq 2} A_{1,t}$

3. $\bigcup_{t\geq 2} A_{s,t}$
4. $\bigcap_{t\geq 2} A_{s,t}$
5. $\bigcup_{s<0}\bigcap_{t\geq 2} A_{s,t}$
6. $\bigcap_{s<0}\bigcup_{t\geq 2} A_{s,t}$

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

Zadanie 203. $\bigcup_{t\in T}(A_t\cup B_t)=\bigcup_{t\in T}A_t\cup\bigcup_{t\in T}B_t$

Zadanie 204. $\bigcap_{t\in T}(A_t\cap B_t)=\bigcap_{t\in T}A_t\cap\bigcap_{t\in T}B_t$

Zadanie 205. $\bigcup_{t\in T}(A_t\cap B_t)\subseteq\bigcup_{t\in T}A_t\cap\bigcup_{t\in T}B_t$

Zadanie 206. $\bigcap_{t\in T}A_t\cup\bigcap_{t\in T}B_t\subseteq\bigcap_{t\in T}(A_t\cup B_t)$

Zadanie 207. $\bigcap_{t\in T}A_t\cup\bigcap_{t\in T}B_t\subseteq\bigcup_{t\in T}(A_t\cup B_t)$

Zadanie 208. $\bigcap_{t\in T}(A_t\cup B_t)\subseteq\bigcup_{t\in T}A_t\cup\bigcup_{t\in T}B_t$

Zadanie 209. $\bigcap_{t,s\in T}(A_t\cup B_s)\subseteq\bigcap_{t\in T}(A_t\cup B_t)$

Zadanie 210. $\bigcup_{t\in T}(A_t\cap B_t)\subseteq\bigcup_{t,s\in T}(A_t\cap B_s)$

Zadanie 211. $\bigcup_{t\in T}(A_t\setminus B_t)\subseteq\bigcup_{t\in T}A_t\setminus\bigcap_{t\in T}B_t$

Zadanie 212. $\bigcap_{t\in T}(A_t\setminus B_t)=\bigcap_{t\in T}A_t\setminus\bigcup_{t\in T}B_t$

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

Zadanie 213. $\bigcup_{t\in T}(A\cup B_t)=A\cup\bigcup_{t\in T}B_t$

Zadanie 214. $\bigcap_{t\in T}(A \cup B_t) = A \cup \bigcap_{t\in T} B_t$

Zadanie 215. $\bigcup_{t\in T}(A \cap B_t) = A \cap \bigcup_{t\in T} B_t$

Zadanie 216. $\bigcap_{t\in T}(A \cap B_t) = A \cap \bigcap_{t\in T} B_t$

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

Zadanie 217. $\bigcup_{t\in T}\bigcup_{s\in S} A_{t,s} = \bigcup_{s\in S}\bigcup_{t\in T} A_{t,s}$

Zadanie 218. $\bigcap_{t\in T}\bigcap_{s\in S} A_{t,s} = \bigcap_{s\in S}\bigcap_{t\in T} A_{t,s}$

Zadanie 219. $\bigcup_{t\in T}\bigcap_{s\in S} A_{t,s} \subseteq \bigcap_{s\in S}\bigcup_{t\in T} A_{t,s}$

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

Zadanie 220. $\bigcup_{t\in T} A_{t,t} \subseteq \bigcup_{t\in T}\bigcup_{s\in T} A_{t,s}$

Zadanie 221. $\bigcap_{t\in T}\bigcap_{s\in T} A_{t,s} \subseteq \bigcap_{t\in T} A_{t,t}$

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

Zadanie 222. $\bigcup_{t\in T} A_t \cup \bigcup_{s\in S} B_s = \bigcup_{t\in T}\bigcup_{s\in S}(A_t \cup B_s)$

Zadanie 223. $\bigcup_{t\in T} A_t \cap \bigcup_{s\in S} B_s = \bigcup_{t\in T}\bigcup_{s\in S}(A_t \cap B_s)$

Zadanie 224. $\bigcap_{t\in T} A_t \cup \bigcap_{s\in S} B_s = \bigcap_{t\in T}\bigcap_{s\in S}(A_t \cup B_s)$

Zadanie 225. $\bigcap_{t\in T} A_t \cap \bigcap_{s\in S} B_s = \bigcap_{t\in T}\bigcap_{s\in S}(A_t \cap B_s)$

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

Zadanie 226. $\bigcap_{n=0}^{\infty} A_n \subseteq \bigcup_{n=0}^{\infty} \bigcap_{k=n}^{\infty} A_k$

Zadanie 227. $\bigcup_{n=0}^{\infty} \bigcap_{k=n}^{\infty} A_k \subseteq \bigcap_{n=0}^{\infty} \bigcup_{k=n}^{\infty} A_k$

Zadanie 228. $\bigcap_{n=0}^{\infty} \bigcup_{k=n}^{\infty} A_k \subseteq \bigcup_{n=0}^{\infty} A_n$

Zadanie 229. $\bigcup_{n=0}^{\infty} A_{n+1} \subseteq \bigcup_{n=0}^{\infty} (A_{n+1} \setminus \bigcup_{m=1}^{n} A_m)$

Zadanie 230. $\bigcup_{n=0}^{m} A_n = \Big(\bigcup_{n=0}^{m-1} (A_n \setminus A_{n+1})\Big) \cup (A_m \setminus A_0) \cup \bigcap_{n=0}^{m} A_n$

Zadanie 231. $\bigcup_{n=0}^{\infty} A_n = \Big(\big(\bigcup_{n=0}^{\infty} A_n\big) \setminus A_0\Big) \cup \Big(\bigcup_{n=1}^{\infty} (A_n \setminus A_{n+1})\Big) \cup \bigcap_{n=0}^{\infty} A_n$

Definicja 71. 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 232. Udowodnij, że jeśli $\{A_n\}_{n\in\mathbb{N}}$ i $\{B_n\}_{n\in\mathbb{N}}$ są zstępującymi rodzinami zbiorów, to

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

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

Zadanie 233. Udowodnij, że jeśli $\{A_n\}_{n\in\mathbb{N}}$ i $\{B_n\}_{n\in\mathbb{N}}$ są wstępującymi rodzinami zbiorów, to

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

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

Zadanie 234. 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 235. Udowodnij, że jeśli $\{A_n\}_{n\in\mathbb{N}}$ jest zstępującą rodziną zbiorów, to

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

Zadanie 236. Udowodnij, że jeśli $\{A_n\}_{n\in\mathbb{N}}$ jest wstępującą rodziną zbiorów, to

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

Zadanie 237. Udowodnij, że jeśli $\{A_n\}_{n\in\mathbb{N}}$ jest zstępującą rodziną zbiorów, to

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

Zadanie 238. Udowodnij, że jeśli $\{A_n\}_{n\in\mathbb{N}}$ jest wstępującą rodziną zbiorów, to

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

Zadanie 239. Niech $\{A_{n,m}\}_{n,m=0}^{\infty}$ będzie rodziną zbiorów indeksowaną parami liczb naturalnych. Pokaż, że jeśli

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

dla wszelkich n i m, to

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

Zadanie 240. Dane są rodziny zbiorów $\{A_i\}_{i\in\mathbb{N}}$ i $\{B_i\}_{i\in\mathbb{N}}$. Wiadomo, że dla każdego i istnieje k takie, że $A_i \subseteq \bigcup_{j=0}^{k} B_j$. Udowodnij, że:

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

Zadanie 241. Rozważmy dowolną rodzinę zbiorów $\mathcal{A}$.

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

Zadanie 242. 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 $\{W_i : i \in \mathbb{N}\}$ będzie wstępującą rodziną zbiorów wypukłych. Pokaż, że zbiór $W = \bigcup_{i \in \mathbb{N}} W_i$ jest wypukły.

5

Relacje

5.1. Para uporządkowana i iloczyn (produkt) kartezjański

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

Aksjomat 72. $\langle a, b\rangle = \langle c, d\rangle$ wtedy i tylko wtedy, gdy $a = c$ oraz $b = d$.

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

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

Zadanie 243. Udowodnij, że zdefiniowana wyżej para $\langle a, b\rangle$ spełnia aksjomat 72.

Definicja 73. *Iloczynem kartezjańskim* dwóch zbiorów nazywamy zbiór wszystkich par uporządkowanych złożonych z elementów tych zbiorów:

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

Czasem zamiast $A \times A$ będziemy pisać A^2.

Przykład 74. Pokażemy, że dla dowolnych zbiorów A i B zachodzi równoważność: $A \times B = \emptyset$ wtedy i tylko wtedy, gdy $A = \emptyset$ lub $B = \emptyset$.

Dowód. Weźmy dowolne zbiory A i B. Wystarczy pokazać dwie implikacje: ($\Rightarrow$) jeśli $A \times B = \emptyset$ to $A = \emptyset$ lub $B \neq \emptyset$, oraz ($\Leftarrow$) jeśli $A = \emptyset$ lub $B = \emptyset$ to $A \times B = \emptyset$.

Dowód ($\Rightarrow$): Przez kontrapozycję wystarczy pokazać, że jeśli $A \neq \emptyset$ i $B \neq \emptyset$ to $A \times B \neq \emptyset$. Załóżmy więc, że $A \neq \emptyset$ i $B \neq \emptyset$. Wtedy istnieją elementy $a \in A$ oraz $b \in B$, a stąd $\langle a, b\rangle \in A \times B$. Zatem $A \times B \neq \emptyset$.

Dowód ($\Leftarrow$): Załóżmy, że $A = \emptyset$ lub $B = \emptyset$. Weźmy dowolne x. Gdyby $x \in A \times B$, to istniałyby takie elementy $a \in A$ oraz $b \in B$, że $x = \langle a, b\rangle$. Wtedy $A \neq \emptyset$ i $B \neq \emptyset$, co przeczy założeniu, że $A = \emptyset$ lub $B = \emptyset$. Zatem $x \notin A \times B$. Ponieważ żaden element nie należy do $A \times B$, z definicji zbioru pustego otrzymujemy $A \times B = \emptyset$. ■

Zadanie 244. Uzupełnij i udowodnij podane wzory.

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

Zadanie 245. Udowodnij, że dla dowolnych zbiorów A i B równość $A \times B = B \times A$ zachodzi wtedy i tylko wtedy, gdy

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

Zadanie 246. Udowodnij, że jeżeli $A \times B = C \times D$, to

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

Zadanie 247. Załóżmy, że $B \subseteq Y$. Czy dla dowolnych zbiorów A i X zachodzi równość

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

5.2. Relacje

Definicja 75. Dowolny podzbiór $R \subseteq A \times B$ produktu kartezjańskiego zbiorów A i B nazywamy *relacją dwuargumentową* (*binarną*). Jeśli $\langle a, b\rangle \in R$, to mówimy, że elementy $a \in A$ i $b \in B$ *są ze sobą w relacji* R. Zamiast pisać $\langle a, b\rangle \in R$, piszemy też niekiedy aRb lub $R(a, b)$. Podzbiory $A \times A$ są *binarnymi relacjami na zbiorze* A.

Przykład 76. Relacjami binarnymi są:

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

Przykład 77. W teorii grafów relację binarną na zbiorze A nazywa się *grafem skierowanym* o wierzchołkach w zbiorze A.

Zadanie 248. Podaj intuicyjny sens poniższych relacji dwuargumentowych na zbiorze $\{1, 2, 3, 4, 5, 6\}$:

a)

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

b)

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

c)

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

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

Definicja 78. Relacja $R \subseteq A \times A$ jest

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

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

Zadanie 249. 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 takich relacji R_1, R_2, R_3 i R_4, że zachodzi

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

Zadanie 250. Na zbiorze $\mathcal{P}(\mathbb{N})$ wszystkich podzbiorów zbioru liczb naturalnych wprowadzamy relację binarną R wzorem

$$R(X, Y) \stackrel{\text{df}}{\Leftrightarrow} \exists m \forall n{>}m \ n \in X \Leftrightarrow n \in Y.$$

Udowodnij, że R jest relacją równoważności.

5.3. 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 79. $\langle a_1, \ldots, a_n \rangle = \langle b_1, \ldots, b_n \rangle \ \Leftrightarrow \ a_1 = b_1 \wedge \ldots \wedge a_n = b_n.$

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:

$$\langle a_0, a_1, \ldots, a_n \rangle \quad = \quad \langle a_0, \langle a_1, \ldots, a_n \rangle \rangle$$

Definicja 80. W oczywisty sposób uogólniamy pojęcie *produktu* na n zbiorów:

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

Dla $n \geq 2$ zamiast

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

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

Definicja 81. *Relacją* n-argumentową nazywamy dowolny podzbiór produktu n zbiorów.

Dla przykładu

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

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

Zadanie 251. Ile jest relacji n-argumentowych na zbiorze 5-elementowym?

5.4. Złożenie relacji. Relacja odwrotna

Definicja 82. Dane są relacje $P \subseteq A \times B$ i $Q \subseteq B \times C$. Relacja

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

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.

W definicji złożenia relacji użyliśmy bardzo rzadko używanej w literaturze notacji $P;Q$, ponieważ taka notacja wydaje się najbardziej naturalna dla informatyków. W literaturze matematycznej najczęściej używa się oznaczenia $Q \circ P$ lub $Q \cdot P$ (zwróć uwagę na odwróconą kolejność argumentów P i Q), przy czym sam operator składania ($\circ$ lub $\cdot$) jest zwykle pomijany i pisze się po prostu QP.

Zadanie 252. Niech A będzie ustalonym niepustym zbiorem. Czy prawdą jest, że dla dowolnej relacji $R \subseteq A^2$ zachodzi

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

gdzie $R;R$ 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 253. Niech R będzie relacją binarną. Które z poniższych stwierdzeń są prawdziwe:

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

jeżeli relacja R jest

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

Twierdzenie 83. Dla dowolnych relacji $R \subseteq A \times B$, $S \subseteq B \times C$ i $T \subseteq C \times D$:

$$\begin{array}{rcl} (R;S);T & = & R;(S;T) \\ (R;S)^{-1} & = & S^{-1};R^{-1} \end{array}$$

Zadanie 254. Rozważmy relacje $R \subseteq A \times B$, $S \subseteq A \times B$ i $T \subseteq B \times C$. Uzupełnij i udowodnij wzory:

$$\begin{array}{rcl} R;I_B & = & R \\ I_A;R & = & R \\ (R \cup S)^{-1} & = & R^{-1} \cup S^{-1} \\ (R \cap S)^{-1} & = & R^{-1} \cap S^{-1} \\ (R^{-1})^{-1} & = & R \\ (R \cup S);T & = & R;T \cup S;T \\ (R \cap S);T & \subseteq & R;T \cap S;T \\ ((R \cup S);T)^{-1} & = & T^{-1};R^{-1} \cup T^{-1};S^{-1} \\ (A \times B)^{-1} & = & B \times A \\ (A \times B);(C \times D) & = & ? \end{array}$$

Zadanie 255. Niech R i S będą symetrycznymi relacjami na zbiorze A. Udowodnij, że jeśli $S;R = R;S$ to relacja $R;S$ jest symetryczna.

Zadanie 256. Niech R i S będą symetrycznymi relacjami na zbiorze A. Udowodnij, że jeśli relacja $R;S$ jest symetryczna, to $S;R = R;S$.

Zadanie 257. Niech R i S będą relacjami równoważności na zbiorze A. Udowodnij, że jeśli relacja $R;S$ jest przechodnia to jest też symetryczna.

Definicja 84. Dla relacji $R \subseteq A^2$ definiujemy $R^0 = I_A$ oraz $R^{n+1} = R^n;R$ dla $n \geq 0$.

Przykład 85. Pokażemy indukcyjnie, że dla każdej liczby naturalnej $n \geq 0$ zachodzi równość $R^n;R = R;R^n$.

Podstawa indukcji: Dla $n = 0$ mamy $R^0;R = I_A;R = R = R;I_A = R;R^0$.

Krok indukcyjny: Weźmy dowolne $n \geq 0$ i załóżmy, że $R^n;R = R;R^n$. Pokażemy, że $R^{n+1};R = R;R^{n+1}$. Z definicji R^{n+1} mamy $R^{n+1};R = (R^n;R);R$. Z założenia indukcyjnego $(R^n;R);R = (R;R^n);R$. Z łączności składania relacji wiemy, że $(R;R^n);R = R;(R^n;R)$ i ponownie z definicji R^{n+1} otrzymujemy $R;(R^n;R) = R;R^{n+1}$. Zatem $R^{n+1};R = R;R^{n+1}$, co kończy dowód.

Zadanie 258. Oblicz $R^2 = R;R$, R^3 i R^4 dla relacji z zadania 248.

Zadanie 259. Wykaż, że jeśli R jest relacją zwrotną i przechodnią, to $R^n = R$ dla każdego $n \geq 1$.

Zadanie 260. Niech $R \subseteq A^2$ będzie dowolną relacją. Udowodnij, że dla dowolnych dodatnich liczb naturalnych i, j zachodzi równość $R^{i+j} = R^i;R^j$.

Zadanie 261. Niech $R \subseteq A^2$ będzie dowolną relacją. Wykaż, że $R \cup R^0 \cup R^{-1}$ jest relacją zwrotną i symetryczną.

Zadanie 262. Niech $R \subseteq A^2$ będzie pewną relacją binarną na zbiorze A oraz

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

Pokaż, że

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

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

Definicja 86. Relację R^+ nazywamy *przechodnim (tranzytywnym) domknięciem* R.

Zadanie 263. Niech $R \subseteq A^2$ będzie dowolną relacją i niech $\bar{R} = \bigcup_{n=1}^{\infty} R^n$. Wykaż, że $\bar{R}$ jest relacją przechodnią.

Zadanie 264. Wykaż, że relacja $\bar{R}$ z poprzedniego zadania jest przechodnim domknięciem relacji R.

5.5. Relacyjny rachunek dziedzin

Relacyjny rachunek dziedzin to jeden z języków zapytań używanych w teorii relacyjnych baz danych. Zapytania w tym języku są wyrażeniami postaci

$$\{\langle x_1, \ldots, x_n\rangle \mid \phi\}$$

gdzie ϕ jest formułą logiki I rzędu ze zmiennymi wolnymi $x_1, \ldots, x_n$.

W zadaniach poniżej rozważmy skończone zbiory osób O, barów B i soków S oraz relacje $\mathit{Bywa} \subseteq O \times B$, $\mathit{Lubi} \subseteq O \times S$ i $\mathit{Podają} \subseteq B \times S$ informujące odpowiednio o tym jakie osoby bywają w jakich barach, jakie osoby lubią jakie soki oraz jakie bary podają jakie soki. Wtedy np. zapytanie

$$\{x \mid \mathit{Lubi}(x, \textsf{malinowy}) \land \exists b.\ \mathit{Podają}(b, \textsf{malinowy}) \land \mathit{Bywa}(x, b)\}$$

oznacza wykaz osób, które lubią sok malinowy i bywają w jakimś barze, w którym jest on podawany.

Zadanie 265. Wyraź w relacyjnym rachunku dziedzin następujące zapytania:

- wykaz osób, które lubią wszystkie soki podawane we wszystkich barach, w których bywają;
- wykaz osób, które bywają tylko w takich barach, w których podawane są wszystkie soki lubiane przez te osoby;
- wykaz osób, które bywają tylko w takich barach, w których mogą się czegoś napić.[1]

Zadanie 266. Wyraź w relacyjnym rachunku dziedzin następujące zapytania:

- wykaz soków podawanych w barze *Jagódka*, których nie lubi żadna osoba bywająca w tym barze.
- wykaz soków lubianych tylko przez osoby bywające w barze *Jagódka*.
- wykaz soków lubianych przez wszystkie osoby bywające w barze *Jagódka*.
- wykaz soków lubianych przez osoby bywające we wszystkich barach, w których podaje się jakikolwiek sok.

[1] bardziej formalnie, przez *osoba o może się czegoś napić w barze b* rozumiemy, że w barze b jest podawany jakiś sok lubiany przez osobę o.

6

Funkcje

Definicja 87. Relację $f \subseteq A \times B$ nazywamy *funkcją o dziedzinie A i zbiorze wartości (przeciwdziedzinie) B*, jeżeli spełnia ona dwa warunki

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

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

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

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

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

Pytanie 88. 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 89. Funkcja $f : A \to B$ jest *różnowartościowa* (jest *infekcją*), jeżeli

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

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

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

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

Zadanie 267. Które spośród relacji z zadania 248 są funkcjami?

W poniższych zadaniach skonstruuj bijekcje f, g oraz h o podanych dziedzinach i przeciwdziedzinach. Nie zapomnij uzasadnić, że skonstruowane funkcje są bijekcjami.

Zadanie 268.

1. $f : \mathbb{Z} \to \mathbb{N}$
2. $g : ((0,1) \times (2,3)) \to (0,2) \times (5,6)$
3. $h : (\mathbb{Z} \times [0,1)) \to \mathbb{R}$

Zadanie 269.

1. $f : \mathbb{N} \to \mathbb{N} \times \{0,1\}$,
2. $g : [0,1) \to [0,\infty)$,
3. $h : \{0,1\}^{\mathbb{N}} \to \{3,4\}^{\mathbb{P}}$.

Tutaj $\mathbb{P}$ oznacza zbiór liczb parzystych, czyli $\mathbb{P} = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N}\ n = 2k\}$.

6.1. Funkcje odwrotne i złożenie funkcji

Na początku tego rozdziału powiedzieliśmy, że funkcje są relacjami — dlatego można je tak jak relacje składać. Funkcje jednak wygodniej składa się w odwrotnej kolejności niż relacje, ponadto składanie funkcji jest (zarówno w matematyce jak i w informatyce) operacją bardzo często wykonywaną i w związku z tym operator składania jest zwykle pomijany (podobnie jak np. operator mnożenia w wyrażeniu $2x$). Jeśli zatem f i g są funkcjami, to gf będzie oznaczać złożenie $g \circ f$ relacji f i g, czyli relację $f;g$.

Twierdzenie 90. 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 gf też jest różnowartościowa. Jeżeli obie funkcje f i g są „na”, to gf też jest „na”.

Definicja 91. 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 92. 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}. Zauważ, że mamy tutaj kolizję oznaczeń: f^{-1} oznacza zarówno funkcję odwrotną do f (która nie zawsze istnieje) jak i relację odwrotną do f (która istnieje zawsze).

Zadanie 270. Niech $f : A \to B$ i $g : B \to C$. Które z poniższych implikacji są prawdziwe?

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

Przykład 93. Pokażemy, że $R \subseteq A \times B$ jest funkcją częściową wtedy i tylko wtedy gdy $R^{-1}; R \subseteq I_B$.

Dowód. Najpierw pokażemy implikację $\Rightarrow$. Załóżmy, że $R \subseteq A \times B$ jest funkcją częściową i pokażemy, że $R^{-1}; R \subseteq I_B$. Weźmy więc dowolny element e zbioru $R^{-1}; R$. Ponieważ $R^{-1}; R$ jest relacją zawartą w $B \times B$, dla pewnych $b_1, b_2 \in B$ mamy $e = \langle b_1, b_2 \rangle$. Z definicji złożenia relacji wiemy, że istnieje takie $a \in A$, że $\langle b_1, a \rangle \in R^{-1}$ oraz $\langle a, b_2 \rangle \in R$. Z definicji relacji odwrotnej otrzymujemy $\langle a, b_1 \rangle \in R$ oraz $\langle a, b_2 \rangle \in R$. Ponieważ R jest funkcją częściową, $b_1 = b_2$, a zatem $e = \langle b_1, b_1 \rangle$ i $e \in I_B$.

Teraz pokażemy implikację $\Leftarrow$. Załóżmy, że $R^{-1}; R \subseteq I_B$ i pokażemy, że R jest funkcją częściową. Weźmy więc dowolne $a \in A$ oraz $b_1, b_2 \in B$ i załóżmy, że $\langle a, b_1 \rangle \in R$ oraz $\langle a, b_2 \rangle \in R$. Z definicji relacji odwrotnej mamy $\langle b_1, a \rangle \in R^{-1}$ i dalej z definicji złożenia relacji otrzymujemy $\langle b_1, b_2 \rangle \in R^{-1}; R$. Z założenia $R^{-1}; R \subseteq I_B$ otrzymujemy $b_1 = b_2$, co kończy dowód faktu, że R jest funkcją częściową. ∎

6.2. Obraz i przeciwobraz zbioru

Definicja 94. Niech $f : A \to B$ będzie funkcją i niech $X \subseteq A$. *Obrazem zbioru X w odwzorowaniu f* nazywamy zbiór

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

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

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

W literaturze często można spotkać inne oznaczenia obrazu i przeciwobrazu zbioru, np. $f(X)$, $f^{-1}(Y)$ i $\vec{f}(X)$, $\vec{f}^{-1}(Y)$. Zwróć uwagę na kolejną kolizję oznaczeń: w zależności od kontekstu f^{-1} może teraz oznaczać funkcję odwrotną, relację odwrotną lub przeciwobraz zbioru.

Twierdzenie 95. Niech $f : A \to B$ będzie funkcją, $\mathcal{X}$ rodziną podzbiorów zbioru A, zaś $\mathcal{Y}$ rodziną podzbiorów zbioru B. Wtedy

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

Pytanie 96. Czy symbol „$\subseteq$” we wzorze (2) można zastąpić symbolem „$=$”? Czy założenia o niepustości rodzin $\mathcal{X}$ i $\mathcal{Y}$ we wzorach (2) i (4) są potrzebne?

Zadanie 271. Niech $f : X \to Y$ oraz $A, B \subseteq X$. Uzupełnij i udowodnij wzory:

$$
\begin{array}{rcl}
f[A \cup B] & = & f[A] \cup f[B] \\
f[A \cap B] & ? & f[A] \cap f[B] \\
f^{-1}[f[A]] & ? & A
\end{array}
$$

Zadanie 272. Niech $f : X \to Y$ oraz $C, D \subseteq Y$. Uzupełnij i udowodnij wzory:

$$
\begin{array}{rcl}
f^{-1}[C \cap D] & = & f^{-1}[C] \cap f^{-1}[D] \\
f^{-1}[C \cup D] & = & ? \\
f[f^{-1}[C]] & ? & C \\
f[f^{-1}[C]] & = & ?
\end{array}
$$

Zadanie 273. 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 $C \subseteq Y$.

Zadanie 274. Rozważmy funkcję $f : A \to B$ i zdefiniujmy funkcję $g : \mathcal{P}(B) \to \mathcal{P}(A)$ wzorem

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

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

Zadanie 275. Udowodnij, że istnieje dokładnie jedna monotoniczna bijekcja $f : \mathbb{N} \to \mathbb{N}$.

Zadanie 276. Udowodnij, że istnieje dokładnie jedna funkcja $f : \mathbb{N} \to \mathbb{N}$ spełniająca warunki

- $f(0) = 1$,
- $\forall i, j \in \mathbb{N} \;\; f(i + j + 1) = f(i) + f(j)$.

Zadanie 277. Udowodnij, że istnieje dokładnie jedna funkcja $f : \mathbb{N} \to \mathbb{N}$ spełniająca warunki

- $f(1) = 1$,
- $\forall i, j \in \mathbb{N} \;\; f(i + j) = f(i) + 2ij + f(j)$.

Zadanie 278. Udowodnij, że jeśli $f : A \to B$ i $g : B \to A$ są takimi funkcjami, że $gf = I_A$ to f jest różnowartościowa a g jest „na”.

Zadanie 279. Udowodnij, że $f : A \to B$ jest różnowartościowa wtedy i tylko wtedy, gdy $f^{-1}[f[X]] = X$ dla wszystkich zbiorów $X \subseteq A$.

Zadanie 280. Udowodnij, że $f : A \to B$ jest „na” wtedy i tylko wtedy, gdy $f[f^{-1}[Y]] = Y$ dla wszystkich zbiorów $Y \subseteq B$.

Zadanie 281. Rozważmy dowolną funkcję $f : A \to B$. Udowodnij, że f jest różnowartościowa wtedy i tylko wtedy, gdy dla wszystkich podzbiorów X, Y zbioru A zachodzi równość

$$f[X] \cap f[Y] = f[X \cap Y].$$

Zadanie 282. Rozważmy dowolną funkcję $f : A \to B$. Udowodnij, że f jest różnowartościowa wtedy i tylko wtedy, gdy dla wszystkich podzbiorów X, Y zbioru A zachodzi równość

$$f[X] \setminus f[Y] = f[X \setminus Y].$$

Zadanie 283. Podaj przykład takiej różnowartościowej funkcji $f : A \to B$ oraz zbioru $Y \subseteq B$, że $f[f^{-1}[Y]] \neq Y$. Podaj przykład takiej funkcji „na” $f : A \to B$ oraz zbioru $X \subseteq A$, że $f^{-1}[f[X]] \neq X$.

Zadanie 284. Czy dla wszystkich funkcji $f : A \to B$ oraz zbiorów $X \subseteq A$ i $Y \subseteq B$ zachodzi równość $f^{-1}[f[X] \setminus Y] = X \setminus f^{-1}[Y]$? Czy zachodzi inkluzja w którąś stronę? Czy odpowiedź zmieni się, jeśli założymy, że f jest różnowartościowa lub „na”?

Zadanie 285. Dla liczb naturalnych k niech $\underline{k}$ oznacza zbiór $\{n \in \mathbb{N} \mid n < k\}$. Rozważmy funkcje $F : \underline{2013}^{\underline{2013}} \times \mathbb{N} \to \underline{2013}^{\underline{2013}}$ i $G : \underline{2013}^{\underline{2013}} \times \mathbb{N} \to \underline{2013}^{\underline{2013}}$ zadane wzorami

$$\begin{aligned} F(f, 0) &= id_{\underline{2013}} \\ F(f, n+1) &= f \circ F(f, n) \\ G(f, 0) &= id_{\underline{2013}} \\ G(f, n+1) &= G(f, n) \circ f \end{aligned}$$

gdzie $id_{\underline{2013}} : \underline{2013} \to \underline{2013}$ jest funkcją identycznościową zbioru $\underline{2013}$. Udowodnij, że $F = G$.

W poniższych zadaniach uznamy wyrażenie za poprawne jeśli dla każdej użytej w nim funkcji (i dla dowolnych zbiorów A, B i C) jej argument należy do dziedziny tej funkcji. Np. dla $f : (A \times B) \to C$ oraz $a \in A$ wyrażenie $f(a)$ nie jest poprawne, bo $a \notin (A \times B)$.

Zadanie 286. Rozważmy funkcje

$$\begin{aligned} f &: (A \times B)^C \to A^{B \times C}, \\ g &: B \times C \to A, \\ h &: C \to A \times B \end{aligned}$$

oraz elementy $a \in A$, $b \in B$ i $c \in C$. Które z wyrażeń poniżej są poprawne? Uzasadnij odpowiedź.

1. $g(f(h))$
2. $(f(g))(a)$
3. $f(h(c))$
4. $(f(h))(b, c)$

Zadanie 287. Rozważmy funkcje

$$\begin{aligned} f &: (A \times B)^C \to C^{A \times B}, \\ g &: A \times B \to C, \\ h &: C \to A \times B \end{aligned}$$

oraz elementy $a \in A$, $b \in B$ i $c \in C$. Które z wyrażeń poniżej są poprawne? Uzasadnij odpowiedź.

1. $(f(h))(a, b)$
2. $(f(c))(a, b)$
3. $(f(h))(h(c))$
4. $g(f(h))$

7

Relacje równoważności

Definicja 97. *Klasą abstrakcji* elementu $a \in A$ względem relacji równoważności $\sim \subseteq A \times A$ nazywamy zbiór

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

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

Definicja 98. Mówimy, że rodzina zbiorów $\{X_i\}_{i \in I}$ jest *podziałem* zbioru A, jeśli

1. zbiory X_i są niepuste:
$$X_i \neq \emptyset \text{ dla każdego } i \in I,$$
2. zbiory X_i pokrywają zbiór A:
$$\bigcup_{i \in I} X_i = A, \quad \text{oraz}$$
3. zbiory X_i są parami rozłączne:
$$X_i \cap X_j = \emptyset,$$
dla wszelkich takich $i, j \in I$, że $X_i \neq X_j$.

Lemat 99. Dla dowolnej relacji równoważności $\sim \subseteq A \times A$ i elementów $a, b \in A$

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

Twierdzenie 100 (Zasada Abstrakcji).

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

Przykład 101. Definiujemy relację $\sim\ \subseteq (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))^2$ wzorem

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

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

Zadanie 288. 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.

Definicja 102. Niech dane będą dwa podziały $\mathcal{P}_1$ i $\mathcal{P}_2$ zbioru A. Mówimy, że podział $\mathcal{P}_1$ jest *drobniejszy* od podziału $\mathcal{P}_2$, jeśli dla każdego $X \in \mathcal{P}_1$ istnieje taki $Y \in \mathcal{P}_2$, że $X \subseteq Y$.

Zadanie 289. 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 290. 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 291. Relacje R i S są relacjami równoważności na tym samym zbiorze. Czy $R \cup S$, $R \cap S$, $R \setminus S$, $R \dot{-} S$ też są relacjami równoważności?

Zadanie 292. Czy dla dowolnych relacji równoważności R i S na tym samym zbiorze, relacja $R;S$ też jest relacją równoważności?

Zadanie 293. Niech R i S będą relacjami równoważności na tym samym zbiorze. Udowodnij, że $R \cup S$ jest relacją równoważności wtedy i tylko wtedy, gdy $R \cup S = R;S$.

Zadanie 294. Podaj przykład takich relacji równoważności R i S, że $R;S$ jest a $R \cup S$ nie jest relacją równoważności.

Zadanie 295. Niech R i S będą relacjami równoważności na tym samym zbiorze. Udowodnij, że $R;S$ jest relacją równoważności wtedy i tylko wtedy, gdy $R;S = S;R$.

Zadanie 296. Niech R i S będą dowolnymi relacjami równoważności na zbiorze A. Udowodnij, że $R \cup S$ jest relacją równoważności wtedy i tylko wtedy, gdy dla wszystkich $a \in A$ zachodzi alternatywa $[a]_R \subseteq [a]_S$ lub $[a]_S \subseteq [a]_R$.

Zadanie 297. 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 298. Niech $R \subseteq A^2$ będzie pewną relacją binarną na zbiorze A oraz

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

Pokaż, że

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

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

Definicja 103. Relację R^* nazywamy *zwrotnym i przechodnim domknięciem* R.

Zadanie 299. Niech $Q \subseteq A^2$ będzie dowolną relacją, $Q^0 = I$, gdzie I jest relacją równości na A i niech $Q^{n+1} = Q^n Q$ dla $n \geq 0$. Kładziemy $\hat{Q} = \bigcup_{n=0}^{\infty} Q^n$. Wykaż, że $\hat{Q}$ jest relacją zwrotną i przechodnią.

Zadanie 300. Wykaż, że relacja $\hat{Q}$ z poprzedniego zadania jest zwrotnym i przechodnim domknięciem relacji Q.

Zadanie 301. Korzystając z zadań poprzednich wykaż, że jeśli R jest dowolną relacją oraz $Q = R \cup R^{-1}$, to Q^* jest relacją równoważności.

Zadanie 302. Udowodnij, że jeśli R jest dowolną relacją oraz $Q = R \cup R^{-1}$, to Q^* jest najmniejszą (w sensie relacji inkluzji) relacją równoważności zawierającą relację R.

Zadanie 303. Udowodnij, że jeżeli R jest relacją taką, że R^* zawiera R^{-1}, to R^* jest relacją równoważności.

Zadanie 304. Dane jest przekształcenie $f : A \to B$. W zbiorze A definiujemy relację $\sim$ wzorem

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

Udowodnij, że $\sim$ jest relacją równoważności. Jakie są klasy abstrakcji tej relacji? Podaj warunek konieczny i dostateczny na to, by $\sim$ była identycznością na A.

Zadanie 305. Dane jest przekształcenie $f : A \to B$ oraz relacja równoważności R na B. W zbiorze A definiujemy relację $\sim$ wzorem

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

Udowodnij, że $\sim$ jest relacją równoważności.

Zadanie 306. Ile jest różnych relacji równoważności na zbiorze czteroelementowym? Ile jest różnych relacji równoważności na zbiorze sześcioelementowym?

Zadanie 307. W zbiorze $\mathbb{N}^{\mathbb{N}}$ definiujemy relacje R_1, R_2, R_3 i R_4 w następujący sposób:

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

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

Zadanie 308. Sprawdź, dla jakich liczb naturalnych k podane relacje na zbiorze $\mathbb{N}$ są zwrotne, symetryczne lub przechodnie. Dla tych z nich, które są relacjami równoważności, opisz ich klasy abstrakcji. Napis $k \mid m$ oznacza, że m jest podzielne przez k.

1. $x R_k y \overset{\text{df}}{\Leftrightarrow} k \mid (x + y)$
2. $x S_k y \overset{\text{df}}{\Leftrightarrow} k \mid (x - y)$
3. $x T_k y \overset{\text{df}}{\Leftrightarrow} x - y = k$

Zadanie 309. Czy relacja R określona na zbiorze wielomianów jednej zmiennej o współczynnikach naturalnych wzorem

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

jest relacją równoważności?

Zadanie 310. Dany jest zbiór X i jego podzbiór $C \subseteq X$. Czy relacja R określona na $\mathcal{P}(X)$ wzorem

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

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

Zadanie 311. W zbiorze wszystkich zbieżnych ciągów nieskończonych o wyrazach wymiernych wprowadzamy relację

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

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

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

Zadanie 313. $X = \mathbb{N} \times \mathbb{N}$,

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

Zadanie 314. $X = \mathbb{R} \times \mathbb{R}$,

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

Zadanie 315. $X = \mathbb{R} \times \mathbb{R}$,

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

Zadanie 316. $X = \mathcal{P}(\mathbb{N})$,

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

Zadanie 317. Na zbiorze $\mathcal{P}(\mathbb{N})$ określamy relację równoważności $\sim$ wzorem

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

(patrz zadanie 312). W zbiorze $\mathcal{P}(\mathbb{N})/\sim$ definiujemy działania

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

Czy powyższe definicje są poprawne?

Zadanie 318. W zbiorze liczb rzeczywistych $\mathbb{R}$ wprowadzamy taką relację $\sim$, że $x \sim y \overset{\text{df}}{\Leftrightarrow} \lfloor x \rfloor = \lfloor y \rfloor$. Udowodnij, że $\sim$ jest relacją równoważności. Opisz jej klasy abstrakcji.

Zadanie 319. W zbiorze $\mathbb{R}/\sim$, gdzie $\sim$ jest relacją z zadania 318, 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?

Zadanie 320. W zbiorze $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\sim$, gdzie $\sim$ jest relacją z Przykładu 101, definiujemy działania arytmetyczne: $[\langle a, b \rangle]_\sim + [\langle c, d \rangle]_\sim = [\langle a + c, b + d \rangle]_\sim$oraz $[\langle a, b \rangle]_\sim \cdot [\langle c, d \rangle]_\sim = [\langle a \cdot c, b \cdot d \rangle]_\sim$. Czy powyższe definicje są poprawne?

Zadanie 321. Czy w zbiorze $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\sim$, gdzie $\sim$ jest relacją z Przykładu 101, można tak zdefiniować działanie arytmetyczne $\oplus$, aby dla dowolnych trzech liczb wymiernych w postaci ułamków $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3} \in \mathbb{Q}$ spełniających warunek $\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_3}{q_3}$ zachodziła równość $[\langle p_1, q_1 \rangle]_\sim \oplus [\langle p_2, q_2 \rangle]_\sim = [\langle p_3, q_3 \rangle]_\sim$?

Zadanie 322. W zbiorze $\mathbb{N}/S_k$, gdzie S_k jest relacją zdefiniowaną w zadaniu 308 definiujemy działania $+_k$ i $\cdot_k$ wzorami

$$\begin{aligned} [x]_{S_k} +_k [y]_{S_k} &= [x + y]_{S_k} \\ [x]_{S_k} \cdot_k [y]_{S_k} &= [xy]_{S_k} \end{aligned}$$

Sprawdź, dla jakich liczb k te definicje są poprawne.

8

Teoria mocy

8.1. Równoliczność zbiorów

Definicja 104. Zbiory A i B *są równoliczne*, jeżeli istnieje bijekcja $f : A \to B$. Piszemy wówczas $A \sim B$.

Przykład 105. Następujące zbiory są równoliczne:

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

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

$$\begin{array}{rll}
(a,b) & \text{oznacza zbiór} & \{x \in \mathbb{R} \mid a < x < b\}, \\
[a,b) & \text{oznacza zbiór} & \{x \in \mathbb{R} \mid a \le x < b\}, \\
(a,b] & \text{oznacza zbiór} & \{x \in \mathbb{R} \mid a < x \le b\}, \\
[a,b] & \text{oznacza zbiór} & \{x \in \mathbb{R} \mid a \le x \le b\}, \\
(a,\infty) & \text{oznacza zbiór} & \{x \in \mathbb{R} \mid a < x\}, \\
O((a,b),r) & \text{oznacza zbiór} & \{(x,y) \in \mathbb{R}^2 \mid (x-a)^2 + (y-b)^2 = r^2\}, \\
\mathbb{N}^+ & \text{oznacza zbiór} & \{n \in \mathbb{N} \mid n > 0\}, \\
\mathbb{Q}^+ & \text{oznacza zbiór} & \{q \in \mathbb{Q} \mid q > 0\}.
\end{array}$$

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

Zadanie 323. $[0, 1)$ oraz $O((0, 0), 1)$

Zadanie 324. $(0, 1)$ oraz $[1, 2]$

Zadanie 325. $(0, 1)$ oraz $\mathbb{R}$

Zadanie 326. $[0, 1)$ oraz $[0, \infty)$

Zadanie 327. $(0, 1)$ oraz $[0, 1)$

Zadanie 328. $[0, 1)$ oraz $\mathbb{R}$

Zadanie 329. $[0, 1)$ oraz $(0, \infty)$

Zadanie 330. $\mathbb{R}$ oraz $\mathbb{R} \setminus \mathbb{N}$

Zadanie 331. $\mathbb{Q}$ oraz $\mathbb{Q}^+$

Zadanie 332. $\mathbb{Q}$ oraz $\mathbb{Q} \setminus [0,1]$

Zadanie 333. $\mathbb{N}$ oraz $\mathbb{Z}$

Zadanie 334. $\mathbb{N}$ oraz $\mathbb{N}^2$

Zadanie 335. $\mathbb{N}$ oraz $\mathbb{N}^3$

Zadanie 336. $\mathbb{N}$ oraz $\{\langle n, m\rangle \in \mathbb{N}^+ \times \mathbb{N}^+ \mid m \perp n\}$

Zadanie 337. $\{\langle n, m\rangle \in \mathbb{N}^+ \times \mathbb{N}^+ \mid m \perp n\}$ oraz $\mathbb{Q}^+$

Zadanie 338. $\mathbb{N}$ oraz $\mathbb{Q}$

Zadanie 339. $\mathbb{Z} \times ((0, 1] \cap \mathbb{Q})$ oraz $\mathbb{Q}$

Zadanie 340. $\mathbb{R}$ oraz $\mathbb{R} \setminus \mathbb{Q}$

Zadanie 341. $(0, 1] \times \mathbb{Z}$ oraz $\mathbb{R}$

Zadanie 342. $(0, 1) \times (0, 1)$ oraz $\mathbb{R} \times \mathbb{R}$

Zadanie 343. $\mathcal{P}(\mathbb{N})$ oraz $\{0, 1\}^{\mathbb{N}}$

Zadanie 344. $\{0, 1\}^{\mathbb{N}}$ oraz $\mathbb{N}^{\mathbb{N}}$

Zadanie 345. $\{x \in \mathbb{R} \mid \sin(x) = 0\}$ oraz $\mathbb{Z}$

Zadanie 346. $[0, 1] \times \mathcal{P}([2, 3])$ oraz $\mathcal{P}([0, 1]) \times [2, 3]$

Zadanie 347. Niech R_1 i R_2 będą takimi relacjami równoważności na A, że $R_1 \cap R_2 = I_A$ oraz $R_1;R_2 = A \times A$ (tutaj I_A jest relacją identyczności na zbiorze A). Dla $i \in \{1, 2\}$ niech $A/_{R_i}$ będzie rodziną klas abstrakcji relacji R_i, tzn. $A/_{R_i} = \{[a]_{R_i} \mid a \in A\}$. Udowodnij, że zbiór A jest równoliczny z produktem kartezjańskim $A/_{R_1} \times A/_{R_2}$.

8.2. Własności pojęcia równoliczności zbiorów

Twierdzenie 106. Dla dowolnych zbiorów A, B, C

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

Zadanie 348. Wykaż, że jeśli $A_1 \sim A_2$, to

$$\begin{aligned} \mathcal{P}(A_1) &\sim \mathcal{P}(A_2), & (1)\\ B^{A_1} &\sim B^{A_2}, & (2)\\ A_1^B &\sim A_2^B, & (3)\\ A_1 \times B &\sim A_2 \times B. & (4) \end{aligned}$$

Zadanie 349. Wykaż, że

$$\begin{aligned} (A^B)^C &\sim A^{(B\times C)}, & (1)\\ (A\times B)^C &\sim A^C \times B^C, & (2)\\ A\times\{a\} &\sim A, & (3)\\ A^{\{a\}} &\sim A, & (4) \end{aligned}$$

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

Zadanie 350. Wykaż, że jeśli $A_1 \cap B_1 = A_2 \cap B_2 = \emptyset$ oraz $A_1 \sim A_2$ i $B_1 \sim B_2$, to

$$\begin{aligned} A_1 \cup B_1 &\sim A_2 \cup B_2, & (1)\\ C^{A_1\cup B_1} &\sim C^{A_2} \times C^{B_2}. & (2) \end{aligned}$$

Powyższe własności uwalniają nas od konieczności żmudnego konstruowania odpowiednich bijekcji, pozwalając w łatwy sposób wyprowadzać nowe fakty na temat równoliczności zbiorów z już poznanych. Dla przykładu skoro $\mathbb{N} \sim \mathbb{Q}$ (zadanie 338), to na mocy własności (2) z zadania 348 wnioskujemy, że $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}^{\mathbb{Q}}$.

Zadanie 351. Przyjmując za wiadome, że $\mathbb{N} \sim \mathbb{N}\times\mathbb{N}$ oraz $\mathbb{R} \sim \{0, 1\}^{\mathbb{N}}$ udowodnij, że $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$.

Zadanie 352. Dla jakich skończonych zbiorów A, B i C:

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

Zadanie 353. Czy istnieją takie zbiory A, B, C, D, że $A \not\sim B$ oraz $C \not\sim D$, ale $A^C \sim B^D$?

8.3. Zbiory skończone

Definicja 107. Napis $\underline{n}$ oznacza zbiór liczb naturalnych mniejszych od n, tj. zbiór $= \{0, 1, \ldots, n-1\}$.

Definicja 108. Zbiór A jest *zbiorem skończonym*, jeśli istnieje taka liczba naturalna $n \in \mathbb{N}$, że $A \sim \underline{n}$. Zbiór, który nie jest skończony nazywamy *nieskończonym*.

Twierdzenie 109.

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

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

Definicja 110. Niech A będzie zbiorem skończonym. Liczbę n taką, że $A \sim \underline{n}$ nazywamy *liczbą elementów* zbioru A i oznaczamy $|A|$. Liczbę elementów zbioru $|A|$ nazywamy też *mocą* zbioru A zwłaszcza gdy jednocześnie zajmujemy się zbiorami skończonymi i nieskończonymi.

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

Zadanie 354. Udowodnij, że podzbiór zbioru skończonego jest skończony

Zadanie 355. Udowodnij, że suma dwóch skończonych zbiorów jest zbiorem skończonym.

Zadanie 356. Udowodnij, że dla dowolnych liczb naturalnych $m, n \in \mathbb{N}$ jest

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

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

Zadanie 357. Wykaż, że jeśli zbiory A i B są skończone, to $|A \times B| = |A| \cdot |B|$.

Zadanie 358. Wykaż, że jeśli zbiory A i B są skończone, to $|A^B| = |A|^{|B|}$.

Zadanie 359. Niech $A^1 = A$ oraz $A^{n+1} = A^n \times A$. Wykaż, że $A^{\underline{n}} \sim A^n$.

Zadanie 360. Niech $\{A_i\}_{i \in \mathbb{N}}$ będzie rodziną podzbiorów zbioru X. Niech (1) oznacza, że A_0 jest zbiorem skończonym, oraz (2) oznacza, że dla każdego n zachodzi $\bigcap_{i=0}^{n} A_i \neq \emptyset$. Pokaż, że: a) jeśli zachodzi (1) i (2), to $\bigcap_{i=0}^{\infty} A_i \neq \emptyset$, b) istnieje taka rodzina zbiorów $\{A_i\}_{i \in \mathbb{N}}$ spełniająca warunek (2), że $\bigcap_{i=0}^{\infty} A_i = \emptyset$.

Zadanie 361. Niech $\{A_i\}_{i \in \mathbb{N}}$ będzie rodziną skończonych podzbiorów zbioru X, taką, że $A_{n_1} \cap \ldots \cap A_{n_k} \neq \emptyset$ dla dowolnych $n_1, \ldots, n_k \in \mathbb{N}$. Pokaż, że $\bigcap_{i=1}^{\infty} A_i \neq \emptyset$.

Zadanie 362. 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 363. Dane są zbiory $A_1, \ldots, A_n$. Przypuśćmy, że $\mathcal{R}$ jest najmniejszą rodziną zbiorów o tej własności, że $A_i \in \mathcal{R}$ dla $i = 1, \ldots, n$ oraz jeśli $X, Y \in \mathcal{R}$, to $X \cup Y \in \mathcal{R}$. Wyznacz maksymalną moc rodziny $\mathcal{R}$.

Zadanie 364. Dane są zbiory $A_1, \ldots, A_n$. Przypuśćmy, że $\mathcal{R}$ jest najmniejszą rodziną zbiorów o tej własności, że $A_i \in \mathcal{R}$ dla $i = 1, \ldots, n$ oraz jeśli $X, Y \in \mathcal{R}$, to $X \cup Y \in \mathcal{R}$ i $X \cap Y \in \mathcal{R}$. Wyznacz maksymalną moc rodziny $\mathcal{R}$. Dla jakich zbiorów $A_1, \ldots, A_n$ wartość $|\mathcal{R}|$ jest największa?

Zadanie 365. Dane są zbiory $A_1, \ldots, A_n$. Przypuśćmy, że $\mathcal{R}$ jest najmniejszą rodziną zbiorów o tej własności, że $A_i \in \mathcal{R}$ dla $i = 1, \ldots, n$ oraz jeśli $X, Y \in \mathcal{R}$, to $X \cup Y \in \mathcal{R}$ i $X \setminus Y \in \mathcal{R}$. Wyznacz maksymalną moc rodziny $\mathcal{R}$. Dla jakich zbiorów $A_1, \ldots, A_n$ wartość $|\mathcal{R}|$ jest największa?

Definicja 111. Przyjmujemy następujące oznaczenia: dla dowolnego zbioru $X \subseteq A$ napis X^1 oznacza zbiór X, zaś napis X^0 oznacza dopełnienie zbioru X do zbioru A, tj. zbiór $A \setminus X$.

Zadanie 366. Dany jest zbiór A i dodatnia liczba naturalna k oraz takie zbiory $X_i \subseteq A$ dla $i = 1, \ldots, k$, że dla każdej funkcji $f : \{1, \ldots, k\} \to \{0, 1\}$ zbiór $\bigcap_{i=1}^{k} X_i^{f(i)}$ ma co najwyżej 1 element. Wyznacz maksymalną moc zbioru A.

Definicja 112. Mówimy, że funkcja dwuargumentowa $f : A \times B \to C$ *istotnie zależy od każdego z argumentów*, jeśli istnieją takie elementy $a \in A$ i $b_1, b_2 \in B$, że $f(a, b_1) \neq f(a, b_2)$ oraz istnieją takie elementy $a_1, a_2 \in A$ i $b \in B$, że $f(a_1, b) \neq f(a_2, b)$.

Zadanie 367. 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 368. 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 369. a) Na prywatce u Jurka jest co najmniej jedna osoba znająca co najmniej jeden z sześciu języków: polski, angielski, francuski, niemiecki, rosyjski i hiszpański. Ponadto nie ma dwóch osób, które znałyby dokładnie te same języki. Oczywiście każdy gość Jurka zna co najmniej dwa języki. Oszacuj z góry i z dołu liczbę osób na prywatce u Jurka.

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

Zadanie 370. Funkcję f określoną w pewnej dziedzinie $\mathrm{dom}(f) \subseteq \mathcal{P}(A)$ i przyjmującą wartości ze zbioru $\{0, 1\}$ nazywamy *funkcją parzystości w zbiorze* $\mathcal{P}(A)$, jeżeli

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

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

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

Zadanie 371. Pokaż, że zbiór wartości dowolnej nierosnącej funkcji

$$f \ : \ \mathbb{N} \to \left\{ n + \frac{m}{m+1} \;\middle|\; n, m \in \mathbb{N} \right\}$$

jest skończony.

8.3.1. Wzór włączeń i wyłączeń

Zadanie 372. 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 373. Korzystając z tego, iż jeżeli zbiory skończone A i B są rozłączne, to $|A \cup B| = |A| + |B|$ udowodnij, że dla dowolnych zbiorów A, B i C (niekoniecznie rozłącznych):

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

Zadanie 374. Udowodnij indukcyjnie, że dla dowolnej rodziny zbiorów skończonych $\{A_i\}_{i=1}^n$ jest prawdziwy tzw. *wzór włączeń i wyłączeń*:

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

Zadanie 375. 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 $\{A_i\}_{i=1}^n$ jest prawdziwy wzór:

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

8.4. Moce zbiorów nieskończonych

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

Definicja 113. Zbiór jest *przeliczalny*, jeśli jest skończony lub jest równoliczny ze zbiorem liczb naturalnych.

Definicja 114. Zbiór równoliczny ze zbiorem liczb rzeczywistych nazywamy *zbiorem mocy continuum.*

Nierównolicznych zbiorów nieskończonych jest nieskończenie wiele. Jest więc nieskończenie wiele różnych nieskończonych liczb kardynalnych. Można na nich określić operacje dodawania, mnożenia i potęgowania oraz relację porządku mające podobne własności, jak odpowiadające im operacje na liczbach naturalnych. Teoria takich liczb nazywa się *arytmetyką liczb kardynalnych*. Tak subtelne teorie mają jednak niewiele zastosowań w informatyce, dlatego nam wystarczą jedynie pojęcia równoliczności, przeliczalności i mocy continuum. Tam, gdzie nie jest to niezbędne, nie należy więc używać pojęcia mocy $|A|$ zbioru A (formalnie nie zdefiniowaliśmy przecież tego obiektu!). W szczególności zamiast pisać $|A| = |B|$ lepiej napisać $A \sim B$. Oba wyrażenia oznaczają bowiem, że zbiory A i B są równoliczne, drugie jednak nie odwołuje się do (dosyć skomplikowanego) pojęcia liczby kardynalnej.

Definicja 115. Mówimy, że moc zbioru A jest nie większa niż moc zbioru B i piszemy $A \preceq B$, jeśli istnieje funkcja różnowartościowa $f : A \to B$.

Definicja 116. Mówimy, że moc zbioru A jest mniejsza niż moc zbioru B i piszemy $A \prec B$, jeśli $A \preceq B$ oraz $A \not\sim B$.

Twierdzenie 117.

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

Twierdzenie 118 (Cantor-Bernstein). Jeśli $A \preceq B$ oraz $B \preceq A$, to $A \sim B$.

Twierdzenie 119. Zbiór liczb rzeczywistych jest równoliczny ze zbiorem $\{0, 1\}^{\mathbb{N}}$. Zatem zbiór $\{0, 1\}^{\mathbb{N}}$ ma moc continuum.

Definicja 120. Jeśli $X \subseteq A$, to $f : A \to \{0, 1\}$ jest *funkcją charakterystyczną* zbioru X, jeśli

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

dla dowolnego $a \in A$.

Fakt 121. Dla dowolnego zbioru A zachodzi $\underline{2}^A \sim \mathcal{P}(A)$.

Twierdzenie 122 (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 takie $a_0 \in A$, że $f(a_0) = A_0$. 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

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

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*. ■

Technika dowodzenia, której użyliśmy w powyższym dowodzie nazywana jest *metodą przekątniową*. Pokazaliśmy w niej, że odpowiednio zmodyfikowany ciąg znajdujący się na przekątnej jest inny niż wszystkie pozostałe rozważane ciągi. Warto ją zapamiętać, bo w przyszłości pojawi się ona na innych przedmiotach, np. do udowodnienia, że nie istnieje program komputerowy, który dla danego na wejściu programu sprawdza, czy ten się zapętla.

Zadanie 376. Używając metody przekątniowej pokaż, że zbiory $\mathbb{N}$ i $\mathbb{R}$ nie są równoliczne.

Twierdzenie 123. Dla każdego A zachodzi $A \prec \mathcal{P}(A)$.

Niektóre z zadań poniżej wymagają użycia *aksjomatu wyboru*. Jest to aksjomat teorii mnogości mówiący, że dla każdej indeksowanej rodziny $\{A_i\}_{i \in I}$ niepustych zbiorów istnieje funkcja $f : I \to \bigcup_{i \in I} A_i$, zwana *funkcją wyboru*, która każdemu indeksowi $i \in I$ przyporządkowuje element $f(i)$ zbioru A_i. Aksjomat wyboru jest niekonstruktywny (nie wiadomo jak skonstruować funkcję wyboru; można też z niego wyprowadzić prawo wyłączonego środka) i jest kontrowersyjny. Korzystając z niego (razem z pozostałymi aksjomatami teorii mnogości) można dokonać *paradoksalnego rozkładu kuli*: zwykłą kulę w przestrzeni trójwymiarowej można podzielić na sześć części w taki sposób, że z tych części, używając tylko obrotów i przesunięć, można złożyć dwie kule takie same jak kula początkowa. Dlatego wielu współczesnych matematyków odrzuca ten aksjomat.

Zadanie 377. Udowodnij, że jeśli zbiory A i B są niepuste, to $A \preceq B$ wtedy i tylko wtedy, gdy istnieje funkcja $f : B \to A$, która jest „na”. (Zadanie wymaga pewnika wyboru.)

Zadanie 378. Udowodnij, że jeżeli $A \subseteq B$, to $A \preceq B$.

Zadanie 379. Czy $A_1 \sim A_2$, $B_1 \sim B_2$ i $A_1 \preceq B_1$, implikuje, że $A_2 \preceq B_2$?

Zadanie 380. Udowodnij, że A jest zbiorem nieskończonym wtedy i tylko wtedy, gdy zawiera podzbiór równoliczny ze zbiorem liczb naturalnych, tj. gdy istnieje taki zbiór $B \subseteq A$, że $B \sim \mathbb{N}$. (Uwaga: zadanie jest trudne, a dowód wymaga skorzystania z pewnika wyboru).

Zadanie 381. Udowodnij, że A jest zbiorem nieskończonym wtedy i tylko wtedy, gdy jest równoliczny ze swoim właściwym podzbiorem, tj. gdy istnieje taki zbiór $B \subseteq A$, że $B \neq A$ i $A \sim B$. (Uwaga: zadanie jest trudne, a dowód wymaga skorzystania z pewnika wyboru).

Zadanie 382. Udowodnij, że A jest zbiorem nieskończonym wtedy i tylko wtedy, gdy istnieją zbiory B i C takie, że $B \cap C = \emptyset$, $B \cup C = A$ i $A \sim B \sim C$. (Uwaga: zadanie jest trudne, a dowód wymaga skorzystania z pewnika wyboru).

Zadanie 383. Wykaż, że istnieje nieskończona rodzina zbiorów nieskończonych o tej własności, że żadne dwa spośród jej elementów nie są równoliczne.

Twierdzenie Cantora-Bernsteina pozwala ustalać równoliczność zbiorów A i B za pomocą konstrukcji dwóch funkcji różnowartościowych.Zbudowanie takich funkcji jest często znacznie łatwiejsze niż skonstruowanie bijekcji przekształcającej zbiór A na B. W poniższych zadaniach konstruując dwie funkcje różnowartościowe udowodnij równoliczność podanych zbiorów.

Zadanie 384. $(0, 1]$ oraz $(0, 1]^2$

Zadanie 385. $(0, 1)$ oraz $(1, 2]$

Zadanie 386. $(0, 1]$ oraz $\underline{2}^{\mathbb{N}}$

Zadanie 387. $\mathbb{N}$ oraz $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$

Zadanie 388. $\mathbb{Z} \times \mathbb{N}^+$ oraz $\mathbb{Q}$

Zadanie 389. $\{0, 1\}^{\mathbb{N}}$ oraz $\mathbb{N}^{\mathbb{N}}$

Zadanie 390. $\mathbb{R}$ oraz $\mathbb{R}^{\mathbb{N}}$

Zadanie 391. $\mathbb{N}$ oraz $\{f : \mathbb{N} \to \{0, 1\} \mid f \text{ jest nierosnąca}\}$

Zadanie 392. $\mathbb{N}$ oraz $\{f : \mathbb{N} \to \{1, 2, 3, 4\} \mid f \text{ jest niemalejąca}\}$

Zadanie 393. $\mathbb{Q}$ oraz $\mathbb{Q} \times \mathbb{Q}$

Zadanie 394. $(0, 1)$ oraz $(0, 1) \times (0, 1)$

Zadanie 395. $\mathbb{R}$ oraz $\mathbb{R} \times \mathbb{R}$

8.5. Wyznaczanie mocy zbiorów

Zadanie 396. Udowodnij, że dla każdej dodatniej liczby naturalnej n zbiór $\mathbb{R}^n$, gdzie $\mathbb{R}$ jest zbiorem liczb rzeczywistych, ma moc continuum.

Zadanie 397. Niech $R_I(x, y)$ oznacza relację zdefiniowaną formułą

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

na $\mathbb{N}^+ \times \mathbb{N}^+$, gdzie $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$, I jest skończonym niepustym zbiorem liczb pierwszych, a $\phi(x, y)$ jest formułą $\exists z\, (x \cdot z = y)$. Niech $Q_I = (\mathbb{N}^+ \times \mathbb{N}^+) \setminus R_I$.

a) Czy R_I jest relacją równoważności? Jeśli tak, podaj liczbę klas abstrakcji relacji R_I.

b) Czy Q_I jest relacją równoważności? Jeśli tak, podaj liczbę klas abstrakcji relacji Q_I.

Zadanie 398. 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 399. Dla ciągu nieskończonego $a = \langle a_1, a_2, a_3, \ldots \rangle$ o wyrazach naturalnych określamy relację R_a w taki sposób, że dla dwóch ciągów nieskończonych o wyrazach naturalnych $b = \langle b_1, b_2, b_3, \ldots \rangle$ i $c = \langle c_1, c_2, c_3, \ldots \rangle$ zachodzi bR_ac, wtedy i tylko wtedy, gdy

$$\forall n{\in}\mathbb{N}\ (a_n = 0 \Rightarrow b_n = c_n).$$

1. Pokaż, że niezależnie od wyboru ciągu a relacja R_a jest relacją równoważności.
2. Jaka jest moc zbioru takich ciągów a, dla których wszystkie klasy abstrakcji R_a są przeliczalne?
3. Jaka jest moc zbioru takich ciągów a, dla których relacja R_a ma przeliczalnie wiele klas abstrakcji?
4. Jaka jest moc zbioru takich ciągów a, dla których relacja R_a ma continuum klas abstrakcji i każda z tych klas jest mocy continuum?
5. Jaka jest moc zbioru takich ciągów a, dla których relacja R_a ma przeliczalnie wiele klas abstrakcji i każda z tych klas jest przeliczalna?
6. Jaka jest moc zbioru takich ciągów a, dla których relacja R_a ma zarówno przeliczalne, jak i nieprzeliczalne klasy abstrakcji?

Zadanie 400. Niech $\{X_n\}_{n\in\mathbb{N}}$ będzie dowolną rodziną podzbiorów zbioru $\mathbb{N}$.

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

Zadanie 401. Rozważamy relację $\sim$ określoną na funkcjach ze zbioru $\mathbb{N}^{\mathbb{N}}$ w następujący sposób:

$$f \sim g \quad \stackrel{\text{df}}{\Leftrightarrow} \quad \exists c{>}0\ \exists k{>}0\ \forall n{>}k\ (f(n) \leq cg(n) \wedge g(n) \leq cf(n)).$$

1. Pokaż, że $\sim$ jest relacją równoważności.
2. Jaka jest moc klasy abstrakcji takiej funkcji f, że $f(n) = 0$ dla każdego $n \in \mathbb{N}$?
3. Jaka jest moc klasy abstrakcji takiej funkcji g, że $g(n) = 1$ dla każdego $n \in \mathbb{N}$?

Zadanie 402. Dla każdej spośród relacji opisanych w zadaniu 307, która jest relacją równoważności wyznacz moc zbioru jej klas abstrakcji oraz moc każdej z jej klas.

Zadanie 403. W zbiorze $\underline{n}$ wprowadzamy relację równoważności $k \simeq l \overset{\text{df}}{\Leftrightarrow} 2|k - l$.

1. Ile klas abstrakcji ma relacja $\simeq$?
2. Ile elementów mają klasy abstrakcji $[0]_\simeq$ i $[1]_\simeq$?
3. Na klasach abstrakcji definiujemy działanie $[k]_\simeq + [l]_\simeq = [(k + l) \bmod n]_\simeq$. Dla jakich n to działanie jest poprawne?

8.6. Zbiory przeliczalne

Twierdzenie 124. Zbiór A jest przeliczalny wtedy i tylko wtedy, gdy $A = \emptyset$ lub istnieje funkcja z $\mathbb{N}$ *na* A.

Definicja 125. *Ciągiem elementów zbioru* A nazywamy funkcję $f : \mathbb{N} \to A$.

Fakt 126. Zbiór niepusty jest przeliczalny, gdy wszystkie jego elementy można ustawić w ciąg.

Twierdzenie 127.

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 $\{A_i\}_{i \in I}$ 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 404. Niech $\mathcal{A}$ będzie niepustą przeliczalną rodziną zbiorów przeliczalnych. Pokaż, że $\bigcup \mathcal{A}$ i $\bigcap \mathcal{A}$ są zbiorami przeliczalnymi. Czy założenie o niepustości $\mathcal{A}$ jest istotne?

Zadanie 405. Niech $A \subseteq \mathbb{N}$ będzie zbiorem nieskończonym. Zdefiniuj bijekcje $f : A \to \mathbb{N}$ i $g : \mathbb{N} \to A$.

Zadanie 406. 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 407. Udowodnij, że jeśli $f : \mathbb{R} \to \mathbb{R}$ jest monotoniczna, to zbiór jej punktów nieciągłości jest przeliczalny.

Zadanie 408. Czy istnieje taki zbiór A, że $\mathcal{P}(A) \sim \mathbb{N}$?

Zadanie 409. 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 410. Zbiory A i B są przeliczalne oraz zbiór $A \times B$ jest nieskończony. Co można powiedzieć o mocach zbiorów A i B?

Zadanie 411. Udowodnij, że zbiór wszystkich skończonych ciągów o elementach ze skończonego zbioru A jest przeliczalny.

Zadanie 412. Udowodnij, że zbiór wszystkich skończonych ciągów o elementach ze przeliczalnego zbioru A jest przeliczalny.

Zadanie 413. Udowodnij, że zbiór wielomianów jednej zmiennej o współczynnikach wymiernych jest przeliczalny.

Zadanie 414. 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 implikacja $x > y \Rightarrow f(x) \geq f(y)$ zachodzi dla wszelkich $x, y \in \mathbb{N}$).

Zadanie 415. Jaka jest moc zbioru nieskończonych ciągów o wyrazach wymiernych?

Zadanie 416. Jaka jest moc zbioru nieskończonych ciągów o wyrazach wymiernych, stałych od pewnego miejsca?

Zadanie 417. Jaka jest moc rodziny skończonych podzbiorów zbioru $\mathbb{N}$? Jaka jest moc rodziny nieskończonych podzbiorów zbioru $\mathbb{N}$?

Zadanie 418. Ile jest ciągów liczb wymiernych zbieżnych do 1?

Zadanie 419. Ile jest rosnących ciągów liczb wymiernych zbieżnych do 1?

Zadanie 420. Czy zbiór nieskończonych nierosnących ciągów o wyrazach naturalnych jest przeliczalny? (Ciąg $(a_i)_{i\in\mathbb{N}}$ jest nierosnący, jeśli $a_i \geq a_{i+1}$ dla każdego $i \in \mathbb{N}$).

Zadanie 421. 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 422. 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 423. Ile jest bijekcji $f : A \to A$, gdy zbiór A jest przeliczalny?

Zadanie 424. Liczba rzeczywista x jest *algebraiczna*, jeśli istnieje taki wielomian jednej zmiennej o współczynnikach wymiernych, że x jest jego pierwiastkiem. Udowodnij, że zbiór liczb algebraicznych jest przeliczalny.

Zadanie 425. Niech $P \subseteq \mathbb{R} \times \mathbb{R}$ 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 abstrakcji $[r]_P$ dla liczb $r \in \mathbb{R}$? Jaka jest moc klasy abstrakcji $[\pi]_P$? Jak jest moc klasy abstrakcji $[\frac{23}{7}]_P$? Czy wszystkie klasy abstrakcji mają tę samą moc?
c) Czy rodzina klas abstrakcji relacji P jest przeliczalna?

Zadanie 426. 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 427. 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 428. 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 429. Czy zbiór relacji równoważności na zbiorze przeliczalnym jest zbiorem przeliczalnym?

Zadanie 430. Dany jest nieskończony przeliczalny zbiór A i liczba $n \in \mathbb{N}$. Ile jest takich relacji równoważności $\sim$ na zbiorze A, że dla każdego $a \in A$ klasa abstrakcji $[a]_\sim$ ma dokładnie n elementów?

Zadanie 431. Ile jest relacji równoważności na przeliczalnym zbiorze A takich, że wszystkie ich klasy abstrakcji są skończone?

Zadanie 432. 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 433. 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 434. Udowodnij, że każdy zbiór rozłącznych odcinków na prostej jest przeliczalny. Pokaż, że istnieje nieprzeliczalny zbiór rozłącznych odcinków na płaszczyźnie.

Zadanie 435. 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 436. 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 437. 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 438. Parasol to bryła złożona z koła o niezerowej średnicy i prostopadłego do niego odcinka o niezerowej długości, który styka się swym końcem ze środkiem koła. Pokaż, że każdy zbiór rozłącznych parasoli w przestrzeni trójwymiarowej jest co najwyżej przeliczalny.

Zadanie 439. Ile jest wszystkich funkcji $f : \mathbb{N} \to \mathbb{N}$? A ile jest funkcji $f : \mathbb{N} \to \mathbb{N}$ których wartość możemy obliczać przy pomocy komputera (tj. takich, dla których istnieje program komputerowy, który wczytuje liczbę naturalną n i wypisuje liczbę $f(n)$ dla dowolnego $n \in \mathbb{N}$)?

8.7. Paradoks niedźwiedzi

Na korytarzu Instytutu Informatyki można czasem usłyszeć o następującym paradoksie, opisanym w trzech kolejnych zadaniach.

Zadanie 440. Myśliwy spotyka w lesie dwa niedźwiedzie i mówi im tak: *Za chwilę założę wam na głowy po jednym kapeluszu. Kapelusze będą białe lub czarne, każdy z was będzie widział kapelusz kolegi ale nie będzie widział własnego. Nie będziecie się mogli w żaden sposób komunikować, a po chwili będziecie musieli jednocześnie powiedzieć jaki każdy z was ma kapelusz na swojej głowie. Jeśli co najmniej jeden z was zgadnie, puszczę was wolno. Ale jeśli obaj się pomylicie, zrobię z waz bigos. Teraz możecie się przez chwilę naradzić.* Czy niedźwiedzie mogą się uratować postępując zgodnie z protokołem narzuconym przez myśliwego? Oczywiście 25-procentowa szansa wylądowania w bigosie jest nie do zaakceptowania.

Zadanie 441. Sytuacja taka jak w poprzednim zadaniu, ale niedźwiedzi jest nieskończenie (przeliczalnie) wiele. Pomylić się może skończenie wiele niedźwiedzi, prawie wszystkie muszą poprawnie odgadnąć.

Zadanie 442. Sytuacja taka jak w poprzednim zadaniu, ale kolorów kapeluszy jest jest nieskończenie (przeliczalnie) wiele. Pomylić się może skończenie wiele niedźwiedzi, prawie wszystkie muszą poprawnie odgadnąć.

Proste rozwiązanie tych zadań jest zaskakujące i u niektórych ludzi może podważyć wiarę w sensowność matematyki. Jest jednak również kontrowersyjne z co najmniej dwóch powodów. Po pierwsze, wymaga użycia aksjomatu wyboru, jest więc niekonstruktywne. Po drugie, każdy niedźwiedź musi w nim zapamiętać aż continuum bitów informacji. Ten drugi powód wydaje się nawet bardziej kontrowersyjny od założenia, że w jednym lesie można spotkać nieskończenie wiele niedźwiedzi swobodnie posługujących się zasadą abstrakcji i aksjomatem wyboru.

9

Relacje porządku

Definicja 128. *Częściowym porządkiem* w zbiorze A nazywamy relację $\leq$ (będącą podzbiorem A^2), która jest *zwrotna*, *słabo antysymetryczna* i *przechodnia*, tzn. prawdziwe są formuły

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

Definicja 129. Jeśli $\leq$ jest częściowym porządkiem na A, to $a < b$ oznacza

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

Definicja 130. *Zbiór częściowo uporządkowany*, to zbiór A z relacją częściowego porządku $\leq$. Zbiór częściowo uporządkowany oznaczamy $\langle A, \leq\rangle$.

Przykład 131. 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 $a|b \overset{\text{df}}{\Leftrightarrow} \exists x(ax = b)$.

Definicja 132. Porządek częściowy $\leq$ w zbiorze A jest *liniowy*, jeśli

$$\text{dla dowolnych } a, b \in A \quad \text{zachodzi } a \leq b \text{ lub } b \leq a.$$

Przykład 133. Porządkiem liniowym jest relacja $\leq$ na zbiorze liczb rzeczywistych. Relacja inkluzji $\subseteq$ na zbiorze $\mathcal{P}(\mathbb{N})$ nie jest porządkiem liniowym.

Definicja 134. *Łańcuchem* w zbiorze uporządkowanym $\langle A, \leq \rangle$ nazywamy taki podzbiór L zbioru A, że dla wszystkich $a, b \in L$ zachodzi $a \leq b$ lub $b \leq a$. *Antyłańcuchem* w $\langle A, \leq \rangle$ nazywamy taki podzbiór L zbioru A, że dla wszystkich $a, b \in L$ jeśli zachodzi $a \leq b$ lub $b \leq a$, to $a = b$.

Innymi słowy, łańcuch to dowolny liniowo uporządkowany podzbiór A, natomiast antyłańcuch to dowolny podzbiór składający się z elementów wzajemnie nieporównywalnych.

9.1. Przykłady porządków

Zadanie 443. 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 444. Podaj przykład przeliczalnego zbioru uporządkowanego, zawierającego zarówno nieskończony łańcuch jak i nieskończony antyłańcuch.

Zadanie 445. Pokaż, że na zbiorze liczb zespolonych $\mathbb{C}$ nie można wprowadzić takiego porządku $\leq$, że jednocześnie:

- zero jest porównywalne z każdą liczbą zespoloną, tj. $z = 0$ lub $z > 0$ lub $z < 0$ dla każdej liczby $z \in \mathbb{C}$;
- porządek $\leq$ jest zgodny z działaniami arytmetycznymi, dokładniej $-z < 0$ i $wz > 0$ dla dowolnych $w, z > 0$ oraz $-z > 0$ dla dowolnego $z < 0$.

Zadanie 446. 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 447. Czy dla danego takiego zbioru X, że $|X| \geq 2$ można określić taką relację R, by równocześnie:

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

Zadanie 448. Podaj przykład porządku liniowego na zbiorze $\mathbb{N}^{\mathbb{N}}$.

Zadanie 449. Podaj przykład porządku liniowego na zbiorze $\mathcal{P}(\mathbb{N})$.

Zadanie 450. Podaj przykład siedmiu różnych porządków liniowych na zbiorze $\mathbb{N}$.

Zadanie 451. 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 135. Niech A będzie dowolnym zbiorem. Będziemy nazywać go *alfabetem* a jego elementy *literami*. *Słowem* nad alfabetem A nazywamy dowolny skończony ciąg liter ze zbioru A. Słowo puste (ciąg długości zero) oznaczamy ϵ. Przez A^* oznaczamy zbiór wszystkich słów nad alfabetem A. Jeżeli $u = u_1 u_2 \ldots u_n$ i $w = w_1 w_2 \ldots w_m$, to uw oznacza *złożenie* (*konkatenację*) słów u i w, tj. słowo $u_1 u_2 \ldots u_n w_1 w_2 \ldots w_m$. Słowo u jest *przedrostkiem* (*prefiksem*) słowa w, jeśli istnieje takie słowo v, że $uv = w$. Podobnie, słowo u jest *przyrostkiem* (*sufiksem*) słowa w, jeśli istnieje takie słowo v, że $vu = w$. Dla słowa w przez $|w|$ będziemy oznaczać jego długość a dla $0 < j \leq |w|$ przez $w(j)$ jego j-tą literę.

Fakt 136. 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 137. Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Na zbiorze A^* skończonych ciągów elementów zbioru A określamy relację $\leq_{lex}$ przyjmując, że dla dowolnych $u, w \in A^*$ zachodzi $u \leq_{lex} w$ wtedy i tylko wtedy, gdy u jest przedrostkiem w lub istnieje $i \leq \min(|u|, |w|)$ takie, że dla $j < i$ zachodzi $u(j) = w(j)$ oraz $u(i) < w(i)$. Relację $\leq_{lex}$ nazywamy *porządkiem leksykograficznym* na A^* generowanym przez porządek $\leq$.

Zadanie 452. Wykaż, że relacja $\leq_{lex}$ jest porządkiem częściowym.

Zadanie 453. Wykaż, że jeśli $\langle A, \leq \rangle$ jest porządkiem liniowym, to $\langle A^*, \leq_{lex} \rangle$ też jest porządkiem liniowym (udowodnij tylko liniowość). Czy zachodzi implikacja w drugą stronę?

Zadanie 454. Rozważmy system komputerowy dla wypożyczalni, w którym można robić rezerwacje (lub jakikolwiek inny system umożliwiający rezerwację czegokolwiek — np sali, rzutnika czy pokoju w hotelu). System taki musi umieć sprawdzać, czy dwie rezerwacje tego samego obiektu ze sobą kolidują. Napisz w języku ANSI C (lub podobnym języku programowania) warunek boolowski[1] sprawdzający, czy rezerwacja od dnia d_1 miesiąca m_1 do dnia d_2 miesiąca m_2 koliduje z rezerwacją od dnia d_3 miesiąca m_3 do dnia d_4 miesiąca m_4. Zakładamy przy tym, że wszystkie daty są w tym samym roku.

Zadanie 455. Przedziałem domkniętym od a do b w zbiorze liniowo uporządkowanym $\langle P, \sqsubseteq \rangle$ nazywamy zbiór $O[a, b] = \{x \in P \mid a \sqsubseteq x \wedge x \sqsubseteq b\}$.

a) Używając jedynie symboli $a, b, c, d, \leq, <, \geq, >$, spójników logicznych i nawiasów napisz formułę logiki pierwszego rzędu, która interpretowana w zbiorze liniowo uporządkowanym $\langle P, \sqsubseteq \rangle$ mówi, że przedziały domknięte $O[a, b]$ i $O[c, d]$ nie są rozłączne.

b) Używając jedynie symboli $d_1, m_1, d_2, m_2, d_3, m_3, d_4, m_4, \leq, <, \geq, >, =$ oraz spójników logicznych i nawiasów napisz formułę logiki pierwszego rzędu, która interpretowana w zbiorze liczb rzeczywistych z naturalnym porządkiem mówi, że w zbiorze $\langle \mathbb{R} \times \mathbb{R}, \leq_{lex} \rangle$ przedziały domknięte $O[\langle m_1, d_1 \rangle, \langle m_2, d_2 \rangle]$ oraz $O[\langle m_3, d_3 \rangle, \langle m_4, d_4 \rangle]$ nie są rozłączne. Oczywiście $\leq_{lex}$ jest tutaj leksykograficznym rozszerzeniem naturalnego porządku w zbiorze liczb rzeczywistych.

Zadanie 456. Napisz w języku ANSI C (lub podobnym języku programowania) funkcję boolowską wykrywającą kolizje w rezerwacjach od godziny g_1 dnia d_1 miesiąca m_1 roku r_1 do godziny g_2 dnia d_2 miesiąca m_2 roku r_2 i od godziny g_3 dnia d_3 miesiąca m_3 roku r_3 do godziny g_4 dnia d_4 miesiąca m_4 roku r_4.

Zadanie 457. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą porządkami liniowymi. Relację $\leq$ na $A \times B$ określamy wzorem

$$\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle \quad \stackrel{\text{df}}{\Leftrightarrow} \quad a_1 \leq_A a_2 \wedge b_1 \leq_B b_2$$

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 co najwyżej jednoelementowy.

Zadanie 458. Kandydaci do objęcia pewnego stanowiska oceniani są w $k \in \mathbb{N}$ różnych kategoriach. W każdej z tych kategorii otrzymują ocenę będącą liczbą naturalną nie mniejszą niż 1 i nie większą niż 6. Kandydat k_1 uważany jest za lepszego niż k_2 (co zapisujemy jako $k_1\ L\ k_2$) jeśli k_1 ma wyższe oceny niż k_2 we wszystkich kategoriach oprócz co najwyżej dwóch. Niech R będzie najmniejszą zwrotną relacją taką, że $RR \subseteq R$ i $L \subseteq R$. Czy R jest częściowym porządkiem, jeśli:

[1] warunek boolowski, czyli coś, co zadziała po wstawieniu w miejsce kropek w instrukcji `if (...) printf("mamy problem")`. W szczególności nie wolno w tym miejscu deklarować nowych zmiennych ani funkcji.

a) $k = 12$,

b) $k = 13$?

Zadanie 459. Niech R będzie relacją zwrotną i przechodnią. *Łańcuchem względem* R nazywamy ciąg $\langle a_1, \ldots, a_n \rangle$ taki, że $\langle a_i, a_{i+1} \rangle \in R$ dla $i \in \{1, \ldots, n-1\}$ oraz $a_i \neq a_j$ dla $i \neq j$. Łańcuch $\langle a_1, \ldots, a_n \rangle$ jest *cyklem względem* R, jeśli $n > 1$ i $\langle a_n, a_1 \rangle \in R$. Udowodnij, że jeśli nie istnieje cykl względem R, to R jest porządkiem częściowym.

Definicja 138. Porządek $\leq$ na zbiorze A jest *gęsty*, gdy dla dowolnych takich $a, b \in A$, że $a < b$, istnieje taki $c \in A$, że $a < c < b$.

Zadanie 460. Niech symbol $\leq$ oznacza liniowy porządek w niepustym, skończonym zbiorze A. Udowodnij, że porządek $\leq$ jest gęsty wtedy i tylko wtedy, gdy zbiór A jest jednoelementowy.

Zadanie 461. *Wielomianem jednej zmiennej* nad zbiorem liczb rzeczywistych $\mathbb{R}$ nazywamy funkcję daną wzorem

$$P(x) \quad = \quad \sum_{i=0}^{n} a_i x^i,$$

gdzie $a_i \in \mathbb{R}$ dla $i = 0, \ldots, n$. Niech $\mathbb{R}[x]$ oznacza zbiór wielomianów jednej zmiennej nad $\mathbb{R}$. a) Wyznacz moc zbioru $\mathbb{R}[x]$. Na zbiorze $\mathbb{R}[x]$ definiujemy relację $\preceq$ w następujący sposób:

$$P \preceq Q \quad \stackrel{\text{df}}{\Leftrightarrow} \quad \exists x{\in}\mathbb{R}\ \forall y{\in}\mathbb{R}\ \ (x \leq y \Rightarrow P(y) \leq Q(y)),$$

dla $P, Q \in \mathbb{R}[x]$. Udowodnij, że relacja $\preceq$ jest porządkiem na $\mathbb{R}[x]$. Czy jest to porządek a) liniowy, b) gęsty?

9.2. Elementy wyróżnione

Definicja 139. 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 $x \leq y$).

W literaturze często element najmniejszy oznacza się $\perp$, zaś największy $\top$.

Definicja 140. Element $x \in X$ jest elementem *maksymalnym* (odpowiednio *minimalnym*) w X, jeśli dla każdego $y \in X$ z warunku $x \leq y$ (odpowiednio $y \leq x$) wynika $x = y$.

Elementy minimalne, maksymalne, najmniejsze i największe w zbiorze uporządkowanym, podobnie jak zdefiniowane w rozdziale 10 kresy, nazywamy *elementami wyróżnionymi*.

Definicja 141. 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 142. Niech $\langle P, \leq\rangle$ będzie częściowym porządkiem i niech $X \subseteq P$. Wtedy element największy w X jest elementem maksymalnym w X.

Twierdzenie 143. Niech $\langle P, \leq\rangle$ będzie zbiorem uporządkowanym. Dla dowolnego zbioru $X \subseteq P$ istnieje co najwyżej jeden element największy tego zbioru.

Zatem każdy zbiór posiada też co najwyżej jeden element najmniejszy. Elementów maksymalnych i minimalnych może być natomiast wiele.

Przykład 144. Niech X będzie zbiorem niepustym i niech $P = \mathcal{P}(X) \setminus \{\emptyset\}$. Wtedy w zbiorze uporządkowanym $\langle P, \subseteq\rangle$ jest $|X|$ elementów minimalnych.

Zadanie 462. Rozważmy relację $|$ na zbiorze $\mathbb{N} \setminus \{0\}$.

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

Zadanie 463.

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

Zadanie 464. 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 465. Znajdź elementy minimalne, maksymalne, największy i najmniejszy w zbiorze $\langle \mathbb{N}^{\mathbb{N}}, R\rangle$ z zadania 473.

9.3. Izomorfizm porządkowy

Definicja 145. 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 $a_1, a_2 \in A$. Funkcję ϕ nazywamy wtedy *izomorfizmem* zbiorów uporządkowanych $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$.

Definicja 146. Niech $\langle P, \leq_P \rangle$ oraz $\langle Q, \leq_Q \rangle$ będą zbiorami częściowo uporządkowanymi. Funkcja $f : P \to Q$ jest *monotoniczna*, jeśli

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

Fakt 147. Funkcja ϕ jest izomorfizmem porządkowym, jeśli jest bijekcją oraz ϕ i ϕ^{-1} są monotoniczne.

Twierdzenie poniżej mówi, że izomorfizmy porządkowe zachowują elementy wyróżnione (na razie jeszcze bez kresów, por. zadanie 495).

Twierdzenie 148. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą zbiorami uporządkowanymi, $\phi : A \to B$ izomorfizmem porządkowym i niech $X \subseteq A$. Wtedy a jest elementem najmniejszym (odpowiednio, minimalnym, największym, maksymalnym) w X wtedy i tylko wtedy, gdy $\phi(a)$ jest elementem najmniejszym (odpowiednio, minimalnym, największym, maksymalnym) w $\phi(X)$.

W poniższych zadaniach $\mathbb{Q}$ oznacza zbiór liczb wymiernych, $\mathbb{R}$ — zbiór liczb rzeczywistych, (a, b) — przedział otwarty o końcach a i b, $[a, b]$ zaś — przedział domknięty.

Zadanie 466. Udowodnij, że funkcja $f : \mathbb{R} \to (-1, 1)$ (gdzie oba zbiory są uporządkowane zwykłą relacją porządku) dana wzorem $f(x) = \frac{x}{1+|x|}$ jest izomorfizmem porządkowym.

Zadanie 467. Udowodnij, że zbiory $\mathbb{Q}$, $\mathbb{Q} \cap (0, 1)$ i $\mathbb{Q} \setminus [0, 1)$ uporządkowane zwykłą relacją porządku są izomorficzne.

Zadanie 468. Udowodnij, że zbiory $\mathbb{Q}$, $\mathbb{Q} \setminus \{0\}$ i $\mathbb{Q} \setminus [0, 1]$ uporządkowane zwykłą relacją porządku są izomorficzne.

Definicja 149. Porządek $\leq$ na zbiorze A jest:

- *gęsty*, jeśli pomiędzy każdą parą elementów zbioru A znajduje się trzeci element, tj. gdy dla dowolnych takich $a, b \in A$, że $a < b$, istnieje taki $c \in A$, że $a < c < b$;
- *bez końców*, jeśli dla dowolnego elementu zbioru A istnieje element od niego większy i element od niego mniejszy, tj. gdy dla każdego $a \in A$ istnieją takie $b, c \in A$, że $b < a < c$.

Dla przykładu zwykły porządek na wszystkich pięciu zbiorach z zadań 467 i 468 jest gęsty i bez końców. Zbiory te są izomorficzne nie przez przypadek, o czym przekonasz się rozwiązując kolejne zadanie. Zauważ ponadto, że zwykły porządek na zbiorze $\mathbb{Q} \setminus (0, 1)$ nie jest gęsty, a na zbiorze $\mathbb{Q} \cap [0, 1]$ nie jest bez końców.

Zadanie 469. Pokaż, że dowolne dwa zbiory przeliczalne uporządkowane liniowymi, gęstymi relacjami porządku bez końców są izomorficzne.

Zadanie 470. 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 471. 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 472. 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 473. W zbiorze $\mathbb{N}^{\mathbb{N}}$ wprowadzamy relację R wzorem

$$\bar{a} R \bar{b} \quad \overset{\text{df}}{\Leftrightarrow} \quad \forall n \, (a_n \leq b_n),$$

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

Zadanie 474. W zbiorze $\mathbb{C}$ liczb zespolonych wprowadzamy porządek

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

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

Definicja 150. Niech $\langle X, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. *Następnikiem* $x \in X$ nazywamy taki element $y \in X$, że $x < y$ oraz w zbiorze X nie istnieje taki element z, że $x < z$ i $z < y$. Podobnie *poprzednikiem* $x \in X$ nazywamy taki element $y \in X$, że $y < x$ oraz w zbiorze X nie istnieje taki element z, że $y < z$ i $z < x$.

Zadanie 475. Udowodnij, że każdy taki niepusty zbiór liniowo uporządkowany $\langle X, \preceq \rangle$, że każdy jego element posiada poprzednik i następnik, oraz że jeśli $x \preceq y$, to zbiór $\{z \mid x \preceq z \wedge z \preceq y\}$ jest skończony, jest izomorficzny ze zbiorem $\langle \mathbb{Z}, \leq \rangle$ liczb całkowitych uporządkowanym standardową relacją mniejszości $\leq$.

Zadanie 476. 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 477. W zbiorze $\mathbb{R}/\sim$, gdzie $\sim$ jest relacją z zadania 318, definiujemy taką relację $\preceq$, że

$$[x]_\sim \preceq [y]_\sim \quad \overset{\text{df}}{\Leftrightarrow} \quad x \sim y \ \vee \ x < y,$$

gdzie $\leq$ jest standardowym porządkiem na liczbach rzeczywistych. Uzasadnij, że definicja $\preceq$ jest poprawna. Udowodnij, że $\langle \mathbb{R}/\sim, \preceq \rangle$ jest zbiorem liniowo uporządkowanym. Pokaż, że $\langle \mathbb{R}/\sim, \preceq \rangle$ i $\langle \mathbb{Z}, \leq \rangle$ są izomorficzne porządkowo, gdzie $\langle \mathbb{Z}, \leq \rangle$ jest zbiorem liczb całkowitych ze standardowym porządkiem.

Zadanie 478. Udowodnij, że zbiory uporządkowane $\langle \mathbb{N} \times \mathbb{Q}, \leq_{lex} \rangle$ i $\langle \mathbb{Q} \times \mathbb{N}, \leq_{lex} \rangle$ nie są izomorficzne.

Zadanie 479. Udowodnij, że zbiory uporządkowane $\langle \mathbb{R}, \leq \rangle$ i $\langle \mathbb{Z} \times [0, 1), \leq_{lex} \rangle$ są izomorficzne.

Zadanie 480. Udowodnij, że zbiory uporządkowane $\langle \mathbb{N} \times \{0, 1\}, \leq_{lex} \rangle$ i $\langle \mathbb{N}, \leq \rangle$ są izomorficzne, oraz że $\langle \mathbb{N} \times \{0, 1\}, \leq_{lex} \rangle$ i $\langle \{0, 1\} \times \mathbb{N}, \leq_{lex} \rangle$ nie są izomorficzne.

9.4. Zawieranie zbiorów jako relacja porządku

Zadanie 481. Udowodnij, że częściowe porządki $\langle \mathcal{P}(\mathbb{N}), \subseteq \rangle$ oraz $\langle \mathcal{P}(\mathbb{N}), \supseteq \rangle$ są izomorficzne.

Definicja 151. Rodzina zbiorów $\{A_t\}_{t \in T}$ jest *prawie rozłączna*, jeśli dla wszelkich różnych $s, t \in T$ zbiór $A_t \cap A_s$ jest skończony.

Zadanie 482 (Sierpiński). Pokaż, że w $\mathcal{P}(\mathbb{N})$ istnieje rodzina mocy continuum zbiorów prawie rozłącznych.

Zadanie 483. Pokaż, że w $\langle \mathcal{P}(\mathbb{N}), \subseteq \rangle$ istnieje antyłańcuch mocy continuum.

Zadanie 484. Pokaż, że w $\langle \mathcal{P}(\mathbb{N}), \subseteq \rangle$ istnieje łańcuch mocy continuum.

Definicja 152. 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 485. Udowodnij, że jeśli $A \subseteq X$ to $\{B \subseteq X \mid A \subseteq B\}$ jest filtrem. Nazywamy go *filtrem głównym wyznaczonym przez* A.

Zadanie 486. Pokaż, że jeśli X jest zbiorem skończonym, to każdy filtr na $\mathcal{P}(X)$ jest główny.

Zadanie 487. Pokaż, że jeśli X jest zbiorem nieskończonym, to istnieje filtr na $\mathcal{P}(X)$, który nie jest główny.

Zadanie 488. 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.

9.5. Liczba relacji porządku

Zadanie 489. Ile jest relacji częściowego porządku w zbiorze n-elementowym?

Zadanie 490. Ile jest relacji porządku liniowego w zbiorze n elementowym?

Zadanie 491. 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?

10

Kresy zbiorów

Definicja 153. Niech $\langle P, \leq\rangle$ będzie częściowym porządkiem i niech $X \subseteq P$. Element $a \in P$ jest *ograniczeniem górnym* zbioru X, jeśli dla każdego $x \in X$ zachodzi $x \leq a$. *Kresem górnym* zbioru X nazywamy najmniejszy element zbioru $\{a \mid a \text{ jest ograniczeniem górnym } X\}$. Kres górny zbioru X oznaczamy $\bigvee X$ lub $\sup X$. Dualnie można zdefiniować pojęcia *ograniczenia dolnego* i *kresu dolnego* (kres dolny zbioru X oznaczamy $\bigwedge X$ lub $\inf X$).

Zadanie 492. 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 154. Relacja podzielności liczb naturalnych $\mid\, \subset \mathbb{N}^2$ jest określona następująco:

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

Zadanie 493. 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 $\sup\{m, n\} = \operatorname{lcm}(m, n)$, gdzie gcd jest największym wspólnym podzielnikiem dwu liczb, a lcm — najmniejszą wspólną wielokrotnością.

Zadanie 494. Czy w $\langle \mathbb{N}, \mid\rangle$ istnieje element a) najmniejszy, b) największy?

Zadanie 495. Niech $\langle A, \leq_A\rangle$ i $\langle B, \leq_B\rangle$ będą zbiorami uporządkowanymi, $\phi : A \to B$ izomorfizmem porządkowym i niech $X \subseteq A$. Udowodnij, że a jest kresem górnym (odpowiednio, dolnym) zbioru X wtedy i tylko wtedy, gdy $\phi(a)$ jest kresem górnym (odpowiednio, dolnym) zbioru $\phi(X)$.

Definicja 155. 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 496. Pokaż, że $\approx$ jest relacją równoważności.

Zadanie 497. Ile jest klas abstrakcji relacji $\approx$? Jaka jest moc każdej z nich?

Definicja 156. 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

$$[f]_\approx \preceq [g]_\approx \quad \overset{\text{df}}{\Leftrightarrow} \quad f \preceq g.$$

Zadanie 498. 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 499. 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 500. Czy istnieje taki ciąg funkcji $\langle f_i : i \in \mathbb{N}\rangle$, że $f_i \preceq f_{i+1}$ dla $i \in \mathbb{N}$, oraz dla każdej funkcji $g : \mathbb{N} \to \mathbb{N}$ istnieje i takie, że $g \preceq f_i$?

Zadanie 501. Wykaż, że każdy przeliczalny podzbiór $X \subseteq \mathcal{F}$ posiada w zbiorze $\mathcal{F}$ ograniczenie górne.

Zadanie 502. Niech $\{A_i \mid i \in \mathbb{N}\}$ będzie podziałem zbioru $\mathbb{N}$ na zbiory nieskończone. Definiujemy ciąg funkcji $\langle f_j : j \in \mathbb{N}\rangle$ kładąc

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

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

Definicja 157. *Nieskończonym łańcuchem wstępującym* w zbiorze uporządkowanym $\langle A, \leq\rangle$ nazywamy ciąg $\langle a_i : i \in \mathbb{N}\rangle$ taki, że $a_i < a_{i+1}$ dla każdego $i \in \mathbb{N}$, gdzie $a < b$ oznacza, że $a \leq b$ i $a \neq b$. Podobnie ciąg $\langle a_i : i \in \mathbb{N}\rangle$ jest *łańcuchem zstępującym*, jeśli $a_{i+1} < a_i$ dla każdego $i \in \mathbb{N}$.

Zadanie 503. Wykaż, że żaden przeliczalny nieskończony ściśle wstępujący łańcuch nie posiada w zbiorze $\mathcal{F}$ kresu górnego.

Zadanie 504. Jak jest największa moc ściśle a) wstępującego, b) zstępującego łańcucha w zbiorze $\mathcal{F}$?

Zadanie 505. Na zbiorze $\{0, 1\}$ wprowadzamy porządek $\leq$ kładąc $0 \leq 1$. Niech $\preceq$ będzie porządkiem leksykograficznym na zbiorze $\{0, 1\}^*$ wyznaczonym przez porządek $\leq$. Wykaż, że w zbiorze $\langle\{0, 1\}^*, \preceq\rangle$ istnieje nieskończony łańcuch wstępujący i nieskończony łańcuch zstępujący. Czy zbiór $\langle\{0, 1\}^*, \preceq\rangle$ posiada element najmniejszy lub największy?

10.1. Kraty

Definicja 158. Porządek $\langle P, \leq\rangle$ jest *kratą zupełną*, jeśli każdy podzbiór zbioru P ma kres górny i kres dolny. Porządek $\langle P, \leq\rangle$ jest *kratą*, jeśli posiada elementy najmniejszy i największy oraz gdy każdy *skończony* podzbiór zbioru P ma kres górny i kres dolny.

Przykład 159. Dla dowolnego zbioru A rodzina $\mathcal{P}(A)$ uporządkowana relacją inkluzji $\subseteq$ jest kratą zupełną.

Twierdzenie 160. 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 506. Niech A będzie dowolnym zbiorem niepustym. Czy $\langle\mathcal{K}, \subseteq\rangle$ jest kratą zupełną, jeżeli $\mathcal{K}$ jest rodziną wszystkich

1. relacji binarnych,
2. relacji równoważności,
3. relacji częściowego porządku

na zbiorze A?

Zadanie 507. Niech $\mathcal{X}$ będzie przeliczalną rodziną podzbiorów $\mathbb{N}$. Udowodnij, że istnieje przeliczalna rodzina $\mathcal{K}$, taka, że $\mathcal{X} \subseteq \mathcal{K}$ i $\langle\mathcal{K}, \subseteq\rangle$ jest kratą.

Zadanie 508. Czy porządek z zadania 461 jest a) kratą, b) kratą zupełną?

10.2. Porządki zupełne

Definicja 161. Niech $\langle P, \leq_P \rangle$ będzie zbiorem częściowo uporządkowanym. Wtedy zbiór $\emptyset \neq X \subseteq P$ jest zbiorem *skierowanym*, jeśli każda para $x, y \in X$ elementów zbioru X ma w X ograniczenie górne, tj. prawdziwa jest formuła

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

Zbiór $\langle P, \leq_P \rangle$ jest *porządkiem zupełnym*, jeśli P ma element najmniejszy oraz każdy skierowany podzbiór X zbioru P ma kres górny.

Definicja 162. 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 312). W zbiorze klas abstrakcji $\mathcal{P}(\mathbb{N})/_\sim$ wprowadzamy taką relację $\leq$, że

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

Zadanie 509. Sprawdź, czy definicja $\leq$ jest poprawna.

Zadanie 510. Sprawdź, czy $\leq$ jest porządkiem częściowym.

Zadanie 511. Znajdź w $\langle \mathcal{P}(\mathbb{N})/_\sim, \leq \rangle$ nieskończony podzbiór liniowo uporządkowany.

Zadanie 512. Znajdź w $\langle \mathcal{P}(\mathbb{N})/_\sim, \leq \rangle$ nieskończony antyłańcuch.

Zadanie 513. Wykaż, że $\langle \mathcal{P}(\mathbb{N})/_\sim, \leq \rangle$ nie jest zupełny.

Zadanie 514. Niech Z oznacza zbiór wszystkich nieskończonych podzbiorów zbioru liczb naturalnych. 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 515. Czy $\langle \mathcal{P}(\mathbb{N})/_\sim, \leq \rangle$ jest kratą?

Definicja 163. W zbiorze $\mathcal{P}(\mathbb{N})/\sim$ definiujemy porządek $\preceq$ kładąc $[X]_\sim \preceq [Y]_\sim$, jeśli $X \cup Y \in [Y]_\sim$.

Zadanie 516. Sprawdź, czy powyższa definicja jest poprawna. Czy $\langle \mathcal{P}(\mathbb{N})/\sim, \preceq \rangle$ jest kratą?

Zadanie 517. Czy zbiór $\{[X_n]_\sim \mid n \in \mathbb{N}\}$, gdzie $X_n = \{2^n k \mid k \in \mathbb{N}\}$ ma kres dolny w $\langle \mathcal{P}(\mathbb{N})/\sim, \preceq \rangle$?

Zadanie 518. Czy w $\langle \mathcal{P}(\mathbb{N})/\sim, \preceq \rangle$ istnieje nieskończony antyłańcuch?

Definicja 164. 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 165.

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

Zadanie 519. Udowodnij, że jeśli $\langle P, \leq_P \rangle$ jest skończoną kratą to każda monotoniczna funkcja $f : P \to P$ jest ciągła.

Zadanie 520. Pokaż, że relacja inkluzji na rodzinie skończonych podzbiorów zbioru liczb naturalnych nie jest porządkiem zupełnym.

Zadanie 521. 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 522. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą porządkami zupełnymi. W produkcie $A \times B$ definiujemy relację $\leq$ jako rozszerzenie leksykograficzne obu porządków, czyli $\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle$ wtedy i tylko wtedy, gdy $a_1 <_A a_2$ lub gdy $a_1 = a_2$ i $b_1 \leq_B b_2$. Udowodnij, że $\langle A \times B, \leq \rangle$ jest porządkiem zupełnym.

Zadanie 523. Podaj przykład takiego porządku zupełnego $\langle A, \leq \rangle$, że porządek leksykograficzny na A^* generowany przez $\leq$ nie jest zupełny.

Zadanie 524. 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 525. 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 526. 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 527. 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 528. Zbiór W na płaszczyźnie jest *wypukły*, jeśli wraz z każdymi dwoma punktami zawiera cały łączący je odcinek, tj. gdy $\overline{ab} \subseteq W$ dla dowolnych punktów $a, b \in W$. Pokaż, że relacja inkluzji na rodzinie wypukłych podzbiorów płaszczyzny jest porządkiem zupełnym.

Zadanie 529. Czy porządek z zadania 461 jest zupełny?

10.3. Twierdzenia o punkcie stałym

Twierdzenie 166 (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 z twierdzenia Knastera-Tarskiego nazywamy *najmniejszym punktem stałym* funkcji f. Element spełniający tylko warunek 1 nazywamy *punktem stałym*.

Twierdzenie 167 (Kleene). 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 530. 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 531. 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 532. Niech R^+ będzie najmniejszym punktem stałym funkcji ϕ_R. Wykaż, że R^+ jest najmniejszą (względem relacji inkluzji $\subseteq$) relacją równoważności zawierającą relację R.

Zadanie 533. Na rodzinie $\mathcal{L} = \mathcal{P}(\{0, 1\}^*)$ wszystkich języków nad alfabetem $\{0, 1\}$ określamy funkcję

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

Znajdź najmniejszy punkt stały funkcji f w zbiorze $\mathcal{L}$ uporządkowanym relacją inkluzji. Czy istnieje największy punkt stały tej funkcji? Ile punktów stałych ma funkcja $g(X) = \{w01 \mid w \in X\} \cup \{\epsilon\}$?

Zadanie 534. Grafem skierowanym o wierzchołkach V i krawędziach E nazywamy taką parę $\langle V, E\rangle$, że V jest skończonym zbiorem oraz $E \subseteq V \times V$. Ścieżką (długości n, o początku w v_0 i końcu w v_n) w grafie $\langle V, E\rangle$ nazywamy taki ciąg wierzchołków $\langle v_0, \ldots, v_n\rangle$, że dla wszystkich $0 \leq i \leq n-1$ zachodzi $\langle v_i, v_{i+1}\rangle \in E$ (w szczególności dla dowolnego wierzchołka v ciąg $\langle v\rangle$ jest ścieżką długości 0). Mówimy, że wierzchołek v jest osiągalny z wierzchołka v_0 jeśli w grafie istnieje ścieżka o początku w v_0 i końcu w v. Udowodnij, że zbiór wierzchołków osiągalnych z v_0 w grafie $\langle V, E\rangle$ jest najmniejszym punktem stałym funkcji $f : \mathcal{P}(V) \to \mathcal{P}(V)$ zadanej wzorem

$$f(X) = \{v_0\} \cup \{v \in V \mid \exists x \in X \;\; \langle x, v\rangle \in E\}.$$

Zadanie 535. Niech $R \subseteq A^2$ będzie relacją binarną na zbiorze A. Udowodnij, że przechodnie domknięcie relacji R jest najmniejszym punktem stałym funkcji $f : \mathcal{P}(A^2) \to \mathcal{P}(A^2)$ danej wzorem $f(X) = R \cup XX$.

10.4. Relacje w zbiorze formuł zdaniowych

Definicja 168. Niech V będzie zbiorem zmiennych zdaniowych. W zbiorze $\mathcal{F}(V)$ formuł zdaniowych, zbudowanych ze zmiennych ze zbioru V, spójnika negacji $\neg$ i spójników koniunkcji $\wedge$, alternatywy $\vee$, implikacji $\Rightarrow$ i równoważności $\Leftrightarrow$ wprowadzamy binarną relację $\sim$ przyjmując, że:

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

Zadanie 536. Wykaż, że $\sim$ jest relacją równoważności.

Zadanie 537. W zbiorze $\mathcal{F}(V)$ wprowadzamy relacje $\sim_1$, $\sim_2$ i $\sim_3$ przyjmując, że

- $\alpha \sim_1 \beta$ wtedy i tylko wtedy, gdy formuła $(\alpha \Leftrightarrow \beta)$ jest spełnialna;
- $\alpha \sim_2 \beta$ wtedy i tylko wtedy, gdy formuła $(\alpha \Leftrightarrow \beta)$ jest sprzeczna;
- $\alpha \sim_3 \beta$ wtedy i tylko wtedy, gdy formuła $(\alpha \Leftrightarrow \beta)$ jest prawdziwa dla dokładnie połowy wartościowań zmiennych występujących w formułach α i β.

Które z tych relacji są relacjami równoważności?

Definicja 169. Niech $\phi_a \in \mathcal{F}(V)$ będzie ustaloną formułą. W zbiorze formuł zdaniowych $\mathcal{F}(V)$ wprowadzamy binarną relację $\sim_{\phi_a}$, przyjmując, że

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

Zadanie 538. Udowodnij, że $\sim_{\phi_a}$ jest relacją równoważności. Opisz klasy równoważności formuł $p \vee \neg p$ i $p \wedge \neg p$.

Definicja 170. 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 539. Sprawdź, że powyższa definicja relacji $\leq$ jest poprawna (nie zależy od wyboru reprezentanta klasy abstrakcji) i że definiuje porządek częściowy.

Zadanie 540. Czy $\langle \mathcal{F}(V)/_\sim, \leq \rangle$ jest kratą?

Zadanie 541. Czy $\langle \mathcal{F}(V)/_\sim, \leq \rangle$ jest kratą zupełną?

Zadanie 542. Przyjmijmy, że zbiór zmiennych V jest przeliczalny nieskończony. Znajdź w zbiorze $\langle \mathcal{F}(V)/_\sim, \leq \rangle$ nieskończony podzbiór liniowo uporządkowany (łańcuch).

Zadanie 543. Przyjmijmy, że zbiór zmiennych V jest przeliczalny nieskończony. Czy można w zbiorze $\langle \mathcal{F}(V)/_\sim, \leq \rangle$ znaleźć nieskończony antyłańcuch?

Zadanie 544. 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 545. Wypisz najkrótszych reprezentantów wszystkich klas abstrakcji relacji $\sim$ gdy zbiór V ma dwa elementy. Narysuj diagram porządku $\leq$ dla tego przypadku.

Zadanie 546. 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 547. Niech $V = \{p_n\}_{n=0}^\infty$ będzie zbiorem zmiennych. Wyznacz kresy (dolny i górny) zbiorów $F_2 = \{[\alpha_n]_\sim\}_{n=0}^\infty$ i $F_3 = \{[\beta_n]_\sim\}_{n=0}^\infty$, 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 548. Niech $V = \{p_n\}_{n=0}^\infty$ będzie zbiorem zmiennych. Wyznacz kresy (dolny i górny) zbioru $F_4 = \{[\gamma_n]_\sim\}_{n=0}^\infty$, gdzie $\gamma_n = \bigvee_{i=0}^n (p_{2i} \vee \neg p_{2i+1})$.

Zadanie 549. 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 550. Niech $\mathcal{F}$ będzie zbiorem formuł zadaniowych zbudowanych ze zmiennych ze zbioru $V = \{p, q, r, \ldots\}$ i spójników implikacji $\Rightarrow$, fałszu $\perp$ i prawdy $\top$. Binarna relacja R na zbiorze $\mathcal{F}$ jest *monotoniczna*, jeśli

1. $\perp R \phi$,
2. $\phi R \top$,
3. jeśli $\phi_1 R \phi_2$ i $\psi_1 R \psi_2$, to $(\phi_2 \Rightarrow \psi_1) R (\phi_1 \Rightarrow \psi_2)$,

dla wszelkich formuł $\phi, \phi_1, \phi_2, \psi_1, \psi_2 \in \mathcal{F}$.

1. Pokaż, że w zbiorze relacji monotonicznych na $\mathcal{F}$ uporządkowanym relacją inkluzji istnieje element najmniejszy. Relację tę będziemy oznaczać $\sqsubseteq$.
2. Pokaż, że relacja $\sqsubseteq$ jest częściowym porządkiem na $\mathcal{F}$. Pokaż, że nie jest to porządek liniowy.
3. Pokaż, że $\langle \mathcal{F}, \sqsubseteq \rangle$ jest kratą.
4. Pokaż, że jeśli $\phi \sqsubseteq \psi$, to $\phi \Rightarrow \psi$ jest tautologią. Pokaż, że implikacja odwrotna nie zachodzi.

11

Dobre porządki i indukcja

11.1. Porządki regularne

Definicja 171. Porządek częściowy $\langle P, \leq \rangle$ jest *regularny* (*dobrze ufundowany*), jeśli w każdym niepustym zbiorze $X \subseteq P$ istnieje element minimalny. Mówimy, że porządek jest *dobry*, jeśli jest liniowy i regularny.

Twierdzenie 172.[1] Jeśli porządek $\langle P, \leq \rangle$ jest regularny, to w zbiorze P nie istnieje nieskończony ciąg ściśle malejący, tj taki ciąg $a_0, a_1, a_2, \ldots$, że $a_{i+1} < a_i$ dla wszystkich $i \in \mathbb{N}$.

Zadanie 551. Pokaż, że porządek $\langle \mathbb{N}, | \rangle$ (por. Przykład 131) jest regularny.

Zadanie 552. 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 553. Niech $\langle A, \leq_A \rangle$ i $\langle B, \leq_B \rangle$ będą dobrymi porządkami. W produkcie $A \times B$ definiujemy relację $\leq$ jako rozszerzenie leksykograficzne obu porządków, czyli $\langle a_1, b_1 \rangle \leq \langle a_2, b_2 \rangle$ wtedy i tylko wtedy, gdy $a_1 <_A a_2$ lub gdy $a_1 = a_2$ i $b_1 \leq_B b_2$. Udowodnij, że $\langle A \times B, \leq \rangle$ jest dobrym porządkiem.

Zadanie 554. Podaj przykład takiego dobrego porządku $\langle A, \leq \rangle$, że porządek leksykograficzny na A^* generowany przez $\leq$ nie jest dobry.

Zadanie 555. 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.

[1] Przy założeniu aksjomatu wyboru prawdziwe jest również twierdzenie odwrotne.

Zadanie 556. 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 557. W zbiorze $\mathbb{N} \setminus \{0\}$ wprowadzamy relację R wzorem

$$xRy \overset{\text{df}}{\Leftrightarrow} (2|x \wedge 2|y \wedge y \leq x) \vee (2|x \wedge \neg(2|y)) \vee (\neg(2|x) \wedge \neg(2|y) \wedge x \leq y).$$

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

Zadanie 558. 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 559. 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 560. 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 561. Niech $\mathcal{F} = \{f \in \{0,1\}^{\mathbb{N}} \mid \{n \in \mathbb{N} \mid f(n) = 1\}$ jest skończony$\}$. W zbiorze $\mathcal{F}$ wprowadzamy relacje $\leq_F$ i $\leq_L$ kładąc

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

1. Czy $\langle \mathcal{F}, \leq_F \rangle$ jest porządkiem liniowym?
2. Czy $\langle \mathcal{F}, \leq_L \rangle$ jest porządkiem liniowym?

3. Czy $\langle \mathcal{F}, \leq_F \rangle$ jest porządkiem regularnym?
4. Czy $\langle \mathcal{F}, \leq_L \rangle$ jest porządkiem regularnym?
5. Czy $\langle \mathcal{F}, (\leq_F)^{-1} \rangle$ jest porządkiem regularnym?
6. Czy $\langle \mathcal{F}, (\leq_L)^{-1} \rangle$ jest porządkiem regularnym?

Zadanie 562. Czy porządek zadany definicją 162 jest regularny?

Zadanie 563. Czy na zbiorze A o mocy większej niż 1 można zdefiniować porządek jednocześnie dobry i gęsty?

Definicja 173. Binarna relacja R na zbiorze X jest *słabo konfluentna*, jeśli dla każdych $x_1, x_2, x_3 \in X$ istnieje taki $x_4 \in X$, że jeśli $x_1 R x_2$ i $x_1 R x_3$, to $x_2 \bar{R} x_4$ i $x_3 \bar{R} x_4$, gdzie $\bar{R}$ jest przechodnim domknięciem relacji R. Relacja R jest *konfluentna*, jeśli dla każdych $x_1, x_2, x_3 \in X$ istnieje taki $x_4 \in X$, że jeśli $x_1 \bar{R} x_2$ i $x_1 \bar{R} x_3$, to również $x_2 \bar{R} x_4$ i $x_3 \bar{R} x_4$, gdzie $\bar{R}$ jest przechodnim domknięciem relacji R.

Zadanie 564. Pokaż, że istnieje relacja R słabo konfluentna, która nie jest konfluentna.

Zadanie 565. Pokaż, że istnieje relacja R słabo konfluentna, której graf jest acykliczny i która nie jest konfluentna.

Definicja 174. Binarna relacja R na zbiorze X jest *ufundowana* jeśli nie istnieje taki nieskończony ciąg $a_0, a_1, a_2, \ldots$, że $a_i \, R \, a_{i+1}$ dla wszystkich $i \in \mathbb{N}$.

Zadanie 566. Pokaż, że jeśli relacja R jest ufundowana i słabo konfluentna, to jest konfluentna.

Zadanie 567. Niech $\mathcal{K}$ będzie taką rodziną podzbiorów zbioru liczb naturalnych, że relacja zawierania na tej rodzinie jest porządkiem regularnym. Pokaż, że każdy łańcuch w tym porządku jest przeliczalny.

Zadanie 568. Dane są dwa niemalejące ciągi liczb naturalnych $\langle a_0, a_1, a_2, \ldots \rangle$ oraz $\langle b_0, b_1, b_2, \ldots \rangle$. Przypuśćmy, że te ciągi „podobnie rosną”, tzn. dla dowolnej liczby naturalnej n spełnione są warunki:

1. jeżeli $a_n < b_n$, to $a_n < a_{n+1}$ oraz $b_n = b_{n+1}$,
2. jeżeli $b_n < a_n$, to $b_n < b_{n+1}$ oraz $a_n = a_{n+1}$.

Udowodnij, że jeżeli liczba c jest wyrazem obu tych ciągów, to c jest wyrazem tych ciągów o tym samym numerze (tj. istnieje taka liczba $i \in N$, że $a_i = c = b_i$).

Zadanie 569. Czy porządek z zadania 461 jest regularny?

11.2. Indukcja

Twierdzenie 175 (zasada indukcji). Niech $\langle P, \leq \rangle$ będzie regularnym porządkiem częściowym. Jeśli $X \subseteq P$ spełnia warunek $\forall x\, ((\forall y{<}x \;\; y \in X) \Rightarrow x \in X)$, to $X = P$.

Przykład 176. *Grafem prostym* o wierzchołkach V i krawędziach E nazywamy taką parę $\langle V, E\rangle$, że V jest skończonym zbiorem oraz $E \subseteq V \times V$ jest relacją antyzwrotną i symetryczną.[2] Pokażemy, że dla wszystkich dodatnich liczb naturalnych n każdy n-wierzchołkowy graf prosty ma nie więcej niż $\frac{n(n-1)}{2}$ krawędzi. Skorzystamy w tym celu z zasady indukcji dla $\langle \mathbb{N}^+, \leq\rangle$ (oczywiście jest to porządek regularny).

Niech

$$X = \{n \in \mathbb{N}^+ \;\;|\;\; \text{każdy } n\text{-wierzchołkowy graf prosty ma nie więcej niż } \tfrac{n(n-1)}{2} \text{ krawędzi}\}.$$

Pokażemy, że spełniony jest warunek

$$\forall n \in \mathbb{N}^+\, ((\forall i{<}n \;\; i \in X) \Rightarrow n \in X) \tag{1}$$

Weźmy dowolną liczbę $n \in \mathbb{N}^+$ i rozważmy następujące dwa przypadki.

Przypadek 1: $n = 1$. Rozważmy dowolny 1-wierzchołkowy graf $G = \langle V, E\rangle$. Ponieważ relacja E jest antyzwrotna, więc graf G nie ma wcale krawędzi (ich liczba jest ograniczona przez 0). Mamy $0 = \frac{1\cdot 0}{2}$, co pokazuje, że w tym przypadku $n \in X$ i implikacja

$$(\forall i{<}n \;\; i \in X) \quad \Rightarrow \quad n \in X \tag{2}$$

jest prawdziwa.

Przypadek 2: $n > 1$. Załóżmy, że prawdziwy jest warunek $\forall i{<}n \;\; i \in X$. Chcemy pokazać, że $n \in X$, czyli że każdy n-wierzchołkowy graf prosty ma nie więcej niż $\frac{n(n-1)}{2}$ krawędzi. Rozważmy zatem dowolny n-wierzchołkowy graf $G = \langle V, E\rangle$. Wybierzmy w zbiorze V dowolny wierzchołek v i usuńmy go z grafu otrzymując graf $G' = \langle V', E'\rangle$, gdzie $V' = V - \{v\}$ oraz $E' = E \cap (V' \times V')$. Graf G' jest $(n-1)$-wierzchołkowy, więc z założenia indukcyjnego liczba krawędzi w E' jest ograniczona przez $\frac{(n-1)(n-2)}{2}$. W zbiorze $E - E'$ jest co najwyżej $n-1$ krawędzi, a zatem łączna liczba krawędzi w E nie przekracza $\frac{(n-1)(n-2)}{2} + (n-1) = \frac{n(n-1)}{2}$. Ponieważ graf G był wybrany dowolnie, więc każdy n-wierzchołkowy graf ma nie więcej niż $\frac{n(n-1)}{2}$ krawędzi, a zatem $n \in X$ i również w tym przypadku implikacja (2) jest prawdziwa.

[2] W języku teorii grafów oznacza to, że nie ma pętli w wierzchołkach i krawędzie nie są skierowane.

Ponieważ liczba n była wybrana jako dowolna, dowiedliśmy prawdziwości warunku (1). Na mocy zasady indukcji otrzymujemy, że $X = \mathbb{N}^+$, czyli dla wszystkich dodatnich liczb naturalnych n każdy n-wierzchołkowy graf prosty ma nie więcej niż $\frac{n(n-1)}{2}$ krawędzi. ∎

Okazuje się, że samodzielne sformułowanie powyższego rozumowania sprawia ogromne kłopoty wielu studentom. Poniżej wymieniamy najczęściej spotykane błędy w tego typu rozumowaniach.

- Sprawdzenie podstawy indukcji dla $n = 1$, $n = 2$ i $n = 3$: Zwykle wystarcza rozważenie jednego przypadku bazowego. Sprawdzenie prawdziwości twierdzenia dla drugiej z kolei liczby jest konieczne tylko wtedy, gdy chcemy skorzystać z założenia, że $n - 2 \in X$ (bo dla $n = 2$ mamy $n - 2 \notin \mathbb{N}^+$ i z takiego założenia nie da się skorzystać); tutaj natomiast nie ma takiej potrzeby.

- Użycie sformułowania „teza z zadania dla $n = k$": zwykle student używający takiego sformułowania nie wie, co ono oznacza. W szczególności nie wiadomo, czy oznacza ono zdanie „$k \in X$" czy może „$k \in X \Rightarrow (k + 1) \in X$", czy też „$\forall k\ k \in X \Rightarrow (k + 1) \in X$" czy „$\forall k\ k \in X$".

- Oparcie dowodu kroku indukcyjnego na schemacie „weźmy dowolny graf $(n - 1)$-wierzchołkowy i dodajmy do niego wierzchołek": tu błąd polega na tym, że mamy coś dowieść dla *wszystkich* grafów n-wierzchołkowych, ale nie da się otrzymać dowolnego grafu n-wierzchołkowego dodając wierzchołek do dowolnego grafu $(n - 1)$-wierzchołkowego. W szczególności dla $n = 4$ nie da się otrzymać trójramiennej gwiazdy dodając wierzchołek do trójkąta.

- Rozpoczęcie dowodu kroku indukcyjnego od sformułowania „niech k będzie liczbą krawędzi w grafie": tu nie wiadomo o jaki graf chodzi, a nie każdy graf ma tyle samo krawędzi.

Zadania poniżej należy rozwiązywać korzystając z zasady indukcji podanej w Twierdzeniu 175. Z innej wersji zasady indukcji można skorzystać tylko pod warunkiem, że umie się tę inną wersję udowodnić.[3]

Zadanie 570. Skończony zbiór liniowo uporządkowany $\langle A, \leq_A \rangle$ ma n elementów, a zbiór uporządkowany $\langle B, \leq_B \rangle$ ma 2 elementy, przy czym $A \cap B = \emptyset$. Na ile sposobów można porządek liniowy na A rozszerzyć o elementy zbioru B (to znaczy znaleźć taki porządek liniowy $\langle A \cup B, \leq \rangle$, że $(a_1 \leq_A a_2) \Leftrightarrow (a_1 \leq a_2)$, dla $a_1, a_2 \in$

[3] Dlaczego? Otóż w przyszłości będziecie musieli często korzystać z indukcji strukturalnej (w której porządek zadany jest przez strukturę termów, grafów, dowodów itp.). Np. przy uzasadnianiu poprawności algorytmu wyprowadzania typu potrzebna będzie indukcja względem budowy dowodu osądu typowego. Teraz nie wiemy jeszcze co to jest osąd typowy, ale jak się dowiemy to nie będzie już czasu na zastanawianie się co to jest indukcja.

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 571. 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 572. Pokaż przez indukcję, że dla każda formuła zbudowana ze zmiennych zdaniowych i spójników $\wedge$, $\vee$ jest spełnialna.

Zadanie 573. Pokaż przez indukcję, że dla każdego zbioru A mocy $n \in \mathbb{N}$ istnieje $n!$ bijekcji $f : A \to A$.

Zadanie 574. Udowodnij przez indukcję, że każdą liczbę naturalną większą od 1 można przedstawić w postaci iloczynu liczb pierwszych. *Wskazówka:* wybierz odpowiedni porządek.

Zadanie 575. Niech $X \subseteq \mathbb{N}$. Udowodnij, że jeśli

- $0 \in X$, $1 \in X$ oraz $2 \in X$,
- dla dowolnego $x \in \mathbb{N}$, z tego, że $x \in X$, $x + 1 \in X$ oraz $x + 2 \in X$ wynika, że $x + 3 \in X$,

to $X = \mathbb{N}$.

Zadanie 576. Mówimy, że graf prosty $G = \langle V, E\rangle$ jest *spójny*, jeśli zwrotne i przechodnie domknięcie relacji E jest równe $V \times V$ (w języku teorii grafów oznacza to, że każde dwa wierzchołki są połączone ścieżką). Pokaż przez indukcję, że (dla wszystkich dodatnich liczb naturalnych n) każdy n-wierzchołkowy graf spójny ma co najmniej $n - 1$ krawędzi.

Zadanie 577. Funkcja Ackermanna zdefiniowana jest wzorem

$$A(x, y) = \begin{cases} y + 1, & \text{dla} \quad x = 0 \\ A(x-1, 1) & \text{dla} \quad x > 0 \text{ i } y = 0 \\ A(x-1, A(x, y-1)) & \text{wpp} \end{cases}$$

Udowodnij indukcyjnie, że istnieje co najwyżej jedna funkcja spełniająca te równości.

Zadanie 578. Smok Strachota ma (skończenie) wiele głów, a każda jego głowa ma (skończenie) wiele paszcz. Kiedy rycerz odetnie Strachocie głowę, w miejsce odciętej odrasta smokowi tyle głów ile ten sobie zażyczy, ale każda z tych nowych głów ma mniej paszcz niż odcięta głowa.

Stanem smoka nazywamy taką funkcję $g : \mathbb{N} \to \mathbb{N}$, że $g(i)$ oznacza liczbę głów o i paszczach. Powiemy, że stan smoka jest *bezpieczny* jeśli w skończenie wielu cięciach można pozbawić smoka wszystkich głów. Udowodnij indukcyjnie, że każdy stan smoka jest bezpieczny.

Wskazówka: Główna (i niemal jedyna) trudność tego zadania to zdefiniowanie odpowiedniego porządku na stanach smoka.

Twierdzenie 177 (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 178 (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 179 (O definiowaniu funkcji przez indukcję noetherowską). Niech $\langle A, \leq\rangle$ będzie zbiorem regularnym i niech B, C będą dowolnymi zbiorami. Niech $B^{\subseteq A\times C}$ oznacza zbiór funkcji częściowych z $A \times C$ w B. Dla dowolnej funkcji $h : B^{\subseteq A\times C} \times A \times C \to B$ 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 579. Udowodnij, że istnieje dokładnie jedna funkcja *suma* $: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ i dokładnie jedna funkcja *iloczyn* $: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ spełniająca równania

$$\begin{aligned}
&suma(n, 0) = n\\
&suma(n, m + 1) = suma(n, m) + 1\\
\\
&iloczyn(n, 0) = 0\\
&iloczyn(n, m + 1) = n + iloczyn(n, m).
\end{aligned}$$

Zadanie 580. Czy istnieje dokładnie jedna funkcja $f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ spełniająca równości $f(\emptyset) = \emptyset$ i $f(X \cup \{n\}) = f(X) \cup \{n\}$ dla wszystkich $n \in \mathbb{N}$?

12

Algebra termów

Definicja 180. *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 181 (Algebra termów). Niech Σ będzie sygnaturą i niech $V = \{v_i \mid i \in \mathbb{N}\}$ będzie zbiorem zmiennych (zakładamy, że $\Sigma \cap V = \emptyset$). Przez $T(\Sigma, V)$ będziemy oznaczać zbiór termów nad Σ, czyli najmniejszy zbiór zawierający zmienne i symbole stałych (to znaczy $V \subseteq T(\Sigma, V)$ i $\Sigma_0 \subseteq T(\Sigma, V)$) i zamknięty względem Σ (to znaczy jeśli $f \in \Sigma_n, t_1, \ldots, t_n \in T(\Sigma, V)$, 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.

Definicja 182. 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 $t' \sqsubseteq t$.

12.1. Inna definicja zbioru termów. Drzewa

Definicja 183. Niech A będzie dowolnym zbiorem. Zbiór $T \subseteq A^*$ jest *drzewem* jeśli jest zamknięty na przedrostki (to znaczy, jeśli $u \prec w$ (u jest przedrostkiem w) oraz $w \in T$, to $u \in T$).

Elementy drzewa nazywamy *wierzchołkami*. Każde drzewo zawiera słowo puste ϵ. Słowo puste nazywamy *korzeniem drzewa*. Jeśli $w \in T$ oraz $wa \in T$ dla $w \in A^*$, $a \in A$, to mówimy, że wa jest *następnikiem* (*synem*) w w T, w nazywamy *poprzednikiem* (*ojcem*) wa. Wierzchołek T, który nie ma następników nazywamy *liściem*. *Ścieżką* w drzewie T nazywamy dowolny podzbiór T liniowo uporządkowany relacją $\prec$. Ścieżka w drzewie T jest *gałęzią*, jeśli jest maksymalnym podzbiorem T

liniowo uporządkowanym relacją $\prec$. Każda gałąź zawiera korzeń drzewa. Jeśli gałąź jest skończona, to zawiera dokładnie jeden liść. *Stopniem* wierzchołka w w drzewie T nazywamy liczbę następników w. *Długością ścieżki* π nazywamy moc zbioru π. *Wysokością drzewa* T nazywamy kres górny długości ścieżek w T. Jeśli drzewo T jest skończone, to jego wysokość jest równa długości najdłuższej gałęzi w T.

Definicja 184. 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 185. *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 186. 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 taką funkcją, że jeśli $w \in T$, $e(w) \in \Sigma_n$, to w ma stopień n.

Definicja 187. 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 $w \in T$.

12.2. Podstawienia

Definicja 188. Niech Σ będzie sygnaturą a V zbiorem zmiennych. *Podstawieniem* w zbiorze termów $T(\Sigma, V)$ nazywamy funkcję przyporządkowującą zmiennym ze zbioru V elementy $T(\Sigma, V)$.

Podstawienie $\sigma : V \to T(\Sigma, V)$ rozszerzamy do funkcji $\hat{\sigma} : T(\Sigma, V) \to T(\Sigma, V)$ kładąc $\hat{\sigma}(x) = \sigma(x)$ dla $x \in V$ oraz $\hat{\sigma}(f(t_1, \ldots, t_n) = f(\hat{\sigma}(t_1), \ldots, \hat{\sigma}(t_n))$. Jeśli nie będzie prowadzić to do nieporozumień, będziemy pisali σ zamiast $\hat{\sigma}$.

Term uzyskany z termu t przez zastąpienie każdego wystąpienia zmiennej x w termie t przez term $\sigma(x)$ nazywamy wartością termu t przy podstawieniu σ i oznaczamy $\sigma(t)$ lub $t\sigma$.

W dalszych częściach będziemy często rozważać podstawienia, które zmieniają tylko skończenie wiele zmiennych. Tradycyjnie podstawienie, które zmienia tylko zmienne $x_1, \ldots, x_n$ i przyporządkowuje im odpowiednio termy $t_1, \ldots, t_n$ oznacza się przez $[x_1/t_1, \ldots, x_n/t_n]$. Dokładniej, $[x_1/t_1, \ldots, x_n/t_n] : V \to T(\Sigma, V)$ jest funkcją zdefiniowaną wzorem

$$[x_1/t_1, \ldots, x_n/t_n](v) = \begin{cases} t_i & \text{jeśli } v = x_i \\ v & \text{w przeciwnym przypadku.} \end{cases}$$

W szczególności $[] : V \to T(\Sigma, V)$ jest funkcją identycznościową zbioru V. W literaturze można spotkać wiele innych sposobów oznaczania podstawień, takich jak $[t_1/x_1, \ldots, t_n/x_n]$, $[x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n]$ czy $[x_1 \mapsto t_1, \ldots, x_n \mapsto t_n]$, lub z użyciem nawiasów klamrowych, np. $\{x_1/t_1, \ldots, x_n/t_n\}$.

12.3. Problem unifikacji

Definicja 189. Niech Σ będzie sygnaturą. *Problemem unifikacji* nazywamy następujące zadanie: „mając dany zbiór $\{(t_1, s_1), \ldots, (t_n, s_n)\}$, znaleźć takie podstawienie σ, żeby dla każdego $i \leq n$ zachodziło $\sigma(t_i) = \sigma(s_i)$." To znaczy, należy znaleźć takie przyporządkowanie termów zmiennym występującym w termach t_1, $s_1, \ldots, t_n$, s_n, żeby po podstawieniu tych termów za odpowiednie zmienne uzyskać termy równe. Podstawienie σ nazywamy *unifikatorem* zbioru $\{(t_1, s_1), \ldots, (t_n, s_n)\}$. Często ten zbiór (nazywany czasem *instancją problemu unifikacji*) zapisujemy jako

$$\{t_1 \stackrel{?}{=} s_1, \ldots, t_n \stackrel{?}{=} s_n\}.$$

Definicja 190. Jeśli σ i τ są unifikatorami zbioru $\{(t_1, s_1), \ldots, (t_n, s_n)\}$, to mówimy, że σ jest *ogólniejsze* od τ, (co oznaczamy $\tau \leq \sigma$) jeśli istnieje takie podstawienie ϱ, że $\tau = \varrho\sigma$. Podstawienie σ nazywamy *najogólniejszym unifikatorem* zbioru

$$\mathcal{S} \quad = \quad \{t_1 \stackrel{?}{=} s_1, \ldots, t_n \stackrel{?}{=} s_n\},$$

jeśli σ jest unifikatorem $\mathcal{S}$ oraz σ jest ogólniejsze od każdego innego unifikatora $\mathcal{S}$.

Algorytm podany na rysunku 11 dla zadanej instancji problemu unifikacji znajduje jego najogólniejszy unifikator lub odpowiada „nie ma unifikatora". Dla przypomnienia: $\widehat{[x/t]}[\mathcal{S}]$ oznacza obraz zbioru $\mathcal{S}$ przez rozszerzenie podstawienia $[x/t]$, natomiast $[x/t]\sigma$ oznacza złożenie funkcji σ i $[x/t]$, przy czym najpierw wykonywana jest funkcja σ.

Zadanie 581. Udowodnij, że algorytm z rysunku 11 zawsze się zatrzymuje.

Zadanie 582. Znajdź unifikator dla podanych instancji problemu unifikacji (lub uzasadnij, że taki nie istnieje) w algebrze termów o sygnaturze $\Sigma = \{a, c, d, f, g, h, p\}$ i zbiorze zmiennych $\mathcal{X} = \{u, v, w, x, y, z, \ldots\}$.

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

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

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

wejście: zbiór równań $\mathcal{S} = \{t_1 \stackrel{?}{=} s_1, \ldots, t_n \stackrel{?}{=} s_n\}$
wyjście: najogólniejszy unifikator σ zbioru $\mathcal{S}$ lub *"nie ma unifikatora"*

$\sigma \leftarrow []$
while $\mathcal{S} \neq \emptyset$ **do**
  select $t \stackrel{?}{=} s$ **from** $\mathcal{S}$
  case $t \stackrel{?}{=} s$ **of**
    $f(t'_1, \ldots, t'_k) \stackrel{?}{=} f(s'_1, \ldots, s'_k)$:
      $\mathcal{S} \leftarrow \mathcal{S} \cup \{t'_1 \stackrel{?}{=} s'_1, \ldots, t'_k \stackrel{?}{=} s'_k\}$
    $f(t'_1, \ldots, t'_k) \stackrel{?}{=} g(s'_1, \ldots, s'_l)$ **where** $f \neq g$:
      return *nie ma unifikatora*
    $x \stackrel{?}{=} t$, **where** $x \in \mathcal{V}$:
      if $x \in \mathrm{FV}(t)$ **and** $x \neq t$ **then**
        return *nie ma unifikatora*
      else
        $\mathcal{S} \leftarrow [x \hat{/} t][\mathcal{S}]$
        $\sigma \leftarrow [x/t]\sigma$
    $t \stackrel{?}{=} x$, **where** $x \in \mathcal{V}$ **and** $t \notin \mathcal{V}$:
      $\mathcal{S} \leftarrow \mathcal{S} \cup \{x \stackrel{?}{=} t\}$
return σ

Rysunek 11. Algorytm unifikacji

4. $\{f(x_1, x_1) \stackrel{?}{=} x_2, f(x_2, x_2) \stackrel{?}{=} x_3, \ldots, f(x_{n-1}, x_{n-1}) \stackrel{?}{=} x_n\}$
5. $\{p(f(y), w, g(z)) \stackrel{?}{=} p(v, u, v)\}$
6. $\{p(a, x, f(g(y))) \stackrel{?}{=} p(z, h(w), f(w))\}$
7. $\{p(z, h(w), g(z)) \stackrel{?}{=} p(v, u, v)\}$

Następne trzy zadania są lematami służącymi do udowodnienia poprawności algorytmu unifikacji z rysunku 11. Nie wolno więc w ich rozwiązaniu korzystać z poprawności tego algorytmu.

Zadanie 583. Udowodnij, że jeśli θ jest unifikatorem $\{x \stackrel{?}{=} t\}$ to istnieje takie podstawienie σ, że $\theta = \sigma[x/t]$.

Zadanie 584. Udowodnij, że jeśli zmienna x występuje w termie t i $t \neq x$ to nie istnieje unifikator $\{x \stackrel{?}{=} t\}$.

Zadanie 585. Udowodnij, że jeśli zmienna x nie występuje w termie t to $[x/t]$ jest najbardziej ogólnym unifikatorem $\{x \stackrel{?}{=} t\}$.

Zadanie 586. W tym zadaniu będziemy rozważać zadania unifikacji składające się z nieskończonej liczby par termów. Udowodnij następujące twierdzenie o zwartości dla problemu unifikacji: zadanie unifikacji $\{t_i \stackrel{?}{=} s_i\}_{i\in I}$, w którym występuje jedynie skończenie wiele różnych zmiennych, ma rozwiązanie wtedy i tylko wtedy, gdy każde jego skończone podzadanie $\{t_i \stackrel{?}{=} s_i\}_{i\in I_0}$, dla $I_0 \subseteq I$, $|I_0| < \infty$, ma rozwiązanie. Pokaż, że twierdzenie jest fałszywe, jeśli zadanie zawiera nieskończenie wiele zmiennych.

13

Elementy logiki formalnej

13.1. Składnia języka pierwszego rzędu

Definicja 191. *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 192. 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 193. Zbiór formuł atomowych jest zbiorem napisów postaci $R(t_1,...,t_n)$, gdzie $R \in \Sigma_n^R$, zaś $t_1, \ldots, t_n$ są termami.

Definicja 194. 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 195. Zbiór zmiennych *wolnych* $\mathrm{FV}(\alpha)$ formuły α definiujemy indukcyjnie:

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

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

Definicja 196. 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 197. Formuła bez zmiennych wolnych nazywa się *zdaniem*.

13.2. Semantyka języka pierwszego rzędu

Definicja 198. *Struktura* $\mathfrak{A}$ *sygnatury* Σ to niepusty zbiór A zwany jej *uniwersum* i *interpretacja*, czyli funkcja $\cdot^{\mathfrak{A}}$, która każdemu symbolowi funkcji $f \in \Sigma_n^F$, gdzie $n \geq 0$, przyporządkowuje funkcję $f^{\mathfrak{A}} : A^n \to A$, każdemu symbolowi relacji $R \in \Sigma_n^R$, gdzie $n > 0$, przyporządkowuje relację $R^{\mathfrak{A}} \subseteq A^n$ i każdemu symbolowi $R \in \Sigma_0^R$ przyporządkowuje wartość logiczną ze zbioru $\{\mathsf{T}, \mathsf{F}\}$.

Definicja 199. *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 200. 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 201. 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 gdy $(t_1^{\mathfrak{A}}[v], \ldots, t_n^{\mathfrak{A}}[v]) \in R^{\mathfrak{A}}$.
3. $\mathfrak{A} \models (t_1 = t_2)[v]$ wtw gdy $t_1^{\mathfrak{A}}[v] = t_2^{\mathfrak{A}}[v]$.
4. $\mathfrak{A} \models (\neg\alpha)[v]$ wtw gdy nie zachodzi $\mathfrak{A} \models \alpha[v]$
5. $\mathfrak{A} \models (\alpha \wedge \beta)[v]$ wtw gdy zachodzą jednocześnie $\mathfrak{A} \models \alpha[v]$ i $\mathfrak{A} \models \beta[v]$.
6. $\mathfrak{A} \models (\alpha \vee \beta)[v]$ wtw gdy $\mathfrak{A} \models \alpha[v]$ lub $\mathfrak{A} \models \beta[v]$.
7. $\mathfrak{A} \models (\alpha \Rightarrow \beta)[v]$ wtw gdy nie zachodzi $\mathfrak{A} \models \alpha[v]$ lub zachodzi $\mathfrak{A} \models \beta[v]$.
8. $\mathfrak{A} \models (\alpha \Leftrightarrow \beta)[v]$ wtw gdy jednocześnie nie zachodzą $\mathfrak{A} \models \alpha[v]$ i $\mathfrak{A} \models \beta[v]$, lub jednocześnie zachodzą $\mathfrak{A} \models \alpha[v]$ i $\mathfrak{A} \models \beta[v]$.
9. $\mathfrak{A} \models (\forall x.\alpha)[v]$ wtw gdy dla każdego elementu $a \in A$ zachodzi $\mathfrak{A} \models \alpha[v_x^a]$.

10. $\mathfrak{A} \models (\exists x.\alpha)[v]$ wtw gdy istnieje element $a \in A$ dla którego zachodzi $\mathfrak{A} \models \alpha[v_x^a]$.

Definicja 202. 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 $\mathfrak{A}$.

Zadanie 587. Korzystając wprost z definicji semantyki języka pierwszego rzędu pokaż, że formuła $\forall x \exists y\ x < y$ jest prawdziwa w strukturze, której uniwersum jest zbiór liczb naturalnych a interpretacją symbolu $<$ jest naturalny porządek na liczbach.

Zadanie 588. Niech ϕ i ψ będą formułami logiki pierwszego rzędu. Korzystając wprost z definicji semantyki języka pierwszego rzędu udowodnij, że następujące formuły są tautologiami.

- $(\exists x\ \phi \Rightarrow \psi) \Rightarrow \forall x\ \phi \Rightarrow \exists x\ \psi$
- $(\forall x\ \phi \Rightarrow \psi) \Rightarrow \exists x\ \phi \Rightarrow \exists x\ \psi$

Zadanie 589. Udowodnij, że dla każdej formuły logiki pierwszego rzędu istnieje równoważna jej formuła nie zawierająca kwantyfikatorów $\forall$.

Zadanie 590. Rozważmy dwa izomorficzne porządki $\mathcal{A} = \langle A, \leq_A \rangle$ i $\mathcal{B} = \langle B, \leq_B \rangle$. Traktujemy te porządki jak struktury nad sygnaturą bez symboli funkcyjnych i z jednym symbolem relacyjnym $\leq$, w których relacje $\leq_A$ i $\leq_B$ są interpretacjami symbolu $\leq$.

1. Udowodnij, że formuła $\forall x \exists y\ x \leq y$ jest prawdziwa w strukturze $\mathcal{A}$ wtedy i tylko wtedy, gdy jest prawdziwa w strukturze $\mathcal{B}$.
2. Udowodnij, że dla każdej formuły ϕ logiki I rzędu, w której nie występują symbole funkcyjne i $\leq$ jest jedynym symbolem relacyjnym zachodzi równoważność
$$\mathcal{A} \models \phi \text{ wtedy i tylko wtedy, gdy } \mathcal{B} \models \phi.$$

13.3. Podstawienia

Twierdzenie 203 (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 204. 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.

13.4. Rezolucja dla rachunku I rzędu

Definicja 205. *Literał* w rachunku kwantyfikatorów to formuła atomowa lub negacja formuły atomowej. *Klauzulą* nazywamy alternatywę skończenie wielu literałów. Alternatywę zera literałów nazywamy klauzulą pustą i oznaczamy $\perp$.

Definicja 206. Jeśli C i D są klauzulami, A i B formułami atomowymi i σ najogólniejszym unifikatorem A i B to klauzulę $\sigma(C \vee D)$ nazywamy *rezolwentą* klauzul $C \vee A$ i $D \vee \neg B$ a klauzulę $\sigma(C \vee A)$ *faktorem* klauzuli $C \vee A \ \vee B$. Rezolucyjnym dowodem sprzeczności zbioru klauzul $\mathcal{F}$ nazywamy ciąg klauzul $C_0, \ldots C_n$ spełniający warunki

- $C_n = \perp$, oraz
- dla wszystkich $i \in \{0, \ldots, n\}$ zachodzi
  - $C_i \in \mathcal{F}$, lub
  - istnieją takie $j, k < i$, że C_i jest rezolwentą C_j i C_k, lub
  - istnieje takie $j < i$, że C_i jest faktorem C_j.

Zadanie 591. Mówimy, że formuła φ logiki I rzędu jest logiczną konsekwencją zbioru formuł $\mathcal{F}$ jeśli w każdej strukturze, w której prawdziwe są wszystkie formuły ze zbioru $\mathcal{F}$ prawdziwa jest również formuła φ.

Udowodnij, że jeśli C i D są klauzulami w logice I rzędu, A i B formułami atomowymi a σ najogólniejszym unifikatorem A i B, to rezolwenta $\sigma(C \vee D)$ jest logiczną konsekwencją klauzul $C \vee A$ i $D \vee \neg B$.

Zadanie 592. Podaj rezolucyjny dowód sprzeczności dla zbioru klauzul

$$\{\neg p(x) \vee \neg p(f(a)) \vee q(y), \quad p(z), \quad \neg p(g(b,u)) \vee \neg q(b)\},$$

gdzie a, b, f, g są symbolami funkcyjnymi, p i q są symbolami relacyjnymi a u, x, y, z są zmiennymi.

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:			

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