1

Zadania egzaminacyjne z rozwiązaniami*

Zadanie 1. Niech ϕ będzie formułą zdaniową zbudowaną ze zmiennych zdaniowych i spójników alternatywy, koniunkcji i negacji (do jej zapisania można oczywiście używać nawiasów). Przez *wartościowanie* rozumiemy w tym zadaniu funkcję, która zmiennym *występującym* w formule ϕ przyporządkowuje wartości ze zbioru $\{0, 1\}$. Niech n będzie dodatnią liczbą naturalną.

a) Udowodnij, że dla każdej liczby naturalnej $k \leq 2^n$ istnieje formuła zdaniowa ϕ zawierająca n zmiennych i spełniona przez dokładnie k wartościowań.

b) Dla jakich liczb k istnieje formuła ϕ zawierająca n zmiennych, w której każda ze zmiennych występuje dokładnie jeden raz i która jest spełniona przez dokładnie k wartościowań?

Rozwiązanie. Część a) jest oczywistą konsekwencją zupełności zbioru spójników złożonego z alternatywy, koniunkcji i negacji. Bierzemy dowolną funkcję boolowską n zmiennych przyjmującą wartość 1 dla k argumentów i korzystając z zupełności stwierdzamy, że jest to funkcja przyporządkowująca układowi zer i jedynej wartość logiczną pewnej formuły przy wartościowaniu wyznaczonym przez ten układ. Dokładniej, bierzemy n zmiennych zdaniowych $p_1, \ldots, p_n$ i tworzymy formuły będące koniunkcją tych zmiennych bądź ich negacji (np. $\neg p_1 \wedge p_2 \wedge \ldots \wedge p_n$). Formuły tej postaci są spełnione przez dokładnie jedno wartościowanie. Alternatywa k różnych formuł takiej postaci (dowolnie wybranych) jest formułą spełnioną przez dokładnie k wartościowań.

Bardziej szczegółowo przedstawimy inne rozwiązanie tego zadania. Przyjmijmy, że $W(\phi)$ oznacza zbiór wartościowań spełniających formułę ϕ. Symbolem $|X|$ oznaczamy liczbę elementów zbioru X.

Fakt 1. Jeżeli w formule ϕ występuje n zmiennych, to $|W(\neg\phi)| = 2^n - |W(\phi)|$.

*Rozdział przygotował A. Kościelski.

Dowód. Jest to oczywisty fakt. Dla formuły ϕ z n zmiennymi jest 2^n wartościowań. Każde z nich spełnia albo ϕ, albo $\neg\phi$, żadne nie może jednocześnie spełniać obu tych formuł.

Fakt 2. Jeżeli żadna zmienna nie występuje jednocześnie w formulach ϕ i ψ, to

$$|W(\phi \wedge \psi)| = |W(\phi)| \cdot |W(\psi)|.$$

Dowód. Rozważmy funkcję, która wartościowaniu h formuły $\phi \wedge \psi$ przyporządkowuje parę dwóch wartościowań: wartościowania będącego obcięciem h do zmiennych formuły ϕ i wartościowania będącego obcięciem h do zmiennych formuły ψ. Różnowartościowość tej funkcji jest oczywista.

Wystarczy teraz zauważyć, że funkcja ta przekształca zbiór $W(\phi \wedge \psi)$ na iloczyn kartezjański $W(\phi) \times W(\psi)$. (Gdzie w tym dowodzie korzysta się z założenia o zmiennych formuł ϕ i ψ?)

Wniosek. Jeżeli zmienna p nie występuje w formule ϕ, to $|W(\phi \wedge p)| = |W(\phi)|$.

Wniosek. Jeżeli w formule ϕ występuje n zmiennych i nie ma wśród nich zmiennej p, to $|W(\phi \vee p)| = 2^n + |W(\phi)|$.

Dowód. Zauważmy, że

$$\begin{aligned}
|W(\phi \vee p)| &= |W(\neg(\neg\phi \wedge \neg p))| \\
&= 2^{n+1} - |W(\neg\phi \wedge \neg p)| \\
&= 2^{n+1} - |W(\neg\phi)| \cdot |W(\neg p)| \\
&= 2^{n+1} - (2^n - |W(\phi)|) \cdot (2 - |W(p)|) \\
&= 2^{n+1} - 2^n + |W(\phi)| \\
&= 2^n + |W(\phi)|.
\end{aligned}$$

Fakt 3. Dla każdej liczby naturalnej $k \leq 2^n$ istnieje formuła zdaniowa z n zmiennymi spełniona przez dokładnie k wartościowań.

Dowód. Fakt ten dowodzimy przez indukcję ze względu na n.

Zauważmy, że $|W(p \wedge \neg p)| = 0$, $|W(p)| = 1$ i $|W(p \vee \neg p)| = 2$. Tym samym twierdzenie jest prawdziwe dla $n = 1$.

Załóżmy, że twierdzenie to zachodzi dla liczby n i weźmy $k \leq 2^{n+1}$. Zachodzi jeden z dwóch przypadków: albo $k \leq 2^n$, albo $2^n < k \leq 2^{n+1}$.

Jeżeli $k \leq 2^n$, to znajdujemy formułę ϕ z n zmiennymi, która jest spełniona przez k wartościowań, i zmienną p, która nie występuje w ϕ. Formuła $\phi \wedge p$ jest spełniona przez k wartościowań i występuje w niej $n + 1$ zmiennych.

Jeżeli $2^n < k \leq 2^{n+1}$, to bierzemy formułę ϕ z n zmiennymi, spełnioną przez $k - 2^n$ wartościowań. Wtedy dla dowolnej zmiennej p nie występującej w ϕ formuła $\phi \vee p$ jest spełniona przez k wartościowań i występuje w niej $n + 1$ zmiennych.

Podobnie dowodzimy następujący fakt:

Fakt 4. Dla każdej nieparzystej liczby naturalnej $k \leq 2^n$ istnieje formuła zdaniowa z n zmiennymi, w której każda zmienna występuje dokładnie jeden raz i która jest spełniona przez dokładnie k wartościowań.

Dowód. Twierdzenie to także dowodzimy przez indukcję ze względu na n. Formułę, w której każda zmienna występuje najwyżej jeden raz, będziemy nazywać *formułą prostą*.

Zauważmy, że $|W(p)| = 1$. Wobec tego dowodzone twierdzenie jest prawdziwe dla $n = 1$.

Załóżmy, że twierdzenie to zachodzi dla liczby n i weźmy nieparzystą liczbę $k \leq 2^{n+1}$. Liczba k jest albo $\leq 2^n$, albo też spełnia nierówności $2^n < k \leq 2^{n+1}$.

Jeżeli $k \leq 2^n$, to znajdujemy prostą formułę ϕ z n zmiennymi, która jest spełniona przez k wartościowań, i zmienną p, która nie występuje w ϕ. Formuła $\phi \wedge p$ jest prosta i spełniona przez k wartościowań, oraz występuje w niej $n+1$ zmiennych.

Jeżeli $2^n < k \leq 2^{n+1}$, to bierzemy prostą formułę ϕ z n zmiennymi, spełnioną przez $k - 2^n$ wartościowań. Wtedy dla dowolnej zmiennej p nie występującej w ϕ, formuła $\phi \vee p$ jest prosta, spełniona przez k wartościowań i występuje w niej $n + 1$ zmiennych.

Fakt 5. Jeżeli ϕ jest formułą, w której każda zmienna występuje najwyżej jeden raz, to ϕ jest spełniona przez nieparzystą liczbę wartościowań.

Dowód. Dowód przeprowadzimy przez indukcję ze względu na liczbę znaków występujących w formule. Formuła, która daje się zapisać za pomocą jednego znaku, jest zmienną i jest spełniona przez jedno wartościowanie.

Przypuśćmy, że $\phi = \neg\psi$ i występuje w niej n zmiennych. Oczywiście, każda zmienna występuje tyle samo razy w ϕ, co w ψ. Z założenia indukcyjnego wynika więc, że ψ jest spełniona przez nieparzystą liczbę wartościowań równą $|W(\psi)|$. Liczba $2^n - |W(\psi)|$ jest nieparzysta i jest równa liczbie wartościowań spełniających ϕ.

Jeżeli w koniunkcji $\phi \wedge \psi$ każda zmienna występuje najwyżej jeden raz (jeżeli koniunkcja ta jest prosta), to ϕ i ψ są proste, i żadna zmienna nie występuje jednocześnie w obu tych formułach. Wobec tego, formuła $\phi \wedge \psi$ jest spełniona przez $|W(\phi)| \cdot |W(\psi)|$ wartościowań. Na mocy założenia indukcyjnego, oba czynniki tego iloczynu są liczbami nieparzystymi. Iloczyn liczb nieparzystych też jest nieparzysty.

Jeszcze trzeba pokazać (można to zrobić w podobny sposób), że alternatywa będąca formułą prostą jest spełniona przez nieparzystą liczbę wartościowań. ∎

Zadanie 2. Wykaż przez indukcję, że dla każdej formuły zdaniowej ϕ zbudowanej ze zmiennych oraz spójników $\wedge$ i $\vee$ (oczywiście do jej zapisania można też używać nawiasów) istnieje formuła ψ postaci $\psi_1 \vee \psi_2 \vee \ldots \vee \psi_n$, taka, że dla każdego $i \leq n$ formuła ψ_i jest koniunkcją zmiennych oraz $(\phi \Leftrightarrow \psi)$ jest tautologią.

Rozwiązanie (szkic). Formuły ϕ i ψ są równoważne wtedy i tylko wtedy, gdy formuła $\phi \Leftrightarrow \psi$ jest tautologią. Zauważmy, że

Fakt 6. Formuła $(\phi_1 \vee \phi_2) \wedge \psi$ jest równoważna $(\phi_1 \wedge \psi) \vee (\phi_2 \wedge \psi)$, czyli formuła

$$(\phi_1 \vee \phi_2) \wedge \psi \Leftrightarrow (\phi_1 \wedge \psi) \vee (\phi_2 \wedge \psi)$$

jest tautologią.

Fakt 7. Formuła

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

jest tautologią. Tautologią jest także formuła

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

Fakt 8. Formuła

$$(\phi_1 \vee \ldots \vee \phi_n) \wedge (\phi'_1 \vee \ldots \vee \phi'_m) \Leftrightarrow$$
$$(\phi_1 \wedge \phi'_1) \vee \ldots \vee (\phi_n \wedge \phi'_1) \vee \ldots \vee (\phi_1 \wedge \phi'_m) \vee \ldots \vee (\phi_n \wedge \phi'_m)$$

jest tautologią.

Korzystając z ostatniego faktu można dowieść własność podaną w zadaniu przez indukcję ze względu na liczbę spójników występujących w formule ϕ.

Jeżeli w formule ϕ nie występują spójniki, to jest ona zmienną. Każda zmienna jest jednoczłonową alternatywą, której jedynym członem jest jednoczłonowa koniunkcja. Tak więc w tym przypadku formuła ϕ ma odpowiednią postać i możemy przyjąć, że $\psi = \phi$.

Jeżeli w formule ϕ występuje przynajmniej jeden spójnik, to jest ona koniunkcją lub alternatywą formuł z mniejszą liczbą spójników. W przypadku alternatywy dalszy dowód jest prosty i zostaje pominięty. Jeżeli $\phi = \phi_1 \wedge \phi_2$, to na podstawie założenia indukcyjnego znajdujemy alternatywy ψ_1 i ψ_2 wymaganej postaci równoważne odpowiednio ϕ_1 i ϕ_2. Wprowadzając odpowiednie oznaczenia możemy przyjąć, że lewa strona równoważności z ostatniego faktu jest równa $\psi_1 \wedge \psi_2$. Formułę ψ definiujemy jako prawą stronę równoważności z tego faktu.

Rozwiązanie (inny sposób). Najpierw sformalizujemy treść zadania.

Symbolem $\mathcal{K}$ będziemy oznaczać najmniejszy w sensie inkluzji spośród zbiorów X spełniających warunki:

1. wszystkie zmienne zdaniowe należą do X,
2. jeżeli ϕ i ψ należą do X, to także formuła $\phi \wedge \psi$ należy do X.

Tak więc $\mathcal{K}$ jest zbiorem koniunkcji zmiennych zdaniowych. Symbolem $\mathcal{A}$ będziemy zaś oznaczać najmniejszy w sensie inkluzji spośród zbiorów X spełniających warunki:

1. $\mathcal{K} \subseteq X$,
2. jeżeli ϕ i ψ należą do X, to także formuła $\phi \vee \psi$ należy do X.

Tak więc $\mathcal{A}$ jest zbiorem alternatyw koniunkcji zmiennych zdaniowych. Posługując się wprowadzonymi oznaczeniami rozwiązywane zadanie można sformułować następująco: dowieść, że dla każdej formuły ϕ, w której występują tylko spójniki $\wedge$ i $\vee$, istnieje formuła $\psi \in \mathcal{A}$ taka, że formuła $\phi \Leftrightarrow \psi$ jest tautologią.

Dowód zostanie przeprowadzony przez indukcję ze względu na liczbę spójników występujących w formule ϕ.

Niech n będzie liczbą naturalną, a ϕ formułą, w której występuje n spójników i są to jedynie spójniki $\wedge$ i $\vee$. Będziemy zakładać, że jeżeli w pewnej formule występuje mniej niż n spójników, to jest ona równoważna formule należącej do $\mathcal{A}$. Przy tym założeniu wykażemy, że ψ też jest równoważna formule należącej do $\mathcal{A}$.

W dowodzie będziemy rozważać kilka przypadków. Najpierw przyjmijmy dodatkowo, że $n = 0$. Wtedy w formule ϕ nie ma spójników, a więc ϕ jest zmienną i — w konsekwencji — należy do $\mathcal{K}$ oraz do $\mathcal{A}$. W tym przypadku przyjmujemy, że $\psi = \phi$. Oczywiście, $\psi \in \mathcal{A}$, a ponadto, formuły ϕ i ψ są w oczywisty sposób równoważne.

Jeżeli $n > 0$, to w ϕ jest przynajmniej jeden spójnik. Wtedy ϕ jest albo koniunkcją, albo alternatywą formuł zawierających mniejszą liczbę spójników niż ϕ. Najpierw załóżmy, że $\phi = \phi_1 \vee \phi_2$. Dla formuł ϕ_1 i ϕ_2 możemy skorzystać z założenia indukcyjnego. Istnieją więc w $\mathcal{A}$ formuły ψ_1 i ψ_2 równoważne odpowiednio ϕ_1 i ϕ_2. Oczywiście, $\psi_1 \vee \psi_2 \in \mathcal{A}$ oraz $\psi_1 \vee \psi_2$ jest równoważne z $\phi_1 \vee \phi_2$.

Jeżeli $\phi = \phi_1 \wedge \phi_2$, to także znajdujemy w $\mathcal{A}$ formuły ψ_1 i ψ_2 równoważne odpowiednio ϕ_1 i ϕ_2. Formuły z $\mathcal{A}$ albo należą do $\mathcal{K}$, albo są alternatywami.

Jeżeli ψ_1 i ψ_2 należą do $\mathcal{K}$, to przyjmujemy, że $\psi = \psi_1 \wedge \psi_2$. Także w tym przypadku jest oczywiste, że $\psi \in \mathcal{K} \subseteq \mathcal{A}$ oraz, że ϕ jest równoważne ψ.

Pozostał do rozważania przypadek, w którym przynajmniej jedna z formuł ψ_1 i ψ_2 jest alternatywą. Załóżmy, że $\psi_1 = \psi_{11} \vee \psi_{12}$. Jeżeli okaże się, że alternatywą jest tylko ψ_2 będziemy postępować dokładnie tak samo. Na mocy prawa rozdzielności koniunkcji względem alternatywy (prawo $(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$) otrzymujemy, że formuła

$$\phi = (\phi_{11} \vee \psi_{12}) \wedge \phi_2$$

jest równoważna formule

$$(\phi_{11} \wedge \phi_2) \vee (\psi_{12} \wedge \phi_2).$$

Nietrudno zauważyć, że w obu członach tej alternatywy jest mniej spójników, niż w formule ϕ. Do tych członów możemy więc zastosować założenie indukcyjne. W ten sposób znajdujemy formuły ψ_1 i ψ_2 takie, że

$$\psi_1 \Leftrightarrow (\phi_{11} \wedge \phi_2) \text{ oraz } \psi_2 \Leftrightarrow (\phi_{12} \wedge \phi_2)$$

są tautologiami. Bez trudu dowodzimy, że formuła

$$\phi \Leftrightarrow (\psi_1 \vee \psi_2)$$

jest tautologią. Ponieważ $\psi_1, \psi_2 \in \mathcal{A}$, więc także $\psi_1 \vee \psi_2 \in \mathcal{A}$. W rozważanym przypadku możemy przyjąć, że $\psi = \psi_1 \vee \psi_2$.

Przedstawiony dowód można rozbić na dwie części dowodząc najpierw, że koniunkcja formuł należących do $\mathcal{A}$ jest równoważna formule należącej do $\mathcal{A}$. ∎

Zadanie 3. Używając jedynie zmiennych, kwantyfikatorów, spójników logicznych, nawiasów i symboli $\in, \mathbb{N}, +, \times, =$ napisz formuły mówiące, że:

a) nie ma największej liczby pierwszej,

b) istnieje taka liczba naturalna, że każda liczba naturalna większa od niej jest sumą nie więcej niż czterech kwadratów liczb pierwszych,

c) istnieje nieskończenie wiele par liczb bliźniaczych.

Para liczb bliźniaczych, to dwie liczby pierwsze różniące się o 2.

Rozwiązanie. Najpierw napiszemy pomocniczą formułę $P(x)$ równą

$$\neg\,\exists a{\in}\mathbb{N}\;\exists b{\in}\mathbb{N}\;\exists r{\in}\mathbb{N}\;\exists s{\in}\mathbb{N}\;(\neg x = a \wedge \neg x = b \wedge x = a + r \wedge x = b + s \wedge x = a \times b).$$

Zauważmy, że formuła $\exists r{\in}\mathbb{N}\,(x = a + r)$ jest równoważna nierówności $x \geq a$. Wobec tego formuła $P(x)$ stwierdza, że liczba x nie jest iloczynem dwóch liczb mniejszych od x, a więc stwierdza, że x jest liczbą pierwszą.
Własność „nie ma największej liczby pierwszej" można wyrazić pisząc

$$\neg\,\exists x{\in}\mathbb{N}\;(P(x) \wedge \forall y{\in}\mathbb{N}\,(P(y) \Rightarrow \exists r{\in}\mathbb{N}\,(x = y + r))).$$

Formuła

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

stwierdza, że „istnieje taka liczba naturalna, że każda liczba naturalna większa od niej jest sumą nie więcej niż czterech kwadratów liczb pierwszych". Zauważmy, że własność $a + a = a$ jest równoważna stwierdzeniu $a = 0$.

Ostatnią z wymienionych w zadaniu własności („istnieje nieskończenie wiele par liczb bliźniaczych") można wyrazić pisząc

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

Aby się o tym przekonać wystarczy zauważyć, że własności $\neg(d+d=d)\wedge d\times d=d+d$ oraz $d=2$ są równoważne a także, że zbiór $\{y\in\mathbb{N}\mid\phi(y)\}$ jest nieskończony wtedy i tylko wtedy, gdy $\forall x\in\mathbb{N}\ \exists y\in\mathbb{N}\ (x\leq y\wedge\phi(y))$. ■

Zadanie 4. Pokaż, że

$$(A_1\cup A_2)\div(B_1\cup B_2)\subseteq(A_1\div B_1)\cup(A_2\div B_2). \tag{1}$$

Czy zawieranie

$$(A_1\cap A_2)\div(B_1\cap B_2)\subseteq(A_1\div B_1)\cup(A_2\div B_2) \tag{2}$$

jest prawdziwe dla dowolnych zbiorów A_1, A_2, B_1 i B_2?

Rozwiązanie. Zaczynamy od pierwszej inkluzji. Zgodnie z definicją, aby dowieść zawieranie $X\subseteq Y$ powinniśmy wziąć dowolny element $x\in X$ i o tym elemencie dowieść, że należy do zbioru Y. Weźmy więc $x\in(A_1\cup A_2)\div(B_1\cup B_2)$. Z definicji różnicy symetrycznej wiemy, że element ten spełnia równoważność

$$x\in(A_1\cup A_2)\Leftrightarrow x\notin(B_1\cup B_2). \tag{3}$$

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

Przypadek 1: $x\in(A_1\cup A_2)$. Z równoważności (3) otrzymujemy, że $x\notin(B_1\cup B_2)$. Wobec tego, zarówno $x\notin B_1$, jak i $x\notin B_2$. Dalsze rozumowanie też będzie polegać na rozważeniu kolejnych przypadków.

Przypadek 1.1: $x\in A_1$. Wiemy już, że $x\notin B_1$. Zachodzi więc także równoważność

$$x\in A_1\Leftrightarrow x\notin B_1, \tag{4}$$

np. dlatego, że w rozważanym przypadku obie strony tej równoważności są prawdziwe, albo dlatego, że dowodzenie tej równoważności polega na wykazaniu dwóch implikacji stwierdzających, że przy pewnych założeniach zachodzą fakty, których prawdziwość udało nam się wcześniej ustalić. Równoważność (4) oznacza, że $x\in(A_1\div B_1)$, i tym bardziej, x należy do prawej strony wzoru (1).

Przypadek 1.2: $x\in A_2$. W tym przypadku, tak jak w poprzednim, dowodzimy, że $x\in A_2\Leftrightarrow x\notin B_2$, i w konsekwencji, x należy do drugiego składnika prawej strony wzoru (1).

Przypadek 2: $x \notin (A_1 \cup A_2)$. Z równoważności (3) otrzymujemy teraz, że $x \in (B_1 \cup B_2)$. Mamy więc sytuację analogiczną do opisanej w przypadku 1. Dalszy dowód prowadzimy tak, jak w przypadku 1 zastępując A_1 i A_2 zbiorami B_1 oraz B_2, i odwrotnie.

Zawieranie (2) jest też prawdziwe dla wszystkich zbiorów i można się o tym przekonać w bardzo podobny sposób. Proponuję, aby zainteresowane osoby same przekształciły podany dowód zawierania (1) w dowód inkluzji (2). W przypadku 1 w przekształconym dowodzie powinna być rozważana sytuacja, w której $x \notin B_1 \cap B_2$.

Rozwiązanie (inny sposób). Będziemy korzystać z następujących praw rachunku zbiorów:

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

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

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

Jeżeli wprowadzimy pojęcie dopełnienia zbioru, to w dowodzie zawierania (2) możemy wykorzystać wzór

$$X \div Y = X^c \div Y^c.$$

Zauważmy, że

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

Zadanie 5. Pokaż, że

1. $A_1 \div \ldots \div A_n$ zawiera te i tylko te elementy, które należą do nieparzystej liczby zbiorów A_i, gdzie $i = 1, \ldots, n$;
2. jeśli zbiory $A_1, \ldots, A_n$ są skończone, to

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

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

$x \in A_1 \div \ldots \div A_n \Leftrightarrow x$ należy do nieparzystej liczby zbiorów spośród $A_1, \ldots, A_n$.

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

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

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

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

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

Dowód będziemy prowadzić przez indukcję. Musimy więc przeformułować zadanie tak, aby było możliwe zastosowanie zasady indukcji. Będziemy dowodzić, że dla każdej liczby naturalnej $n \geq 1$, dla dowolnej rodziny zbiorów $A_1, \ldots, A_n$ indeksowanej zbiorem $\{1, \ldots, n\}$ zachodzi teza zadania. Fakt, że dla dowolnej rodziny zbiorów $A_1, \ldots, A_n$ zachodzi teza zadania, oznaczmy symbolem $\phi(n)$. W dowodzie skorzystamy z zasady indukcji, która stwierdza, że aby dowieść zdanie postaci $\forall n \geq 1\ \phi(n)$ wystarczy pokazać, że dla dowolnego $n \geq 1$, z tego, że $\phi(k)$ zachodzi dla $k < n$ wynika, że także zachodzi $\phi(n)$. Osoby, które nie są przekonane do tego schematu indukcji, mogą spróbować przerobić podany dowód na dowód korzystający ze zwykłego schematu indukcji, ale wtedy trzeba dowodzić tezę w postaci $\forall n \geq 1 \forall k \leq n\ \phi(k)$.

Przypuśćmy, że $n \geq 2$ oraz

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

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

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

1. $x \in A_1 \div \ldots \div A_n$,
2. $x \notin A_1 \div \ldots \div A_k$,

3. x należy do parzystej liczby zbiorów spośród $A_1, \ldots, A_k$,

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

W drugim przypadku przeprowadzamy analogiczne rozumowanie. Zauważmy też, że z rozwiązanego, ogólniejszego zadania wynika, że różnica symetryczna jest łączna.

Część 1, rozwiązanie wymagające łączności różnicy symetrycznej. Oczywiście, $A \div B \subseteq A \cup B$. Stąd przez łatwą indukcję otrzymujemy, że $A_1 \div \ldots \div A_n \subseteq A_1 \cup \ldots \cup A_n$. Z tego wzoru wynika, że elementy nie należące do żadnego ze zbiorów $A_1, \ldots, A_n$ nie należą także do różnicy $A_1 \div \ldots \div A_n$.

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

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

Zauważmy, że x nie należy do zbiorów

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

Stąd wynika, że x nie należy także do różnicy $A_1 \div \ldots \div A_n$.

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

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

$$A_1 \div (A_2 \div \ldots \div A_n) = A_1 \div \ldots \div A_n.$$

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

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

Weźmy skończony zbiór X zawierający zbiory $A_1, \ldots, A_n$. Niech Ch_A oznacza funkcję określoną w zbiorze X, przyjmującą wartości 0 i 1, przyjmującą wartość 1 dokładnie dla tych argumentów, które należą do A. Zauważmy, że

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

Będziemy przekształcać prawą stronę dowodzonego wzoru. Mamy więc

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

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

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

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

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

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

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

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

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

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

Teraz zauważmy, że liczba $2^{-1}(1-(-1)^m)$ jest równa 0 lub 1, i jest równa 1 wtedy i tylko wtedy, gdy m jest liczbą nieparzystą. Stąd otrzymujemy, że

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

i to kończy dowód. ∎

Zadanie 6. Dla jakich zbiorów C prawdziwe jest zdanie stwierdzające, że dla dowolnych zbiorów A i B zachodzi

$$A \times C \subseteq B \times C \Rightarrow A \subseteq B\,? \tag{1}$$

Rozwiązanie. Najpierw spróbujemy dowieść implikację (1). Mamy więc zbiory A, B i C, zakładamy, że zbiory te spełniają założenie $A \times C \subseteq B \times C$. W tej sytuacji staramy się dowieść, że $A \subseteq B$. Aby dowieść to zawieranie, bierzemy $x \in A$ i próbujemy wykazać, że $x \in B$. Oczywiście, powinniśmy skorzystać z założenia. Łatwo zauważyć, że w tym celu przydałaby się para o pierwszej współrzędnej x i drugiej należącej do C. Aby taką parę utworzyć, musimy mieć element zbioru C. Jest to proste pod warunkiem, że C jest zbiorem niepustym. Wtedy zbiór C ma przynajmniej jeden element. Jeden z elementów zbioru C oznaczamy symbolem c i tworzymy parę $\langle x, c\rangle$. Ta para należy do iloczynu kartezjańskiego $A \times C$. Na podstawie założenia stwierdzamy, że należy także do iloczynu $B \times C$. Jeżeli $\langle x, c\rangle \in B \times C$, to także $x \in B$.

Przedstawione rozumowanie pozwala dowieść implikację (1), ale wymaga dodatkowego założenia, że zbiór C jest niepusty. Nietrudno zauważyć, że w przypadku, gdy C jest zbiorem pustym, to puste są także zbiory $A \times C$ i $B \times C$, i w konsekwencji, poprzednik implikacji (1) jest prawdziwy dla dowolnych zbiorów A i B. Jeżeli przyjmiemy, że A jest dowolnym zbiorem niepustym (np. zbiorem liczb naturalnych), a B jest zbiorem pustym, to następnik implikacji (1) będzie fałszywy, i to samo będzie można powiedzieć o całej implikacji.

Ostatecznie otrzymujemy, że implikacja $A \times C \subseteq B \times C \Rightarrow A \subseteq B$ zachodzi dla wszystkich zbiorów A i B wtedy i tylko wtedy, gdy C nie jest zbiorem pustym.

Zadanie 7. Inwolucją nazywamy odwzorowanie $f : A \to A$ takie, że ff jest identycznością na A. Czy inwolucja jest bijekcją na A? Pokaż, że każdą bijekcję można przedstawić jako złożenie dwóch inwolucji.

Rozwiązanie. *Część 1: każda inwolucja jest bijekcją.* Przypuśćmy, że $f : A \to A$ jest inwolucją. Spełnia więc dla dowolnego $x \in A$ równość $f(f(x)) = x$. Taka funkcja f jest typu „na": wartość $x \in A$ przyjmuje dla argumentu $f(x)$. Jest to też funkcja różnowartościowa. Aby się o tym przekonać, weźmy dwa argumenty $x, y \in A$ takie, że $f(x) = f(y)$. Dla takich argumentów zachodzi też równość $f(f(x) = f(f(y))$. Jeżeli f jest inwolucją, to stąd wynika, że $x = y$.

Część 2. Ta część zadania jest znacznie trudniejsza. Rozwiązując to zadanie zauważyłem, że jest właściwie tylko jedna bijekcja, którą trzeba przedstawić jako złożenie inwolucji. Tą bijekcją jest funkcja S przekształcająca zbiór liczb całkowitych $\mathbb{Z}$ w $\mathbb{Z}$ zdefiniowana wzorem $S(n) = n + 1$.

Krok 1. Aby przedstawić S jako złożenie inwolucji, weźmy funkcje $f, g : \mathbb{Z} \to \mathbb{Z}$ zdefiniowane wzorami $f(n) = -n$ oraz $g(n) = -(n+1)$. Funkcje te są inwolucjami. Sprawdzenie tego faktu wymaga jedynie elementarnych rachunków. Mamy też

$$f(g(n)) = f(-(n + 1)) = n + 1 = S(n).$$

Tak więc $S = fg$.

Krok 2. Załóżmy, że $m > 0$. Symbolem k mod m będziemy oznaczać resztę z dzielenia liczby k przez m, a więc najmniejszą nieujemną liczbę x taką, że $k - x$ dzieli się przez m. Korzystając z przedstawienia z kroku 1 można bez trudu przedstawić w postaci złożenia inwolucji funkcję $S_m : \{i \in \mathbb{N} : i < m\} \to \{i \in \mathbb{N} : i < m\}$ zdefiniowaną wzorem

$$S_m(n) = S(n) \bmod m = (n+1) \bmod m = \begin{cases} n+1 & \text{jeżeli } n < m-1 \\ 0 & \text{jeżeli } n = m-1. \end{cases}$$

Weźmy funkcję $f_m : \{i \in \mathbb{N} \mid i < m\} \to \{i \in \mathbb{N} \mid i < m\}$ taką, że

$$f_m(n) = f(n) \bmod m = (-n) \bmod m = \begin{cases} m-n & \text{jeżeli } n > 0 \\ 0 & \text{jeżeli } n = 0 \end{cases}$$

oraz funkcję $g_m : \{i \in \mathbb{N} \mid i < m\} \to \{i \in \mathbb{N} \mid i < m\}$ taką, że

$$g_m(n) = g(n) \bmod m = (-(n+1)) \bmod m = m - n - 1.$$

Ponieważ dodawanie i dodawanie modulo m mają własności przysługujące dodawaniu w pierścieniu, i tylko takie własności były wykorzystywane w kroku 1, więc funkcje f_m i g_m są inwolucjami i zachodzi równość $S_m = f_m g_m$. Osoby, dla których przytoczony argument nie jest jasny, mogą sprawdzić bezpośrednio wymagane równości.

Krok 3. Weźmy teraz bijekcję $s : A \to A$ i załóżmy, że zbiór A jest rozłączną sumą dwóch zbiorów A_1 i A_2 przekształcanych przez funkcję s w siebie (zakładamy więc, że $A_1 \cap A_2 = \emptyset$, $A = A_1 \cup A_2$, $s(x) \in A_1$ dla dowolnego $x \in A_1$ oraz analogiczną własność dla zbioru A_2).

Niech $s^{(1)}$ oznacza obcięcie funkcji s do zbioru A_1 (tak więc $s^{(1)} : A_1 \to A_1$ i $s^{(1)}(x) = s(x)$ dla wszystkich $x \in A_1$). Podobnie, niech $s^{(2)}$ oznacza obcięcie funkcji s do A_2. Funkcje $s^{(1)}$ i $s^{(2)}$ są bijekcjami. Zauważmy, że jeżeli $s^{(1)}$ i $s^{(2)}$ są złożeniami inwolucji, to złożeniem inwolucji jest również funkcja s.

Jeżeli $s^{(1)} = f^{(1)} g^{(1)}$ i $s^{(2)} = f^{(2)} g^{(2)}$ dla inwolucji $f^{(1)}$, $g^{(1)}$, $f^{(2)}$ i $g^{(2)}$, to $s = fg$ dla inwolucji $f, g : A \to A$ zdefiniowanych wzorami

$$f(x) = \begin{cases} f^{(1)}(x) & \text{jeżeli } x \in A_1 \\ f^{(2)}(x) & \text{jeżeli } x \in A_2 \end{cases} \quad \text{oraz} \quad g(x) = \begin{cases} g^{(1)}(x) & \text{jeżeli } x \in A_1 \\ g^{(2)}(x) & \text{jeżeli } x \in A_2. \end{cases}$$

Sprawdzenie podanych wyżej własności pozostawiam zainteresowanym.

Przedstawioną konstrukcję bez trudu można uogólnić na przypadek, w którym zbiór A jest sumą trzech zbiorów, lub jest sumą dowolnej skończonej liczby zbiorów. Można też ją uogólnić na przypadek dowolnego podziału zbioru A, także nieskończonego.

Krok 4. Mając bijekcję $s : A \to A$ podzielę zbiór A na takie fragmenty, dla których s będzie można łatwo przedstawić w postaci złożenia inwolucji.

Przyjmijmy, że jeżeli n jest dodatnią liczbą naturalną, to s^n oznacza n-krotne złożenie funkcji s. Tak więc $s^1 = s$, $s^2 = ss$, $s^{n+1} = ss^n$. Umówmy się także, że s^0 jest funkcją identycznościową w zbiorze A. Jeżeli natomiast n jest liczbą ujemną, to s^n oznacza $(-n)$-krotne złożenie $(s^{-1})^{-n}$ funkcji odwrotnej do s. Dowodzi się, że dla dowolnych liczb całkowitych n i m zachodzi wzór $s^{n+m} = s^n s^m$ lub nieco inaczej, dla dowolnego $x \in A$ zachodzi wzór $s^{n+m}(x) = s^n(s^m(x))$.

Zdefiniujemy teraz relację R w zbiorze A przyjmując, że

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

dla dowolnych $x, y \in A$. Relacja R jest relacją równoważności. Rozbija więc zbiór A na klasy abstrakcji, czyli na zbiory postaci $\{y \in A \mid xRy\}$. Różne klasy abstrakcji są rozłączne. Jest też oczywiste, że jeżeli $z \in \{y \in A \mid xRy\}$, to także $s(z) \in \{y \in A \mid xRy\}$. W dalszym ciągu będziemy przedstawiać funkcję s (a właściwie jej obcięcie) w postaci złożenia inwolucji na każdej klasie abstrakcji relacji R.

Krok 5. Przypuśćmy, że prócz bijekcji $s : X \to X$ mamy bijekcje $t : Y \to Y$ i $\phi : Y \to X$ takie, że $s\phi = \phi t$. Jeżeli wtedy funkcja t jest złożeniem dwóch inwolucji, to funkcja s też ma tę własność.

Jeżeli $t = fg$ dla inwolucji $f, g : Y \to Y$, to

$$s(\phi(y)) = (s\phi)(y) = (\phi t)(y) = (\phi fg)(y) = ((\phi f\phi^{-1})(\phi g\phi^{-1}))(\phi(y)).$$

Ponieważ funkcja ϕ jest typu „na", z udowodnionej równości wynika, że

$$s = (\phi f\phi^{-1})(\phi g\phi^{-1}).$$

Wystarczy jeszcze zauważyć, że złożenia $(\phi f\phi^{-1})$ i $(\phi g\phi^{-1})$ są inwolucjami.

Krok 6. W dalszym ciągu będziemy zajmować się klasą abstrakcji ustalonego elementu $a_0 \in A$, a więc zbiorem $A_0 = \{y \in A \mid a_0Ry\}$. Zdefiniujmy pomocniczą funkcję $\phi : \mathbb{Z} \to A_0$ przyjmując, że

$$\phi(n) = s^n(a_0).$$

Funkcji ϕ przekształca zbiór liczb całkowitych na klasę A_0. Dalej będziemy badać funkcję ϕ. Są możliwe dwa przypadki: albo dla pewnej liczby $m > 0$ zachodzi równość $\phi(m) = a_0$, albo też dla wszystkich $m > 0$ mamy $\phi(m) \neq a_0$. Najpierw zajmiemy się drugim przypadkiem.

Krok 7. Jeżeli $\phi(m) \neq a_0$ dla wszystkich liczb naturalnych m, to funkcja ϕ jest różnowartościowa. Aby się o tym przekonać załóżmy, że jest przeciwnie, a więc, że $\phi(m_1) = \phi(m_2)$ dla pewnych m_1 i $m_2 > m_1$. Jeżeli $m_1 < 0$, to

$$a_0 = s^{-m_1}(\phi(m_1)) = s^{-m_1}(\phi(m_2)) = s^{-m_1}(s^{m_2}(a_0)) = \phi(m_2 - m_1),$$

a to nie jest możliwe w rozważanym przypadku. Jeżeli natomiast $m_1 \geq 0$, to

$$s^{m_1}(a_0) = \phi(m_1) = \phi(m_2) = s^{m_1}(\phi(m_2 - m_1))$$

i z różnowartościowości s^{m_1} otrzymujemy, że $a_0 = \phi(m_2 - m_1)$. To też w rozważanym przypadku nie może zachodzić.

Zauważmy jeszcze, że

$$(s\phi)(n) = s(\phi(n)) = s(s^n(a_0)) = s^{n+1}(a_0) = \phi(n+1) = \phi(S(n)) = (\phi S)(n).$$

Tak więc $s\phi = \phi S$. W kroku 1 jest pokazane, że S jest złożeniem inwolucji. Wobec tego, z własności podanej w kroku 5 otrzymujemy, że s jest złożeniem inwolucji na zbiorze A_0.

Krok 8. Jeżeli $\phi(m) = a_0$ dla pewnej liczby naturalnej $m > 1$, to bierzemy najmniejszą liczbę m_0 o tej własności. Następnie pokazujemy, że funkcja ϕ przekształca różnowartościowo zbiór $\{x \in \mathbb{N} \mid x < m_0\}$ na klasę abstrakcji A_0. Fakt ten pozwala powtórzyć rozumowanie z kroku 7. Tym razem korzystamy z rozkładu na inwolucje funkcji S_{m_0}, opisanego w kroku 2. ∎

Zadanie 8. Przypuśćmy, że $f : X \to Y$, $A \subseteq X$ oraz $B \subseteq Y$. Udowodnij, że

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

Rozwiązanie. Pokażemy, że

$$y \in f(A \cap f^{-1}(B)) \Leftrightarrow y \in f(A) \cap B$$

dla dowolnego y. Stąd i z zasady ekstensjonalności wynika dowodzona równość. Aby dowieść podaną równoważność zauważmy, że następujące formuły są równoważne:

1. $y \in f(A \cap f^{-1}(B))$,
2. $\exists x(x \in A \cap f^{-1}(B) \wedge f(x) = y)$,
3. $\exists x(x \in A \wedge x \in f^{-1}(B) \wedge f(x) = y)$,
4. $\exists x(x \in A \wedge f(x) \in B \wedge f(x) = y)$,
5. $\exists x(x \in A \wedge f(x) = y \wedge y \in B)$,
6. $(\exists x(x \in A \wedge f(x) = y)) \wedge y \in B$,
7. $y \in f(A) \wedge y \in B$,
8. $y \in f(A) \cap B$.

Rozwiązanie (inny sposób). Najpierw udowodnimy zawieranie $f(A \cap f^{-1}(B)) \subseteq f(A) \cap B$. Przypuśćmy, że $y \in f(A \cap f^{-1}(B))$. Istnieje więc $x \in A \cap f^{-1}(B)$ taki, że $f(x) = y$. Ten istniejący x oznaczmy symbolem x_0. Mamy więc $x_0 \in A \cap f^{-1}(B)$ oraz $f(x_0) = y$. Oczywiście, element x_0 ma dwie własności: $x_0 \in A$ oraz $f(x_0) = y$. Istnieje więc taki x, że $x \in A$ oraz $f(x) = y$. Stąd wynika, że $y \in f(A)$.

Element x_0 należy także do $f^{-1}(B)$. Jeżeli skorzystamy z definicji przeciwobrazu, to otrzymamy, że $y = f(x_0) \in B$. Rozważany y należy więc do $f(A)$ i do B, czyli $y \in f(A) \cap B$. To kończy dowód interesującego nas zawierania.

Udowodnimy jeszcze zawieranie przeciwne, czyli $f(A) \cap B \subseteq f(A \cap f^{-1}(B))$. W tym celu weźmy $y \in f(A) \cap B$. Taki y należy do $f(A)$, a więc istnieje $x \in A$ takie, że $f(x) = y$. Jeden z tych elementów oznaczmy symbolem x_0. Mamy więc, że $x_0 \in A$ oraz $f(x_0) = y$. Ponieważ $y \in B$, więc także $f(x_0) \in B$. Ta ostatnia własność implikuje, że $x_0 \in f^{-1}(B)$. Element x_0 jest jednym z takich x, dla których $x \in A$, $x \in f^{-1}(B)$ oraz $f(x) = y$. Istnieje więc x takie, że $x \in A \cap f^{-1}(B)$ oraz $f(x) = y$. Stąd i z definicji pojęcia obrazu wynika, że $y \in f(A \cap f^{-1}(B))$ i tym samym zostało wykazane dowodzone zawieranie.

Interesująca nas równość wynika z udowodnionych zawierań i zasady ekstensjonalności.

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

$$\text{jeśli } C \subseteq D \text{ to } f(C) \subseteq f(D)$$

oraz zawierania

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

a także z dwóch znanych własności przekroju:

$$\text{jeśli } E \subseteq C \text{ i } E \subseteq D \text{ to } E \subseteq C \cap D$$

i

$$C \cap D \subseteq C \text{ oraz } C \cap D \subseteq D.$$

Z podanych własności wynika, że

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

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

i — w konsekwencji —

$$f(A \cap f^{-1}(B)) \subseteq f(A) \cap B.$$

Zadanie 9. Udowodnij, że na to, by relacja R była:

1. zwrotna, potrzeba i wystarcza, by $I \subseteq R$, gdzie I jest relacją identyczności;
2. symetryczna, potrzeba i wystarcza, by $R^{-1} = R$;
3. przechodnia, potrzeba i wystarcza, by $RR \subseteq R$;
4. relacją równoważności, potrzeba i wystarcza, by $I \subseteq R \wedge R^{-1} = R \wedge RR \subseteq R$.

Rozwiązanie. Jest to bardzo proste zadanie, tak proste, że chciałoby się napisać tylko, że jest oczywiste. Warunki $I \subseteq R$ i $RR \subseteq R$ są niemal identyczne odpowiednio z warunkami z definicji zwrotności i symetryczności relacji R. Z tego powodu przedstawiony dowód może będzie zbyt szczegółowy. Weźmy zbiór X i relację $R \subseteq X \times X$.

Część 1. Pokażemy, że R jest relacją zwrotną w zbiorze X wtedy i tylko wtedy, gdy $I \subseteq R$. Dowód równoważności składa się oczywiście z dowodu dwóch implikacji.

Najpierw załóżmy, że R jest relacją zwrotną w zbiorze X. Aby dowieść, że $I \subseteq R$, weźmy dowolny element $p \in I$. Oczywiście, p jest parą uporządkowaną (ponieważ I jest relacją), obie współrzędne p należą do X (gdyż I jest relacją w zbiorze X) i są sobie równe (dlatego, że I jest relacją identyczności). Tak więc $p = \langle x, x\rangle$ dla pewnego $x \in X$. Ponieważ R jest zwrotna, więc $p = \langle x, x\rangle \in R$. W ten sposób dowód zawierania $I \subseteq R$ został zakończony.

Aby dowieść zwrotność relacji R, wystarczy dla dowolnego elementu $x \in X$ pokazać, że para $\langle x, x\rangle$ należy do R. Oczywiście, $\langle x, x\rangle \in I$ na podstawie definicji relacji identycznościowej. Stąd i z zawierania $I \subseteq R$ otrzymujemy, że $\langle x, x\rangle \in R$.

Część 2. Teraz pokażemy, że relacja R jest symetryczna wtedy i tylko wtedy, gdy $R^{-1} = R$. Podobnie jak w części 1 udowodnimy dwie implikacje.

Jeżeli relacja R jest symetryczna, to dowolna para $\langle x, y\rangle$ z relacji R (a właściwie dowolny element relacji R) należy także do relacji R^{-1}. Tak jest, ponieważ z warunku $\langle x, y\rangle \in R$ wynika, że $\langle y, x\rangle \in R$, a to z kolei oznacza, że $\langle x, y\rangle \in R^{-1}$. Przedstawione rozumowanie świadczy o tym, że symetryczna relacja R spełnia warunek $R \subseteq R^{-1}$. Podobnie dowodzimy zawieranie odwrotne: jeżeli $\langle x, y\rangle \in R^{-1}$, to korzystając z definicji relacji odwrotnej otrzymujemy, że $\langle y, x\rangle \in R$, a jeżeli skorzystamy jeszcze z symetryczności R, to otrzymamy, że $\langle x, y\rangle \in R$. Dla relacji symetrycznej prawdziwe są więc dwa zawierania: $R \subseteq R^{-1}$ i $R^{-1} \subseteq R$. Wobec tego, prawdziwa jest też równość $R = R^{-1}$.

W drugą stronę, relacja spełniająca warunek $R = R^{-1}$ spełnia także zawieranie $R \subseteq R^{-1}$. To zawieranie oznacza, że R jest relacją symetryczną. Jeżeli bowiem $\langle x, y\rangle \in R$, to na podstawie tego zawierania mamy, że $\langle y, x\rangle \in R^{-1}$. Jeżeli teraz skorzystamy z definicji relacji odwrotnej, to otrzymamy, że $\langle y, x\rangle \in R$.

Część 3. Pokażemy jeszcze, że przechodniość relacji R jest równoważna zawieraniu $RR \subseteq R$.

Załóżmy, że R jest relacją przechodnią i $\langle x, y\rangle \in RR$. Z definicji złożenia relacji wynika, że istnieje z taki, że $\langle x, z\rangle \in R$ i $\langle z, y\rangle \in R$. Jeden z takich z oznaczmy symbolem z_0. Element z_0 ma więc dwie własności: $\langle x, z_0\rangle \in R$ oraz $\langle z_0, y\rangle \in R$. Z przechodniości relacji R otrzymujemy, że $\langle x, y\rangle \in R$. Kończy to dowód zawierania $RR \subseteq R$.

Jeżeli $RR \subseteq R$, to relacja R jest przechodnia. Aby się o tym przekonać weźmy x, y i z takie, że $\langle x, y\rangle \in R$ i $\langle y, z\rangle \in R$. Z definicji złożenia relacji wynika, że $\langle x, z\rangle \in RR$. Założone zawieranie implikuje więc, że $\langle x, z\rangle \in R$, i to kończy dowód przechodniości relacji R.

Część 4. Z części 1, 2 i 3 wynika równoważność z części 4. Aby się o tym przekonać, wystarczy zauważyć, że jeżeli zdania ϕ_i są równoważne zdaniom ψ_i dla $i = 1, 2, 3$, to koniunkcja $\phi_1 \wedge \phi_2 \wedge \phi_3$ jest równoważna koniunkcji $\psi_1 \wedge \psi_2 \wedge \psi_3$. ■

Zadanie 10. Niech f będzie bijekcją przekształcającą zbiór A w A. Zdefiniujmy relację $R \subseteq A^2$ przyjmując, że

$$x R y \;\Leftrightarrow\; f(x) = y.$$

Symbolem R_∞ oznaczamy przechodnie domknięcie relacji R, czyli relację $\bigcup_{n=1}^{\infty} R^n$, gdzie $R^1 = R$ oraz $R^{n+1} = R^n R$. Czy

1. R_∞ jest relacją równoważności?
2. R_∞ jest relacją równoważności, jeśli A jest zbiorem skończonym?

Rozwiązanie. *Część 1.* Najpierw zauważmy, że jeżeli funkcję f będziemy traktować jak relację, to warunek $f(x) = y$ będzie równoważny z $\langle x, y\rangle \in f$. Tak więc relacja R jest tożsama z funkcją f. Wobec tego, relacja R^n jest niczym innym, jak n-krotnym złożeniem funkcji f.

Na ogół przechodnie domknięcie relacji R zdefiniowanej w zadaniu nie jest relacją równoważności. Tak jest np. dla zbioru liczb całkowitych $\mathbb{Z}$ i funkcji $f : \mathbb{Z} \to \mathbb{Z}$ zdefiniowanej wzorem $f(k) = k + 1$. Funkcja f jest oczywiście bijekcją. Dla dowolnego $n \in \mathbb{N}$ relacja R^n spełnia dla wszystkich $x, y \in \mathbb{Z}$ równoważność

$$x R^n y \Leftrightarrow y = x + n.$$

Jeżeli przedstawione argumenty nie implikują tej równoważności w sposób oczywisty, to proponuję sprawdzenie jej przez indukcję ze względu na n.

Dla tej funkcji f relacja R_∞ nie jest zwrotna, a nawet jest antyzwrotna. Dla wszystkich $x \in \mathbb{Z}$, założenie $x R_\infty x$ można sprowadzić do sprzeczności w następujący sposób: warunek $x R_\infty x$ oznacza, że $\langle x, x\rangle \in \bigcup_{n=1}^{\infty} R^n$. Tak więc dla pewnej

liczby $m > 0$ mamy $\langle x, x\rangle \in R^m$, czyli $x R^m x$. Z podanej charakteryzacji relacji R^m wynika, że $x = x + m$. Jest to możliwe tylko, gdy $m = 0$. Przeczy to jednak warunkowi $m > 0$.

Jeżeli R_∞ nie jest zwrotna, to nie jest relacją równoważności. Można też dowieść w podobny sposób, że R_∞ nie jest też symetryczna.

Część 2. Założenie o skończoności zbioru A implikuje, że R_∞ jest relacją równoważności. Dla dowolnego $x \in A$, rozważamy funkcję $I : \mathbb{N} \to A$ taką, że $I(n) = f^n(x)$ dla wszystkich $n \in \mathbb{N}$ ($I(n)$ to wartość n-krotnego złożenia funkcji f dla argumentu x, $f^0(x) = x$). Gdyby funkcja I była różnowartościowa, to zbiór A byłby nieskończony. Dla skończonego zbioru A funkcja I nie jest różnowartościowa. Tak więc możemy znaleźć dwie liczby naturalne p i q, takie, że $p < q$ oraz $f^p(x) = I(p) = I(q) = f^q(x)$. Składanie funkcji jest operacją łączną i zachowuje różnowartościowość. Wobec tego, $f^p(x) = f^q(x) = f^p(f^{q-p}(x))$. Różnowartościowość funkcji f^p implikuje także równość $f^{p-q}(x) = x$. Udowodniliśmy więc, że jeżeli A jest zbiorem skończonym, to dla dowolnego $x \in A$ istnieje liczba dodatnia r taka, że

$$f^r(x) = x. \tag{1}$$

Udowodniona własność oznacza, że relacja R_∞ jest zwrotna. Aby się o tym przekonać, bierzemy $x \in A$ i liczbę $r > 0$ spełniającą (1). Z równości (1) wynika, że $\langle x, x\rangle \in f^r = R^r$. Zawieranie $R^r \subseteq R_\infty$ implikuje zaś, że $\langle x, x\rangle \in R_\infty$.

Równość (1) implikuje także, że jeżeli iterujemy obliczanie wartości funkcji f zaczynając od argumentu x, to otrzymujemy w kółko te same wartości

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

Spostrzeżenie to pozwala dowieść symetryczność relacji R_∞. Najpierw jednak zauważmy, że równość (1) zachodzi także dla wszystkich wielokrotności r. Świadczą o tym następujące obliczenia będące fragmentem dowodu indukcyjnego:

$$f^{(k+1)r}(x) = f^{kr}(f^r(x)) = f^{kr}(x) = x.$$

Teraz możemy przystąpić do dowodu, że relacja R_∞ jest symetryczna. Przypuśćmy, że $\langle x, y\rangle \in R_\infty$. Na podstawie definicji R_∞ stwierdzamy, że $\langle x, y\rangle \in R^n$ dla pewnej dodatniej liczby naturalnej n. Ponieważ relacja R^n jest równa f^n, więc $f^n(x) = y$. Weźmy liczbę naturalną k taką, że $n < kr$. Dla tej liczby k mamy $kr - n > 0$ oraz

$$f^{kr-n}(y) = f^{kr-n}(f^n(x)) = f^{kr}(x) = x.$$

Udowodniona równość oznacza, że

$$\langle y, x\rangle \in f^{kr-n} = R^{kr-n} \subseteq R_\infty.$$

Przechodniość relacji R_∞ wynika z jednego z zadań w rozdziale o relacjach w *Materiałach do zajęć* (zadanie nr 212 w wydaniu z roku 2011).

Z przedstawionych rozumowań otrzymujemy, że jeżeli zbiór A jest skończony, to relacja R_∞ jest zwrotna i symetryczna. Wiemy też, że jest przechodnia. Tak więc dla zbioru skończonego A, relacją R_∞ jest równoważnością. ∎

Zadanie 11. Przypuśćmy, że V jest skończonym zbiorem zmiennych zdaniowych, $R \subseteq V^2$ jest przechodnią relacją w zbiorze V, a $p_0, q_0 \in V$ są dwiema różnymi zmiennymi zdaniowymi. Niech Φ będzie formułą zdaniową

$$p_0 \wedge \neg q_0 \wedge \bigwedge_{(p,q)\in R} (p \Rightarrow q).$$

Pokaż, że formuła Φ jest sprzeczna wtedy i tylko wtedy, gdy $(p_0, q_0) \in R$.

Rozwiązanie. Najpierw udowodnimy, że jeżeli $(p_0, q_0) \notin R$, to formuła Φ jest spełnialna. Zrobimy to definiując wartościowanie spełniające Φ.

Zauważmy, że chcemy zdefiniować wartościowanie, przy którym będzie prawdziwa formuła p_0, będą prawdziwe wszystkie implikacje $p \Rightarrow q$ takie, że $(p, q) \in R$, i — w konsekwencji — będą prawdziwe wszystkie zmienne q takie, że $(p_0, q) \in R$, oraz możliwie dużo zmiennych będzie fałszywych, gdyż q_0 powinna być fałszywa. Weźmy więc wartościowanie w, przy którym prawdziwa jest zmienna p_0 oraz wszystkie zmienne q takie, że $(p_0, q) \in R$, a pozostałe zmienne są fałszywe.

Pokażemy, że przy wartościowaniu w koniunkcja Φ jest prawdziwa. W tym celu wystarczy pokazać, że wszystkie jej człony są prawdziwe.

Oczywiście, pierwszy człon (p_0) jest prawdziwy przy wartościowaniu w. Ponieważ $q_0 \neq p_0$ i $(p_0, q_0) \notin R$, więc zmienna q_0 jest fałszywa przy wartościowaniu w, a drugi człon formuły Φ (negacja q_0) jest prawdziwy.

Pozostałe człony koniunkcji Φ są postaci $p \Rightarrow q$ dla zmiennych p i q takich, że $(p, q) \in R$. Weźmy więc p i q takie, że $(p, q) \in R$. Jeżeli zmienna p jest fałszywa przy wartościowaniu w, to implikacja $p \Rightarrow q$ jest przy tym wartościowaniu prawdziwa.

Przypuśćmy więc, że zmienna p jest prawdziwa przy wartościowaniu w. Wtedy są możliwe dwa przypadki: albo $p = p_0$, albo $(p_0, p) \in R$. W każdym przypadku (w drugim z przechodniości R) mamy, że $(p_0, q) \in R$. Tak więc zmienna q oraz implikacja $p \Rightarrow q$ są prawdziwe przy wartościowaniu w. W ten sposób dowiedliśmy spełnialności formuły Φ.

Udowodnimy jeszcze metodą nie wprost, że jeżeli $(p_0, q_0) \in R$, to formuła Φ jest sprzeczna. Załóżmy więc, że koniunkcja Φ jest prawdziwa przy pewnym wartościowaniu. Przy tym wartościowaniu są prawdziwe wszystkie człony Φ, a więc m.in. formuły p_0, $\neg q_0$ oraz — na mocy założenia $(p_0, q_0) \in R$ — implikacja $p_0 \Rightarrow q_0$. Oczywiście, nie jest to możliwe, gdyż implikacja $p_0 \Rightarrow q_0$ jest fałszywa przy każdym wartościowaniu, przy którym formuły p_0 i $\neg q_0$ są prawdziwe. ∎

Zadanie 12. Na zbiorze X określone są takie relacje równoważności Q i R, że

1. każda klasa równoważności relacji Q ma q elementów,
2. każda klasa relacji R ma r elementów oraz
3. istnieje klasa równoważności relacji Q, która ma dokładnie jeden element wspólny z każdą klasą równoważności relacji R.

Ile elementów ma zbiór X?

Rozwiązanie. Przyjmijmy, że A oznacza tę klasę równoważności relacji Q, o której jest mowa w punkcie 3), a K — zbiór klas równoważności relacji R.

Wszystkie przedstawione rozwiązania korzystają z faktu, że zbiory K i A mają tyle samo elementów. Jeżeli to wiemy, to na podstawie warunku 1) stwierdzamy, że K ma q elementów. Relacja równoważności R wyznacza więc podział zbioru X na q rozłącznych klas równoważności, które mają po r elementów. Stąd otrzymujemy, że X ma $q \cdot r$ elementów. Dalej pokażę, jak dowodzić, że $|A| = |K|$.

Sposób 1. Niech $f : K \to A$ będzie funkcją, która dla klasy $Y \in K$ przyjmuje wartość $f(Y) \in Y \cap A$. Punkt 3) ze sformułowania zadania gwarantuje poprawność tej definicji.

Pokażemy, że funkcja f jest bijekcją. Jeżeli $f(Y) = f(Z)$ dla pewnych klas klas $Y, Z \in K$, to $f(Y) \in (Y \cap A) \cap (Z \cap A) \subseteq Y \cap Z$. W tym przypadku klasy Y i Z nie są rozłączne, a to jest możliwe tylko wtedy, gdy $Y = Z$. Wobec tego f jest różnowartościowa.

Weźmy teraz $a \in A$. Oczywiście, klasa równoważności $[a]_R$ należy do K. Gdyby $f([a]_R) \neq a$, to zbiór $[a]_R \cap A$ miałby przynajmniej dwa elementy: $f([a]_R)$ oraz a, a to przeczy warunkowi 3). Tak więc funkcja f jest typu „na".

Sposób 2. Tym razem definiujemy funkcję $g : A \to K$, która elementowi $a \in A$ przyporządkowuje klasę $[a]_R$ (przyjmujemy, że $g(a) = [a]_R$). Podobnie jak w pierwszym rozwiązaniu, funkcja g jest bijekcją.

Jeżeli $[a]_R = [b]_R$ dla $a, b \in A$, to do klasy $[a]_R$ należy zarówno a, jak i b. Z wyboru A mamy jednak, że do dowolnej klasy równoważności może należeć tylko jeden element zbioru A, więc $a = b$.

Jeżeli Y jest dowolną klasą równoważności relacji R, to z warunku 3) (a raczej z wyboru A) znajdujemy w niej pewien element $a \in A$. Wobec tego, klasy równoważności $[a]_R$ i Y nie są rozłączne. Takie klasy muszą być równe. Otrzymaliśmy więc, że $g(a) = [a]_R = Y$.

Sposób 3. Zauważmy, że

$$A = A \cap X = A \cap \bigcup_{Y \in K} Y = \bigcup_{Y \in K} A \cap Y$$

(druga równość wynika stąd, że suma klas równoważności jest równa dziedzinie relacji równoważności). Zbiory $A \cap Y_1$ i $A \cap Y_2$ dla różnych klas równoważności Y_1 i Y_2 są rozłączne, ponieważ klasy te są rozłączne. Wobec tego

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

■

Zadanie 13. Niech A, B będą dowolnymi zbiorami. Kiedy równanie

$$A \cup X = B$$

1. ma dokładnie jedno rozwiązanie,
2. ma nieskończenie wiele rozwiązań,
3. nie ma rozwiązań?

Rozwiązanie. Jeżeli równanie $A \cup X = B$ ma rozwiązanie, to jest taki zbiór C, że $A \cup C = B$. Wtedy oczywiście zbiór A jest podzbiorem B. Także na odwrót, jeżeli $A \subseteq B$, to zbiór $X = B \setminus A$ spełnia równanie $A \cup X = B$.

Udowodniliśmy więc, że równanie $A \cup X = B$ ma rozwiązanie wtedy i tylko wtedy, gdy $A \subseteq B$. Tym samym odpowiedzieliśmy na pytanie 3: równanie $A \cup X = B$ nie ma rozwiązania wtedy i tylko wtedy, gdy $A \not\subseteq B$.

Załóżmy, że $A \subseteq B$. Scharakteryzujemy rozwiązania równania $A \cup X = B$. Warunek $A \cup C = B$ implikuje, że C jest podzbiorem B oraz zawiera różnicę $B \setminus A$. Prawdziwa jest także implikacja odwrotna: jeżeli $B \setminus A \subseteq C \subseteq B$, to

$$B = A \cup (B \setminus A) \subseteq A \cup C \subseteq A \cup B = B,$$

a więc C spełnia równanie $A \cup X = B$. Tak więc zbiorem rozwiązań równania $A \cup X = B$ jest

$$\{X : B \setminus A \subseteq X \subseteq B\}.$$

Policzymy jeszcze liczbę elementów tego zbioru, albo jego moc. W tym celu definiujmy funkcję f określoną w zbiorze $\mathcal{P}(A)$ wszystkich podzbiorów zbioru A i przyjmującą wartości dane wzorem

$$f(Y) = Y \cup (B \setminus A).$$

Łatwo dowodzi się, że funkcja f przekształca $\mathcal{P}(A)$ na zbiór rozwiązań równania $A \cup X = B$. Co więcej, jest to funkcja różnowartościowa. Jeżeli bowiem $f(Y_1) = f(Y_2)$ dla pewnych $Y_1, Y_2 \in \mathcal{P}(A)$, to

$$Y_1 = (Y_1 \cup (B \setminus A)) \cap A = f(Y_1) \cap A = f(Y_2) \cap A = (Y_2 \cup (B \setminus A)) \cap A = Y_2.$$

Tak więc funkcja f ustala równoliczność zbioru $\mathcal{P}(A)$ i zbioru rozwiązań równania $A \cup X = B$. Oznacza to, że równanie $A \cup X = B$ ma tyle elementów, co zbiór $\mathcal{P}(A)$ (albo zbiór rozwiązań równania $A \cup X = B$ jest tej samej mocy, co zbiór $\mathcal{P}(A)$).

Teraz łatwo odpowiedzieć na pytania 1 i 2. Jeżeli A jest niepusty to ma przynajmniej dwa podzbiory: zbiór pusty i samego siebie. Tak więc równanie $A \cup X = B$ ma dokładnie jedno rozwiązanie wtedy i tylko wtedy, gdy A jest zbiorem pustym.

Zbiory skończone mają skończenie wiele podzbiorów, a nieskończone — nieskończenie wiele. Wobec tego, równanie $A \cup X = B$ ma nieskończenie wiele rozwiązań wtedy i tylko wtedy, gdy A jest zbiorem nieskończonym. ∎

Zadanie 14. Niech $\alpha : \mathbb{N} \to \{0, 1\}$ będzie ciągiem zerojedynkowym. Symbolem $\sim_\alpha$ oznaczamy relację w zbiorze $\{0, 1\}^{\mathbb{N}}$ nieskończonych ciągów zerojedynkowych zdefiniowaną formułą

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

Czy istnieje taki ciąg α, dla którego:

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

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

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

Rozwiązanie. Ustalmy α i przyjmijmy, że $A = \{n \in \mathbb{N} \mid \alpha(n) = 1\}$. Oczywiście, $\sim_\alpha$ jest relacją równoważności. Przyjmijmy, że N_α jest zbiorem klas równoważności tej relacji. Symbolem $[x]_\alpha$ będziemy oznaczać klasy abstrakcji relacji $\sim_\alpha$.

Fakt 9. Zbiór N_α i zbiór $\{0, 1\}^A$ są równoliczne.

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

$$\bar{\xi}(n) \quad = \quad \begin{cases} \xi(n), & \text{jeżeli } n \in A, \\ 0, & \text{w przeciwnym razie.} \end{cases}$$

Zdefiniujmy jeszcze wzorem

$$f(\xi) \quad = \quad [\bar{\xi}]_\alpha$$

funkcję $f : \{0, 1\}^A \to N_\alpha$. Funkcja ta jest różnowartościowa i typu „na".

Aby dowieść różnowartościowość funkcji f weźmy dwa (różne) argumenty ξ_1 i ξ_2 tej funkcji. Są to funkcje określone w zbiorze A. Istnieje więc liczba $n \in A$ taka, że $\xi_1(n) \neq \xi_2(n)$. Funkcje $\bar{\xi}_1$ i $\bar{\xi}_2$ też przyjmują różne wartości dla argumentu n:

$$\bar{\xi}_1(n) = \xi_1(n) \neq \xi_2(n) = \bar{\xi}_2(n).$$

Oznacza to, że $\bar{\xi}_1 \not\sim_\alpha \bar{\xi}_2$. Stąd otrzymujemy, że klasy $[\bar{\xi}_1]_\alpha$ i $[\bar{\xi}_2]_\alpha$ są różne (różnią się np. elementem $\bar{\xi}_1$).

Weźmy dowolną klasę ze zbioru N_α i jej reprezentanta γ. Pokażemy, że $[\gamma\,]_\alpha$ jest wartością funkcji f. W tym celu weźmy funkcję $\delta : A \to \{0, 1\}$ będącą obcięciem γ do zbioru A (a więc spełniającą $\delta(n) = \gamma(n)$ dla wszystkich $n \in A$) i zauważmy, że także $\bar{\delta}(n) = \gamma(n)$ dla wszystkich $n \in A$. To jednak oznacza, że $\bar{\delta} \sim_\alpha \gamma$. Wobec tego, $f(\delta) = [\bar{\delta}]_\alpha = [\gamma\,]_\alpha$.

Dowód (inny sposób). Weźmy funkcję $g : \{0, 1\}^{\mathbb{N}} \to \{0, 1\}^A$ przyporządkowującą funkcji $\gamma \in \{0, 1\}^{\mathbb{N}}$ obcięcie funkcji γ do zbioru A. Oczywiście, funkcja g jest typu „na". Świadczy o tym np. równość $g(\bar{\xi}) = \xi$.

Funkcja g spełnia także równoważność

$$g(\gamma_1) = g(\gamma_2) \Leftrightarrow \gamma_1 \sim_\alpha \gamma_2.$$

Równoważność ta implikuje, że wzór

$$G([\gamma\,]_\alpha) = g(\gamma\,)$$

jest poprawną definicją funkcji $G : N_\alpha \to \{0, 1\}^A$ i – co więcej – funkcja ta jest różnowartościowa. Ponieważ g jest typu „na", więc także G jest typu „na".

Fakt 10. Klasy równoważności relacji $\sim_\alpha$ są równoliczne ze zbiorem $\{0, 1\}^{\mathbb{N}\setminus A}$.

Dowód. Weźmy dowolną funkcję $\beta \in \{0, 1\}^{\mathbb{N}}$ i zdefiniujmy funkcję $f : [\beta]_\alpha \to \{0, 1\}^{\mathbb{N}\setminus A}$. Funkcja f elementowi $\gamma \in [\beta]_\alpha$ przyporządkowuje obcięcie γ do zbioru $\mathbb{N} \setminus A$. Aby dowieść podany fakt pokażemy, że funkcja f jest bijekcją.

Weźmy więc różne funkcje $\gamma_1, \gamma_2 \in [\beta]_\alpha$. Ponieważ należą do jednej klasy równoważności relacji $\sim_\alpha$, więc przyjmują te same wartości dla dowolnego argumentu ze zbioru A. Wobec tego, przyjmują różne wartości dla pewnego $n \notin A$. Ich obcięcia od zbioru $\mathbb{N} \setminus A$ też przyjmują różne wartości dla tego samego argumentu, a więc są różne. To dowodzi, że funkcja f jest różnowartościowa.

Aby dowieść, że funkcja f jest typu „na", weźmy dowolną funkcję $\xi \in \{0, 1\}^{\mathbb{N}\setminus A}$ i zdefiniujmy $\gamma \in \{0, 1\}^{\mathbb{N}}$ takie, że

$$\gamma(n) = \begin{cases} \beta(n), & \text{jeżeli } n \in A, \\ \xi(n), & \text{w przeciwnym razie.} \end{cases}$$

Oczywiście, funkcje γ i β są w relacji $\sim_\alpha$ oraz obcięcie γ do $\mathbb{N} \setminus A$ jest równe ξ. Tak więc $f(\gamma) = \xi$.

Fakt 11. Jeżeli zbiór $A \subseteq \mathbb{N}$ jest nieskończony, to zbiór $\{0, 1\}^A$ jest nieprzeliczalny.

Dowód. Nieskończony podzbiór A zbioru liczb naturalnych jest równoliczny ze zbiorem liczb naturalnych $\mathbb{N}$. Jeżeli zbiór A jest równoliczny z $\mathbb{N}$, to także zbiory $\{0,1\}^A$ i $\{0,1\}^{\mathbb{N}}$ są równoliczne. Ten ostatni zbiór jest nieprzeliczalny na podstawie twierdzenia Cantora. Oznacza to, że także zbiór $\{0,1\}^A$ jest nieprzeliczalny.

Wniosek. Zbiór N_α klas równoważności relacji $\sim_\alpha$ jest albo skończony, albo nieprzeliczalny.

Dowód. Są możliwe dwa przypadki: albo zbiór A jest skończony i wtedy zbiór $\{0,1\}^A$ i równoliczny z nim zbiór N_α są skończone, albo zbiór A jest nieskończony i zarówno zbiór $\{0,1\}^A$ jak i równoliczny z nim zbiór N_α są nieprzeliczalne.

Z powyższego wniosku wynika negatywna odpowiedź na pytanie a): dla żadnego α zbiór klas równoważności relacji $\sim_\alpha$ nie jest przeliczalny i nieskończony.

Wniosek. Klasy abstrakcji relacji $\sim_\alpha$ są albo skończone, albo nieprzeliczalne.

Dowód. Ten wniosek dowodzimy dokładnie tak, jak poprzedni.

Z ostatniego wniosku otrzymujemy negatywną odpowiedź na pytanie c): dla żadnego α żadna klasa klasa równoważności nie jest nieskończona przeliczalna.

Negatywna odpowiedź na pytanie c) implikuje także negatywną odpowiedź na pytanie b). Odpowiedź na pytanie b) można też łatwo wyprowadzić z ostatniego wniosku. ∎

Zadanie 15. Niech $f : \mathbb{R} \to \mathbb{R}$. Mówimy, że $x \in \mathbb{R}$ jest lokalnym maksimum funkcji f, jeżeli istnieje taka dodatnia liczba rzeczywista r, że dla każdego $y \in \mathbb{R}$

$$(x - r < y < x + r \wedge x \neq y) \Rightarrow f(x) > f(y)$$

Udowodnij, że dla każdej funkcji $f : \mathbb{R} \to \mathbb{R}$ zbiór jej lokalnych maksimów jest przeliczalny.

Rozwiązanie. Nie należy ulec pokusie i próbować udowodnić powyższe twierdzenie w następujący, niesłuszny sposób:

Dowód (fałszywy!). Z każdym z maksimów lokalnych x związujemy taki przedział zawierający x, że dla każdej liczby z tego przedziału z wyjątkiem x funkcja f przyjmuje wartości mniejsze niż $f(x)$ (taki przedział istnieje na mocy definicji). Z każdego takiego przedziału wybieramy liczbę wymierną. Zbudowaliśmy więc odwzorowanie przekształcające zbiór maksimów funkcji w zbiór liczb wymiernych, który jest przeliczany.

Niestety nie zadbaliśmy o to, by odwzorowanie powyższe było różnowartościowe! Jednym z warunków, który by to zagwarantował, jest wymaganie, by przedziały otaczające maksima były rozłączne. Nie zawsze jednak takie przedziały da się wybrać. Podam przykłady funkcji, dla których nie można skonstruować takiej rodziny parami rozłącznych przedziałów zawierających wszystkie maksima lokalne, że w każdym przedziale jest najwyżej jedno maksimum.

Rozważmy funkcję $f_1 : \mathbb{R} \to \mathbb{R}$ zdefiniowaną wzorem

$$f_1(x) = \begin{cases} \sin\left(\frac{1}{x}\right), & \text{dla } x \neq 0, \\ 2, & \text{dla } x = 0. \end{cases}$$

Łatwo sprawdzić, że funkcja f_1 przyjmuje maksimum lokalne dla $x = 0$ i dla wszystkich $x = \frac{1}{2k\pi}$ dla $k \in Z$.

Podobnie jest w przypadku funkcji f_2 zdefiniowanej wzorem

$$f_2(x) = \begin{cases} x^2\left(\sin\left(\frac{1}{x}\right) - 2\right), & \text{dla } x \neq 0, \\ 0, & \text{dla } x = 0, \end{cases}$$

która dodatkowo jest ciągła, a nawet różniczkowalna.

Weźmy teraz funkcję $f : \mathbb{R} \to \mathbb{R}$ przyjmującą wartości

$$f(x) = \begin{cases} \frac{1}{n}, & \text{jeżeli } x = \frac{m}{n}, \text{ gdzie } n \text{ i } m \text{ są liczbami} \\ & \text{względnie pierwszymi i } n > 0, \\ 1, & \text{jeżeli } x = 0, \\ 0, & \text{jeżeli } x \notin \mathbb{Q}. \end{cases}$$

Dla tej funkcji zbiór lokalnych maksimów jest równy zbiorowi liczb wymiernych. Zauważmy od razu ważną własność funkcji f: dla dowolnej dodatniej liczby k i dla dowolnej liczby całkowitej a, funkcja f nie przyjmuje wartości $1/k$ dla argumentów $x \in (a/k, (a+1)/k)$.

Najpierw pokażemy, że $3/7$ jest lokalnym maksimum f. Oczywiście, $f(3/7) = 1/7$. Zauważmy, że w przedziale $(2/7, 4/7)$ funkcja f przyjmuje wartość $1/7$ tylko dla $x = 3/7$. Funkcja f przyjmuje też wartości większe od $1/7$ i są to wartości 1, 1/2, 1/3, 1/4, 1/5 i 1/6. Ale f nie przyjmuje wartości 1 w przedziale $(0, 1)$, nie przyjmuje wartości $1/2$ w przedziale $(0, 1/2)$, nie przyjmuje wartości $1/3$ dla $x \in (1/3, 2/3)$, wartości $1/4$ dla $x \in (1/4, 2/4)$, wartości $1/5$ dla $x \in (2/5, 3/5)$ oraz wartości $1/6$ dla $x \in (2/6, 3/6)$. Zauważmy, że do wszystkich wymienionych przedziałów należy $3/7$. Co więcej, dla argumentów należących do przekroju wymienionych przedziałów (z wyjątkiem $x = 3/7$) funkcja f nie przyjmuje wartości $\geq 1/7$. Przekrojem tym jest $(2/5, 1/2)$. Dla $x \in (2/5, 1/2)$ z wyjątkiem $x = 3/7$ funkcja f przyjmuje wartości mniejsze od $1/7$. Zmniejszając ten przedział można spowodować, że

jego środkiem stanie się punkt 3/7. Tak więc 3/7 jest jednym z maksimów lokalnych funkcji f.

Przedstawione rozumowanie można powtórzyć dla każdej z liczb wymiernych. Jeżeli m/n jest nieskracalnym przedstawieniem liczby wymiernej i $n > 0$, to definiujemy

$$a_k = \max\left\{a \in \mathbb{Z} \;\middle|\; \frac{a}{k} < \frac{m}{n}\right\}.$$

Oczywiście, $\frac{a_k}{k} < \frac{m}{n} \leq \frac{a_k+1}{k}$. Jeżeli $0 < k < n$, to także $\frac{m}{n} < \frac{a_k+1}{k}$, gdyż przedstawienie liczby wymiernej w postaci nieskracalnego ułamka z dodatnim mianownikiem jest jednoznaczne i liczba m/n nie daje się przedstawić w postaci l/k.

Przyjmijmy, że

$$p = \max\{a_1, \ldots, a_n\} \text{ oraz } q = \min\{a_1 + 1, \ldots, a_{n-1} + 1, a_n + 2\}.$$

Liczby p i q są tak dobrane, że

$$(p, q) = \bigcap_{k=1}^{n-1} (a_k, a_k + 1) \cap (a_n, a_n + 2).$$

Oczywiście, $m/n \in (p, q)$. Ze wspomnianej własności funkcji f otrzymujemy, że na przedziale (p, q) nie przyjmuje ona wartości $> 1/n$ oraz – z wyjątkiem argumentu m/n – nie przyjmuje wartości $1/n$. Wobec tego, na przedziałach $(p, m/n)$ i $(m/n, q)$ funkcja f przyjmuje tylko wartości $< 1/n$. Aby wykazać, że liczba m/n spełnia warunek z definicji maksimum lokalnego wystarczy zastąpić przedział (p, q) mniejszym i symetrycznym względem punktu m/n.

Można konstruować jeszcze bardziej skomplikowane funkcje o interesujących nas własnościach. Prawdopodobnie można dowieść, że dla dowolnego przeliczalnego zbioru $X \subseteq \mathbb{R}$ istnieje funkcja $f : \mathbb{R} \to \mathbb{R}$, która ma maksima lokalne dokładnie w punktach należących do X.

Dowód (poprawny). Weźmy funkcję $f : \mathbb{R} \to \mathbb{R}$ i zdefiniujmy zbiór

$$M = \{x \in \mathbb{R} \mid x \text{ jest maksimum lokalnym funkcji } f\}.$$

Aby rozwiązać zadanie wystarczy dowieść, że M jest przeliczalny. Przeliczalność zbioru M wykażemy dowodząc, że istnieje różnowartościowa funkcja

$$g : M \to Q \times Q.$$

Od funkcji g będziemy wymagać, aby dla argumentu $m \in M$ jej wartością była para liczb wymiernych r_1 i r_2 taka, że $r_1 < m < r_2$ i dla wszystkich $x \in \mathbb{R}$ spełniony jest warunek

$$r_1 < x < r_2 \wedge x \neq m \Rightarrow f(x) < f(m).$$

Oczywiście, dla każdego $m \in M$ takie liczby r_1 i r_2 istnieją. Dzięki temu, korzystając z przeliczalności produktu $Q \times Q$ można zdefiniować funkcję g przyjmując, że $g(m)$ jest pierwszą w ustalonej numeracji zbioru $Q \times Q$ parą o podanych własnościach.

Teraz wystarczy dowieść, że funkcja g jest różnowartościowa. Przypuśćmy, że mamy dwa różne elementy $m_1, m_2 \in M$ takie, że $g(m_1) = g(m_2)$. Jeżeli $g(m_1) = (r_1, r_2)$, to $m_1, m_2 \in (r_1, r_2)$ i z podanej własności g możemy wywnioskować dwie nierówności:

$$f(m_2) < f(m_1) \text{ oraz } f(m_1) < f(m_2).$$

Z drugiej strony, te nierówności nie mogą być jednocześnie prawdziwe. Uzyskana w ten sposób sprzeczność dowodzi różnowartościowości funkcji g, a to z kolei implikuje przeliczalność zbioru M. ∎

Zadanie 16. Pokaż, że zbiory: liczb wymiernych ze zwykłym porządkiem i skończonych niepustych ciągów liczb wymiernych z porządkiem leksykograficznym generowanym przez zwykły porządek na liczbach wymiernych *są* izomorficzne. *Wsk.:* skorzystaj z wyników poprzednich zadań.

Rozwiązanie. W tym zadaniu należy skorzystać z twierdzenia, które mówi, że każde dwa przeliczalne porządki liniowe, które są gęste i bez końców, są izomorficzne (jest to jedno z zadań w rozdziale o izomorfizmie porzadkowym w *Materiałach do zajęć*). Aby skorzystać z tego twierdzenia, należy pokazać, że:

1. zbiór skończonych, niepustych ciągów o wyrazach wymiernych jest przeliczalny (jest to jedno z zadań w rozdziale o zbiorach przeliczalnych),
2. porządek leksykograficzny wyznaczony przez porządek liniowy jest porządkiem liniowym (to z kolei jedno z zadań w rozdziale o przykładach porządków),
3. porządek leksykograficzny w zbiorze skończonych, niepustych ciągów o wyrazach wymiernych jest gęsty,
4. oraz nie ma w nim elementu największego, ani najmniejszego.

Aby dowieść gęstość rozważanego porządku weźmy dwa skończone, niepuste ciągi a i b liczb wymiernych odpowiednio o wyrazach $a_1, a_2, \ldots, a_n$ i $b_1, b_2, \ldots, b_m$. Załóżmy, że ciąg a jest mniejszy w sensie porządku leksykograficznego od ciągu b. Są możliwe dwa przypadki: albo $n < m$ oraz $a_i = b_i$ dla wszystkich $i = 1, \ldots, n$, albo też dla pewnej liczby $k \leq n, m$ zachodzi nierówność $a_k < b_k$ i spełnione są równości $a_i = b_i$ dla $i = 1, \ldots, k-1$. Jeżeli zachodzi pierwszy przypadek, to bierzemy ciąg c o wyrazach $b_1, b_2, \ldots, b_n, b_{n+1} - 1$. W drugim przypadku bierzemy ciąg c o wyrazach $b_1, b_2, \ldots, b_{k-1}, (a_k + b_k)/2$. Bez trudu sprawdzamy, że w obu przypadkach ciąg c jest większy w sensie porządku leksykograficznego od ciągu a i mniejszy od ciągu b.

Jest też oczywiste, że jeżeli a_1 jest pierwszym wyrazem ciągu a, to jednoelementowy ciąg, którego wyrazem jest liczba $a_1 + 1$ jest większy od a, a jednoelementowy ciąg, którego wyrazem jest liczba $a_1 - 1$ jest mniejszy od a. Tak więc w rozważanym porządku leksykograficznym nie ma elementu największego, ani najmniejszego.

Zadanie 17. Niech $\Sigma = \{+, a\}$ będzie sygnaturą zawierającą dwuargumentowy symbol funkcji $+$ i symbol stałej a. Dla dowolnej dodatniej liczby naturalnej n niech $A_n = \{0, 1, \ldots, n-1\}$, $\oplus_n$ oznacza dodawanie modulo n, zaś $a_n = 0$. Rozważmy algebry $\mathcal{A}_n = \langle A_n, \oplus_n, a_n \rangle$. Udowodnij, że jeżeli $k = l \cdot m$, to istnieje homomorfizm h algebry $\mathcal{A}_k$ na algebrę $\mathcal{A}_l$ (surjekcja) taki, że $|h^{-1}(\{0\})| = m$. Podaj przykład takich k, l i m, dla których istnieją co najmniej dwa takie homomorfizmy. Ile jest takich homomorfizmów, jeśli zamiast sygnatury Σ będziemy rozważać sygnaturę $\Sigma' = \{+, a, b\}$ zawierającą dwa symbole stałych a i b oraz algebry $\mathcal{A}'_n = \langle A_n, \oplus_n, a_n, b_n \rangle$, gdzie $b_n = 1$?

Rozwiązanie. Resztę z dzielenia k przez l będę oznaczać także symbolem $k \bmod l$. Zauważmy, że każdy element A_k jest sumą pewnej liczby jedynek (daje się przedstawić w postaci $1 \oplus_k \ldots \oplus_k 1$). Wobec tego 1 generuje A_k. Homomorfizm wystarczy zdefiniować na zbiorze generatorów. Przyjmijmy więc, że $h : A_k \to A_l$ jest homomorfizmem i $h(1) = a$. Wtedy

$$h(n) = h(\underbrace{1 \oplus_k \ldots \oplus_k 1}_{n \text{ razy}}) = \underbrace{h(1) \oplus_l \ldots \oplus_l h(1)}_{n \text{ razy}} = (a \cdot n) \bmod l.$$

Fakt 12. Jeżeli l dzieli k, to funkcja $h_a : A_k \to A_l$ zdefiniowana wzorem

$$h_a(x) = (a \cdot x) \bmod l$$

jest homomorfizmem algebr $\mathcal{A}_k$ i $\mathcal{A}_l$.

Dowód. Zauważmy najpierw, że definicja funkcji h_a zależy od k i l, mimo że wprowadzone oznaczenie na to nie wskazuje. Oczywiście, $h_a(0) = 0$. Wystarczy więc dowieść, że dla wszystkich $x, y \in A_k$ zachodzi równość $h_a(x \oplus_k y) = h_a(x) \oplus_l h_a(y)$. Zauważmy, że

$$a \cdot x = p \cdot l + h_a(x) \text{ oraz } a \cdot y = q \cdot l + h_a(y)$$

dla pewnych liczb naturalnych p i q. Z tych samych powodów zachodzi równość

$$x + y = r \cdot k + (x \oplus_k y).$$

Łącząc podane równości otrzymujemy

$$a \cdot r \cdot k + a \cdot (x \oplus_k y) = a \cdot (x + y) = (p + q) \cdot l + h_a(x) + h_a(y).$$

Ponieważ l dzieli k, więc

$$h_a(x \oplus_k y) = a \cdot (x \oplus_k y) \bmod l = (h_a(x) + h_a(y)) \bmod l = h_a(x) \oplus_l h_a(y).$$

Część 1. Korzystając z podanego faktu można łatwo rozwiązać pierwszą część zadania. Wystarczy zauważyć, że jeżeli $k = l \cdot m$, to $h_1 : A_k \to A_l$ jest homomorfizmem takim, że $h_1(x) = x$ dla $x = 0, \ldots, l-1$, a więc jest homomorfizmem algebry $\mathcal{A}_k$ na algebrę $\mathcal{A}_l$. Mamy także

$$\begin{aligned} h_1^{-1}(0) &= \{x < l \cdot m \mid x \bmod l = 0\} = \{x < l \cdot m \mid l \text{ dzieli } x\} = \\ &= \{i \cdot l \mid i < m\} = g(\{i \mid i < m\}) \end{aligned}$$

dla funkcji $g : \mathbb{N} \to \mathbb{N}$ takiej, że $g(i) = i \cdot l$. Funkcja g jest oczywiście różnowartościowa. Wobec tego zbiór $h_1^{-1}(0)$ jest równoliczny ze zbiorem $\{i \mid i < m\}$, który oczywiście ma m elementów, i też ma m elementów.

Część II. Aby rozwiązać drugą część zadania wystarczy dodatkowo zauważyć, że jeżeli weźmiemy $k = l = 3$, to odpowiednia funkcja h_2 przekształca A_3 na A_3 ($h_2(1) = 2$ i $h_2(2) = 1$) i — wobec tego — jest homomorfizmem algebry $\mathcal{A}_3$ na algebrę $\mathcal{A}_3$. Funkcje h_1 i h_2 są w tym przypadku różne, ponieważ $1 = h_1(1) \neq h_2(1) = 2$. Podobnie jest w przypadku funkcji $h_2 : A_6 \to A_3$ (jest to inna funkcja niż poprzednia, mimo że jest tak samo oznaczana!). Można dowieść, że dla dowolnej wielokrotności k liczby l, funkcja h_a przekształca A_k na A_l wtedy i tylko wtedy, gdy a jest względnie pierwsze z l.

Część III. Z definicji homomorfizmu wynika, że homomorfizmy algebry $\mathcal{A}'_k$ w algebrę $\mathcal{A}'_l$ są to dokładnie homomorfizmy algebry $\mathcal{A}_k$ w algebrę $\mathcal{A}_l$ przekształcające 1 na 1. Aby więc odpowiedzieć na ostatnie pytanie wystarczy ustalić, ile jest homomorfizmów przekształcających algebrą $\mathcal{A}_k$ na algebrę $\mathcal{A}_l$ i przeprowadzających 1 na 1. Pokażemy, że jeżeli l dzieli k, to jest dokładnie jeden taki homomorfizm. Oczywiście, jest taki homomorfizm (jest nim h_1). Przypuśćmy, że h też jest takim homomorfizmem. Wtedy

$$h(n) = h(\underbrace{1 \oplus_k \ldots \oplus_k 1}_{n \text{ razy}}) = \underbrace{h(1) \oplus_l \ldots \oplus_l h(1)}_{n \text{ razy}} = \underbrace{h_1(1) \oplus_l \ldots \oplus_l h_1(1)}_{n \text{ razy}} = h_1(n)$$

dla wszystkich $n \in A_k$. Wobec tego, homomorfizmy h i h_1 są identyczne. Bardziej elegancki dowód tego faktu powinien być indukcyjny. ∎

Zadanie 18. Niech $A_0, A_1, A_2, \ldots$ będzie ciągiem zbiorów takim, że

$$A_{n+1} = \Big(\bigcup_{i=0}^{n} A_i\Big) \times \Big(\bigcup_{i=0}^{n} A_i\Big)$$

dla wszystkich $n \in \mathbb{N}$. Przyjmijmy, że

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

Pokaż, że $B \times B \subseteq B$.

Rozwiązanie. Aby dowieść zawieranie $B \times B \subseteq B$ wystarczy z założenia $X \in B \times B$ wywnioskować, że $X \in B$. Załóżmy więc, że $X \in B \times B$. Elementami iloczynu kartezjańskiego $B \times B$ są pary uporządkowane o współrzędnych należących do B. Przypuśćmy, że X jest parą uporządkowaną $\langle a, b\rangle$ o współrzędnych $a, b \in B$, czyli $X = \langle a, b\rangle$. Zbiór B jest sumą mnogościową wyrazów ciągu $A_0, A_1, A_2, \ldots$ Wobec tego, elementy a i b należą do pewnych składników tej sumy. Przyjmijmy, że $a \in A_p$ oraz $b \in A_q$ dla pewnych liczb $p, q \in \mathbb{N}$. Stąd oczywiście wynika, że

$$a, b \in \bigcup_{i=0}^{\max\{p,q\}} A_i.$$

Łatwo zauważyć, że

$$X = \langle a, b\rangle \in \left(\bigcup_{i=0}^{\max\{p,q\}} A_i\right) \times \left(\bigcup_{i=0}^{\max\{p,q\}} A_i\right) = A_{\max\{p,q\}+1}.$$

Zbiór $A_{\max\{p,q\}+1}$ jest jednym ze składników sumy równej B. Ponieważ

$$X \in A_{\max\{p,q\}+1},$$

więc także $X \in B$.

Zadanie 19. Rozważmy formuły zdaniowe ϕ, w których występują jedynie spójniki równoważności i negacji. Niech ϕ^- oznacza formułę, którą otrzymujemy usuwając z ϕ wszystkie znaki negacji. Udowodnij, że

1. jeżeli symbol negacji występuje w ϕ parzystą liczbę razy, to $\phi \Leftrightarrow \phi^-$ jest tautologią,
2. jeżeli symbol negacji występuje w ϕ nieparzystą liczbę razy, to $\phi \Leftrightarrow \neg\phi^-$ jest tautologią.

Zauważ, że operacja $^-$ ma następujące własności: $(\neg\phi)^- = \phi^-$ oraz $(\phi \Leftrightarrow \psi)^- = \phi^- \Leftrightarrow \psi^-$.

Przypomnijmy, że formuły zdaniowe ϕ i ψ są równoważne wtedy i tylko wtedy, gdy formuła $\phi \Leftrightarrow \psi$ jest tautologią. Napis $\phi \equiv \psi$ oznacza, że formuły ϕ i ψ są równoważne. Będziemy korzystać z następujących znanych i łatwych do wykazania własności:

1. formuły $\neg\neg\phi$ i ϕ są równoważne,
2. każde dwie z formuł $(\neg\phi) \Leftrightarrow \psi$, $\neg(\phi \Leftrightarrow \psi)$ i $\phi \Leftrightarrow (\neg\psi)$ są równoważne,
3. formuły $(\neg\phi) \Leftrightarrow (\neg\psi)$ i $\phi \Leftrightarrow \psi$ są równoważne.

Niech $\mathcal{F}$ oznacza zbiór wszystkich formuł zdaniowych, w których nie występują spójniki różne od negacji i równoważności. Przyjmijmy też, że symbol $\mathcal{F}_n$ oznacza zbiór tych formuł należących do $\mathcal{F}$, w których występuje najwyżej n spójników.

Rozwiązanie (najbardziej naturalne). Pokażemy przez indukcję ze względu na n, że dla każdej liczby naturalnej n i dla każdej formuły $\phi \in \mathcal{F}_n$ zachodzą następujące implikacje:

1. jeżeli w formule ϕ negacja występuje na parzystej liczbie miejsc, to formuła $\phi \Leftrightarrow \phi^-$ jest tautologią,
2. jeżeli w formule ϕ negacja występuje na nieparzystej liczbie miejsc, to formuła $\phi \Leftrightarrow \neg\phi^-$ jest tautologią.

Z tego pozornie bardziej ogólnego faktu bez trudu można wywnioskować tezę rozwiązywanego zadania.

Pierwsza część dowodu indukcyjnego. Jeżeli $n = 0$, to $\mathcal{F}_n = \mathcal{F}_0$ jest zbiorem zmiennych zdaniowych. Wobec tego, dla formuł $\phi \in \mathcal{F}_0$ zachodzi równość $\phi = \phi^-$. Pierwsza z dowodzonych implikacji jest konsekwencją tego, że formuły postaci $p \Leftrightarrow p$ są tautologiami. Druga zachodzi, ponieważ jej poprzednik jest fałszywy.

Druga część dowodu indukcyjnego. Zakładamy, że formuły ze zbioru $\mathcal{F}_n$ mają obie podane własności i bierzemy formułę $\phi \in \mathcal{F}_{n+1}$. Możemy dodatkowo założyć, że $\phi \notin \mathcal{F}_n$ (dla formuł z $\mathcal{F}_n$ teza zachodzi na mocy założenia indukcyjnego). Oczywiście, wszystkie formuły ze zbioru $\mathcal{F}$ są negacjami, równoważnościami lub zmiennymi i formuła ϕ nie jest zmienną (w przeciwnym razie należałaby do $\mathcal{F}_0 \subseteq \mathcal{F}_n$).

Przypadek 1: formuła ϕ jest negacją. Przyjmijmy, że $\phi = \neg\psi$. W tym przypadku, $\phi^- = \psi^-$. Oczywiście, formuła $\psi \in \mathcal{F}_n$ i dla formuły ψ możemy skorzystać z założenia indukcyjnego. W zależności od liczby wystąpień negacji w formule ψ, tautologią jest albo formuła $\psi \Leftrightarrow \psi^-$ (gdy negacja występuje w ϕ parzystą liczbę razy), albo formuła $\psi \Leftrightarrow \neg\psi^-$ (w przeciwnym przypadku).

Jeżeli w formule ϕ negacja występuje na parzystej liczbie pozycji, to w formule ψ występuje na nieparzystej i tautologią jest formuła $\psi \Leftrightarrow (\neg\psi^-)$. Tautologią jest także formuła $(\neg\psi) \Leftrightarrow \psi^-$, która jest równa formule $\phi \Leftrightarrow \phi^-$.

Jeżeli w formule ϕ negacja występuje w nieparzystej liczbie miejsc, to w formule ψ występuje w parzystej i formuła $\psi \Leftrightarrow \psi^-$ jest tautologią. Wtedy także tautologią jest formuła $(\neg\psi) \Leftrightarrow (\neg\psi^-)$ identyczna z formuła $\phi \Leftrightarrow (\neg\phi^-)$.

Przypadek 2: formuła ϕ jest równoważnością. Przyjmijmy, że $\phi = \psi_1 \Leftrightarrow \psi_2$ dla pewnych formuł $\psi_1, \psi_2 \in \mathcal{F}_n$. Tym razem zachodzi wzór $\phi^- = \psi_1^- \Leftrightarrow \psi_2^-$. Dalej powinniśmy rozważać cztery przypadki.

Przypadek 2.1: negacja występuje w ϕ nieparzystą, a w ψ_1 parzystą liczbę razy. W tym przypadku negacja występuje w ψ_2 nieparzystą liczbę razy. Dla formuł ψ_1 i ψ_2 możemy skorzystać z założenia indukcyjnego. Wobec tego, formuły ψ_1 i ψ_1^-

są równoważne, a także równoważne są ψ_2 i $\neg\psi_2^-$. Wobec tego formuła $\phi = \psi_1 \Leftrightarrow \psi_2$ jest równoważna z $\psi_1^- \Leftrightarrow \neg\psi_2^-$. Korzystając z własności 2), Formuła ϕ jest równoważna z $\neg(\psi_1^- \Leftrightarrow \psi_2^-) = \neg\phi^-$.

Przypadek 2.2: negacja występuje w ϕ i ψ_1 nieparzystą liczbę razy. W tym i kolejnych przypadkach przeprowadzamy rozumowanie podobne do wyżej przedstawionego.

Aby zakończyć rozwiązanie, powinniśmy jeszcze rozważyć następujące przypadki:

Przypadek 2.3: negacja występuje w ϕ parzystą, a w ψ_1 nieparzystą liczbę razy.

Przypadek 2.4: negacja występuje w ϕ i ψ_1 parzystą liczbę razy.

Rozwiązanie (sugerowane przez jedną z prac egzaminacyjnych). Przypuśćmy, że mamy daną formułę $\phi \in \mathcal{F}$ i wartościowanie h (zmiennych występujących w tej formule). Symbolem $\phi[h]$ oznaczamy wartość logiczną formuły ϕ przy wartościowaniu h. Dla danego wartościowania, indeksem $i_h(\phi)$ formuły ϕ nazywamy sumę liczby negacji występujących w ϕ i liczby wystąpień w ϕ zmiennych fałszywych przy wartościowaniu h. Na przykład, jeżeli $h(p) = 1$, $h(q) = 0$ oraz $\phi = (q \Leftrightarrow p) \Leftrightarrow \neg(q \Leftrightarrow (\neg q \Leftrightarrow p))$, to $i_h(\phi) = 5$.

Lemat 13. Przypuśćmy, że mamy formułę $\phi \in \mathcal{F}$ i wartościowanie h zmiennych tej formuły. Formuła ϕ jest spełniona przy wartościowaniu h wtedy i tylko wtedy, gdy $i_h(\phi)$ jest liczbą parzystą.

Dowód. Dowód tego lematu pozostawiamy jako ćwiczenie.

Wniosek. Formuła $\phi \in \mathcal{F}$ jest tautologią wtedy i tylko wtedy, gdy występuje w niej parzysta liczba negacji i każda zmienna zdaniowa występuje parzystą liczbę razy.

Dowód. Weźmy formułę $\phi \in \mathcal{F}$ i najpierw załóżmy, że jest tautologią. Formuła ϕ jest więc spełniona dla każdego wartościowania. Niech h wartościowaniem, które wszystkim zmiennym z formuły ϕ przyporządkowuje 1 (prawdę). Dla tego wartościowania indeks $i_h(\phi)$ jest liczbą negacji występujących w ϕ. Na podstawie powyższego lematu indeks ten jest liczbą parzystą.

Aby pokazać, że zmienna p występuje w ϕ parzystą liczbę razy weźmy wartościowanie h_p, które zmiennej p przyporządkowuje 0 (fałsz), a pozostałym zmiennym — 1 (prawdę). Dla tego wartościowania indeks $i_{h_p}(\phi)$ jest liczbą parzystą i jest równy sumie liczb wystąpień w ϕ negacji i wystąpień zmiennej p. Odejmując od indeksu liczbę wystąpień negacji otrzymujemy liczbę wystąpień zmiennej p. Liczba ta, jako różnica dwóch liczb parzystych jest parzysta.

Aby dowieść implikację przeciwną do udowodnionej, wystarczy zauważyć, że jeżeli w formule ϕ negacja i każda zmienna występuje parzystą liczbę razy, to dla

dowolnego wartościowania indeks tej formuły jest liczbą parzystą. W tej sytuacji, z powyższego lematu wynika, że formuła ϕ jest spełniona dla dowolnego wartościowania. ■

Korzystając z podanego wniosku bez trudu możemy sprawdzić, czy formuły takie, jak $\phi \Leftrightarrow \phi^-$ lub $\phi \Leftrightarrow \neg\phi^-$ są tautologiami.

Rozwiązanie (też sugerowane). Z lematu podanego w poprzednim rozwiązaniu wynika następujący, oczywisty wniosek:

Wniosek. Przypuśćmy, że formułę ψ otrzymujemy wymazując w formule $\phi \in \mathcal{F}$ jeden znak negacji. Wtedy, dla dowolnego wartościowania h wartości logiczne $\phi[h]$ i $\psi[h]$ są różne. ■

Weźmy teraz formułę $\phi \in \mathcal{F}$ i wymazujmy w niej kolejno symbole negacji tak długo, aż wymażemy wszystkie. Przypuśćmy, że w ten sposób otrzymujemy ciąg formuł

$$\phi = \phi_0, \phi_1, \ldots, \phi_n.$$

Oczywiście, $\phi_n = \phi^-$ i n jest liczbą znaków negacji występujących w ϕ. Z powyższego wniosku wynika, że dla dowolnego wartościowania h ciąg wartości logicznych

$$\phi[h] = \phi_0[h], \phi_1[h], \ldots, \phi_n[h] = \phi^-[h]$$

zawiera na przemian 0 i 1. Stąd wynika, że jeżeli n jest liczbą parzystą, to $\phi[h] = \phi^-[h]$ dla dowolnego wartościowania h. Podobnie, jeżeli n jest liczbą nieparzystą, to $\phi[h] \neq \phi^-[h]$ dla dowolnego wartościowania h. Teraz teza zadania jest już oczywista.

Rozwiązanie (jeszcze inna wersja). To rozwiązanie też rozpoczniemy od wykazania pomocniczego lematu.

Lemat 14. Jeżeli w formule $\phi \in \mathcal{F}$ występuje dokładnie jeden symbol negacji, to formuła $\phi \Leftrightarrow \neg\phi^-$ jest tautologią.

Dowód. Lemat ten udowodnimy przez indukcję ze względu na liczbę spójników występujących w $\mathcal{F}$. Dla formuł $\phi \in \mathcal{F}_0$ jest on oczywisty, gdyż dla takich formuł nie jest spełnione założenie lematu.

Przypuśćmy, że lemat zachodzi dla formuł ze zbioru $\mathcal{F}_n$ i weźmy formułę $\phi \in \mathcal{F}_{n+1}$. Są możliwe dwa przypadki.

Przypadek 1: formuła ϕ jest negacją. Jeżeli $\phi = \neg\psi$, to $\phi^- = \psi^-$ i dodatkowo — na podstawie założenia — w formule ψ nie występuje negacja, a więc $\psi^- = \psi$. Nietrudno zauważyć, że w tym przypadku w formule $\phi \Leftrightarrow \neg\phi^-$ po obu stronach równoważości znajduje się to samo.

Przypadek 2: formuła ϕ jest równoważnością. Jeżeli $\phi = \psi_1 \Leftrightarrow \psi_2$ i negacja występuje w ϕ w dokładnie jednym miejscu, to występuje w dokładnie jednym miejscu dokładnie jednej z formuł ψ_1 lub ψ_2. Dla ustalenia uwagi przyjmijmy, że negacja występuje w ψ_1.

Z założenia indukcyjnego wynika, że formuły ψ_1 i $\neg\psi_1^-$ są równoważne. Jest oczywiste, że $\psi_2^- = \psi_2$. Na podstawie własności 2) podanej na początku mamy, że formuła $\neg\phi^-$, czyli $\neg(\psi_1^- \Leftrightarrow \psi_2^-)$, jest równoważna formule $(\neg\psi_1^-) \Leftrightarrow \psi_2^-$, a ta z kolei — na podstawie założenia indukcyjnego — jest równoważna $\psi_1 \Leftrightarrow \psi_2^-$, czyli formule ϕ. ■

Załóżmy, że w formule ϕ jest symbol negacji i ten symbol poprzedza formułę δ. Przyjmijmy, że jeżeli wymażemy w ϕ tę negację wraz z formułą δ i w to miejsce wstawimy nową zmienną zdaniową q, to otrzymamy formułę ψ. Nietrudno zauważyć, że jeżeli teraz w formule ψ zastąpimy zmienną q formułą $\neg\delta$ to otrzymamy formułę $\psi(\neg\delta)$ identyczną z wyjściową formułą ϕ.

W formułach ψ i δ występuje mniej spójników, niż w ϕ. Z założenia indukcyjnego otrzymujemy, że zależnie od przypadku, formuły $\psi \Leftrightarrow \neg\psi^-$ oraz $\delta \Leftrightarrow \neg\delta^-$ lub podobne formuły bez negacji są tautologiami. Dalej korzystamy z dwóch faktów: zastępując w formułach równoważnych (lub w tautologii) pewną zmienną zdaniową dowolną formuła otrzymujemy formuły równoważne (lub odpowiednio: otrzymujemy tautologię) oraz zastępując w dowolnej formule pewien jej fragment formułą równoważną otrzymujemy formułę równoważną. Na przykład, jeżeli w formule ϕ występuje nieparzysta liczba spójników negacji oraz spójniki te podzieliły się tak, że podane wyżej formuły są tautologiami, to następujące formuły są równoważne:

$$\phi \;=\; \psi(\neg\delta),\; \neg\psi^-(\neg\delta),\; \neg\psi^-(\delta^-) \;=\; \neg\phi^-.$$

Sformułowany wyżej lemat przydaje się w innych przypadkach.

Zadanie 20. Czy prawdziwe jest zdanie: „Dla dowolnych zbiorów A i B, jeśli $A \times B \subseteq B \times A$, to $A = \emptyset \vee B = \emptyset \vee A = B$"?

Rozwiązanie. Tak, zdanie powyższe jest prawdziwe dla dowolnych zbiorów A i B. Istotnie, przypuśćmy, że $A \times B \subseteq B \times A$ oraz $A \neq \emptyset$ i $B \neq \emptyset$. Pokażemy, że $A = B$. Skoro $A \neq \emptyset$, to istnieje pewien element $a_0 \in A$. Dla dowolnego $b \in B$ mamy wówczas $\langle a_0, b\rangle \in A \times B$. Skoro $A \times B \subseteq B \times A$, to $\langle a_0, b\rangle \in B \times A$. Zatem $b \in A$. Ponieważ w powyższym rozumowaniu b jest dowolne, więc $B \subseteq A$. Analogicznie skoro $B \neq \emptyset$, to istnieje pewien element $b_0 \in B$. Dla dowolnego $a \in A$ jest wtedy $\langle a, b_0\rangle \in A \times B$. Skoro $A \times B \subseteq B \times A$, to $\langle a, b_0\rangle \in B \times A$. Zatem $a \in B$. Pokazaliśmy więc, że $A \subseteq B$. Skoro $B \subseteq A$ oraz $A \subseteq B$, to $A = B$.

Zadanie 21. Pokaż, że $A \setminus (B \setminus (C \setminus D)) = (A \setminus B) \cup ((A \cap C) \setminus D)$ dla dowolnych zbiorów A, B, C i D.

Rozwiązanie. Zauważmy, że równoważne są każde dwie z niżej podanych formuł:

1. $x \in A \setminus (B \setminus (C \setminus D))$,
2. $x \in A \wedge \neg(x \in B \wedge \neg(x \in C \wedge x \notin D))$,
3. $x \in A \wedge (x \notin B \vee (x \in C \wedge x \notin D))$,
4. $(x \in A \wedge x \notin B) \vee (x \in A \wedge (x \in C \wedge x \notin D))$,
5. $(x \in A \wedge x \notin B) \vee ((x \in A \wedge x \in C) \wedge x \notin D)$,
6. $x \in (A \setminus B) \cup ((A \cap C) \setminus D)$.

Równoważność dwóch pierwszych formuł wynika z definicji działań mnogościowych, drugiej i trzeciej – z prawa de Morgana i prawa podwójnej negacji, dwóch kolejnych – z prawa rozdzielności koniunkcji względem alternatywy, następnej pary – z prawa łączności dla koniunkcji, a dwóch ostatnich – znowu z definicji działań mnogościowych. W ten sposób, dla dowolnego x dowiedliśmy równoważność

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

Oznacza to, że

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

W tej sytuacji równość

$$A \setminus (B \setminus (C \setminus D)) = (A \setminus B) \cup ((A \cap C) \setminus D))$$

wynika z zasady ekstensjonalności.

Przedstawione rozwiązanie zawiera elementy sformalizowanego rachunku logicznego. Czytając takie rozwiązanie nie wiadomo, czy osoba, która je przedstawiła rozumie, co robi, czy też nauczyła się tylko mechanicznie wykonywać dziwne i niezrozumiałe przekształcenia. Co więcej, takie rozwiązania są możliwe tylko w prostych przypadkach, a zadań bardziej interesujących nie można rozwiązać w ten sposób. Nie polecałbym tej metody ze względów dydaktycznych, mimo że jej zaletą jest czytelność. Zauważmy także, że czytając podręczniki wyjątkowo spotykamy się z takimi rozumowaniami. Również przekonując siebie i kolegów o słuszności różnych stwierdzeń zwykle robimy to w inny sposób.

Rozwiązanie. Udowodnię teraz dwa zawierania

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

oraz

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

nie korzystając z formalnego rachunku logicznego (a więc tak naprawdę znowu skorzystam z zasady ekstensjonalności).

Dowód (pierwszego zawierania). Weźmy dowolny $x \in A \setminus (B \setminus (C \setminus D))$. Nietrudno zauważyć, że elementy zbioru $A \setminus B$ należą do $(A \setminus B) \cup ((A \cap C) \setminus D))$. Wobec tego, dalej wystarczy rozważać tylko te elementy x, które nie należą do $A \setminus B$.

Element x należący do $A \setminus (B \setminus (C \setminus D))$ należy również do zbioru A. Jeżeli nie należy do $A \setminus B$, to należy do B. Wiemy też, że $x \notin B \setminus (C \setminus D)$. Jeżeli x należący do B nie znalazł się w tej różnicy, to należy do $C \setminus D$. Otrzymaliśmy więc, że $x \in A$, $x \in C$ oraz $x \notin D$. Teraz łatwo sprawdzić, że x należy do drugiego składnika sumy $(A \setminus B) \cup ((A \cap C) \setminus D))$. To kończy dowód pierwszej inkluzji.

Dowód (drugiego zawierania). Aby dowieść drugą inkluzję, weźmy $x \in (A \setminus B) \cup ((A \cap C) \setminus D)$. Są dwa rodzaje takich elementów x. Taki x może należeć do $A \setminus B$. Wtedy $x \in A$ oraz $x \notin B$. Warunkiem należenia do $B \setminus (C \setminus D)$ jest między innymi należenie do B. Wobec tego, $x \notin B \setminus (C \setminus D)$. Ponieważ $x \in A$, więc także $x \in A \setminus (B \setminus (C \setminus D))$.

Powinniśmy się jeszcze zająć elementami $x \in (A \cap C) \setminus D$. Te elementy należą do A i do $C \setminus D$. Elementy zbioru $C \setminus D$ zostały usunięte ze zbioru $B \setminus (C \setminus D)$, więc $x \notin B \setminus (C \setminus D)$. Oznacza to że x spełnia oba warunki wymagane od elementów $A \setminus (B \setminus (C \setminus D))$, czyli $x \in A \setminus (B \setminus (C \setminus D))$. Udowodniliśmy więc drugie zawieranie i tym samym dowiedliśmy, że

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

Rozwiązanie. Zamiast wyprowadzać równość z zadania bezpośrednio z definicji działań mnogościowych można skorzystać z własności tych działań. Takie rozwiązanie może być oparte na następującym rachunku:

$$A \setminus (B \setminus (C \setminus D)) = A \cap (B \cap (C \cap D^c)^c)^c = A \cap (B^c \cup (C \cap D^c)) =$$

$$= (A \cap B^c) \cup (A \cap C \cap D^c) = (A \setminus B) \cup ((A \cap C) \setminus D).$$

W powyższych wzorach ^{c} oznacza operację dopełnienia. Pierwsza równość wynika ze związku między różnicą i dopełnieniem, czyli z wzoru $X \setminus Y = X \cap Y^c$ zastosowanego trzy razy. Druga równość jest konsekwencją prawa de Morgana $(X \cap Y)^c = X^c \cup Y^c$. Trzecia wynika z prawa rozdzielności przekroju względem sumy mnogościowej. Ostatnia jest konsekwencją związku między różnicą a dopełnieniem oraz łączności przekroju.

Przedstawione rozwiązanie może być niezrozumiałe dla osób, które nie słyszały o dopełnieniu. Jest to bardzo naturalne działanie mnogościowe, jeżeli rozważamy podzbiory ustalonego zbioru zwanego wtedy przestrzenią. Z pewną ostrożnością może być wykorzystywane w każdej sytuacji.

Jeżeli P jest przestrzenią, to dopełnieniem zbioru $X \subseteq P$ nazywamy różnicę $P \setminus X$ i oznaczamy ją symbolem X^c. Zauważmy, że dopełnienie to jest właściwie dopełnienie do ustalonego zbioru (w tym przypadku P) i można dopełniać do różnych

zbiorów. Zauważmy również, że dla tak zdefiniowanego dopełnienia i dla $X \subseteq P$ zachodzi wzór

$$X \setminus Y = X \cap (P \setminus Y) = X \cap Y^c$$

oraz podane wyżej prawo de Morgana.

Z treści zadania nie wynika, że zbiory A, B, C i D są zawarte w jakiejś naturalnej przestrzeni. Zawsze jednak możemy przyjąć, że $P = A \cup B \cup C \cup D$ (lub $P = A \cup B \cup C$). Taka definicja P gwarantuje prawdziwość wzoru $X \setminus Y = X \cap Y^c$ w wymaganym zakresie.

Rozwiązanie. Zadanie to można także rozwiązać sprawdzając podaną równość dla konkretnych zbiorów. Spróbuję uzasadnić poprawność tej metody nie zachowując pełnej ogólności. Będziemy teraz dokładnie analizować pierwsze z rozwiązań. Najpierw wprowadźmy kilka oznaczeń. Niech

$$L_{ABCD} = A \setminus (B \setminus (C \setminus D)) \text{ oraz } P_{ABCD} = (A \setminus B) \cup ((A \cap C) \setminus D).$$

Będziemy też rozważać zmienne zdaniowe a, b, c i d (odpowiadają one zbiorom lub zmiennym A, B, C i D), a także formuły zdaniowe z tymi zmiennymi oraz wartościowania takich formuł. Przyjmijmy, że h^x_{ABCD} oznacza wartościowanie zmiennych a, b, c i d takie, że

$$h^x_{ABCD}(a) = T \;\Leftrightarrow\; x \in A$$

i spełniające analogiczne warunki dla pozostałych zmiennych, a H_{ABCD} oznacza zbiór wszystkich takich wartościowań. Symbolem $h^x_{ABCD}(\phi)$ będę oznaczać wartość logiczną formuły ϕ przy wartościowaniu h^x_{ABCD}.

Zauważmy, że w rozwiązaniu 1 zostały skonstruowane dwie formuły zdaniowe ϕ i ψ takie, że

$$\forall A, B, C, D\ \forall x\ (x \in L_{ABCD} \;\Leftrightarrow\; h^x_{ABCD}(\phi) = T)$$

oraz

$$\forall A, B, C, D\ \forall x\ (x \in P_{ABCD} \;\Leftrightarrow\; h^x_{ABCD}(\psi) = T).$$

Formuły te nie zależą od zbiorów A, B, C i D, a jedynie od wyrażeń występujących po obu stronach równości, np. formuła ϕ jest równa $a \wedge \neg(b \wedge \neg(c \wedge \neg d))$ bez względu na to, co oznaczają symbole A, B, C i D.

Z podanych własności wynika, że

$$\forall A, B, C, D\ (\forall x\ (x \in L_{ABCD} \Leftrightarrow x \in P_{ABCD}) \;\Leftrightarrow$$
$$\Leftrightarrow\; \forall x\ (h^x_{ABCD}(\phi) = T \Leftrightarrow h^x_{ABCD}(\psi) = T))$$

oraz

$$\forall A, B, C, D\ (L_{ABCD} = P_{ABCD} \;\Leftrightarrow\; \forall h \in H_{ABCD}\ h(\phi \;\Leftrightarrow\; \psi) = T). \quad (2)$$

Twierdzenie 15. Jeżeli A', B', C' i D' są jakimikolwiek zbiorami dla których zbiór $H_{A'B'C'D'}$ zawiera wszystkie możliwe wartościowania, oraz zachodzi równość

$$L_{A'B'C'D'} = P_{A'B'C'D'}$$

to

$$\forall A, B, C, D\ L_{ABCD} = P_{ABCD}$$

(a więc jeżeli równość $L = P$ zachodzi dla jednej (specyficznej) czwórki zbiorów, to zachodzi dla wszystkich możliwych czwórek).

Dowód. Aby dowieść podane twierdzenie skorzystamy z własności (2) dla $A = A'$, $B = B'$, $C = C'$ i $D = D'$. W ten sposób otrzymujemy, że

$$L_{A'B'C'D'} = P_{A'B'C'D'} \ \Leftrightarrow\ \forall h \in H_{A'B'C'D'}\ h(\phi \ \Leftrightarrow\ \psi) = T.$$

Na mocy założenia o zbiorze $H_{A'B'C'D'}$ prawa strona tej równoważności stwierdza, że formuła $\phi \ \Leftrightarrow\ \psi$ jest tautologią. Zakładamy ponadto lewą stronę tej równoważności. Stąd otrzymujemy, że formuła $\phi \ \Leftrightarrow\ \psi$ jest tautologią.

Weźmy cztery dowolne zbiory A, B, C i D. Chcemy teraz z własności (2) wywnioskować, że $L_{ABCD} = P_{ABCD}$. Aby to zrobić, wystarczy wykazać, że

$$\forall h \in H_{ABCD}\ h(\phi \ \Leftrightarrow\ \psi) = T.$$

Fakt ten jest oczywistą konsekwencją tego, że $\phi \ \Leftrightarrow\ \psi$ jest tautologią (tautologię są spełnione dla wszystkich wartościowań, a więc także dla wartościowań ze zbioru H_{ABCD}). □

Aby wykorzystać to twierdzenie trzeba jeszcze skonstruować zbiory A', B', C' i D' takie, że zbiór $H_{A'B'C'D'}$ zawiera wszystkie możliwe wartościowania zmiennych zdaniowych a, b c i d. Weźmy dowolne wartościowanie h tych zmiennych. Dla tego wartościowania wybieramy (dowolnie) pewien element x_h. Z wybranych w ten sposób elementów konstruujemy potrzebne nam zbiory w następujący sposób: x_h uznajemy za element zbioru A' wtedy i tyko wtedy, gdy $h(a) = T$. Analogicznie definiujemy pozostałe zbiory.

Dla zdefiniowanych w ten sposób zbiorów sprawdzamy dowodzoną równość. Jeżeli równość ta zachodzi, to z wykazanego twierdzenia otrzymujemy, że zachodzi dla wszystkich możliwych zbiorów.

Zadanie 22. Rodzina zbiorów $\{X_n\}_{n=0}^{\infty}$ jest *zstępująca*, jeżeli $X_{n+1} \subseteq X_n$ dla każdego $n \in \mathbb{N}$. Ciąg liczb naturalnych $(a_n)_{n=0}^{\infty}$ jest *rosnący*, jeżeli $a_n < a_{n+1}$ dla każdego $n \in \mathbb{N}$. Niech $(a_n)_{n=0}^{\infty}$ będzie rosnącym ciągiem liczb naturalnych, a $\{X_n\}_{n=0}^{\infty}$ — zstępującą rodziną zbiorów. Udowodnij, że

$$\bigcap_{n=0}^{\infty} X_n = \bigcap_{n=0}^{\infty} X_{a_n}.$$

Rozwiązanie.

Lemat 16. Jeżeli ciąg $(a_n)_{n\in\mathbb{N}}$ jest rosnący, to $a_n \geq n$ dla każego $n \in \mathbb{N}$.

Dowód. Przez indukcję względem n. Skoro $a_0 \in \mathbb{N}$, to $a_0 \geq 0$. Przypuśćmy, że $a_n \geq n$. Skoro ciąg jest rosnący, to $a_{n+1} > a_n \geq n$. Zatem $a_{n+1} \geq n+1$.

Lemat 17. Jeżeli rodzina $\{X_n\}_{n\in\mathbb{N}}$ jest zstępująca, to $X_n \subseteq X_m$ dla wszelkich $n, m \in \mathbb{N}$ takich, że $m \leq n$.

Dowód. Przez indukcję względem n. Jeżeli $m \leq 0$, to $m = 0$, więc $X_0 \subseteq X_m$. Przypuśćmy, że $X_n \subseteq X_m$ dla $m \geq n$. Skoro rodzina jest zstępująca, to $X_{n+1} \subseteq X_n \subseteq X_m$ dla $m \geq n$. Ponieważ nadto $X_{n+1} \subseteq X_m$ dla $m = n+1$, to $X_{n+1} \subseteq X_m$ dla dowolnego $m \leq n+1$.

Na mocy zasady ekstensjonalności wystarczy pokazać, że dla dowolnego x spełniona jest równoważność

$$x \in \bigcap_{n\in\mathbb{N}} X_n \;\Leftrightarrow\; x \in \bigcap_{m\in\mathbb{N}} X_{a_m}.$$

Z definicji przekroju rodziny zbiorów oznacza to, że dla dowolnego x zachodzi

$$\forall_{n\in\mathbb{N}}\, x \in X_n \;\Leftrightarrow\; \forall_{m\in\mathbb{N}}\, x \in X_{a_m}.$$

Aby wykazać żądaną w zadaniu równoważność, uzasadnimy osobno dwie implikacje.

„$\Rightarrow$” Wiemy, że dla dowolnej liczby naturalnej n zachodzi $x \in X_n$. Dla każdego m liczba a_m jest liczbą naturalną, zatem $x \in X_{a_m}$.

„$\Leftarrow$” Przypuśćmy, że $x \in X_{a_m}$ dla dowolnego m. Niech $n \in \mathbb{N}$. Z lematu 16 wiemy, że $a_n \geq n$. Z założenia wynika, że $x \in X_n$. Z lematu 17 wnioskujemy, że $X_{a_n} \subseteq X_n$. Zatem $x \in X_n$.

Rozwiązanie. Nie jest to rozwiązanie najprostsze, ale zawiera pomysł, który pozwala na odejście od bardzo formalnego rachunku logicznego. Aby uprościć wzory uzupełniamy dany ciąg liczb naturalnych o wyraz $a_{-1} = -1$. Tak uzupełniony ciąg jest nadal rosnący i każda liczba naturalna jest większa od pierwszego wyrazu tego ciągu (czyli od wyrazu o numerze -1).

Główna część rozwiązania wynika z następujących wzorów:

$$\bigcap_{n=0}^{\infty} X_n = \bigcap_{k=0}^{\infty} \bigcap_{n=a_{k-1}+1}^{a_k} X_n = \bigcap_{n=0}^{\infty} X_{a_n}.$$

Dalej wystarczy uzasadnić równości z tego wzoru.

Oczywiście, zaczynamy od dowodu pierwszej równości. Równość ta zachodzi, ponieważ po obu stronach równości mamy właściwie przekroje tej samej rodziny zbiorów. Aby bardziej formalnie wykazać zawieranie

$$\bigcap_{n=0}^{\infty} X_n \subseteq \bigcap_{k=0}^{\infty} \bigcap_{n=a_{k-1}+1}^{a_k} X_n,$$

weźmy dowolny element $x \in \bigcap_{n=0}^{\infty} X_n$. Wystarczy wykazać, że $x \in X_n$ dla dowolnych liczb $k \in \mathbb{N}$ oraz $n \in \mathbb{N}$ takich, że $a_{k-1} < n \leq a_k$. Jest to bezpośrednia konsekwencja wyboru elementu x.

Odwrotne zawieranie wynika z faktu, że każda liczba naturalna znajduje się między dwoma, kolejnymi wyrazami ciągu $\{a_n\}_{n=0}^{\infty}$, a dokładniej

$$\forall n \in \mathbb{N}\ \exists k \in \mathbb{N}\ a_{k-1} < n \leq a_k.$$

Jeżeli trzeba to udowodnić, to warto posłużyć się zasadą indukcji.

Aby dowieść to drugie zawieranie, bierzemy $x \in \bigcap_{k=0}^{\infty} \bigcap_{n=a_{k-1}+1}^{a_k} X_n$ i dowolną liczbę $n \in \mathbb{N}$. Będziemy uzasadniać, że $x \in X_n$. Dla liczby n znajdujemy $k \in \mathbb{N}$ takie, że $a_{k-1} < n \leq a_k$. Z założonej własności x wynika najpierw, że $x \in \bigcap_{n=a_{k-1}+1}^{a_k} X_n$, a następnie, że $x \in X_n$. W ten sposób pierwsza równość została udowodniona.

Druga równość jest konsekwencją zstępowania rodziny $\{X_n\}_{n=0}^{\infty}$. Przekrój skończenie wielu zbiorów porównywalnych w sensie inkluzji jest najmniejszym z tych zbiorów, czyli

$$\bigcap_{n=a_{k-1}+1}^{a_k} X_n = X_{a_{k-1}+1} \cap X_{a_{k-1}+2} \cap \ldots \cap X_{a_k} = X_{a_k}.$$

Oznacza to, że przekroje po obu stronach drugiej równości są przekrojami tego samego ciągu zbiorów, a więc są równe. Trochę dokładniejsze uzasadnienie powyższej równości może korzystać z zasady indukcji i wzorów

$$\bigcap_{n=p}^{q+1} X_n = (\bigcap_{n=p}^{q} X_n) \cap X_{q+1} = X_q \cap X_{q+1} = X_{q+1}.$$

Zadanie 23. Niech A będzie n-elementowym zbiorem uporządkowanym liniowo relacją $\leq$, gdzie $n \geq 5$. Na zbiorze A^2 definiujemy relację $\preceq$ w następujący sposób:

$$\langle a_1, a_2 \rangle \preceq \langle b_1, b_2 \rangle \quad \Leftrightarrow \quad (a_1 = b_1 \wedge a_2 = b_2) \vee (a_1 < b_1 \wedge a_2 < b_2),$$

gdzie $a < b$ oznacza, że $a \leq b$ i $a \neq b$.

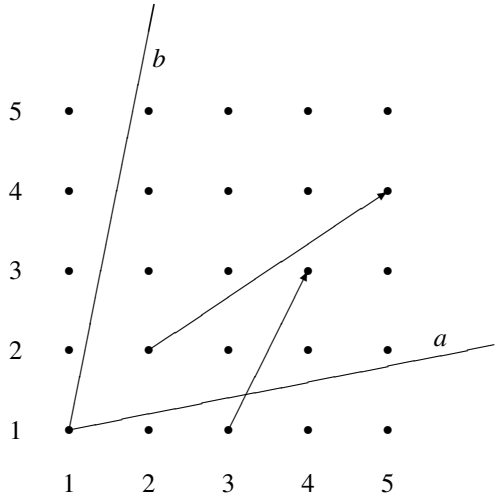
Wśród poniższych zdań wskaż zdania prawdziwe.

1. Porządek $\preceq$ jest regularny.
2. W $\langle A^2, \preceq\rangle$ istnieje element najmniejszy.
3. Liczba elementów maksymalnych w A^2 wzgledem porządku $\preceq$ wynosi
   - n
   - $n-1$
   - $\lfloor\sqrt{2}\,n-1\rfloor$
   - $2n-1$
   - $2n+1$
4. Liczba elementów zbioru A^2, które są jednocześnie minimalne i maksymalne wzgledem porządku $\preceq$ wynosi
   - $n-1$
   - 1
   - 0
   - $n+1$
   - 2
5. Liczba elementów minimalnych w A^2 wzgledem porządku $\preceq$ wynosi
   - n
   - $\lfloor\sqrt{2}\,n-1\rfloor$
   - $n+1$
   - $2n-1$
   - n^2
6. W $\langle A^2, \preceq\rangle$ istnieje łańcuch długości
   - n
   - $\lfloor\sqrt{2}\,n-1\rfloor$
   - $\lfloor n/2\rfloor$
   - $n+1$
   - 2

Rozwiązanie. Poniższy rysunek przedstawia kwadrat kartezjański zbioru

$$A = \{1, 2, 3, 4, 5\}$$

i pozwala opisać relację $\preceq$. Różne pary z A^2 są w relacji $\preceq$, jeżeli można na tym rysunku poprowadzić strzałkę od pierwszej (mniejszej) pary do drugiej (większej) i strzałka ta jest nachylona do prostej poziomej pod kątem przynajmniej takim, jak prosta a, i najwyżej takim, jak prosta b.



Strzałki znajdujące się na rysunku świadczą o tym, że $(2,2) \preceq (5,4)$ oraz $(3,1) \preceq (4,3)$. Analizując rysunek łatwo ustalić elementy minimalne w A^2. Są to pary, w których nie może kończyć się żadna strzałka, a więc pary postaci $(1,i)$ oraz $(i,1)$ dla $i = 1,2,3,4,5$. Widać też, że elementami maksymalnymi są pary postaci $(5,i)$ oraz $(i,5)$ dla $i = 1,2,3,4,5$. Można także przekonać się, że najdłuższy łańcuch w A^2 ma postać

$$(1,1) \prec (2,2) \prec (3,3) \prec (4,4) \prec (5,5).$$

Spostrzeżenia te łatwo uogólnia się i pozwala to rozwiązać zadanie 6.

Niech A oznacza teraz dowolny n elementowy ($n \geq 5$) zbiór liniowo uporządkowany. Przyjmijmy, że m oznacza najmniejszy element zbioru A, a M – element największy. Oczywiście, $m \neq M$.

Część 3. Przypuśćmy, że $(x,y) \in A^2$ oraz $x, y \neq m$. Wtedy $(m,m) \prec (x,y)$. Oznacza to, że pary (x,y) takie, że $x, y \neq m$ nie są elementami minimalnymi. To spostrzeżenie można też wyrazić stwierdzając, że zbiór elementów minimalnych w A^2 zawiera się w zbiorze

$$X = \{(m,x) \in A^2 : x \in A\} \cup \{(x,m) \in A^2 : x \in A\}.$$

Łatwo dowodzi się, że X jest zbiorem wszystkich elementów minimalnych w A^2, a więc że każda należąca do niego para jest elementem minimalnym. Na przykład, dla każdego $x \in A$ para (m,x) jest elementem minimalnym. W przeciwnym razie musiałaby istnieć inna para (a,b) taka, że $(a,b) \prec (m,x)$. Wtedy zachodziłaby nierówność $a < m$ przecząca definicji m.

Teraz łatwo ustalić liczbę elementów minimalmych. Przekrój zbiorów $\{(m,x) \in A^2 : x \in A\}$ oraz $\{(x,m) \in A^2 : x \in A\}$ jest równy $\{(m,m)\}$. Zbiory te są n elementowe, ponieważ są równoliczne z A. Na przykład, funkcja $f : A \to \{(m,x) \in A^2 : x \in A\}$ zdefiniowana równością $f(x) = (m,x)$ jest bijekcją. Tak więc liczba elementów minimalnych w A^2 jest równa

$$|X| = |\{(m,x) \in A^2 : x \in A\}| + |\{(x,m) \in A^2 : x \in A\}| - |\{(m,m)\}| = 2n - 1.$$

Część 4. Podobnie, jak w przypadku elementów minimalnych, zbiór elementów maksymalnych jest równy

$$Y = \{(M,x) \in A^2 : x \in A\} \cup \{(x,M) \in A^2 : x \in A\}$$

i ma $2n-1$ elementów. Wszystkie potrzebne fakty dowodzimy analogicznie.

Część 2. Dla każdego zbioru A o przynajmniej dwóch elementach, w zbiorze A^2 bez trudu znajdujemy trzy elementy minimalne: (M,m), (m,m) oraz (m,M). Jeżeli w jakimś zbiorze uporządkowanym są dwa elementy minimalne, to nie ma w nim elementu najmniejszego. Przypuśćmy, że jednak jest element najmniejszy i jest nim para (a,b). Wtedy zachodzą nierówności $(a,b) \preceq (m,M)$ oraz $(a,b) \preceq (m,m)$. Ponieważ pary (m,M) i (m,m) są różne, więc przynajmniej w jednym przypadku mamy nierówność ostrą. Jeżeli $(a,b) \prec (m,M)$, to $a < m$. Przeczy to definicji m. Podobnie w drugim przypadku. Otrzymana sprzeczność świadczy o nieistnieniu w zbiorze A^2 elementu najmniejszego.

Część 6. Zbiór elementów A^2, które są jednocześnie minimalne i maksymalne, to przekrój $X \cap Y$. Obliczymy ten zbiór. Zauważmy, że przekrój pierwszych składników z przedstawień zbiorów X i Y jest pusty (należące do nich pary różnią się pierwszą współrzędną). Podobnie jest w przypadku drugich składników. Ponadto,

$$\{(m,x) \in A^2 : x \in A\} \cap \{(x,M) \in A^2 : x \in A\} = \{(m,M)\},$$

a przekrój ostatniej pary składników jest równy $\{(M,m)\}$. Stąd nietrudno wywnioskować, że

$$X \cap Y = \{(m,M),(M,m)\}.$$

Wobec tego, w zbiorze A^2 są dwa takie elementy, które jednocześnie są minimalne i maksymalne, i są to (m,M) oraz (M,m).

Część 5. Zajmiemy się teraz łańcuchami w A^2. Jeżeli A jest zbiorem n elementowym, to łatwo zdefiniować łańcuch długości n. Tworzą go pary postaci (x,x) dla wszystkich $x \in A$. Pokażemy, że nie można z elementów A^2 utworzyć łańcucha dłuższego. Rozważmy funkcję $f : A^2 \to A$ przyporządkowującą parze (x,y) jej pierwszą współrzędną x. Jest to funkcja rosnącą, a więc warunek $(a,b) \prec (x,y)$ implikuje, że $a < x$. Funkcje rosnące są różnowartościowe. Wobec tego, długość

dowolnego łańcucha jest równa liczbie elementów zbioru jego pierwszych współrzędnych. Ponieważ pierwsze współrzędne są elementami A, więc długość łańcuchów nie przekracza $|A| = n$. W A^2 jest łańcuch długości n. Ponieważ fragment łańcucha też jest łańcuchem, więc są też łańcuchy długości 2 oraz $\lfloor n/2 \rfloor$. Nie ma natomiast łańcuchów długości $n+1$, ani $\lfloor \sqrt{2}n - 1 \rfloor$. Nie ma tych ostatnich, gdyż dla $n \geq 5$ zachodzi nierówność $n < \lfloor \sqrt{2}n - 1 \rfloor$.

Część 1. Każdy porządek w zbiorze skończonym jest regularny. Wynika to w sposób oczywisty wprost z definicji porządku regularnego.

Udowodnimy jeszcze podane twierdzenie korzystając z zasady indukcji (noetherowskiej dla zwykłego porządku w $\mathbb{N}$). Weźmy niepusty zbiór uporządkowany A o n elementach i dowolny element $a \in A$. Może jest to element minimalny. W przeciwnym razie, zbiór

$$X = \{x \in A : x < a\}$$

jest niepusty, ma mniej elementów niż A (brakuje w nim np. a) i jest uporządkowany tą samą relacją, co zbiór A. Korzystając z założenia indukcyjnego znajdujemy element $m \in X$, który jest minimalny w zbiorze X. Element m jest także minimalny w zbiorze A. W przeciwnym razie w zbiorze A istniałby element x taki, że $x < m$. Ponieważ $x < m < a$, więc $x \in X$. Przeczy to jednak założeniu o tym, że m jest minimalny w zbiorze X.

Zadanie 24. Niech $f : \mathbb{N} \to \mathbb{N}$. Symbol f^n oznacza n-krotne złożenie funkcji f:

$$\begin{aligned} f^0(x) &= x, \\ f^{n+1}(x) &= f(f^n(x)), \end{aligned}$$

dla dowolnych $n, x \in \mathbb{N}$. Rozważmy relację $R \subseteq \mathbb{N} \times \mathbb{N}$ taką, że

$$x R y \Leftrightarrow \exists n, m \in \mathbb{N}\ f^n(x) = f^m(y).$$

Pokaż, że R jest relacją równoważności. Ile klas abstrakcji ma relacja R, jeżeli funkcja f jest zdefiniowana wzorem $f(x) = \lfloor x/2 \rfloor$? Opisz te klasy abstrakcji i uzasadnij odpowiedzi.

Rozwiązanie. Rozwiązanie zadania 2 powinno zawierać między innymi dowód zwrotności i symetryczności relacji R. Ten fragment zadania jest bardzo prosty, prawie oczywisty. Wiele osób miało jednak kłopoty z przedstawieniem rozwiązania. Były one spowodowane koniecznością posługiwania się kwantyfikatorami egzystencjalnymi. Te same problemy występują w dowodzie przechodniości relacji R. Zamiast dowodzić, że R jest relacją równoważności pokażemy tylko przechodniość R i zrobimy to bardzo szczegółowo.

Przechodniość relacji R. Przypuśćmy, że mamy funkcję f i posługując się tą funkcją zdefiniowaliśmy relację R. Weźmy trzy liczby naturalne x, y i z takie, że

xRy i yRz. Z definicji relacji R wynika, że

$$\exists n, m \in \mathbb{N}\ f^n(x) = f^m(y) \ \wedge\ \exists n, m \in \mathbb{N}\ f^n(y) = f^m(z).$$

W szczególności, istnieją liczby naturalne n i m takie, że zachodzi równość $f^n(x) = f^m(y)$. Zwrot „istnieją liczby" znaczy, że takie liczby są. Być może nie wiemy jakie to liczby, może ich wyliczenie jest bardzo trudne i tego jeszcze nie zrobiliśmy, a może konkretna wartość tych liczb nie jest dla nas istotna. Ale mamy gwarancję, że one są. Symbole n i m raczej nie oznaczają tych liczb. Pomagają jedynie wyrazić własności, których oczekujemy od tych liczb: jedna z nich powinna pojawić się w równości $f^n(x) = f^m(y)$ w miejscu n, druga – w miejscu m. Jeżeli te liczby są, to albo możemy ustalić ich wartość, albo przynajmniej możemy sobie wyobrażać, że to zrobiliśmy. Wtedy możemy je oznaczyć. Przyjmijmy, że są to liczby a i b. Dokładniej, a jest tą liczbą, która odpowiada symbolowi n, zaś b odpowiada symbolowi m. Liczby a i b zostały więc wybrane tak, aby zachodziła równość $f^a(x) = f^b(y)$.

W podobny sposób z drugiej części założenia możemy wywnioskować, że są liczby c i d takie, że $f^c(y) = f^d(z)$.

Jeżeli $f^a(x) = f^b(y)$, to także $f^{a+1}(x) = f(f^a(x)) = f(f^b(y)) = f^{b+1}(y)$. Nakładając jeszcze raz f na obie strony otrzymanej równości dostajemy równość $f^{a+2}(x) = f^{b+2}(y)$. Łatwo udowodnić przez indukcję, że równość $f^{a+k}(x) = f^{b+k}(y)$ zachodzi dla wszystkich liczb naturalnych k. Wobec tego, zachodzi także równość $f^{a+c}(x) = f^{b+c}(y)$. W ten sam sposób z równości $f^c(y) = f^d(z)$ możemy wywnioskować, że $f^{b+c}(y) = f^{b+d}(z)$. Ponieważ równość jest przechodnia, więc $f^{a+c}(x) = f^{b+d}(z)$. Są więc takie liczby $n = a + c$ i $m = b + d$, że $f^n(x) = f^m(z)$. Tym samym wykazaliśmy istnienie liczb n i m spełniających równość $f^n(x) = f^m(z)$.

Dowiedliśmy więc, że xRz, a przeprowadzone rozumowanie uzasadnia przechodniość relacji R.

Klasy abstrakcji R. Łatwo zauważyć, że jeżeli funkcja f jest zdefiniowana wzorem $f(x) = \lfloor x/2 \rfloor$, to dla dowolnego n odpowiednie, wielokrotne złożenie funkcji f przyporządkowuje liczbie n wartość 0. Zgodnie z definicją relacji R fakt ten oznacza, że $0Rn$. Tak więc 0 jest w relacji R z dowolną liczbą naturalną n. Wykażemy to w sposób bardziej precyzyjny korzystając z zasady indukcji. W dowodzie zastosujemy indukcję noetherowską.

Niech n będzie dowolną liczbą naturalną. Jako założenie indukcyjne przyjmujemy, że własność $0Rm$ zachodzi dla wszystkich liczb naturalnych $m < n$. Chcemy wykazać, że także zachodzi własność $0Rn$. Jeżeli $n = 0$, to zwrotność relacji R gwarantuje, że $0Rn$. Dalej możemy więc zakładać, że n jest liczbą dodatnią. Wtedy

$$f(n) = \lfloor n/2 \rfloor \leq n/2 < n.$$

Oznacza to, że dla liczby $f(n)$ możemy skorzystać z założenia indukcyjnego. W ten

sposób otrzymujemy, że $0Rf(n)$. Z definicji relacji R bez trudu wynika, że $f(n)Rn$. Ponieważ relacja R jest przechodnia, więc także $0Rn$.

Klasa abstrakcji $[0]$ relacji R wyznaczona przez 0 jest zawarta w zbiorze liczb naturalnych. Wykazaliśmy też, że zawiera wszystkie liczby naturalne. Wobec tego, $[0] = \mathbb{N}$. Ponieważ klasy abstrakcji relacji R są niepuste i tworzą podział $\mathbb{N}$, więc R nie może mieć innych klas abstrakcji.

Zadanie 25. Czy istnieje relacja równoważności

(a) w zbiorze $\mathbb{N}$, której wszystkie klasy abstrakcji są nieskończone i jest ich nieskończenie wiele?

(b) w zbiorze $\mathbb{R}$, której wszystkie klasy abstrakcji są przeliczalne i jest ich przeliczalnie wiele?

Rozwiązanie. Aby rozwiązać to zadanie, dobrze jest przypomnieć sobie zasadę abstrakcji (z rozdziału o relacjach równoważności w *Materiałach do zajęć*). Zasadę tę przedstawimy teraz nieco nieformalnie. Stwierdza ona, że zamiast zajmować się relacjami równoważności można (w sposób równoważny) zajmować się podziałami na klasy abstrakcji.

Zamiast pytać się o istnienie relacji równoważności, przeformułujemy zadanie i najpierw zapytamy o istnienie odpowiedniego podziału, np. podziału zbioru liczb naturalnych na nieskończenie wiele zbiorów nieskończonych. Na to pytanie odpowiedź jest pozytywna.

Wyobraźmy sobie kwadrat. Jeden z jego boków nazwiemy podstawą, drugi, sąsiadujący z pierwszym – wysokością. Nietrudno zauważyć, że kwadrat można podzielić na odcinki równoległe do podstawy. Każdy z nich ma tyle punktów, co podstawa, i jest ich tyle, co punktów wysokości. Podobnie jest z kwadratem kartezjańskim zbioru liczb naturalnych. Oczywiście,

$$\mathbb{N}^2 = \bigcup_{n\in\mathbb{N}} \{\langle i, n\rangle : i \in \mathbb{N}\} = \bigcup_{n\in\mathbb{N}} L_n$$

dla zbiorów $L_n = \{\langle i, n\rangle : i \in \mathbb{N}\}$. Tak więc zbiór $\mathbb{N}^2$ można podzielić na nieskończenie wiele zbiorów L_n, z których każdy jest nieskończony.

Zbiory L_n tworzą podział (wszystkie razem, dokładniej: podziałem jest rodzina $\{L_n : n \in \mathbb{N}\}$). Oczywiście, zbiory L_n są niepuste. Dla różnych liczb n i m mamy $L_n \cap L_m = \emptyset$. Aby się o tym przekonać wystarczy zauważyć, że w przeciwnym razie, z należenia pewnej pary do przekroju $L_n \cap L_m$ wynika, że pierwsza współrzędna tej pary jest jednocześnie równa n i m, co nie jest możliwe. Ostatnim warunek z definicji podziału został już wcześniej zauważony.

Nieskończoność zbioru L_n (dla każdej, ustalonej liczby n) jest konsekwencją równoliczności zbioru L_n ze zbiorem liczb naturalnych. Równoliczność ustala oczywiście funkcja $k_n : \mathbb{N} \to L_n \subseteq \mathbb{N}^2$ zdefiniowana wzorem $k_n(i) = \langle i, n\rangle$.

Nieskończoność całej rodziny zbiorów dowodzimy pokazując, że funkcja $l : \mathbb{N} \to \{L_n : n \in \mathbb{N}\}$ taka, że $l(n) = L_n$, jest bijekcją.

Tak więc udało się nam zdefiniować nieskończony podział zbioru $\mathbb{N}^2$ na nieskończone zbiory. A mieliśmy to zrobić dla zbioru $\mathbb{N}$. Możemy teraz skorzystać z równoliczności $\mathbb{N}$ i $\mathbb{N}^2$.

Niech $f : \mathbb{N} \to \mathbb{N}^2$ będzie bijekcją. Przyjmijmy, że

$$X_n = \vec{f}^{-1}(L_n) = \{j \in \mathbb{N} : f(j) \in L_n\}.$$

Tak zdefiniowane zbiory, czyli przeciwobrazy zbiorów L_n wyznaczone przez funkcję f, tworzą podział zbioru liczb naturalnych. Pomijam szczegółowy dowód tego faktu, wszystko, co trzeba, wynika z własności przeciwobrazów.

Przedstawione rozwiązanie miało pokazać, jak można znaleźć potrzebny podział zbioru liczb naturalnych. Osoby, które mają już trochę doświadczenia, mogą konstruować podziały zbioru liczb naturalnych na wiele sposobów. Możemy np. przyjąć, że

$$Y_n = \{2^n \cdot i \in \mathbb{N} : i \in \mathbb{N}\},$$

albo, posługując się ciągiem $\langle p_n \rangle_{n\in\mathbb{N}}$ kolejnych liczb pierwszych, zdefiniować zbiory

$$Z_n = \{i \in \mathbb{N} : p_n \text{ dzieli } i \wedge \forall k < n \;\; p_k \text{ nie dzieli } i\}.$$

Rodziny $\{Y_n : n \in \mathbb{N}\}$ oraz $\{Z_n : n \in \mathbb{N}\}$ też tworzą nieskończone podziały zbioru liczb naturalnych złożone ze zbiorów nieskończonych.

Mając podział $\{X_n : n \in \mathbb{N}\}$ zbioru liczb naturalnych należy jeszcze wskazać relację równoważności R, której klasy równoważności tworzą ten właśnie podział. Odnoszę wrażenie, że powinno teraz wystarczyć powołanie się na zasadę abstrakcji. Niemal równie łatwo jest powtórzyć dowód zasady abstrakcji. Trzeba zdefiniować R i można to zrobić na dwa sposoby: albo pisząc

$$R = \bigcup_{n\in\mathbb{N}} X_n^2,$$

albo, w sposób równoważny,

$$aRb \iff \exists n \in \mathbb{N}\ \langle a, b\rangle \in X_n^2.$$

Sprawdzenie, że tak zdefiniowana relacja R jest relacją równoważności nie powinno być trudne. Łatwo też wykazać, że klasa abstrakcji $[a]_R$ jest tym zbiorem X_n, do którego należy liczba a.

Druga część zadania (część (b)) też wynika z zasady abstrakcji, ale w tym przypadku odpowiedź jest negatywna. Nie istnieje relacja równoważności w zbiorze $\mathbb{R}$, która ma przeliczalnie wiele przeliczalnych klas abstrakcji. Zgodnie z zasadą abstrakcji, suma mnogościowa wszystkich klas abstrakcji relacji równoważności jest

dziedziną relacji, a więc w rozważanym przypadku — zbiorem liczb rzeczywistych $\mathbb{R}$. Ze znanego i ważnego twierdzenia o sumowaniu zbiorów przeliczalnych wynika, że jeżeli sumujemy przeliczalną rodzinę takich zbiorów, to otrzymujemy zbiór przeliczalny. Gdyby więc istniała taka relacja, zbiór liczb rzeczywistych byłby przeliczalny. Zbiór liczb rzeczywistych nie jest jednak przeliczalny (jest to twierdzenie Cantora), a uzyskana w ten sposób sprzeczność dowodzi, że nie istnieje interesująca nas relacja równoważności.

Zadanie 26. Udowodnij, że jeśli $\{A_i\}_{i\in\mathbb{N}}$ jest indeksowaną rodziną skończonych zbiorów liczb naturalnych, to uogólniony iloczyn kartezjański $\prod_{i\in\mathbb{N}} A_i$ jest zbiorem skończonym lub ma moc co najmniej continuum.

Rozwiązanie. W tym zadaniu pierwszą trudnością do pokonania jest mnogość sytuacji, jakie mogą wystąpić. Będziemy więc rozważać kilka przypadków. Zrobimy to też w sposób bardziej szczegółowy, niż było to wymagane na egzaminie.

Przypadek 1: dla pewnego $i \in \mathbb{N}$ zbiór A_i jest pusty. Z warunku $\alpha \in \prod_{i\in\mathbb{N}} A_i$ łatwo wyprowadzić sprzeczność, gdyż $\alpha(i) \in A_i$ dla wszystkich I, także dla i takiego, że $A_i = \emptyset$. Wobec tego, zbiór $\prod_{i\in\mathbb{N}} A_i$ jest pusty, a więc skończony.

Przypadek 2: wszystkie zbiory A_i są niepuste. Zdefiniujmy zbiór I wzorem

$$I = \{i \in \mathbb{N} : |A_i| \geq 2\}.$$

Przypadek 2.1: $I = \emptyset$ W tym przypadku równość $|A_i| = 1$ zachodzi dla wszystkich $i \in \mathbb{N}$ i warunek

$$\alpha(i) \in A_i$$

definiuje funkcję α określoną w zbiorze liczb naturalnych $\mathbb{N}$. Przytoczoną definicję można też wyrazić nieco inaczej: $\alpha(i)$ jest tym (jedynym) elementem, który należy do A_i. To, że wszystkie zbiory A_i są jednoelementowe, gwarantuje, że wartości $\alpha(i)$ są dobrze zdefiniowane. Jeżeli zgodzimy się z tym, że funkcja α jest dobrzez zdefiniowana, to stwierdzenie, że $\alpha \in \prod_{i\in\mathbb{N}} A_i$ nie budzi wątliwości. Tak więc interesujący nas zbiór ma przynajmniej jeden element. Pokażemy jeszcze, że nie może mieć dwóch elementów.

Gdyby dwie (różne) funkcje α i β należały do uogólnionego iloczynu $\prod_{i\in\mathbb{N}} A_i$, to musiałyby się różnić dla pewnego argumentu. Przyjmijmy, że $\alpha(i_0) \neq \beta(i_0)$. Wtedy zbiór A_{i_0} musiałby mieć przynajmniej dwa elementy, właśnie $\alpha(i_0)$ oraz $\beta(i_0)$. Uzyskana sprzeczność dowodzi, że produkt $\prod_{i\in\mathbb{N}} A_i$ ma najwyżej jeden element. Ostatecznie otrzymujemy, że w rozważanym przypadku jest to zbiór jednoelementowy, a więc skończony.

Przypadek 2.2: zbiór I jest niepusty i skończony. Najpierw pokażemy, że na moc (liczbę elementów) produktu uogólnionego nie mają wpływu te zbiory A_i, które są jednoelementowe. Zauważmy, że uogólnione produkty

$$\prod_{i\in\mathbb{N}} A_i \text{ oraz } \prod_{i\in I} A_i$$

są równoliczne. Aby to wykazać, definiujemy funkcję

$$f : \prod_{i\in\mathbb{N}} A_i \to \prod_{i\in I} A_i$$

przyjmując, że

$$f(\alpha) = \alpha|I$$

($\alpha|I$ oznacza obcięcie funkcji α do zbioru I, czyli funkcję określoną na I i przyjmującą dla dowolnego argumentu te same wartości, co α), a następnie pokazujemy, że jest to bijekcja.

Tak więc, aby wykazać skończoność zbioru $\prod_{i\in\mathbb{N}} A_i$, wystarczy wykazać skończoność zbioru $\prod_{i\in I} A_i$. Ten zbiór składa się z funkcji $\alpha : I \to \bigcup_{i\in I} A_i$, a więc jest podzbiorem $\left(\bigcup_{i\in I} A_i\right)^I$. Ten ostatni zbiór jest skończony i wynika to ze znanych twierdzeń: suma skończonej rodziny zbiorów skończonych jest zbiorem skończonym, oraz stwierdzającego, że jest skończenie wiele funkcji określonych na ustalonym, skończonym zbiorze i przyjmujących wartości w ustalonym skończonym zbiorze.

Przypadek 2.3: zbiór I jest nieskończony. Ponieważ $I \subseteq \mathbb{N}$, więc istnieje bijekcja $f : I \to \mathbb{N}$. Posługując się f zdefiniujemy różnowartościową funkcję

$$F : \{0,1\}^{\mathbb{N}} \to \prod_{i\in\mathbb{N}} A_i.$$

Przyjmijmy, że

$$F(\alpha)(i) = \begin{cases} \min A_i & \text{jeżeli } \alpha(f(i)) = 0 \text{ oraz } i \in I \\ \max A_i & \text{jeżeli } \alpha(f(i)) = 1 \text{ oraz } i \in I \\ \min A_i & \text{jeżeli } i \notin I. \end{cases}$$

Jest oczywiste, że $F(\alpha) \in \prod_{i\in\mathbb{N}} A_i$ dla dowolnej funkcji $\alpha \in \{0,1\}^{\mathbb{N}}$. Aby dowieść różnowartościowość F, weźmy dwie różne funkcje $\alpha, \beta \in \{0,1\}^{\mathbb{N}}$. Przyjmijmy, że $\alpha(s) \neq \beta(s)$. Możemy dodatkowo założyć, że $\alpha(s) = 0$ i $\beta(s) = 1$. Korzystając z tego, że f jest bijekcją, bierzemy $t \in I$ takie, że $f(t) = s$. Z definicji F otrzymujemy, że $F(\alpha)(t) = \min A_t$ oraz $F(\beta)(t) = \max A_t$. Ponieważ $t \in I$, więc zbiór A_t ma przynajmniej dwa elementy. Tak więc $\min A_t < \max A_t$. Stąd wynika, że $F(\alpha)(t) < F(\beta)(t)$ oraz $F(\alpha) \neq F(\beta)$.

Zbiór $\{0, 1\}^{\mathbb{N}}$ ma moc continuum. Z istnienia różnowartościowej funkcji F wynika, że zbiór $\prod_{i\in\mathbb{N}} A_i$ ma moc nie mniejszą niż continuum. Łatwo też można dowieść, że jest mocy continuum.

Komentarz. Zadanie to pozostaje prawdziwe, jeżeli zamiast $\mathbb{N}$ weźmieny dowolny, niepusty zbiór indeksów X. Wtedy jednak nie będziemy wiedzieć o zbiorze I, że jest podzbiorem $\mathbb{N}$ i – w przypadku, gdy I jest nieskończony – będziemy musieli wykazać, że istnieje różnowartościowa funkcja $f : \mathbb{N} \to I$. Często to się robi w następujący sposób: wybiera się dowolny element $i_0 \in I$ i przyjmuje, że $f(0) = i_0$, a następnie definiuje $f(n)$ jako wybrany element zbioru $I \setminus \{f(0), \ldots, f(n-1)\}$ (nieskończoność I gwarantuje niepustość tej różnicy). Wiadomo jednak, że takie rozumowanie nie spełnia rygorystycznie rozumianych zasad logiki. Ale bywa też uznawane za poprawne. Podobne rozumowanie jest potrzebne w dowodzie równoważności dwóch definicji ciągłości funkcji w punkcie, podanych przez Cauchy'ego i Heinego. Proponuje obejrzeć dowód tej równoważności w podręcznikach do analizy matematycznej.

Dowody matematyczne muszą być skończone, dawać się w pełni zapisać i to bez używania trzech kropek ... Reguła dowodzenia nazywana regułą opuszczania kwantyfikatora egzystencjalnego pozwala wybrać jeden z wielu elementów, których istnienie jest zagwarantowane. Posługując się tą regułą możemy przytoczonym dowodzie zdefiniować $f(0)$, następnie $f(1)$, a nawet wartości funkcji f np. dla miliarda argumentów (w jakimś bardzo długim dowodzie), ale nie możemy tej reguły zastosować nieskończenie wiele razy. Przytoczony schemat definiowania funkcji f nie jest też poprawną definicją rekurencyjną (proszę starannie przeczytać sformułowanie twierdzenia o definiowaniu przez indukcję). Może jednak zostać wyprowadzony z aksjomatu wyboru: ten aksjomat m.in. pozwala nadać mu postać poprawnej definicji indukcyjnej. Aby dowiedzieć się coś więcej o aksjomacie wyboru, proponuję zajrzeć do książek poświęconych teorii mnogości.

Podobne kłopoty wystąpią w zadaniu 12, gdy opuścimy założenie, że A_i są zbiorami liczb naturalnych.

Uwaga. Proponowałbym, aby wzór

$$|\prod_{i=1}^{n} A_i| = \prod_{i=1}^{n} |A_i|$$

– słuszny dla skończonych zbiorów A_i – dowodzić przez indukcję, korzystając znanego wzoru $|A \times B| = |A| \cdot |B|$ (A i B to zbiory skończone, $|A|$ oznacza liczbę elementów zbioru A) i faktu: zbiory

$$\prod_{i=1}^{n} A_i \quad \text{oraz} \quad \left(\prod_{i=1}^{n-1} A_i\right) \times A_n$$

są równoliczne.

Zadanie 27. (a) Niech $\langle A, \leq \rangle$ będzie skończonym zbiorem częściowo uporządkowanym. Udowodnij, że jeśli A ma element najmniejszy, to $\langle A, \leq \rangle$ jest porządkiem zupełnym.

(b) Niech $\langle A, \leq \rangle$ będzie skończonym porządkiem zupełnym. Udowodnij, że jeśli funkcja $f : A \to A$ jest monotoniczna, to jest ciągła.

Rozwiązanie (część a). Na mocy założenia w zbiorze A jest element najmniejszy.

Należy jeszcze wykazać, że każdy skierowany podzbiór A ma kres górny. Najpierw wykażę pomocniczy fakt.

Fakt 18. W każdym skończonym, niepustym zbiorze skierowanym jest element największy.

Dowód. W dowodzie skorzystam z indukcji ze względu na liczbę elementów. Oczywiście, w zbiorze jednoelementowym jego jedyny element jest największym.

Załóżmy, że X jest skierowany i ma $n + 1$ elementów. W każdym niepustym i skończonym zbiorze uporządkowanym jest element minimalny. Przyjmijmy, że x_0 jest elementem minimalnym w X. Zbiór $X \setminus \{x_0\}$ ma n elementów i jest skierowany. Gdyby bowiem usunięcie x_0 spowodowało, że pewna para nie ma ograniczenia, to x_0 byłby niemniejszy od każdego elementu tej pary, i nie mógłby być elementem minimalnym.

Na mocy założenia indukcyjnego, zbiór $X \setminus \{x_0\}$ ma element największy. Niech to będzie element a. Ponieważ X jest zbiorem skierowanym, możemy z X wybrać element b taki, że $a \leq b$ oraz $x_0 \leq b$. Nietrudno zauważyć, że b jest elementem największym w X. Jest on większy od wszystkich elementów $X \setminus \{x_0\}$, ponieważ $a \leq b$ i oczywiście jest większy od jedynego elementu X spoza tego zbioru, czyli x_0.

Trzeba jeszcze zauważyć, że jeżeli w jakimś zbiorze X jest element największy a, to jest on kresem górnym zbioru X. Element a ogranicza zbiór X z góry, ponieważ jest największy. Jest on też mniejszy lub równy od każdego ograniczenia górnego zbioru X, ponieważ jest jednym z elementów zbioru X.

Rozwiązanie (część b). Przypuśćmy, że $f : A \to A$ jest funkcją monotoniczną. Należy wykazać, że f zachowuje kresy górne zbiorów skierowanych. Weźmy więc dowolny zbiór skierowany $X \subseteq A$ i niech m będzie jego kresem górnym. Zbiór X jest skończony, ponieważ A jest skończony. W takiej sytuacji, kres górny m jest również elementem największym w zbiorze X i, co najważniejsze, należy do X. Można to wywnioskować np. z jednoznaczności pojęcia kresu i tego, że element największy też jest kresem górnym.

Teraz powinniśmy dowieść, że $f(m)$ jest kresem górnym obrazu $\vec{f}(X)$. Element $f(m)$ jest ograniczeniem górnym obrazu. Dowolny element $\vec{f}(X)$ jest postaci $f(x)$ dla pewnego $x \in X$ i zachodzi $x \leq m$, gdyż m ogranicza zbiór X z góry. Stąd

$f(x) \leq f(m)$ na mocy założenia o monotoniczności funkcji f. Element $f(m)$ jest najmniejszym ograniczeniem górnym obrazu, ponieważ $f(m) \in \vec{f}(X)$ i jest również jednym z ograniczanych elementów.

Zadanie 28. W zbiorze *Fin* wszystkich skończonych podzbiorów zbioru liczb naturalnych określamy relację $\preceq$ w następujący sposób. Dla zbiorów $X, Y \in Fin$ zachodzi $X \preceq Y$ wtedy i tylko wtedy, gdy

$$X = Y \text{ lub } \max(X \div Y) \in Y,$$

gdzie $\div$ oznacza różnicę symetryczną, a $\max(A)$ jest największą w sensie naturalnego porządku liczbą w zbiorze A. Udowodnij, że $\langle Fin, \preceq \rangle$ jest dobrym porządkiem.

Rozwiązanie. Będziemy sprawdzać po kolei wszystkie warunki z definicji dobrego porządku.

Zwrotność. Ten warunek jest wynika z definicji porządku $\preceq$ w sposób oczywisty.

Zauważmy teraz dwa oczywiste fakty.

Fakt 19. Jeżeli X i Y są różnymi zbiorami, to warunki $n \in X$ i $n \in Y$ są równoważne dla wszystkich $n > \max(X \div Y)$.

Fakt 20. Jeżeli $\max(X \div Y) \in Y$, to $\max(X \div Y) \notin X$.

Słaba antysymetryczność. Dowód przeprowadzimy metodą nie wprost. Załóżmy, że mamy dwa zbiory X i Y takie, że $X \preceq Y$ i $Y \preceq X$, które – na mocy założenia dowodu nie wprost – są różne.

Ponieważ $X \neq Y$, więc nierówności między tymi zbiorami implikują, że $\max(X \div Y) \in Y$ oraz $\max(Y \div X) = \max(X \div Y) \in X$. Z drugiego faktu otrzymujemy, że $\max(X \div Y) \notin X$. Uzyskana w ten sposób sprzeczność dowodzi, że relacja $\preceq$ jest słabo antysymetryczna.

Przechodniość. Dość trudno podać ideę dowodu przechodniości relacji $\preceq$, ale jest widoczne podobieństwo tego porządku i porządku antyleksykograficznego. Jeżeli ograniczamy się np. do trzech zbiorów skończonych, to możemy je uważać za podzbiory zbioru liczb naturalnych mniejszych od pewnego $n \in \mathbb{N}$ i utożsamiać w zwykły sposób z ciągami zerojedynkowymi długości n. Przy takim utożsamianiu zbiorów i ciągów, porządek $\preceq$ odpowiada właśnie porządkowi antyleksykograficznemu w zbiorze ciągów. Dalej przechodniość udowodnimy być może w sposób mało intuicyjny, ale naśladujący dowód przechodniości dla porządku (anty)leksykograficznego.

Weźmy trzy zbiory X, Y i Z i załóżmy, że $X \preceq Y$ i $Y \preceq Z$. Symbol $X \prec Y$ będzie oznaczać, że $X \preceq Y$ i $X \neq Y$. Nietrudno zauważyć, że dowód przechodniości wystarczy przeprowadzić tylko dla zbiorów parami różnych. Możemy więc założyć, że $X \prec Y$ oraz $Y \prec Z$ i z tego założenia mamy wyprowadzić, że $X \preceq Z$.

Symbolem m oznaczamy $\max(X \div Y)$. Wiemy (na mocy przyjętych założeń), że $m \in Y$ i $m \notin X$.

Przypadek 1: $\max(Y \dot{-} Z) < m$. W tym przypadku, $\max(X \dot{-} Z) = m$. Wynika to z dwóch spostrzeżeń: Po pierwsze, dla $n > m$ warunki $n \in X$, $n \in Y$ oraz $n \in Z$ są jednocześnie albo prawdziwe, albo fałszywe. W szczególności, dla $n > m$ warunki $n \in X$ oraz $n \in Z$ są równoważne. Z drugiej strony, warunek $m \in X$ jest fałszywy, warunek $m \in Y$ jest prawdziwy i równoważny warunkowi $m \in Z$.

Jeżeli już dowiedliśmy równość $\max(X \dot{-} Z) = m$, to z powyższego rozumowania otrzymujemy jeszcze, że $\max(X \dot{-} Z) \in Z$. Tak więc $X \prec Z$ i, tym bardziej, $X \preceq Z$.

Przypadek 2: $\max(Y \dot{-} Z) = m$. Ta sytuacja prowadzi do sprzeczności i nie może zajść. Liczba $m = \max(Y \dot{-} Z)$ należy bowiem do Z, gdyż $Y \prec Z$. Z faktu 2 otrzymujemy, że $m \notin Y$. Ale m należy także do Y, ponieważ $X \prec Y$.

Przypadek 3: $\max(Y \dot{-} Z) > m$. W tym przypadku, dla $n > \max(Y \dot{-} Z)$ warunki $n \in X$, $n \in Y$ i $n \in Z$ mają tę samą wartość logiczną. Podobnie, warunki $\max(Y \dot{-} Z) \in X$ i $\max(Y \dot{-} Z) \in Y$ są równoważne. Co więcej, wobec nierówności $Y \prec Z$, są fałszywe. Wiemy też, że warunek $\max(Y \dot{-} Z) \in Z$ jest prawdziwy.

Z tych faktów otrzymujemy, że $\max(X \dot{-} Z) = \max(Y \dot{-} Z) \in Z$. Oznacza to, że zarówno $X \prec Z$, jak i $X \preceq Z$.

Liniowość. Aby dowieść liniowość porządku $\preceq$, wystarczy z założenia $X \neq Y$ wywnioskować, że albo $X \prec Y$, albo $Y \prec X$. Jest oczywiste, że jeżeli $X \neq Y$, to różnica symetryczna $X \dot{-} Y$ jest niepusta, liczba $\max(X \dot{-} Y)$ jest dobrze określona (pamiętajmy, że X i Y są skończone) oraz

$$\max(X \dot{-} Y) \in X \dot{-} Y = (X \setminus Y) \cup (Y \setminus X).$$

Stąd wynika, że $\max(X \dot{-} Y) \in X$ (i wtedy $Y \prec X$) lub też $\max(X \dot{-} Y) \in Y$ (czyli $X \prec Y$).

Regularność. Aby dowieść regularność porządku $\prec$, trzeba najpierw zauważyć

Fakt 21. Jeżeli $X \preceq Y$, to $X \subseteq \{i \in \mathbb{N} : i \leq \max(Y)\}$.

Dowód. Zauważmy, że liczba $\max(X \dot{-} Y) \in Y$ i jest mniejsza od $\max(Y)$. Elementy zbioru X dzielą na mniejsze lub równe $\max(X \dot{-} Y)$ i, z tego powodu, mniejsze od $\max(Y)$ oraz na większe od $\max(X \dot{-} Y)$. Te większe – na mocy pierwszego faktu – należą do Y i dlatego nie przekraczają $\max(Y)$.

Załóżmy, że relacja $\preceq$ nie jest regularna. Istnieje więc nieskończony, zstępujący ciąg zbiorów $X_i \in \mathit{Fin}$. Ten ciąg spełnia więc nierówności

$$X_{n+1} \prec X_n$$

dla wszystkich $n \in \mathbb{N}$. Z przechodniości porządku $\prec$ otrzymujemy, że

$$X_n \prec X_m$$

dla wszystkich liczb liczb spełniających nierówność $n > m$. Stąd wynika, że funkcja $f : \mathbb{N} \to Fin$ zdefiniowana wzorem $f(n) = X_n$ jest różnowartościowa. Z nierówności $X_n \prec X_0$ i trzeciego faktu wynika też, że

$$X_n \subseteq [0, \max X_0] = \{i \in \mathbb{N} : i \leq \max X_0\}.$$

Wobec tego, zbiór $[0, \max X_0]$ jest skończony i ma nieskończenie wiele podzbiorów. Jest to niemożliwe, a uzyskana sprzeczność dowodzi regularności $\preceq$.

Zadanie 29. Jeśli φ jest formułą rachunku zdań, to przez $V(\varphi)$ oznaczamy zbiór zmiennych zdaniowych występujących w φ. Niech $\varphi, \varphi_1, \ldots, \varphi_n, \psi$ będą formułami rachunku zdań.

(a) Udowodnij, że $(\bigvee_{i=1}^{n} \varphi_i) \to \psi$ jest tautologią wtedy i tylko wtedy, gdy $\varphi_i \to \psi$ są tautologiami dla wszystkich $i \in \{1, \ldots, n\}$.

(b) Niech p będzie zmienną zdaniową nie występującą w φ ani w ψ. Udowodnij, że $\varphi \wedge p \to \psi$ jest tautologią wtedy i tylko wtedy, gdy $\varphi \to \psi$ jest tautologią.

(c) Udowodnij, że jeśli $\varphi \to \psi$ jest tautologią, to istnieje taka formuła rachunku zdań ρ, że $V(\rho) = V(\varphi) \cap V(\psi)$ oraz $\varphi \to \rho$ i $\rho \to \psi$ są tautologiami.

Rozwiązanie zadania 29 (a). Nietrudno zauważyć, że to zadanie wystarczy rozwiązać dla $n = 2$. Oczywiście, także to spostrzeżenie wymaga jakiegoś uzasadnienia. Zacznijmy od rozwiązania w tym prostym przypadku.

1. Jest wiele metod rozwiązywania tego zadania. Możemy np. zauważyć, że formuła

$$((\varphi_1 \vee \varphi_2) \to \psi) \longleftrightarrow ((\varphi_1 \to \psi) \wedge (\varphi_2 \to \psi))$$

jest tautologią. Fakt ten można sprawdzić metodą zerojedynkową (choć nie polecałbym tej metody). Jeżeli równoważność jest tautologią, to oczywiście lewa strona tej równoważności jest tautologią wtedy i tylko wtedy, gdy prawa jest tautologią.

2. Można też bezpośrednio dowieść implikacje w obie strony. Na przykład załóżmy, że formuły $\varphi_1 \to \psi$ oraz $\varphi_2 \to \psi$ są tautologiami. Spróbujemy dowieść, że także formuła φ

$$(\varphi_1 \vee \varphi_2) \to \psi$$

jest tautologią. W tym celu bierzemy dowolne wartościowanie zmiennych zdaniowych σ i staramy się wyliczyć wartość logiczną $\hat{\sigma}((\varphi_1 \vee \varphi_2) \to \psi)$. Możemy założyć, że $\hat{\sigma}(\varphi_1 \vee \varphi_2) = \top$ (w przeciwnym razie, cała implikacja miałaby przy wartościowaniu σ wartość logiczną $\top$). Tak więc jeden z członów alternatywy ma przy wartościowaniu σ wartość logiczną $\top$. Przyjmijmy, że $\hat{\sigma}(\varphi_1) = \top$. Założyliśmy jednak, że $\varphi_1 \to \psi$ jest tautologią, a więc $\hat{\sigma}(\varphi_1 \to \psi) = \top$. Stąd otrzymujemy, że $\hat{\sigma}(\psi) = \top$ oraz każda implikacja o następniku ψ (także φ) ma przy wartościowaniu σ wartość logiczną $\top$.

Dowiedliśmy, że formuła φ ma wartość logiczną $\top$ przy każdym wartościowaniu. Tak więc jest to tautologia.

3. Implikację odwrotną można dowieść przedstawionymi metodami i proponuję zrobić to jako ćwiczenie. Teraz przedstawię pewien argument świadczący o prawdziwości tej implikacji (można uważać go za mało zrozumiały dowód). Zauważmy, że można uzasadnić każdą formułę o następującym schemacie

$$((\varphi_1 \vee \varphi_2) \to \psi) \to (\varphi_1 \to \psi).$$

Tak jest, ponieważ z każdego członu potrafimy wywnioskować alternatywę. Jeżeli więc z alternatywy potrafimy wywnioskować ψ, to tę formułę potrafimy wywnioskować także dowolnego członu tej alternatywy.

4. Słuszność równoważności z zadania w pełnej ogólności łatwo dowodzi się przez indukcję ze względu na n. Jest oczywiste, że równoważność zachodzi dla $n = 1$. Wtedy obie strony równoważności mówią to samo. Aby przeprowadzić drugi krok dowodu indukcyjnego wystarczy zauważyć, że następujące stwierdzenia są równoważne

(a) $(\bigvee_{i=1}^{n+1} \varphi_i) \to \psi$ jest tautologią,

(b) $(\bigvee_{i=1}^{n} \varphi_i) \to \psi$ oraz $\varphi_{n+1} \to \psi$ są tautologiami,

(c) formuły $\varphi_i \to \psi$ są tautologiami dla wszystkich i takich, że $1 \leq i \leq n+1$.

Równoważność warunków (a) i (b) wynika np. z punktu 1, a warunków (b) i (c) — z założenia dowodu indukcyjnego.

Rozwiązanie zadania 29 (b). To zadanie jest bardzo podobne do poprzedniego, ale tym razem nie da się zastosować metody z punktu 1. Formuły

$$(\varphi \to \psi) \longleftrightarrow ((\varphi \wedge p) \to \psi)$$

nie są bowiem tautologiami. Jednak otrzymujemy tautologię, jeżeli znak $\longleftrightarrow$ zastąpimy przez $\to$. Tylko jedną z implikacji z zadania 29 (b) można dowieść metodami z zadania 29 (a). Dalej przedstawię tylko dowód implikacji odwrotnej.

5. Załóżmy więc, że formuła $(\varphi \wedge p) \to \psi$ jest tautogią. Pokażę, że tautologią jest też formuła $\varphi \to \psi$. Zrobię to w zwykły sposób. Wezmę dowolne wartościowanie zmiennych zdaniowych σ takie, że $\hat{\sigma}(\varphi) = \top$ i pokażę, że $\hat{\sigma}(\psi) = \top$.

Mając takie wartościowanie σ tworzę inne wartościowanie δ. Wartościowanie to dla wszystkich zmiennych z wyjątkiem p przyjmuje takie same wartości, jak σ. Ponadto przyjmujemy, że $\delta(p) = \top$ (zmieniłem więc wartościowanie σ dla jednej ze zmiennych lub dodatkowo zdefiniowałem je dla nowej zmiennej). Definicję tę można też zapisać w następującej postaci

$$\delta(x) = \begin{cases} \sigma(x) & \text{jeżeli } x \neq p \\ \top & \text{jeżeli } x = p. \end{cases}$$

Istotne jest to, że formuły takie jak φ i ψ, a więc formuły, w których nie występuje zmienna p, mają te same wartości dla obu wartościowań. Mamy więc

$$\hat{\sigma}(\varphi) = \hat{\delta}(\varphi) \text{ oraz } \hat{\sigma}(\psi) = \hat{\delta}(\psi).$$

Jeżeli ktoś w to nie wierzy, to powinien dowieść przytoczoną własność przez tzw. indukcję ze względu na budowę formuły.

Dalszy dowód jest już prosty. Założyliśmy, że formuła φ jest spełniona przy wartościowaniu σ. Jest więc też spełniona przy wartościowaniu δ. Także formuła $(\varphi \wedge p) \to \psi$ jest spełniona przy wartościowaniu δ (ponieważ jest to tautologia). Stąd otrzymujemy, że $\hat{\sigma}(\psi) = \hat{\delta}(\psi) = \top$.

Rozwiązanie zadania 29 (c). To zadanie jest dość trudne. Punkty (a) i (b) można jednak uważać za wskazówkę. Fakt z tego zadania jest prostą wersją tzw. lematu Craiga. Będziemy go dowodzić stopniowo, dla coraz bardziej skomplikowanych formuł φ.

6. Najpierw lemat Craiga udowodnimy dla formuł φ, które są koniunkcjami zmiennych zdaniowych i negacji zmiennych zdaniowych. Dodatkowo będziemy zakładać o tych koniunkcjach, że żadna zmienna nie występuje w nich dwukrotnie, a więc nie są postaci $p \wedge p \wedge \ldots$ lub $p \wedge \neg p \wedge \ldots$. Dowód zostanie przeprowadzony przez indukcję ze względu na liczbę elementów zbioru $V(\varphi) \setminus V(\psi)$.

Jeżeli zbiór $V(\varphi) \setminus V(\psi)$ ma zero elementów (czyli jest pusty), to możemy przyjąć, że $\rho = \varphi$. W tym przypadku wszystkie wymagane własności ρ są oczywiste: $V(\rho) = V(\varphi) = V(\varphi) \cap V(\psi)$, gdyż w rozważanym przypadku $V(\varphi) \subseteq V(\psi)$, formuła $\rho \to \psi$ jest tautologią na mocy założenia, a formuła $\varphi \to \rho$ jest tautologią, ponieważ jest to formuła $\varphi \to \varphi$, która oczywiście jest tautologią.

Jeżeli zbiór $V(\varphi) \setminus V(\psi)$ jest niepusty, to wybieramy z niego dowolną zmienną p i przedstawiamy formułę φ w postaci $\varphi' \wedge p$ lub $\varphi' \wedge \neg p$. Na mocy dodatkowego założenia, w formule φ' nie występuje już zmienna p. Dalszy dowód w obu przypadkach jest taki sam. Zauważmy, że na mocy zadania 29 (b) formuła $\varphi' \to \psi$ jest tautologią. Dla drugiej formuły korzystamy z oczywistego uogólnienia zadania 29 (b).

W tej sytuacji możemy skorzystać z założenia indukcyjnego dla φ'. Pozwala to znaleźć formułę ρ taką, że

$$V(\rho) = V(\varphi') \cap V(\psi) \text{ oraz } \varphi' \to \rho \text{ i } \rho \to \psi \text{ są tautologiami.}$$

Nietrudno zauważyć formuła ρ ma też własności wymagane w lemacie Craiga dla formuły φ. Mamy bowiem

$$V(\varphi) \cap V(\psi) = (V(\varphi') \cup \{p\}) \cap V(\psi) = V(\varphi') \cap V(\psi) \cup \{p\} \cap V(\psi) = V(\varphi') \cap V(\psi) = V(\rho)$$

(przedostatnia równość wynika stąd, że $p \notin V(\psi)$). Ponadto, $\varphi \to \rho$ jest tautologią, ponieważ tautologiami są $\varphi \to \varphi'$ oraz $\varphi' \to \rho$.

7. Teraz pokażemy, że jeżeli lemat Craiga jest prawdziwy dla pewnych formuł φ_1 i φ_2, to jest też prawdziwy dla alternatywy $\varphi_1 \vee \varphi_2$.

Przypuśćmy więc, że $(\varphi_1 \vee \varphi_2) \to \psi$ jest tautologią oraz istnieją formuły ρ_1 i ρ_2 takie, że

$$V(\rho_1) = V(\varphi_1) \cap V(\psi) \text{ oraz } \varphi_1 \to \rho_1 \text{ i } \rho_1 \to \psi \text{ są tautologiami.}$$

oraz

$$V(\rho_2) = V(\varphi_2) \cap V(\psi) \text{ oraz } \varphi_2 \to \rho_2 \text{ i } \rho_2 \to \psi \text{ są tautologiami.}$$

Wtedy formuła $\rho_1 \vee \rho_2$ spełnia tezę lematu Craiga dla $\varphi_1 \vee \varphi_2$. Formuła $(\rho_1 \vee \rho_2) \to \psi$ jest tautologią na mocy zadania 29 (a). Ponieważ formuły $\varphi_1 \to \rho_1$ oraz $\rho_1 \to (\rho_1 \vee \rho_2)$ są tautologiami, więc to samo można powiedzieć o $\varphi_1 \to (\rho_1 \vee \rho_2)$. W tych samych powodów tautologią jest $\varphi_2 \to (\rho_1 \vee \rho_2)$. Jeżeli teraz skorzystamy z zadania 29 (a), to otrzymamy, że tautologią jest także $(\varphi_1 \vee \varphi_2) \to (\rho_1 \vee \rho_2)$. Pozostaje jeszcze wyliczyć $V(\varphi_1 \vee \varphi_2)$. Oczywiście zachodzą następujące równości:

$$V(\varphi_1 \vee \varphi_2) \cap V(\psi) = V(\varphi_1) \cap V(\psi) \cup V(\varphi_2) \cap V(\psi) = V(\rho_1) \cup V(\rho_2) = V(\rho_1 \vee \rho_2).$$

8. Z udowodnionych wyżej faktów, stosując bardzo łatwą indukcję, możemy wyprodzić lemat Craiga dla wszystkich formuł φ, które są dane w alternatynej (dysjunkcyjnej) postaci normalnej (a więc są alternatywami, a każdy z (być może wielu) członów tej alternatywy jest koniunkcją zmiennych zdaniowych i negacji zmiennych zdaniowych). Ponadto, dysjunkty takich formuł powinny spełniać dodatkowy warunek: żadna zmienna nie może wystąpić w nich dwukrotnie.

Dowód lematu Craiga w całej okazałości wymaga jeszcze powołania się na dwa fakty. Po pierwsze trzeba wiedzieć, że dowolna formuła φ jest równoważna formule w alternatywnej postaci normalnej. Co więcej, można żądać od takiej postaci normalnej, aby spełniała wspomniany dodatkowy warunek oraz występowały w niej dokładnie te zmienne, co w φ. Po drugie, jeżeli lemat Craiga jest prawdziwy dla formuły φ, to jest prawdziwy także dla każdej formuły równoważnej z φ, która jest zapisana za pomocą tych samych zmiennych, co φ.

9. Przedstawione uzasadnienie lematu Craiga zawiera drobną usterkę. Dobrym ćwiczeniem byłoby przerwanie w tej chwili czytania dalszej części tego tekstu i podjęcie próby samodzielnego znalezienia tej usterki. Takie usterki często prowadzą do fałszywych wniosków. Tym razem usterka wskazuje tylko na pewne trudności. Podczas egzaminu jedna osoba zwróciła na to uwagę i twierdziła nie do końca słusznie, że lemat Craiga jest fałszywy.

To, czy zadanie 29 (c) jest prawdziwe, zależy od szczegółów z definicji formuły. W „Materiałach do zajęć" przyjmuje się, że formułami są też symbole $\top$ i $\bot$. Klasyczne definicje formuły jednak nie zawierają tego warunku. W mojej ocenie częściej przyjmuje się, że to nie są formuły.

W pewnym miejscu przedstawionego rozumowania, rozważaliśmy m.in. koniunkcję φ (jednej lub więcej) zmiennych, w której jest zmienna p, i stwierdziliśmy, że ta koniunkcja daje się przedstawić w postaci $\varphi' \wedge p$. Powinniśmy rozważać także sytuację, w której $\varphi = p$. Formuły p nie da się tak przedstawić, chyba że symbol φ' może oznaczać $\top$. Jeżeli $\top$ nie jest formułą, to lemat Craiga wymaga ostrożniejszego sformułowania.

10. Przedstawię jeszcze inny dowód lematu Craiga, który wydaje się nieco prostszy. Będziemy się w nim posługiwać pojęciem wartościowania. Aby określić wartość formuły φ dla wartościowania σ musimy założyć, że σ jest określone dla zmiennych występujących w φ. Poza tym, dziedzina σ nie odgrywa zwykle większej roli. W przedstawianym dowodzie będziemy musieli jednak kontrolować dziedziny wartościowań.

Niech φ i ψ spełniają warunki podane w sformułowaniu zadania 29 (c). Przyjmijmy, że X oznacza zbiór

$$\{\sigma : V(\varphi) \cap V(\psi) \to \{\bot, \top\} : \exists \sigma' : V(\varphi) \to \{\bot, \top\} \ \ \sigma'(\varphi) = \top \wedge \sigma \subseteq \sigma'\}$$

(napis $\sigma \subseteq \sigma'$ oznacza, że σ' jest rozszerzeniem σ, albo σ jest obcięciem σ', czyli spełnia równość $\sigma(p) = \sigma'(p)$ dla wszystkich $p \in V(\varphi) \cap V(\psi)$).

Mając zbiór X konstruujemy formułę ρ, w której występują wszystkie zmienne ze zbioru $V(\varphi) \cap V(\psi)$ i żadne inne, oraz dla dowolnego wartościowania $\sigma : V(\varphi) \cap V(\psi) \to \{\bot, \top\}$ zachodzi równoważność

$$\hat{\sigma}(\rho) = \top \iff \sigma \in X.$$

Metoda konstrukcji takiej formuły jest znana np. z dowodu twierdzenia o istnieniu alternatywnych postaci normalnych. Proszę zwrócić uwagę, że drobne kłopoty pojawiają się, gdy zbiór $V(\varphi) \cap V(\psi)$ jest pusty.

Pokażemy, że formuła ρ ma żądane własności. W dowodzie wielokrotnie będziemy korzystać z oczywistego faktu: jeżeli mamy dwa wartościowania σ, σ' zmiennych występujących w formule φ spełniające warunek $\sigma \subseteq \sigma'$, to $\sigma(\varphi) = \sigma'(\varphi)$.

Najpierw pokażemy, że $\varphi \to \rho$ jest tautologią. Weźmy więc dowolne wartościowanie σ' zmiennych z $V(\varphi)$ (tylko takie zmienne występują w tej implikacji). Możemy dodatkowo założyć, że $\hat{\sigma}'(\varphi) = \top$. Pokażemy, że $\hat{\sigma}'(\psi) = \top$. Niech σ będzie obcięciem wartościowania σ' do zmiennych ze zbioru $V(\varphi) \cap V(\psi)$. Oczywiście, $\sigma \in X$. Z definicji ρ otrzymujemy, że $\hat{\sigma}(\rho) = \top$. W końcu, ze przytoczonego faktu o wartościowaniach wnioskujemy, że $\hat{\sigma}'(\rho) = \top$.

Tę samą metodę wykorzystamy do pokania, że implikacja $\rho \to \psi$ jest tautologią. Niech ν będzie wartościowaniem zmiennych występujących w $\rho \to \psi$ takim, że $\hat{\nu}(\rho) = \top$. Dziedziną ν jest zbiór $V(\psi)$. Jeżeli obetniemy ν do zmiennych ze zbioru $V(\varphi) \cap V(\psi)$, to otrzymamy wartościowanie, które będziemy oznaczać symbolem σ.

Oczywiście, $\hat{\sigma}(\rho) = \top$ oraz $\sigma \in X$. Wartościowanie σ można rozszerzyć do wartościowania σ' spełniającego formułę φ. Wartościowania σ' i ν przypisują te same wartości zmiennym ze zbioru $V(\varphi) \cap V(\psi)$. Można więc je rozszerzyć do wartościowania ν' przypisującemu wartości wszystkim zmiennym ze zbioru $V(\varphi) \cup V(\psi)$. Dla tego wartościowania jest spełniona formuła φ, ponieważ ν' jest rozszerzeniem σ'. Spełniona jest także formuła ψ, ponieważ formuła $\varphi \to \psi$ jest tautologią. Oznacza to, że zachodzi także równość $\hat{\nu}(\psi) = \top$, gdyż ν' jest rozszerzeniem ν. Dowiedliśmy więc, że wszystkie wartościowania spełniające ρ spełniają także ψ. Stąd wynika, że $\rho \to \psi$ jest tautologią.

Zadanie 30. Rozważmy zbiór $\mathbb{N}^{\mathbb{N}}$ wszystkich funkcji z $\mathbb{N}$ w $\mathbb{N}$. Dla danej funkcji f niech $R_f = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N} \;\; f(m) = n\}$ oznacza zbiór wartości przyjmowanych przez tę funkcję. W $\mathbb{N}^{\mathbb{N}}$ definiujemy relację $\sim$ wzorem

$$f \sim g \overset{\text{df}}{\Leftrightarrow} R_f = R_g.$$

Oczywiście $\sim$ jest relacją równoważności.

(a) Udowodnij, że każda klasa abstrakcji relacji $\sim$ jest albo jednoelementowa, albo ma moc continuum.

(b) Udowodnij, że zbiór ilorazowy (czyli zbiór wszystkich klas abstrakcji) relacji $\sim$ ma moc continuum.

(c) Podaj przykład podziału zbioru $\mathbb{N}^{\mathbb{N}}$ na continuum rozłącznych zbiorów mocy continuum.

Rozwiązanie zadania 30 (a). Zbiory wartości funkcji określonych na niepustym zbiorze są niepuste. Tak więc wszystkie rozważane w tym zadaniu zbiory R_f są niepuste. Zbiory te są więc albo jednoelementowe, albo mają przynajmniej dwa elementy.

Niech $f : \mathbb{N} \to \mathbb{N}$ będzie funkcją taką, że zbiór jej wartości R_f ma dokładnie jeden element i $a \in R_f$. Funkcja f jest ściśle określona. Jej dziedzina jest ustalona, a jej wartością może by tylko a. Jest więc to funkcja stale równa a.

Jeżeli g jest funkcją taką, że $g \sim f$, to g ma ten sam zbiór wartości, co f. Też jest stale równa a, czyli jest identyczna z f. Stąd wynika, że klasa abstrakcji $[f]_\sim$ (relacji $\sim$ wyznaczona przez f) ma dokładnie jeden element.

Teraz zajmiemy się funkcjami f, które przyjmują przynajmniej dwie wartości, w tym wartości a i b ($a \neq b$). Oczywiście, $a, b \in R_f$. Posługując się twierdzeniem Cantora-Bernsteina pokażemy, że klasa abstrakcji $[f]_\sim$ ma moc continuum. Oczywiście, klasa ta jest zawarta w zbiorze wszystkich funkcji określonych i przyjmujących wartości w zbiorze N. Takich funkcji jest continuum. Wystarczy jeszcze pokazać, że klasa $[f]_\sim$ ma moc przynajmniej continuum. W tym celu zdefiniujemy różnowartościową funkcję

$$\varphi : \{a, b\}^N \to [f]_\sim.$$

Przyjmijmy, że $g : N \to \{a, b\}$ i wartość $\varphi(g)$ jest funkcją definiowana wzorem

$$\varphi(g)(n) = \begin{cases} f(\frac{n-1}{2}) & \text{jeżeli } n \text{ jest nieparzyste,} \\ g(\frac{n}{2}) & \text{w przeciwnym razie.} \end{cases}$$

Najpierw przekonajmy się, że $\varphi(g) \sim f$. Wyliczmy więc zbiór $R_{\varphi(g)}$ wartości funkcji $\varphi(g)$. Funkcja ta przyjmuje w na zbiorze liczb nieparzystych wszystkie wartości, które przyjmuje funkcja f. Dodatkowo, na zbiorze liczb parzystych przyjmuje wartości a lub b. Tak więc

$$R_f \subseteq R_{\varphi(g)} \subseteq R_f \cup \{a, b\} = R_f.$$

W ten sposób otrzymujemy, że $R_{\varphi(g)} = R_f$, a to oznacza, że $\varphi(g) \sim f$ i ponadto

$$\varphi : \{a, b\}^N \to [f]_\sim.$$

Powinniśmy jeszcze przekonać się, że funkcja φ jest różnowartościowa. Jest to bardzo proste: jeżeli mamy dwa różne argumenty funkcji φ, czyli różne funkcje g_1 i g_2, to różnią się one wartościami dla pewnego argumentu, powiedzmy dla liczby $k \in \mathbb{N}$. Wtedy (będące funkcjami) wartości $\varphi(g_1)$ i $\varphi(g_2)$ różnią się dla argumentu $2 \cdot k$.

Rozwiązanie zadania 30 (b). Jest to bardzo proste zadanie. Aby je rozwiązać wystarczy powołać się na dwa lub trzy oczywiste fakty.

Pierwszy z nich dotyczy relacji równoważności. Jeżeli mamy funkcję $r : X \to Y$ i w zbiorze X definiujemy relację równoważności $\sim$ przyjmując, że

$$x \sim y \iff r(x) = r(y).$$

to zbiór klas abstrakcji $X/_\sim$ tej relacji jest równoliczny ze zbiorem $r(X)$ wartości funkcji r na zbiorze X. Odpowiednią bijekcję łatwo wskazać. Jest nią funkcja $\rho : X/_\sim \to r(X)$ zdefiniowana wzorem

$$\rho([x]_\sim) = r(x).$$

Dalej wystarczy sprawdzić wszystkie wymagane własności ρ, w tym poprawność definicji ρ. Robi się to w sposób standardowy.

Z przytoczonego faktu zastosowanego do relacji $\sim$ z zadania 30 wynika, że zbiór klas abstrakcji tej relacji jest równoliczny ze zbiorem niepustych podzbiorów zbioru liczb naturalnych. Gdyby ktoś czuł potrzebę uzasadnienia czegoś w tym miejscu, to powinien podać konstrukcję funkcji, której zbiór wartości jest danym niepustym zbiorem. Na przykład, jeżeli $a \in A \subseteq \mathbb{N}$, to funkcja f taka, że

$$f(n) = \begin{cases} n & \text{jeżeli } n \in A, \\ a & \text{w przeciwnym razie} \end{cases}$$

spełnia równość $R_f = A$.

W końcu trzeba zauważyć, że zbiór niepustych podzbiorów $\mathbb{N}$ różni się od zbioru $\mathcal{P}(\mathbb{N})$ wszystkich podzbiorów $\mathbb{N}$ jednym elementem. Ten drugi zbiór jest mocy continuum, a więc oba są mocy continuum. Fakt ten wynika z teorii mocy. Można się o tym przekonać np. sprawdzając, że zbiory $\mathcal{P}(N)$, $\mathcal{P}(N\setminus\{0\})$ oraz $\{X \subseteq N : 0 \in X\}$ są równoliczne. Ponieważ zachodzą oczywiste zawierania

$$\{X \subseteq N : 0 \in X\} \subseteq \{X \subseteq N : X \neq \emptyset\} \subseteq \mathcal{P}(N),$$

więc z twierdzenia Cantora-Bernsteina otrzymujemy, że zbiór $\{X \subseteq N : X \neq \emptyset\}$ ma moc continuum.

Rozwiązanie zadania 30 (c). Każda relacja równoważności definiuje podział swojej dziedziny. Także relacja $\sim$ definiuje podział zbioru $\mathbb{N}^{\mathbb{N}}$. Z punktu (b) wynika, że jest to podział na continuum zbiorów, ale niektóre z nich (na mocy punktu (a)) nie mają mocy continuum. Jedna z metod rozwiązania zadania (c) polega na poprawieniu podziału wyznaczonego przez relację $\sim$ tak, aby spełniał warunki zadania. Można to zrobić dołączając małe klasy abstrakcji do dużej.

Niech $S \in \mathbb{N}^{\mathbb{N}}$ oznacza jakąkolwiek funkcję, która nie jest stała, a C_i – funkcję stale równą i (oczywiście, rozważamy tylko funkcje należące do $\mathbb{N}^{\mathbb{N}}$). Utwórzmy sumę

$$U = [S]_\sim \cup \bigcup_{i=0}^{\infty} [C_i]_\sim.$$

Jest to suma wszystkich jednoelementowych klas abstrakcji relacji $\sim$ i jednej klasy mocy continuum. Oczywiście, jest to zbiór mocy continuum, gdyż jest zawarty w zbiorze $\mathbb{N}^{\mathbb{N}}$ i zawiera zbiór $[S]_\sim$ mocy continuum. Jeżeli do tego zbioru dołączymy pozostałe klasy abstrakcji, nie wyznacone ani przez funkcje stałe, ani przez S, to otrzymamy podział

$$\mathcal{P} = \{U\} \cup \{[f]_\sim : f \neq S \wedge f \text{ nie jest stała}\}$$

zbioru $\mathbb{N}^{\mathbb{N}}$ na zbiory mocy continuum. Można mieć wątpliwości, czy w ten sposób otrzymaliśmy podział mocy continuum.

Zdefiniowany podział ma jednak moc continuum. Aby to uzasadnić, można skorzystać z ogólnego i niebanalnego twierdzenia, że odejmując od zbioru mocy continuum zbiór przeliczalny otrzymujemy zbiór mocy continuum. Dobierając odpowiednio S można to też uzasadnić w sposób elementarny: jest continuum podzbiorów zbioru $\mathbb{N} \setminus \{0, 1\}$. Jest więc continuum podzbiorów $\mathbb{N}$, do których należą liczby 0 i 1. W końcu jest continuum klas abstrakcji relacji $\sim$ wyznaczonych przez funkcje przyjmujące wartości 0 i 1, czyli należących do zbioru

$$\{[f]_\sim : 0, 1 \in R_f\}.$$

Co więcej, nie ma wśród tych klas abstrakcji klas wyznaczonych przez funkcje stałe (ich wartościami jest najwyżej jedna z liczb 0 i 1) oraz przez funkcję S zdefiniowaną wzorem $S(n) = n + 1$ (nie przyjmuje wartości 0). Tak więc

$$\{[f]_\sim : 0, 1 \in R_f\} \subseteq \{[f]_\sim : f \neq S \wedge f \text{ nie jest stała}\} \subseteq \mathcal{P}.$$

Stąd podział $\mathcal{P}$ ma continuum elementów.

Zadanie 30 (c) można też rozwiązać inną metodą. Każde dwa zbiory mocy continuum są równoliczne. W szczególności, zbiór X mocy continuum jest równoliczny z X^2, także ze zbiorem $\mathbb{R}^2$ i z płaszczyzną geometryczną (utożsamianą z $\mathbb{R}^2$). Otóż płaszczyznę bardzo łatwo podzielić na continuum zbiórów mocy continuum. Wystraczy podzielić ja na proste równoległe np. do osi OX. Ponieważ także zbiór X można utożsamiać z płaszczyzną, też można go tak podzielić.

Przedstawię to rozwiązanie jeszcze nieco dokładniej. Weźmy więc zbiór X mocy continuum i bijekcję $f : X \to X^2$. Rodzina zbiorów

$$\{\{(x, y) \in X^2 : y \in X\} : x \in X\}$$

jest podziałem zbioru X^2. Każdy element tego podział jest równoliczny ze zbiorem X. Także cały ten podział jest równoliczny z X. Nietrudno sprawdzić, że rodzina przeciwobrazów

$$\{f^{-1}(\{(x, y) \in X^2 : y \in X\}) : x \in X\}$$

jest podziałem zbioru X i ma oczekiwane własności. Aby rozwiązać zadanie 30 (c), przedstawione rozumowanie trzeba przeprowadzić dla zbioru $X = \mathbb{N}^{\mathbb{N}}$.

Zadanie 31. Niech A będzie dowolnym zbiorem. *Multizbiorem* nad A nazywamy dowolną funkcję $S : A \to \mathbb{N}$ (mówimy wtedy, że $S(x)$ jest liczbą wystąpień elementu x w multizbiorze S). Rodzinę wszystkich multizbiorów nad A oznaczamy $\mathcal{M}(A)$. Jeśli S_1 i S_2 są multizbiorami, to ich przekrój $S_1 \cap S_2$, sumę $S_1 \cup S_2$ i różnicę $S_1 \setminus S_2$ definiujemy wzorami

$$\begin{aligned} (S_1 \cap S_2)(x) &= \min(S_1(x), S_2(x)) \\ (S_1 \cup S_2)(x) &= S_1(x) + S_2(x) \\ (S_1 \setminus S_2)(x) &= \max(S_1(x) - S_2(x), 0). \end{aligned}$$

Mówimy, że S_1 jest podzbiorem S_2 i piszemy $S_1 \subseteq S_2$, jeśli istnieje taki multizbiór X, że $S_1 \cup X = S_2$.

(a) Czy dla dowolnych multizbiorów X, Y, Z nad zbiorem A zachodzi równość

$$X \setminus (Y \cup Z) = (X \setminus Y) \setminus Z \ ?$$

(b) Czy dla dowolnych multizbiorów X, Y, Z nad zbiorem A zachodzi równość

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \ ?$$

(c) Czy $\langle \mathcal{M}(A), \subseteq \rangle$ jest porządkiem? Czy jest to porządek zupełny?

Wszystkie odpowiedzi należy uzasadnić.

Rozwiązanie zadania 31 Pozornie wydaje się, że to zadanie dotyczy zbiorów i można je rozwiązać podobnie, jak zadania z rachunku zbiorów. Nic bardziej mylnego. W zadaniach 31 (a) i (b) mamy dowieść równość dwóch funkcji. I trzeba to zrobić tak, jak dowodzi się równość funkcji. Funkcje występujące w tym zadaniu mają tę samą dziedzinę. Trzeba więc rozstrzygać tylko, czy interesujące nas funkcje dla dowolnego argumentu przyjmują te same wartości.

Równość

$$X \setminus (Y \setminus Z) = (X \setminus Y) \setminus Z$$

zachodzi wtedy i tylko wtedy, gdy dla dowolnego $a \in A$ zachodzi równość

$$(X \setminus (Y \setminus Z))(a) = ((X \setminus Y) \setminus Z)(a).$$

Ta ostatnia równość jest na mocy definicji równoważna warunkowi

$$\max(X(a) - \max(Y(a) - Z(a), 0), 0) = \max(\max(X(a) - Y(a), 0) - Z(a), 0).$$

Po odpowiednich podstawieniach z tej ostatniej równości otrzymujemy

$$\max(x - \max(y - z, 0), 0) = \max(\max(x - y, 0) - z, 0).$$

Ta równość jest prawdziwa bez względu na wartości x, y i z. Pomijam jej dowód. Wynika z niej prawdziwość równości z zadania 31 (a).

Równość z zadania 31 (b) jest fałszywa. Jest natomiast równoważna równości

$$\min(x, y + z) = \min(x, y) + \min(x, y).$$

Jest ona fałszywa np. dla $x = 3$, $y = 2$ i $z = 2$. Biorąc trzy funkcję określone w zbiorze A: funkcję X stale równą 3 oraz Y i Z – stale równe 2 , możemy wykazać fałszywość równości z zadania 31 (b).

Zdefiniowana w zadaniu 31 relacja $\subseteq$ porządkuje multizbiory z $\mathcal{M}(A)$. Może trochę łatwiej to się dowodzi, jeżeli scharakteryzujemy relację $\subseteq$ w języku funkcji. Dowolne multizbiory X i Y spełniają warunek $X \subseteq Y$ wtedy i tylko wtedy, gdy

$$X(a) \leq Y(a)$$

dla wszystkich $a \in A$. Tak więc relacja zawierania między multizbiorami to jeden z częściej spotykanych porządków w zbiorze funkcji.

Zawieranie w rodzinie multizbiorów nie jest porządkiem zupełnym. Jeżeli przyjmiemy, że X_n jest multizbiorem, do którego wszystkie elementy należą n razy, czyli

jest funkcją stale równą n, to zbiór $\{X_n : n \in N\}$ nie ma kresu górnego. Co więcej, nie ma on ograniczenia górnego. Gdyby bowiem Y ograniczało ten zbiór z góry, $a \in A$ i $Y(a) = m$, to z warunku $X_{m+1} \subseteq Y$ można by wywnioskować, że

$$m + 1 = X_{m+1}(a) \leq Y(a) = m,$$

a to nie powinno się dać zrobić.

Zadanie 32. Niech $\langle A, \leq \rangle$ będzie zbiorem dobrze uporządkowanym (czyli zbiorem liniowo uporządkowanym, w którym każdy niepusty podzbiór ma element najmniejszy). W zbiorze $A \times A$ porządek leksykograficzny jest zdefiniowany wzorem

$$\langle x_1, x_2 \rangle \leq_{lex} \langle y_1, y_2 \rangle \overset{\text{df}}{\Leftrightarrow} (x_1 \leq y_1 \wedge x_1 \neq y_1) \vee (x_1 = y_1 \wedge x_2 \leq y_2).$$

W zbiorze $X = (\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0\})$ definiujemy porządek $\preceq$ wzorem

$$\langle x_1, x_2 \rangle \preceq \langle y_1, y_2 \rangle \overset{\text{df}}{\Leftrightarrow} \frac{x_1}{x_2} < \frac{y_1}{y_2} \vee \left(\frac{x_1}{x_2} = \frac{y_1}{y_2} \wedge x_1 \leq y_1 \right).$$

(a) Udowodnij, że $\langle A \times A, \leq_{lex} \rangle$ jest zbiorem dobrze uporządkowanym (nie trzeba dowodzić, że relacja $\leq_{lex}$ jest porządkiem, ani że jest to porządek liniowy).

(b) Czy $\langle X, \preceq \rangle$ jest izomorficzny z $\langle \mathbb{Q}, \leq \rangle$?

(c) Czy $\langle X, \preceq \rangle$ jest izomorficzny z $\langle \mathbb{N} \times \mathbb{N}, \leq_{lex} \rangle$?

Uzasadnij odpowiedzi.

Rozwiązanie zadania 32 (a). Porządek leksykograficzny w kwadracie kartezjańskim dobrze uporządkowanego zbioru $\langle A, \leq \rangle$ jest regularny, a więc spełnia zasadę minimum. Weźmy dowolny niepusty zbiór $X \subseteq A \times A$. Przyjmijmy, że

$$Y = \{y \in A : \exists z \in A \ \langle y, z \rangle \in X\}.$$

Jest to niepusty podzbiór A. Korzystając z zasady minimum w zbiorze A znajdujemy najmniejszy element w zbiorze Y. Niech ntym elementem najmniejszym będzie a. Teraz definiujmy zbiór

$$Z = \{z \in A : \langle a, z \rangle \in X\}.$$

Z definicji a wynika, że zbiór Z jest niepusty. Ponownie korzystamy z zasady minimum i znajdujemy w Z element najmniejszy. Tym razem oznaczamy go symbolem b.

Nietrudno zauważyć, że $\langle a, b \rangle$ jest najmniejszym elementem w zbiorze X. Aby się o tym przekonać weźmy dowolny element $\langle y, z \rangle$ w zbiorze X. Jest oczywiste, że $y \in Y$. Z definicji a otrzymujemy, że $a \leq y$. Gdyby się okazało, że $a \neq y$, to

z definicji porządku leksykograficznego wynikałoby, że $\langle a, b\rangle \leq_{lex} \langle y, z\rangle$. Załóżmy więc, że $a = y$. Wtedy z jest elementem zbioru Z i na mocy definicji b zachodzi nierówność $b \leq z$. Łatwo sprawdzić, że także w tym przypadku zachodzi nierówność $\langle a, b\rangle \leq_{lex} \langle y, z\rangle$.

Rozwiązanie zadania 32 (b) i (c). Najpierw spróbujmy sobie wyobrazić zbiory uporządkowane $\langle X, \prec\rangle$ i $\langle \mathbb{N} \times \mathbb{N}, \leq_{lex}\rangle$.

Pierwszy z tych zbiorów składa się z przedstawień dodatnich liczb wymiernych i rozpada się fragmenty złożone z przedstawień tej samej liczby. Całe te fragmenty są uporządkowane tak, jak przedstawiane przez nie liczby. Wewnątrz fragmentów porządek jest wyznaczony przez liczniki przedstawień i ma takie własności, jak porządek w zbiorze liczb naturalnych.

Drugi ze zbiorów ma podobną strukturę. Też składa się z fragmentów, tym razem są to zbiory par o ustalonej pierwszej współrzędnej. Poszczególne fragmenty, jak i zbiór fragmentów są uporządkowane, jak zbiór liczb naturalnych.

Porządki $\langle \mathbb{Q}, \leq\rangle$ i $\langle X, \prec\rangle$ nie są izomorficzne. Porządek w zbiorze liczb wymiernych jest gęsty. Natomiast fragmenty drugiego porządku $\langle X, \prec\rangle$ składają się z „kolejnych" wyrazów. Na przykład, między parami $\langle 1, 1\rangle$ i $\langle 2, 2\rangle$ (przedstawiającymi liczbę 1) nie ma żadnych innych elementów. Nie jest więc to porządek gęsty. Z drugiej strony, łatwo sprawdzić, że izomorfizm zachowuje gęstość. Gdyby porządek $\langle X, \prec\rangle$ był izomorficzny z $\langle \mathbb{Q}, \leq\rangle$, to byłby gęsty.

Podobnie, nie są izomorficzne porządki $\langle X, \prec\rangle$ i $\langle \mathbb{N} \times \mathbb{N}, \leq_{lex}\rangle$. Pierwszy z nich przypomina porządek w zbiorze dodatnich liczb wymiernych i nie ma elementu najmniejszego. W drugim jest element najmniejszy i jest to para $\langle 0, 0\rangle$.

Fakt z zadania 32 (c) można też dowieść w inny sposób. Z punktu (a) wynika, że porządek $\langle \mathbb{N} \times \mathbb{N}, \leq_{lex}\rangle$ jest dobry. Porządek izomorficzny z dobrym też jest dobry. Porządek $\langle X, \prec\rangle$ nie jest jednak dobry. Jest w nim ciąg malejący, np. złożony z elementów $\langle 1, 1\rangle$, $\langle 1, 2\rangle$, $\langle 1, 3\rangle$, ...