

Podstawy matematyki dla informatyków

Semestr zimowy 2025/26

- ▶ Jacek Chrząszcz,
chrzaszcz@mimuw.edu.pl,
- ▶ Paweł Urzyczyn,
urzy@mimuw.edu.pl.

1

2

Ogólnodostępna strona przedmiotu

<http://www.mimuw.edu.pl/~urzy/Pmat>

- ▶ Skrypt: pomat.pdf
- ▶ Zadania: zadania25.pdf
- ▶ Obrazki: slajdy250.pdf

Moodle

<https://moodle.mimuw.edu.pl/course/view.php?id=2570>

- ▶ Jak wyżej.
- ▶ Zagadki itp. ...
- ▶ Forum ogólne i dla poszczególnych grup, czat, ...

3

Konsultacje

Wszyscy prowadzący zajęcia odbywają w ustalonych godzinach konsultacje dla studentów.

Konsultacje P. Urzyczyna: poniedziałki, zdalnie:

<https://us02web.zoom.us/j/84593508534>

od 19:00 do ostatniego klienta.

Konsultacje J. Chrząszcza: TBA

Uwaga: te terminy mogą ulegać zmianom.

4

Zaliczenie przedmiotu

Aby zaliczyć przedmiot należy
zaliczyć ćwiczenia i zdać egzamin.

1. O zaliczeniu ćwiczeń decyduje prowadzący ćwiczenia.
2. Aby zaliczyć ćwiczenia należy koniecznie zaliczyć:
 - ▶ prace domowe;
 - ▶ klasówkę;
 - ▶ inne zagadki.
3. W razie wątpliwości patrz punkt 1.

5

Ocena końcowa

Ocena końcowa z przedmiotu zostanie ustalona (w pierwszym terminie) na podstawie maksimum z dwóch wielkości:

1. Wynik egzaminu
2. Średnia ważona wyniku klasówki (30%) i egzaminu (70%)

Punkty z ewentualnej klasówki poprawkowej nie liczą się do wyniku końcowego.

W drugim terminie ocena końcowa będzie ustalana na podstawie samego egzaminu.

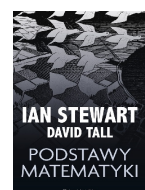
6

Klasówka

Klasówka będzie w czwartek 11 grudnia
(zamiast wykładu)

Różne książki dla dociekliwych

- ▶ Stewart, Tall,
- ▶ Kuratowski,
- ▶ Kuratowski, Mostowski,
- ▶ Błaszczyk, Turek,
- ▶ Guzicki, Zakrzewski,
- ▶ Rasiowa.
- ▶ Zbiory zadań:
 - ▶ Marek, Onyszkiewicz,
 - ▶ Guzicki, Zakrzewski,
 - ▶ Ławrow, Maksimowa.



7

8

- Ian Stewart, David Tall, *The Foundations of Mathematics*,
- David Makinson, *Sets, Logic and Maths for Computing*
- Kees Doets and Jan van Eijck, *The Haskell Road to Logic, Maths and Programming*
- Glynn Winskel, *Set Theory for Computer Science*

9

Juliusz Słowacki wielkim poetą był

Chodzi mi o to, aby język giętki
 Powiedział wszystko, co pomyśli głowa
 (...)
 Aby przeleciał wszystko ducha skrzydłem.
 Strofa być winna taktem, nie wędzidłem.
 (Beniowski, Pieśń piąta)

11

Dwuwartościowa logika: 1 = prawda, 0 = fałsz

α	β	$\neg\alpha$	$\alpha \wedge \beta$	$\alpha \vee \beta$	$\alpha \leftrightarrow \beta$
0	0	1	0	0	1
0	1	1	0	1	0
1	0	0	0	1	0
1	1	0	1	1	1

Przykład: wyrażenie $\alpha \vee \neg\alpha$ ma zawsze wartość 1.
 Takie wyrażenia nazywamy *tautologiami*.

13

Implikacja materialna

α	β	$\alpha \rightarrow \beta$
0	0	1
0	1	1
1	0	0
1	1	1

Wartość logiczna implikacji zależy wyłącznie od wartości logicznych stwierdzeń α i β , a nie zależy od związku przyczynowo-skutkowego, następstwa w czasie, itp.

Ważne: Implikacja $\alpha \rightarrow \beta$ znaczy to samo, co $\neg\alpha \vee \beta$

15

Co to są „podstawy matematyki”?

Dwa znaczenia:

- podstawowe wiadomości o matematyce;
- *metamatematyka* - dział matematyki zajmujący się językiem i strukturą samej matematyki:
 - logika, teoria zbiorów, teoria obliczeń, ...

10

Spójniki zdaniowe

Koniunkcja: napis $\alpha \wedge \beta$ czytamy „ α i β ”;
Alternatywa: napis $\alpha \vee \beta$ czytamy „ α lub β ”;
Implikacja: napis $\alpha \rightarrow \beta$ czytamy „jeśli α to β ”;
Równoważność: napis $\alpha \leftrightarrow \beta$ czytamy „ α wtedy i tylko wtedy, gdy β ”;
Negacja: napis $\neg\alpha$ czytamy „nieprawda, że α ”.
Fałsz oznaczamy symbolem $\perp$, *prawdę* symbolem $\top$.

12

Przemienność i łączność

Wielocłonowe koniunkcje i alternatywy piszemy bez nawiasów, np. $\alpha \wedge \beta \wedge \gamma \wedge \delta$, i w dowolnej kolejności.

Ale nie piszemy tak: $p \vee q \wedge r$,
 bo $(p \vee q) \wedge r$ znaczy co innego niż $p \vee (q \wedge r)$

14

Które z następujących zdań jest materialnie prawdziwe?

- Jeśli przycisk jest wciśnięty, to dzwonek dzwoni.
- Jeśli dzwonek dzwoni, to przycisk jest wciśnięty.

16

Ogólny:

Napis $\forall x W(x)$ czytamy: „Każde x ma własność $W(x)$ ”
albo „Dla każdego x zachodzi $W(x)$ ”

Szczegółowy:

Napis $\exists x W(x)$ czytamy: „Pewne x ma własność $W(x)$ ”
albo „Istnieje takie x , że $W(x)$ ”.

17

Zmienne wolne i związane

Interpretacja stwierdzenia „ $x > 4$ ” zależy od wartości x .

Interpretacja zdania $\forall x: \mathbb{N}. x > 4$ nie zależy od wartości x .

Zdanie $\forall x: \mathbb{N}. x > 4$ wyraża tę samą myśl co $\forall y: \mathbb{N}. y > 4$.

(Każda liczba naturalna jest większa niż cztery.)

W formule $x > 4$ zmienna x jest *wolna*.

W zdaniu $\forall x: \mathbb{N}. x > 4$ zmienna x jest *związana*.

19

„Odpowiednie dać rzeczy – słowo”¹

W matematyce posługujemy się językiem naturalnym.

Róbmy to w sposób precyzyjny i jednoznaczny.

I pamiętajmy o różnicach pomiędzy językami.

¹Norwid też.

21

Ćwiczenie (fałszywi przyjaciele)

Jak wypowiedzieć zaprzeczenie zdania:

1. *Liczby m i n są względnie pierwsze.*

Odpowiedź:

Liczby m i n nie są względnie pierwsze.

2. *Liczby m i n są pierwsze.*

Odpowiedź:

Któraś z liczb m i n nie jest pierwsza.

23

Ogólny:

$\forall x: \mathbb{N}. W(x)$ albo $\forall x \in \mathbb{N}. W(x)$ czytamy:
„Każde x , które jest liczbą naturalną, ma własność $W(x)$ ”

Szczegółowy:

$\exists x: \mathbb{N}. W(x)$ albo $\exists x \in \mathbb{N}. W(x)$ czytamy:
„Pewne x , które jest liczbą naturalną, ma własność $W(x)$ ”

Napis $\forall x W(x)$ zwykle oznacza $\forall x: \mathcal{D}. W(x)$, gdzie $\mathcal{D}$ jest domyślną dziedziną dla zmiennej x .

18

Które zmienne są tu wolne, a które związane?

$$\forall x: \mathbb{N} (x > 0 \vee x \leq y) \rightarrow x = 1$$

Zasięg kwantyfikatora obejmuje tylko zielone x .

Jak to lepiej zapisać?

$$\forall z: \mathbb{N} (z > 0 \vee z \leq y) \rightarrow x = 1$$

20

Ćwiczenie (fałszywi przyjaciele)

Czy te dwa zdania są podobne?

Liczby m i n są pierwsze.

Liczby m i n są względnie pierwsze.

Pierwsze zdanie mówi o własnościach pojedynczych liczb:

$Pierwsze(m) \wedge Pierwsze(n)$.

Drugie zdanie mówi o związku między liczbami:

$Względnie_pierwsze(m, n)$.

22

Zaprzeczenie zdania z kwantyfikatorem

Prawa De Morgana dla kwantyfikatorów:

$\neg \exists x. W(x)$ wtedy i tylko wtedy, gdy $\forall x. \neg W(x)$.

$\neg \forall x W(x)$ wtedy i tylko wtedy, gdy $\exists x. \neg W(x)$.

24

Ćwiczenie

Jak brzmi zaprzeczenie zdania

Żaden pies nie goni każdego kota?

Najpierw zastanówmy się, co dokładnie mówi to zdanie.

Możemy je zapisać tak:

$\forall x: \text{Pies}. \neg \forall y: \text{Kot}. \text{Goni}(x, y)$,

bo zwrot „żaden...nie” oznacza tyle, co „ $\forall \dots \neg$ ”.

Negacją tego zdania będzie więc:

$\exists x: \text{Pies}. \neg \neg \forall y: \text{Kot}. \text{Goni}(x, y)$, czyli

$\exists x: \text{Pies}. \forall y: \text{Kot}. \text{Goni}(x, y)$,

co po polsku powiemy tak:

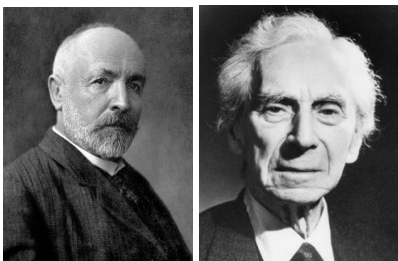
Pewien pies goni każdego kota.

Teoria zbiorów

25

26

Georg Cantor, Bertrand Russell



27

Georg Cantor:

Zbiorem nazywamy zgromadzenie w jedną całość wyraźnie wyróżnionych przedmiotów naszej intuicji lub naszej myśli.

$\{x \mid W(x)\}$ oznacza zbiór wszystkich x o własności $W(x)$.

$y \in A$ oznacza, że y jest elementem zbioru A .

$$y \in \{x \mid W(x)\} \Leftrightarrow W(y)$$

Zbiór $\{x \mid W(x)\}$ to „zmaterializowane” kryterium $W(x)$.

28

Kłopoty ze zbiorami (Antynomia Russella)

$\{x \mid W(x)\}$ oznacza zbiór wszystkich x o własności $W(x)$

$$R = \{x \mid x \text{ jest zbiorem i } x \notin x\}$$

Jeśli $R \in R$, to $R \notin R$... ale jeśli $R \notin R$, to $R \in R$!

29

Typy

Zbiór $\{x \mid W(x)\}$ to „zmaterializowane” kryterium $W(x)$.

Ale nie każde kryterium $W(x)$ ma sens dla dowolnego x .

Wartości zmiennej x należą zawsze do pewnej dziedziny $\mathcal{D}$.
Takie dziedziny nazywamy *typami*.

Zbiory tworzymy wybierając elementy ustalonego typu:

$$\{x: \mathcal{D} \mid W(x)\}$$

Zbiór elementów typu $\mathcal{D}$ sam nie musi być typu $\mathcal{D}$.

30

Definiowanie zbiorów: wycinanie

- ▶ $\{x: \mathcal{D} \mid W(x)\}$, gdy elementy są typu $\mathcal{D}$.

$$y \in \{x: \mathcal{D} \mid W(x)\} \Leftrightarrow y: \mathcal{D} \wedge W(y).$$

- ▶ $\{x \in A \mid W(x)\}$, gdy chodzi o *podzbiór* zbioru A .

$$y \in \{x \in A \mid W(x)\} \Leftrightarrow y \in A \wedge W(y).$$

- ▶ Można napisać $\{x \mid W(x)\}$ gdy typ jest oczywisty.

31

Definiowanie zbiorów: wyliczanie

- ▶ $\{1, 3, 5, 7\}$ to zbiór o elementach $1, 3, 5, 7$.

- ▶ Podobnie $\{2\}$, $\{x, y\}$, $\{\{0, 1\}, \{0, 2\}, \{1, 6\}\}$, itp.

- ▶ Takiej notacji używamy ostrożnie:

- ▶ $\{x_1, \dots, x_n\}$;
- ▶ $\{x_1, x_2, x_3, \dots\}$.

32

Definiowanie zbiorów: zastępowanie

Jeśli dla każdego $x \in X$ określone jest jakieś $a_x \in Y$, to zbiór

$$\{b \in Y \mid \exists x(x \in X \wedge b = a_x)\}$$

zapisujemy prościej tak:

$$\{a_x \mid x \in X\}.$$

Na przykład, zbiór $\{2x^2 \mid x \in (-1, 2)\}$ to przedział $[0, 8)$.

Uwaga: Z tego, że $2y^2 \in \{2x^2 \mid x \in (-1, 2)\}$

nie wynika, że $y \in (-1, 2)$.

33

Zbiór pusty

Mówimy, że zbiór jest *pusty*, gdy nie ma żadnego elementu.

Fakt

Każdy typ $\mathcal{D}$ ma dokładnie jeden pusty podzbiór.

Dowód: Gdyby były dwa, to miałyby te same elementy. $\square$

Zbiór pusty oznaczamy symbolem $\emptyset$.

35

Zbiór potęgowy:

Elementami zbioru $P(A)$ są wszystkie podzbiory zbioru A

$$X \in P(A) \quad \Leftrightarrow \quad X \subseteq A$$

Zbiory obiektów typu $\mathcal{D}$ są typu $P(\mathcal{D})$.

$$P(A) = \{X : P(\mathcal{D}) \mid X \subseteq A\} : P(P(\mathcal{D}))$$

Przykład: $P(\{0, 1\}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$
 $P(\emptyset) = \{\emptyset\}, \quad P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$

37

Złote myśli

$$x \in A \cup B \quad \Leftrightarrow \quad x \in A \vee x \in B$$

$$x \in A \cap B \quad \Leftrightarrow \quad x \in A \wedge x \in B$$

$$x \in A - B \quad \Leftrightarrow \quad x \in A \wedge x \notin B$$

$$x \in -A \quad \Leftrightarrow \quad x \notin A$$

39

Równość zbiorów (zasada jednoznaczności)

Zbiory A i B są *równe* (jest to jeden i ten sam zbiór) wtedy i tylko wtedy, gdy mają dokładnie te same elementy.

$$A = B \quad \Leftrightarrow \quad \forall z(z \in A \leftrightarrow z \in B)$$

A zatem $\{a, b\}$, $\{b, a\}$, $\{b, a, b\}$ i $\{a, b, b, a\}$ to to samo.

34

Zawieranie (inkluzja):

$$A \subseteq B \quad \Leftrightarrow \quad \forall z(z \in A \rightarrow z \in B).$$

$$A = B \quad \Leftrightarrow \quad A \subseteq B \wedge B \subseteq A$$

Notacja:

$A \not\subseteq B$ oznacza, że $\neg A \subseteq B$. Inaczej:

$$A \not\subseteq B \quad \Leftrightarrow \quad \exists z(z \in A \wedge z \notin B).$$

$A \subsetneq B$ oznacza, że $A \subseteq B$, ale $A \neq B$

36

Działania na zbiorach

Niech $A, B \subseteq \mathcal{D}$. Wówczas:

- **Sumą** zbiorów A i B nazywamy zbiór
 $A \cup B = \{x : \mathcal{D} \mid x \in A \vee x \in B\}.$
- **Iloczyn** lub **przecięcie** zbiorów A i B to zbiór
 $A \cap B = \{x : \mathcal{D} \mid x \in A \wedge x \in B\}.$
- **Różnicą** zbiorów A i B nazywamy zbiór
 $A - B = \{x : \mathcal{D} \mid x \in A \wedge x \notin B\}.$
- **Dopełnienie** zbioru A (do typu $\mathcal{D}$) to zbiór
 $-A = \{x : \mathcal{D} \mid x \notin A\}$
(czyli różnica $\mathcal{D} - A$).

38

Złote myśli

$$x \in A \cup B \quad \Leftrightarrow \quad x \in A \vee x \in B$$

$$x \notin A \cup B \quad \Leftrightarrow \quad x \notin A \wedge x \notin B$$

$$x \in A \cap B \quad \Leftrightarrow \quad x \in A \wedge x \in B$$

$$x \notin A \cap B \quad \Leftrightarrow \quad x \notin A \vee x \notin B$$

40

Ćwiczenie (prawo De Morgana)

- Dla dowolnych A, B zachodzi równość:

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

Dowód: Bo dla dowolnego x mamy równoważność:

$$x \notin A \cup B \leftrightarrow x \notin A \wedge x \notin B,$$

czyli

$$\forall x (x \in \neg(A \cup B) \leftrightarrow x \in \neg A \cap \neg B).$$

- Dla dowolnych A i B zachodzi równość:

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

41

Nie zawsze jest tak łatwo

Równość $A = B$ nie zawsze jest taka oczywista.

Często trzeba osobno dowodzić, że $A \subseteq B$

i osobno, że $B \subseteq A$.

42

Nie zawsze jest tak łatwo

Jak udowodnić, że $A \subseteq B$?

Najpierw trzeba zapytać: co to znaczy?

Odpowiedź: $A \subseteq B$ znaczy, że $\forall x (x \in A \rightarrow x \in B)$.

„Dla każdego x , jeśli $x \in A$, to $x \in B$.”

Należy więc pokazać, że **każdy** $x \in A$ należy do B .

Dokładniej: należy założyć, że $x \in A$ i udowodnić, że $x \in B$, gdzie x jest dowolne (tj. nic więcej o nim nie wiadomo).

„Rozpatrzmy dowolne $x \in A$. Wtedy ”

... .. Zatem $x \in B$.”

43

Ćwiczenie:

Udowodnić, że jeśli $A \cup B \subseteq C$, to $A - B \subseteq C - B$.

Założmy, że $A \cup B \subseteq C$.

(Cel 1: $A - B \subseteq C - B$)

Rozpatrzmy dowolne $x \in A - B$.

(Cel 2: $x \in C - B$)

Ponieważ $x \in A - B$, więc $x \in A$ oraz $x \notin B$.

Skoro $x \in A$, to $x \in A \cup B$.

A więc z założenia wynika $x \in C$.

Ponadto $x \notin B$, więc $x \in C - B$.

(Cel 2 osiągnięty)

Zatem $\forall x (x \in A - B \rightarrow x \in C - B)$,

czyli $A - B \subseteq C - B$.

(Cel 1 osiągnięty)

Zatem jeśli $A \cup B \subseteq C$, to $A - B \subseteq C - B$.

44

Ćwiczenie:

Udowodnić, że jeśli $A \cup B \subseteq C$, to $A - B \subseteq C - B$.

Założmy, że $A \cup B \subseteq C$.

(Cel 1: $A - B \subseteq C - B$)

Rozpatrzmy dowolne $x \in A - B$.

(Cel 2: $x \in C - B$)

Ponieważ $x \in A - B$, więc $x \in A$ oraz $x \notin B$.

Skoro $x \in A$, to $x \in A \cup B$.

A więc z założenia wynika $x \in C$.

Ponadto $x \notin B$, więc $x \in C - B$.

(Cel 2 osiągnięty)

Zatem $\forall x (x \in A - B \rightarrow x \in C - B)$,

czyli $A - B \subseteq C - B$.

(Cel 1 osiągnięty)

Zatem jeśli $A \cup B \subseteq C$, to $A - B \subseteq C - B$.

45

Ćwiczenie: Udowodnić, że jeśli $A - B = \emptyset$, to $A \subseteq B$.

Założmy, że $A - B = \emptyset$.

(Cel 1: $A \subseteq B$)

Rozpatrzmy dowolne $x \in A$.

(Cel 2: $x \in B$)

Założmy, że $x \notin B$.

(Cel 3: sprzeczność)

Skoro $x \in A$ i $x \notin B$, to $x \in A - B$.

Ale $A - B = \emptyset$, więc $x \in \emptyset$, sprzeczność.

(Cel 3 osiągnięty)

Zatem $x \in B$.

(Cel 2 osiągnięty)

Zatem $\forall x (x \in A \rightarrow x \in B)$, czyli $A \subseteq B$.

(Cel 1 osiągnięty)

Zatem jeśli $A - B = \emptyset$ to $A \subseteq B$.

46

Jeśli $A - B = \emptyset$ to $A \subseteq B$

Założmy, że $A - B = \emptyset$.

(Cel 1: $A \subseteq B$)

Rozpatrzmy dowolne $x \in A$.

(Cel 2: $x \in B$)

Założmy, że $x \notin B$.

(Cel 3: sprzeczność)

Skoro $x \in A$ i $x \notin B$, to $x \in A - B$.

Ale $A - B = \emptyset$, więc $x \in \emptyset$, sprzeczność.

(Cel 3 osiągnięty)

Zatem $x \in B$.

(Cel 2 osiągnięty)

Zatem $\forall x (x \in A \rightarrow x \in B)$, czyli $A \subseteq B$.

(Cel 1 osiągnięty)

Zatem jeśli $A - B = \emptyset$ to $A \subseteq B$.

To samo, krócej:

Niech $A - B = \emptyset$ oraz $x \in A$. Gdyby $x \notin B$,

to $x \in A - B = \emptyset$, sprzeczność. Zatem $x \in B$.

47

Wnioskowanie przez zaprzeczenie

Twierdzenie: Jeśli $A - B = \emptyset$, to $A \subseteq B$.

Dowód: Niech $A - B = \emptyset$ oraz $x \in A$. Gdyby $x \notin B$, to $x \in A - B = \emptyset$, sprzeczność. Zatem $x \in B$.

Dowód powyżej używa metody **wnioskowania przez zaprzeczenie**, którą można wyrazić za pomocą schematu:

$$(\neg p \rightarrow \perp) \rightarrow p.$$

„Jeśli założenie $\neg p$ prowadzi do sprzeczności, to zachodzi p ”
(Bo musi być albo p albo $\neg p$.)

48

Przykład: Jeśli $A - B \subseteq C$, to $A \subseteq B \cup C$.

Założmy, że $A - B \subseteq C$.	(Cel 1: $A \subseteq B \cup C$)
Rozpatrzmy dowolne $x \in A$.	(Cel 2: $x \in B \cup C$)
Wiadomo, że $x \in B$ lub $x \notin B$.	
Przypuśćmy, że $x \in B$.	(Cel 3: $x \in B \cup C$)
Wtedy $x \in B \cup C$.	(Cel 3 osiągnięty)
Przypuśćmy, że $x \notin B$.	(Cel 4: $x \in B \cup C$)
Ponieważ $x \in A$ i $x \notin B$, więc $x \in A - B$.	
Ponieważ $x \in A - B$ oraz $A - B \subseteq C$, więc $x \in C$.	
Wtedy $x \in B \cup C$.	(Cel 4 osiągnięty)
W każdym przypadku $x \in B \cup C$.	(Cel 2 osiągnięty)
Zatem $\forall x(x \in A \rightarrow x \in B \cup C)$.	(Cel 1 osiągnięty)
Zatem jeśli $A - B \subseteq C$, to $A \subseteq B \cup C$.	

49

Wnioskowanie przez przypadki

Twierdzenie: Jeśli $A - B \subseteq C$ to $A \subseteq B \cup C$.

Dowód (zwięzły):

Niech $x \in A$. Jeśli $x \in B$, to oczywiście $x \in B \cup C$.
W przeciwnym razie $x \in A - B \subseteq C$, więc $x \in C$,
czyli także $x \in B \cup C$.

Ten dowód używa metody wnioskowania przez przypadki,
którą można wyrazić za pomocą schematu:

$$(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r) \rightarrow r.$$

Najczęściej stosujemy go tak:

$$(p \rightarrow r) \wedge (\neg p \rightarrow r) \rightarrow r.$$

50

Działania uogólnione

Suma uogólniona rodziny zbiorów $\mathcal{R}$:

$$\bigcup \mathcal{R} = \{x \mid \exists A(A \in \mathcal{R} \wedge x \in A)\}.$$

Uwaga: $\bigcup \{A, B\} = A \cup B$.

Uogólniony iloczyn niepustej rodziny $\mathcal{R}$:

$$\bigcap \mathcal{R} = \{x \mid \forall A(A \in \mathcal{R} \rightarrow x \in A)\}.$$

Na przykład jeśli $\mathcal{R} = \{\{0, 2\}, \{2, 1\}, \{2\}\}$,

to $\bigcup \mathcal{R} = \{0, 1, 2\}$ oraz $\bigcap \mathcal{R} = \{2\}$.

51

Złote myśli:

$$x \in \bigcup \mathcal{R} \Leftrightarrow \exists A(A \in \mathcal{R} \wedge x \in A).$$

$$x \in \bigcap \mathcal{R} \Leftrightarrow \forall A(A \in \mathcal{R} \rightarrow x \in A).$$

52

Działania nieskończone

Suma uogólniona rodziny $\mathcal{R}$:

$$\bigcup \mathcal{R} = \{x \mid \exists A(A \in \mathcal{R} \wedge x \in A)\}.$$

Uogólniony iloczyn niepustej rodziny $\mathcal{R}$:

$$\bigcap \mathcal{R} = \{x \mid \forall A(A \in \mathcal{R} \rightarrow x \in A)\}.$$

Na przykład jeśli $A_t = \{(x, y) \mid x^2 + y^2 \leq t^2\}$, to:

$$\begin{aligned} \bigcup \{A_t \mid t \in \mathbb{R}\} &= \mathbb{R}^2 = \bigcup_{t \in \mathbb{R}} A_t \\ \bigcap \{A_t \mid t \in \mathbb{R}\} &= \{(0, 0)\} = \bigcap_{t \in \mathbb{R}} A_t. \end{aligned}$$

Dlaczego?

53

Łatwe ćwiczenia

► Jeśli $A \in \mathcal{R}$, to $\bigcap \mathcal{R} \subseteq A \subseteq \bigcup \mathcal{R}$.

► Jeśli $\mathcal{R} \neq \emptyset$, to $\bigcap \mathcal{R} \subseteq \bigcup \mathcal{R}$.

► Jeśli $\mathcal{R} = \emptyset$, to $\bigcup \mathcal{R} = \emptyset$.

► Jeśli $\emptyset \in \mathcal{R}$, to $\bigcap \mathcal{R} = \emptyset$.

54

Dygresja: fałszywi przyjaciele

- Stwierdzenie „dla pewnego $A \in \mathcal{R}$ zachodzi $x \in A$ ” zapisujemy tak:

$$\exists A \in \mathcal{R}. x \in A, \quad \text{albo tak:} \quad \exists A(A \in \mathcal{R} \wedge x \in A).$$

- Stwierdzenie „dla każdego $A \in \mathcal{R}$ zachodzi $x \in A$ ” zapisujemy tak:

$$\forall A \in \mathcal{R}. x \in A, \quad \text{albo tak:} \quad \forall A(A \in \mathcal{R} \rightarrow x \in A).$$

55

Ćwiczenie: Udowodnić, że $\bigcup P(A) = A$, dla dowolnego A .

Rozwiązanie: Najpierw udowodnimy, że $\bigcup P(A) \subseteq A$,
potem, że $A \subseteq \bigcup P(A)$.

($\subseteq$) Przypuśćmy, że $a \in \bigcup P(A)$. To znaczy, że istnieje
element α zbioru $P(A)$ o własności $a \in \alpha$.

Ustalmy więc takie $\alpha \in P(A)$, że $a \in \alpha$.

Wtedy $a \in \alpha \subseteq A$, skąd $a \in A$.

($\supseteq$) Niech $a \in A$. Wtedy $a \in \{a\}$ oraz $\{a\} \in P(A)$.

Wskazaliśmy więc element α zbioru $P(A)$ o własności $a \in \alpha$.

Zatem $a \in \bigcup P(A)$.

56

Jak używamy założenia egzystencjalnego?

... istnieje element α zbioru $P(A)$ o własności $a \in \alpha$.

Ustalmy więc takie $\alpha \in P(A)$, że $a \in \alpha$.

Wtedy $a \in \alpha \subseteq A$,...

Sens: symbol α oznacza jakiś domniemany obiekt, o którym nic nie wiadomo, oprócz tego, że $\alpha \in P(A)$ oraz $a \in \alpha$.

57

Częsty błąd: „nie to samo x ”

Nie udowodnimy, że jeśli $A \neq \emptyset$ i $B \neq \emptyset$, to $A \cap B \neq \emptyset$.

Skoro $A \neq \emptyset$, to istnieje takie x , że $x \in A$.

Skoro $B \neq \emptyset$, to istnieje takie y , że $y \in B$.

Teraz widać, że możliwe jest $x \neq y$.

59

Relacje

Dowolny podzbiór r iloczynu kartezjańskiego $A \times B$ nazywamy relacją z A do B . Jeśli $A = B$, to relacja jest w zbiorze A .

Jeśli $\langle x, y \rangle \in r$, to często piszemy $x r y$.

Przykłady: relacja pusta $\emptyset$, relacja pełna $A \times A$,
relacja identycznościowa (równość) $1_A = \{\langle a, a \rangle \mid a \in A\}$,
relacja porządku $\leq_{\mathbb{N}} = \{\langle x, y \rangle \in \mathbb{N} \mid x \leq y\}$, itp.

61

Suma rozłączna (koprodukt, suma prosta)

$$A \oplus B = \{\langle d \rangle_1 \mid d \in A\} \cup \{\langle e \rangle_2 \mid e \in B\}$$

Element sumy rozłącznej $A \oplus B$ jest

- ▶ albo postaci $\langle a \rangle_1$, gdzie $a \in A$ (lewa kopia elementu a),
- ▶ albo postaci $\langle b \rangle_2$, gdzie $b \in B$ (prawa kopia elementu b).

Lewe i prawe kopie są zawsze różne:

$\langle x \rangle_i = \langle y \rangle_j$ wtedy i tylko wtedy, gdy $x = y$ oraz $i = j$.

Konwencja: Często przyjmujemy, że $A, B \subseteq A \oplus B$.
To wygodne, ale niebezpieczne!

63

Częsty błąd: „nie to samo x ”

„Udowodnimy”, że jeśli $A \neq \emptyset$ i $B \neq \emptyset$, to $A \cap B \neq \emptyset$.

Skoro $A \neq \emptyset$, to istnieje takie x , że $x \in A$.

Skoro $B \neq \emptyset$, to istnieje takie x , że $x \in B$.

No to $x \in A$ i $x \in B$, więc $x \in A \cap B$?!

Na czym polega błąd?

Nazwa x jest związana dwa razy.

Jak uniknąć błędu? Używać różnych zmiennych.

58

Para uporządkowana

$$\langle a, b \rangle = \langle d, e \rangle \iff a = d \text{ oraz } b = e.$$

Jeśli $d : \mathcal{D}$ oraz $e : \mathcal{E}$ to para $\langle d, e \rangle$ jest typu $\mathcal{D} \times \mathcal{E}$.

Iloczyn kartezjański (produkt)

Jeśli $A \subseteq \mathcal{D}$ i $B \subseteq \mathcal{E}$, to

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

Notacja: $A^2 = A \times A$, $A^3 = (A \times A) \times A$, itd.

60

Ćwiczenie

Udowodnić, że jeśli $A \times B \subseteq C \times D$, oraz $B \neq \emptyset$, to $A \subseteq C$.

Rozwiązanie: Mamy udowodnić, że $A \subseteq C$.

Niech $a \in A$. Ponieważ $B \neq \emptyset$, więc zbiór B ma jakiś element. Nazwijmy go b .
Wtedy $\langle a, b \rangle \in A \times B \subseteq C \times D$, skąd $\langle a, b \rangle \in C \times D$.
A zatem $a \in C$.

Uwaga: jeśli $B = \emptyset$, to $A \times B = \emptyset$ dla każdego A .
Wtedy np. $\{1, 2\} \times \emptyset = \emptyset \subseteq \{3, 4\} \times \{5\}$, chociaż $\{1, 2\} \not\subseteq \{3, 4\}$.

62

Przykład

Zwykła suma $\{0, 1\} \cup \{0\}$ ma dwa elementy:

$$\{0, 1\} \cup \{0\} = \{0, 1\}$$

Suma prosta $\{0, 1\} \oplus \{0\}$ ma trzy elementy:

$$\{0, 1\} \oplus \{0\} = \{\langle 0 \rangle_1, \langle 1 \rangle_1, \langle 0 \rangle_2\}$$

64

Funkcje

Definicja wprost:

$$f(x) = x + y \quad \lambda x. x + y$$

Definicja warunkowa:

$$g(n) = \begin{cases} n/2, & \text{jeśli } n \text{ jest parzyste;} \\ 3n + 1, & \text{w przeciwnym przypadku.} \end{cases}$$

$$g(n) = \text{if } (n \text{ jest parzyste}) \text{ then } n/2 \text{ else } 3n + 1.$$

65

66

Definiowanie funkcji

Definicja implicite:

$$h(n) = \lambda m. \mathbb{N}. (3 \cdot m \leq n) \wedge (n < 3 \cdot (m + 1))$$

Napis $\lambda x. W(x)$ czytamy: „jedyne x o własności $W(x)$ ”

Definicja rekurencyjna:

$$f(n) = \text{if } n = 0 \text{ then } 0 \text{ else } f(n - 1) + 2.$$

67

Funkcje całkowite i częściowe

Napis $f : A \rightarrow B$ oznacza, że f jest funkcją z A do B .
(Każdemu $a \in A$ przypisane jest dokładnie jedno $f(a) \in B$.)

Napis B^A oznacza zbiór wszystkich funkcji z A do B .
To samo oznacza napis $A \rightarrow B$.

$f : A \multimap B$ oznacza, że f jest funkcją częściową z A do B .
(Niektórym $a \in A$ przypisane są $f(a) \in B$.)

Dziedzina funkcji:

$$\text{Dom}(f) = \{x \mid f(x) \text{ jest określone}\}.$$

(Jeśli $f : A \rightarrow B$, to $\text{Dom}(f) = A$.)

68

Funkcje

Przeciwdziedzina funkcji $f : A \rightarrow B$ to zbiór B .

Przy tej definicji przeciwdziedzina zależy od kontekstu.

Bo jeśli $f : A \rightarrow B$ i $B \subseteq C$, to także $f : A \rightarrow C$.

Zbiór wartości funkcji $f : A \rightarrow B$ to zbiór

$$\text{Rg}(f) = \{y \in B \mid \exists x \in A. f(x) = y\} = \{f(x) \mid x \in A\}$$

Jeśli $f : A \rightarrow B$, to $\text{Dom}(f) = A$ oraz $\text{Rg}(f) \subseteq B$.

69

Równość funkcji

Dla $f, g : A \rightarrow B$,

$$f = g \quad \text{wtedy i tylko wtedy, gdy} \quad \forall x : A. f(x) = g(x);$$

$$f \neq g \quad \text{wtedy i tylko wtedy, gdy} \quad \exists x : A. f(x) \neq g(x).$$

Wykres funkcji:

$$\mathcal{W}(f) = \{\langle x, y \rangle \mid f(x) = y\}$$

Funkcje o tym samym wykresie są równe.

70

Ćwiczenie

$$f = g \quad \text{wtedy i tylko wtedy, gdy} \quad \forall x : A. f(x) = g(x);$$

Ile jest różnych funkcji:

- ▶ ze zbioru pustego do pustego? 1
- ▶ ze zbioru pustego do niepustego? 1
- ▶ ze zbioru niepustego do pustego? 0
- ▶ ze zbioru jednoelementowego do jednoelementowego? 1
- ▶ ze zbioru jednoelementowego do dwuelementowego? 2
- ▶ ze zbioru dwuelementowego do pięcioelementowego? 25

71

Własności funkcji

72

$f : A \rightarrow B$

- Funkcja *różnowartościowa* (injekcja), ozn. $f : A \xrightarrow{1-1} B$
 $\forall x, y \in A (x \neq y \rightarrow f(x) \neq f(y))$
 $\forall x, y \in A (f(x) = f(y) \rightarrow x = y)$
- Funkcja *na* B (surjekcja), ozn. $f : A \xrightarrow{na} B$
 $\forall y \in B \exists x \in A (f(x) = y)$
 Inaczej: $B = \text{Rg}(f)$.
- Funkcja różnowartościowa i na, to *bijekcja* ($f : A \xrightarrow{1-1}_{na} B$).

Jeśli istnieje bijekcja $f : A \xrightarrow{1-1}_{na} B$, to piszemy $A \sim B$
 i mówimy, że zbiory A i B są *równoliczne*.

73

Ćwiczenie

Niech $f : \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ będzie taka, że
 $f(\langle C, D \rangle) = C \cap D$, dla dowolnych $C, D \subseteq \mathbb{N}$.

Czy funkcja f jest różnowartościowa?

Odpowiedź: Nie, bo na przykład

$$f(\langle \{0\}, \{1\} \rangle) = \emptyset = f(\langle \{2\}, \{1\} \rangle).$$

Czy funkcja f jest na $\mathcal{P}(\mathbb{N})$?

Odpowiedź: Tak, bo dla dowolnego $A \in \mathcal{P}(\mathbb{N})$ mamy

$$A = f(\langle A, A \rangle).$$

75

Przykłady

Funkcja identycznościowa $\text{id}_A : A \rightarrow A$ jest bijekcją.

Funkcja następnika $s : \mathbb{N} \rightarrow \mathbb{N}$ jest różnowartościowa.

Niech $\pi_1 : A \times B \rightarrow A$ i $\pi_2 : A \times B \rightarrow B$ będą określone tak:

$$\pi_1(\langle a, b \rangle) = a, \quad \pi_2(\langle a, b \rangle) = b.$$

Dla $A, B \neq \emptyset$, te funkcje (*rzutowania*) są surjekcjami.

Niech $\text{in}_1 : A \rightarrow A \oplus B$ i $\text{in}_2 : B \rightarrow A \oplus B$ będą określone tak:

$$\text{in}_1(a) = \langle a \rangle_1, \quad \text{in}_2(b) = \langle b \rangle_2$$

Te funkcje (*włożenia*) są różnowartościowe.

74

Takie proste twierdzenie...

... które wcale nie jest takie oczywiste.

Twierdzenie

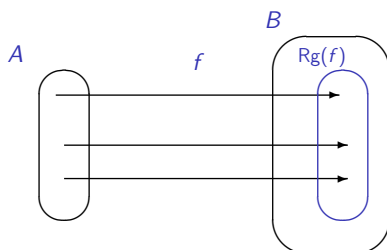
Jeśli A i B są niepustymi zbiorami,

to następujące warunki są równoważne:

- Istnieje injekcja z A do B ;
- Istnieje surjekcja z B na A .

76

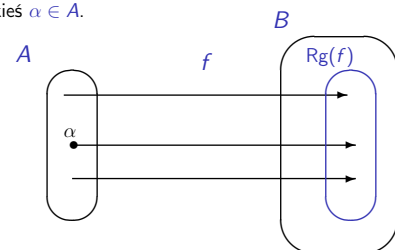
Jeśli $A \neq \emptyset$ i $f : A \xrightarrow{1-1} B$, to istnieje $g : B \xrightarrow{na} A$.



77

Jeśli $A \neq \emptyset$ i $f : A \xrightarrow{1-1} B$ to istnieje $g : B \xrightarrow{na} A$.

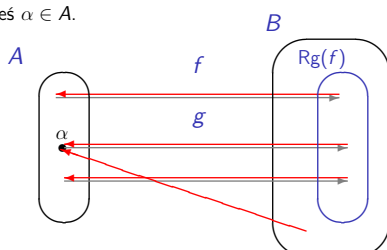
Jest jakiś $\alpha \in A$.



78

Jeśli $A \neq \emptyset$ i $f : A \xrightarrow{1-1} B$ to istnieje $g : B \xrightarrow{na} A$.

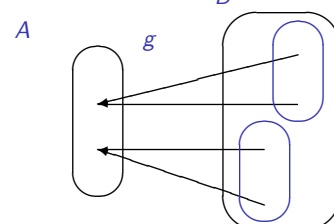
Jest jakiś $\alpha \in A$.



$$g(b) = \text{if } b = f(a) \text{ then } a \text{ else } \alpha$$

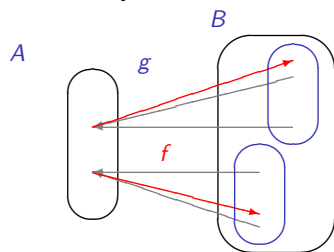
79

Jeśli $g : B \xrightarrow{na} A$ to istnieje $f : A \xrightarrow{1-1} B$.



80

Jeśli $g : B \xrightarrow{\text{na}} A$ to istnieje $f : A \xrightarrow{1-1} B$.



$f(a) = \text{„jakiejkolwiek } b \text{ takie, że } g(b) = a\text{”}$

Operacje na funkcjach

81

82

Obcięcie

Obcięcie funkcji $f : A \rightarrow B$ do podzbioru $C \subseteq A$, to taka funkcja $f|_C : C \rightarrow B$, że $f|_C(a) = f(a)$ dla $a \in C$.
Wtedy $\text{Dom}(f|_C) = C$.

Funkcja odwrotna

Funkcja odwrotna do $f : A \xrightarrow{1-1} B$ to funkcja $f^{-1} : B \rightarrow A$
 $f^{-1}(y) = x \Leftrightarrow x \in A, f(x) = y$.

Jest określona tylko dla funkcji różnowartościowej. Wtedy:

$$f^{-1}(y) = x \Leftrightarrow f(x) = y.$$

Wartość $f^{-1}(y)$ jest określona dla $y \in \text{Rg}(f)$.

Funkcja f^{-1} przyjmuje wszystkie wartości w zbiorze $\text{Dom}(f)$:

$$f^{-1} : \text{Rg}(f) \xrightarrow{\text{na}} \text{Dom}(f).$$

Funkcja odwrotna jest różnowartościowa, bo jeśli $f^{-1}(y) = f^{-1}(z) = x$, to $y = f(x) = z$.

Ostatecznie:

$$f^{-1} : \text{Rg}(f) \xrightarrow[na]{1-1} \text{Dom}(f).$$

83

84

$$f^{-1} : \text{Rg}(f) \xrightarrow[na]{1-1} \text{Dom}(f)$$

Wniosek:

Jeśli $f : A \xrightarrow{1-1} B$, to $f^{-1} : \text{Rg}(f) \xrightarrow[na]{1-1} A$.

(bo wtedy $\text{Dom}(f) = A$)

Jeśli f jest bijekcją z A do B , to f^{-1} jest bijekcją z B do A .

(bo wtedy $\text{Rg}(f) = B$).

Wniosek: Jeśli $A \sim B$, to $B \sim A$.

Złożenie funkcji

Niech $f : A \rightarrow B$ oraz $g : B \rightarrow C$. Złożeniem funkcji f i g nazywamy funkcję $g \circ f : A \rightarrow C$ określoną równaniem

$$(g \circ f)(x) = g(f(x)).$$

Przykład: $(\lambda x. x + 1) \circ (\lambda x. 2x) = \lambda x. 2x + 1$.
 $(\lambda x. 2x) \circ (\lambda x. x + 1) = \lambda x. 2(x + 1)$.

85

86

Własności operacji składania

Niech $f : A \rightarrow B$ oraz $g : B \rightarrow C$. Złożeniem funkcji f i g nazywamy funkcję $g \circ f : A \rightarrow C$ określoną równaniem

$$(g \circ f)(x) = g(f(x)).$$

Fakt

- 1) Jeśli $f : A \rightarrow B$, $g : B \rightarrow C$ i $h : C \rightarrow D$, to $h \circ (g \circ f) = (h \circ g) \circ f$.
- 2) Jeśli $f : A \xrightarrow{1-1} B$, to $f^{-1} \circ f = \text{id}_A$ oraz $f \circ f^{-1} = \text{id}_B$.
- 3) Jeśli $f : A \rightarrow B$, to $f \circ \text{id}_A = f = \text{id}_B \circ f$.

Własności operacji składania

Niech $f : A \rightarrow B$ oraz $g : B \rightarrow C$. Złożeniem funkcji f i g nazywamy funkcję $g \circ f : A \rightarrow C$ określoną równaniem

$$(g \circ f)(x) = g(f(x)).$$

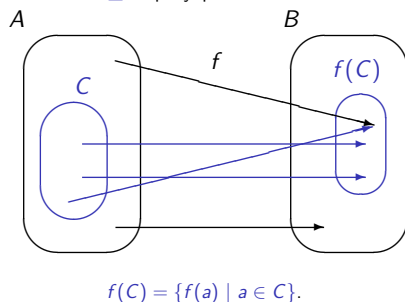
Fakt

- 1) Jeśli $f : A \xrightarrow{1-1} B$ oraz $g : B \xrightarrow{1-1} C$ to $g \circ f : A \xrightarrow{1-1} C$.
- 2) Jeśli $f : A \xrightarrow{\text{na}} B$ oraz $g : B \xrightarrow{\text{na}} C$ to $g \circ f : A \xrightarrow{\text{na}} C$.

87

88

Obraz podzbioru $C \subseteq A$ przy przekształceniu $f : A \rightarrow B$



89

Obraz

Niech $f : A \rightarrow B$. **Obraz** zbioru $C \subseteq A$ przy przekształceniu f to zbiór

$$f(C) = \{b \in B \mid \exists a \in \text{Dom}(f) (a \in C \wedge f(a) = b)\}.$$

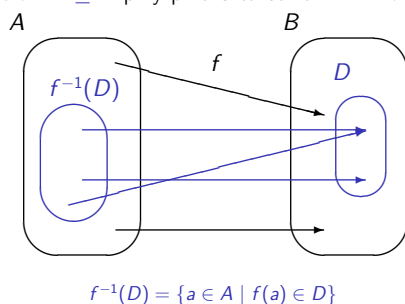
W skrócie:

$$f(C) = \{f(a) \mid a \in C\}.$$

Inne oznaczenia obrazu: $\tilde{f}(C)$, $f[C]$.

90

Przeciwwobraz $D \subseteq B$ przy przekształceniu $f : A \rightarrow B$



91

Przeciwwobraz

Przeciwwobraz zbioru $D \subseteq B$ przy $f : A \rightarrow B$ to zbiór:

$$f^{-1}(D) = \{a \in \text{Dom}(f) \mid f(a) \in D\} \subseteq A.$$

Dla funkcji całkowitej to po prostu:

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

92

Ćwiczenie

Niech $f : P(\mathbb{N}) \times P(\mathbb{N}) \rightarrow P(\mathbb{N})$ będzie taka, że $f(\langle C, D \rangle) = C \cap D$, dla dowolnych $C, D \subseteq \mathbb{N}$.

Znaleźć przeciwwobraz zbioru $\{\mathbb{N}\}$ przy f , czyli $f^{-1}(\{\mathbb{N}\})$.

Czy to pytanie ma sens? Czy $\{\mathbb{N}\} \subseteq P(\mathbb{N})$?

Tak, bo $\mathbb{N} \in P(\mathbb{N})$, więc $\{\mathbb{N}\} \subseteq P(\mathbb{N})$.

$$\begin{aligned} \text{Rozwiązanie: } f^{-1}(\{\mathbb{N}\}) &= \{\langle C, D \rangle \mid f(\langle C, D \rangle) \in \{\mathbb{N}\}\} \\ &= \{\langle C, D \rangle \mid C \cap D = \mathbb{N}\} \\ &= \{\langle \mathbb{N}, \mathbb{N} \rangle\} \end{aligned}$$

93

Ćwiczenie

Niech $f : P(\mathbb{N}) \times P(\mathbb{N}) \rightarrow P(\mathbb{N})$ będzie taka, że $f(\langle C, D \rangle) = C \cap D$, dla dowolnych $C, D \subseteq \mathbb{N}$.

$\mathcal{P}_r$ - zbiór wszystkich liczb parzystych.

Znaleźć obraz $f(P(\mathcal{P}_r) \times P(\mathcal{P}_r))$.

Rozwiązanie: Niech $L = f(P(\mathcal{P}_r) \times P(\mathcal{P}_r))$.

$$\begin{aligned} L &= \{f(\langle C, D \rangle) \mid \langle C, D \rangle \in P(\mathcal{P}_r) \times P(\mathcal{P}_r)\} \\ &= \{C \cap D \mid C \subseteq \mathcal{P}_r \wedge D \subseteq \mathcal{P}_r\} \\ &= P(\mathcal{P}_r) \end{aligned}$$

Istotnie:

Jeśli $C, D \subseteq \mathcal{P}_r$, to $C \cap D \subseteq \mathcal{P}_r$, zatem $L \subseteq P(\mathcal{P}_r)$.

Jeśli $E \subseteq \mathcal{P}_r$, to $E = E \cap E$, zatem $P(\mathcal{P}_r) \subseteq L$.

94

Funkcje wieloargumentowe

Funkcje o dwóch i więcej argumentach traktujemy jak zwykłe funkcje określone na iloczynie kartezjańskim.

Jeśli $f : A \times B \rightarrow C$, to zamiast $f(\langle x, y \rangle)$ piszemy $f(x, y)$.

Na przykład dodawanie liczb naturalnych to funkcja typu

$$\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

No zaraz, ale co to w ogóle jest dodawanie?

Mówimy ciągle o liczbach naturalnych.

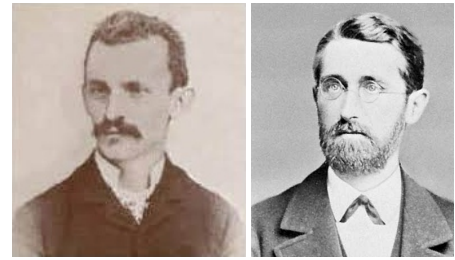
Niby wszyscy wiedzą co to jest.

Ale chyba trzeba to jakoś usystematyzować.

95

96

Liczby naturalne



97

98

Liczby naturalne (Giuseppe Peano, 1889, 1891)

1. Zero jest liczbą naturalną.
2. Każda liczba naturalna n ma *następnik* $s(n)$, który jest liczbą naturalną.
3. Liczby o tych samych następnikach są równe.
4. Zero nie jest następnikiem żadnej liczby naturalnej.
5. Jeśli zero ma pewną własność W , oraz
 - ▶ z tego że jakaś liczba naturalna ma własność W wynika, że jej następnik też ma własność W ,
 to każda liczba naturalna ma własność W .

99

Zbiór (typ) $\mathbb{N}$ liczb naturalnych

- ▶ Elementy typu $\mathbb{N}$:
 1. $0 : \mathbb{N}$.
 2. Jeśli $n : \mathbb{N}$, to także $s(n) : \mathbb{N}$.
(Innych elementów nie ma.)
- ▶ Oznaczenia:
 - ▶ $s(0) = 1, s(1) = 2$, itd.
- ▶ Własności:
 3. Funkcja $s : \mathbb{N} \rightarrow \mathbb{N}$ jest różnowartościowa.
 4. $0 \notin \text{Rg}(s)$.
 5. Jeśli $W(0)$ oraz $\forall n : \mathbb{N} (W(n) \rightarrow W(s(n)))$, to $\forall n : \mathbb{N}. W(n)$.

100

Wnioskowanie przez indukcję

Teza: $\forall n : \mathbb{N}. W(n)$

Należy udowodnić, że:

1. zachodzi $W(0)$;
2. $\forall n : \mathbb{N} (W(n) \rightarrow W(s(n)))$.

101

Przykład dowodu przez indukcję

Twierdzenie: $\forall n : \mathbb{N}. s(n) \neq n$.**Dowód:** Stosujemy schemat indukcji do warunku

$$W(n) : s(n) \neq n.$$

Trzeba sprawdzić, że $W(0)$ oraz $\forall n : \mathbb{N} (W(n) \rightarrow W(s(n)))$.

- (1) Krok bazowy $s(0) \neq 0$ wynika z aksjomatu $\forall m. s(m) \neq 0$.
- (2) Krok indukcyjny: $\forall n : \mathbb{N} (s(n) \neq n \rightarrow s(s(n)) \neq s(n))$.

Rozpatrzmy dowolne $n \in \mathbb{N}$ i założymy, że $s(n) \neq n$.Gdyby $s(s(n)) = s(n)$, to z własności następnika wynika $s(n) = n$, a to nieprawda (z założenia indukcyjnego). Zatem $s(s(n)) \neq s(n)$.

102

Wnioskowanie przez indukcję:

Cel: $\forall n : \mathbb{N} W(n)$

⋮	
Zatem $W(0)$.	(Krok bazowy wykonany)
Niech $n \in \mathbb{N}$	(Cel 1: $W(n) \rightarrow W(s(n))$)
Założmy, że $W(n)$.	(Cel 2: $W(s(n))$)
⋮	
Zatem $W(s(n))$.	(Cel 2 osiągnięty)
Zatem $W(n) \rightarrow W(s(n))$.	(Cel 1 osiągnięty)
Zatem $\forall n : \mathbb{N} (W(n) \rightarrow W(s(n)))$.	(Krok indukcyjny wykonany)
Zatem $\forall n : \mathbb{N} W(n)$	

103

Definiowanie przez indukcję: przykład

Dla dowolnego $n \in \mathbb{N}$ określamy odcinek początkowy $\bar{n}$ wyznaczony przez n :

$$\bar{0} = \emptyset \quad \overline{s(n)} = \bar{n} \cup \{n\}.$$

Co jest sumą wszystkich takich odcinków?

Coś takiego: $\bar{0} \cup \bar{1} \cup \bar{2} \dots$?Lepiej tak to napisać: $\bigcup_{n \in \mathbb{N}} \bar{n}$. Albo tak: $\bigcup \{\bar{n} \mid n \in \mathbb{N}\}$.

Teraz widać po co nam potrzebne sumy uogólnione.

104

Dodawanie (funkcja typu $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$):

$$\begin{aligned} 0 + n &= n; \\ s(m) + n &= s(m + n). \end{aligned}$$

Mnożenie:

$$\begin{aligned} 0 \cdot n &= 0; \\ s(m) \cdot n &= m \cdot n + n. \end{aligned}$$

105

Schemat definiowania przez indukcję

Definicja funkcji $f : \mathbb{N} \times D_1 \times \dots \times D_k \rightarrow E$ przez indukcję ze względu na pierwszy argument:

$$\begin{aligned} f(0, d_1, \dots, d_k) &= g(d_1, \dots, d_k); \\ f(s(m), d_1, \dots, d_k) &= h(m, d_1, \dots, d_k, f(m, d_1, \dots, d_k)). \end{aligned}$$

Na przykład dodawanie ($k = 1$, $D_1 = \mathbb{N}$, $E = \mathbb{N}$):

$$\begin{aligned} 0 + n &= n; \\ s(m) + n &= s(m + n). \end{aligned}$$

Tutaj $g(n) = n$ oraz $h(m, n, k) = s(k)$.

Używając tego schematu definiujemy mnożenie, potęgowanie...

107

Dowodzenie przez indukcję

W podobny sposób dowodzimy wielu innych własności liczb naturalnych. Na przykład

- ▶ że dodawanie jest przemienne;
- ▶ że mnożenie jest łączne i przemienne, itp.

Z przemienności dodawania wynika m.in., że

$$s(n) = s(0 + n) = s(0) + n = n + s(0).$$

A więc $s(n) = n + 1$.

Podobnie, $n = 0 + n = n + 0$. A więc $n + 0 = n$.

109

Nierówności liczb naturalnych

Definicja:

- napis $m \leq n$ oznacza, że $m + k = n$, dla pewnego k ;
- napis $m < n$ oznacza, że $m \leq n$, ale $m \neq n$.

Wniosek:

Jeśli $m < n$, to oczywiście $m + k = n$, dla pewnego $k \neq 0$.

I na odwrót (ale to wymaga dowodu przez indukcję).

111

$$\begin{aligned} 0 + n &= n & 0 \cdot n &= 0 \\ s(m) + n &= s(m + n) & s(m) \cdot n &= m \cdot n + n \end{aligned}$$

$$\begin{aligned} 2 \cdot 2 &= 1 \cdot 2 + 2 = (0 \cdot 2 + 2) + 2 = \\ (0 + 2) + 2 &= 2 + 2 = s(1 + 2) = \\ s(s(0 + 2)) &= s(s(2)) = s(s(s(0))) = 4. \end{aligned}$$

106

Dowodzenie przez indukcję

$$0 + n = n \quad s(m) + n = s(m + n)$$

Fakt

Dodawanie jest łączne: dla dowolnych liczb $m, k, l \in \mathbb{N}$ zachodzi równość $m + (k + l) = (m + k) + l$.

Dowód: Indukcja ze względu na m .

Udowodnimy, że każda liczba $m : \mathbb{N}$ ma własność

$$\forall k, l : \mathbb{N}. m + (k + l) = (m + k) + l.$$

Po pierwsze, $0 + (k + l) = (k + l) = (0 + k) + l$.

Po drugie z warunku $m + (k + l) = (m + k) + l$ wynika

$$s(m) + (k + l) = s(m + (k + l)) = s((m + k) + l) = s(m + k) + l = (s(m) + k) + l \quad \text{i dobrze.} \quad \square$$

108

Przykład

Definiujemy ciąg zbiorów $\{A_n\}_{n \in \mathbb{N}}$:

$$A_0 = \{0, 2\}, \quad A_{n+1} = \{x + y \mid x, y \in A_n\}.$$

To też szczególny przypadek schematu

$$\begin{aligned} f(0, d_1, \dots, d_k) &= g(d_1, \dots, d_k); \\ f(s(m), d_1, \dots, d_k) &= h(m, d_1, \dots, d_k, f(m, d_1, \dots, d_k)). \end{aligned}$$

$$(k = 0, \quad f : \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N}), \quad h(m, X) = \{x + y \mid x, y \in X\}).$$

Ćwiczenie:

$$\bigcup_{n \in \mathbb{N}} A_n = \text{Parzyste}.$$

110

Własności nierówności

Trzy łatwe ćwiczenia:

(1) Dla dowolnych $m, n \in \mathbb{N}$:

$$m \leq n, \text{ wtedy i tylko wtedy, gdy } m < s(n).$$

(2) Dla dowolnych $m, n \in \mathbb{N}$:

$$m \leq n \text{ wtedy i tylko wtedy, gdy } s(m) \leq s(n).$$

Przypomnijmy, że $\bar{0} = \emptyset \quad \overline{s(n)} = \bar{n} \cup \{n\}$.

(3) Dla dowolnego $n \in \mathbb{N}$:

$$\bar{n} = \{k \in \mathbb{N} \mid k < n\}.$$

112

- Zwrotność: $\forall n \in \mathbb{N}. n \leq n$.
- Przechodność: $\forall nm \in \mathbb{N}. n \leq m \wedge m \leq k \rightarrow n \leq k$.
- Antysymetria: $\forall nm \in \mathbb{N}. n \leq m \wedge m \leq n \rightarrow n = m$.
- Spójność: $\forall nm \in \mathbb{N}. n \leq m \vee m \leq n$.

Mówimy, że relacja $\leq$ jest *liniowym porządkiem*.

113

Wróćmy do funkcji

Ćwiczenie

Ćwiczenie: Niech $\varphi : P(A \times B) \rightarrow P(A)^B$, gdzie:

$$\varphi(\Delta)(b) = \{a \in A \mid \langle a, b \rangle \in \Delta\},$$

dla dowolnego $\Delta \in P(A \times B)$ i dowolnego $b \in B$.

Pokazać, że ta funkcja jest na $P(A)^B$.

Rozwiązanie: Każdy element zbioru $P(A)^B$ ma być wartością funkcji φ . Elementy zbioru $P(A)^B$ to funkcje z B do $P(A)$.

Rozpatrzmy więc dowolną funkcję $F : B \rightarrow P(A)$.

Szukamy takiego zbioru Δ , że $\varphi(\Delta) = F$.

Czyli takiego, że $\varphi(\Delta)(b) = F(b)$, dla dowolnego $b \in B$.

Inaczej, $\{a \in A \mid \langle a, b \rangle \in \Delta\} = F(b)$.

Albo tak: $\langle a, b \rangle \in \Delta \Leftrightarrow a \in F(b)$.

No to weźmy $\Delta = \{\langle a, b \rangle \mid a \in F(b)\}$. Wtedy dla $b \in B$:

$$\varphi(\Delta)(b) = \{a \in A \mid \langle a, b \rangle \in \Delta\} = \{a \in A \mid a \in F(b)\} = F(b).$$

117

Równoliczność zbiorów

Definicja

Zbiory A i B są *równoliczne* (tej samej *mocy*), gdy istnieje bijekcja $f : A \xrightarrow[\text{na}]{1-1} B$. Piszemy $A \sim B$ lub $\overline{A} = \overline{B}$.

Z poprzedniego ćwiczenia wynika, że $P(A \times B) \sim P(A)^B$.

119

- Zwrotność: $\forall n \in \mathbb{N}. n \leq n$.
- Przechodność: $\forall nm \in \mathbb{N}. n \leq m \wedge m \leq k \rightarrow n \leq k$.
- Antysymetria: $\forall nm \in \mathbb{N}. n \leq m \wedge m \leq n \rightarrow n = m$.
- Spójność: $\forall nm \in \mathbb{N}. n \leq m \vee m \leq n$.

Dowody opuszczamy z braku czasu.

114

Ćwiczenie: Niech $\varphi : P(A \times B) \rightarrow P(A)^B$, gdzie:

$$\varphi(\Delta)(b) = \{a \in A \mid \langle a, b \rangle \in \Delta\},$$

dla dowolnego $\Delta \in P(A \times B)$ i dowolnego $b \in B$.

Pokazać, że ta funkcja jest różnowartościowa.

Rozwiązanie: Dla $\Delta \neq \Sigma$ ma zachodzić $\varphi(\Delta) \neq \varphi(\Sigma)$.

Niech więc $\Delta \neq \Sigma$. Co to znaczy?

Że istnieje para $\langle x, y \rangle$ należąca do $\Delta - \Sigma$, lub istnieje para $\langle x, y \rangle$ należąca do $\Sigma - \Delta$. Przypuśćmy, że zachodzi pierwszy przypadek (drugi jest podobny).

Mamy pokazać, że $\varphi(\Delta) \neq \varphi(\Sigma)$. Co to znaczy?

Trzeba wskazać takie b , żeby $\varphi(\Delta)(b) \neq \varphi(\Sigma)(b)$.

Wystarczy wskazać takie a, b , że $\langle a, b \rangle \in \Delta$, ale $\langle a, b \rangle \notin \Sigma$.

Można przyjąć $a = x$ i $b = y$.

116

Równoliczność

Proste własności

Dla dowolnych A, B, C :

- $A \sim A$;
- jeśli $A \sim B$, to $B \sim A$;
- jeśli $A \sim B$ i $B \sim C$, to $A \sim C$;
- jeśli $A \sim \emptyset$, to $A = \emptyset$.

120

Zbiory skończone

Odcinek początkowy wyznaczony przez n , to zbiór $\bar{n} = \{m : \mathbb{N} \mid m < n\}$, ozn. też przez $\mathcal{O}(n)$. (Czasem utożsamia się liczbę n z odcinkiem $\bar{n}$.)

Definicja: Zbiór jest *skończony* wtedy i tylko wtedy, gdy jest równoliczny z pewnym odcinkiem postaci $\bar{n}$.

Pytanie: Czy tylko z jednym takim?

121

122

Lemat (ćwiczenie)

Niech $a \notin A$ i $b \notin B$. Wówczas:

- ▶ Injekcja $f : A \cup \{a\} \xrightarrow{1-1} B \cup \{b\}$ istnieje wtedy i tylko wtedy, gdy istnieje injekcja $g : A \xrightarrow{1-1} B$.
- ▶ Dla $B \neq \emptyset$, surjekcja $f : A \cup \{a\} \xrightarrow{na} B \cup \{b\}$ istnieje wtedy i tylko wtedy, gdy istnieje surjekcja $g : A \xrightarrow{na} B$.
- ▶ $A \cup \{a\} \sim B \cup \{b\}$ wtedy i tylko wtedy, gdy $A \sim B$.

123

124

Fakt

1. Jeśli istnieje injekcja $f : \bar{m} \xrightarrow{1-1} \bar{n}$, to $m \leq n$.
2. Jeśli istnieje surjekcja $f : \bar{m} \xrightarrow{na} \bar{n}$, to $m \geq n$.

Wniosek

Dla każdych $m, n \in \mathbb{N}$, jeśli $\bar{m} \sim \bar{n}$ to $m = n$.

Wniosek

Jeśli $A \sim \bar{n}$ i $A \sim \bar{m}$, to $m = n$.

Morał: Zbiór A jest skończony wtedy i tylko wtedy, gdy jest równoliczny z *dokładnie jednym* odcinkiem postaci $\bar{n}$.

Mówimy, że zbiór A jest n -elementowy i piszemy $\bar{\bar{A}} = n$.

125

126

Zasada szufladkowa

Wniosek

Jeśli zbiór A jest n -elementowy, zbiór B jest m -elementowy, oraz $n > m$, to nie istnieje funkcja różnowartościowa z A do B .

Wniosek

Jeśli 6 gołębi siedzi w 5 szufladach, to przynajmniej w jednej szufladzie są dwa.

Wniosek

Jeśli ze zbioru $\{0, 1, \dots, 13\}$ wybierzemy 8 różnych liczb, to dwie z nich różnią się o 7.

Dowód: Bo jest tylko 7 możliwych reszt modulo 7. □

127

128

Fakt

1. Jeśli istnieje injekcja $f : \bar{m} \xrightarrow{1-1} \bar{n}$, to $m \leq n$.
2. Jeśli istnieje surjekcja $f : \bar{m} \xrightarrow{na} \bar{n}$, to $m \geq n$.

Dowód jest przez indukcję ze względu na m .

Szczegóły opuszczamy.

Fakt

1. Jeśli istnieje injekcja $f : \bar{m} \xrightarrow{1-1} \bar{n}$, to $m \leq n$.
2. Jeśli istnieje surjekcja $f : \bar{m} \xrightarrow{na} \bar{n}$, to $m \geq n$.

Wniosek

Niech zbiór A ma m elementów, a zbiór B ma n elementów.

1. Jeśli istnieje injekcja $f : A \xrightarrow{1-1} B$, to $m \leq n$.
2. Jeśli istnieje surjekcja $f : A \xrightarrow{na} B$, to $m \geq n$.

Fakt

1. Jeśli istnieje injekcja $f : \bar{m} \xrightarrow{1-1} \bar{n}$, to $m \leq n$.
2. Jeśli istnieje surjekcja $f : \bar{m} \xrightarrow{na} \bar{n}$, to $m \geq n$.

Wniosek

Nie istnieje funkcja różnowartościowa $f : \overline{s(n)} \xrightarrow{1-1} \bar{n}$.

Wniosek

Nie istnieje funkcja różnowartościowa $f : \mathbb{N} \xrightarrow{1-1} \bar{n}$. Zatem zbiór liczb naturalnych $\mathbb{N}$ jest nieskończony.

Dowód: W przeciwnym razie $f|_{\overline{s(n)}} : \overline{s(n)} \xrightarrow{1-1} \bar{n}$. □

Własności zbiorów skończonych

- Zbiór A jest skończony wtw, gdy $A \cup \{a\}$ jest skończony.
- Każdy podzbiór zbioru skończonego jest skończony.
- Jeśli A nieskończony, B skończony, to $A - B \neq \emptyset$.
- Jeśli A jest skończony i $f : B \xrightarrow{1-1} A$, to B jest skończony.
- Jeśli A jest skończony i $f : A \xrightarrow{na} B$, to B jest skończony.
- Jeśli A, B skończone to $A \oplus B, A \cup B, A \times B$ skończone.

Bo jeśli $a \notin A$, to $A \sim \bar{n}$ wtedy i tylko wtedy, gdy $A \cup \{a\} \sim \overline{s(n)}$.

Łatwa indukcja z pomocą poprzedniego punktu.

Bo inaczej $A \subseteq B$ i A skończony.

Bo wtedy $B \sim \text{Rg}(f) \subseteq A$.

Bo wtedy istnieje $g : B \xrightarrow{1-1} A$.

Indukcja (ćwiczenie).

129

Twierdzenie

Jeśli A jest skończony, oraz $f : A \rightarrow A$, to:

f jest różnowartościowa $\Leftrightarrow f$ jest na A .

Próba dowodu ($\Rightarrow$): Indukcja ze względu na moc A .

Dowodzimy, że każda liczba $n : \mathbb{N}$ spełnia warunek:

Dla każdego A i każdej funkcji $f : A \rightarrow A$, jeśli $\bar{A} = n$, to:

f jest różnowartościowa $\Rightarrow f$ jest na A .

Jeśli $A = \emptyset$, to funkcja f jest pusta i teza jest oczywista.

Jeśli A ma $s(n)$ elementów, to $A = A' \cup \{a\}$, gdzie $a \notin A'$ oraz A' ma n elementów.

Chcemy więc zastosować założenie indukcyjne do zbioru A' .

Funkcja $f|_{A'} : A' \rightarrow A$ jest różnowartościowa... ale to nie

jest funkcja z A' do A' i założenie indukcyjne nie pasuje!

Co robić? Wzmocnić tezę!

131

Twierdzenie

Jeśli zbiory skończone A i B są równoliczne oraz $f : A \rightarrow B$, to:

f jest różnowartościowa $\Leftrightarrow f$ jest na B .

Dowód: ($\Rightarrow$) Indukcja ze względu na liczbę elementów A .

Jeśli $A = \emptyset$, to funkcja f jest pusta i teza jest oczywista.

Jeśli A ma $s(n)$ elementów, to $A = A' \cup \{a\}$, gdzie $a \notin A'$ oraz A' ma n elementów.

Wtedy także $B = B' \cup \{f(a)\}$, gdzie $f(a) \notin B'$ oraz $\bar{B'} = n$.

Funkcja $f|_{A'} : A' \rightarrow B'$ jest różnowartościowa i z założenia indukcyjnego jest na B' .

Zatem „cała” funkcja f jest na B .

133

Zbiory nieskończone

Jeszcze o zbiorach skończonych

Udowodnimy silniejsze twierdzenie.

Twierdzenie

Jeśli zbiory skończone A i B są równoliczne oraz $f : A \rightarrow B$, to:

f jest różnowartościowa $\Leftrightarrow f$ jest na B .

Wniosek

Jeśli A jest skończony oraz $f : A \rightarrow A$, to:

f jest różnowartościowa $\Leftrightarrow f$ jest na A .

130

132

Twierdzenie

Jeśli zbiory skończone A i B są równoliczne oraz $f : A \rightarrow B$, to:

f jest różnowartościowa $\Leftrightarrow f$ jest na B .

Dowód: ($\Leftarrow$) Indukcja ze względu na liczbę elementów A .

Jeśli $A = \emptyset$, to funkcja f jest pusta i teza jest oczywista.

Jeśli $\bar{A} = s(n)$, to $A = A' \cup \{a\}$, $B = B' \cup \{f(a)\}$, gdzie $a \notin A'$, $f(a) \notin B'$, oraz $\bar{A'} = \bar{B'} = n$.

Zauważmy, że $f|_{A'} : A' \rightarrow B'$, tj. funkcja $f|_{A'}$ nie przyjmuje wartości $f(a)$. Inaczej byłaby to surjekcja ze zbioru n -elementowego do zbioru $s(n)$ -elementowego.

Ponadto funkcja $f|_{A'} : A' \rightarrow B'$ jest na B' , więc z założenia indukcyjnego jest różnowartościowa.

Zatem funkcja f jest też różnowartościowa.

134

Motywujący przykład:

Niech

$\mathbb{P}r = \{n \in \mathbb{N} \mid n \text{ jest parzyste}\}$,

$\mathbb{N}p = \{n \in \mathbb{N} \mid n \text{ jest nieparzyste}\}$.

Zbiory $\mathbb{P}r$ i $\mathbb{N}p$ są równoliczne, bo mamy funkcję

$$\lambda n. n + 1 : \mathbb{P}r \xrightarrow[na]{1-1} \mathbb{N}p.$$

Ale także zbiory $\mathbb{P}r$ i $\mathbb{N}$ są równoliczne, bo

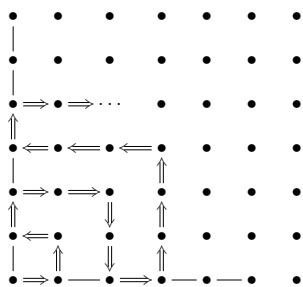
$$\lambda n. 2n : \mathbb{N} \xrightarrow[na]{1-1} \mathbb{P}r.$$

Zatem „połowa” może być równoliczna z całością.

135

136

Przykład: Zbiory $\mathbb{N} \times \mathbb{N}$ i $\mathbb{N}$ są równoliczne.



137

Funkcje pary z $\mathbb{N} \times \mathbb{N}$ do $\mathbb{N}$

► $t(m, n) = 2^m 3^n$ (różnowartościowa)

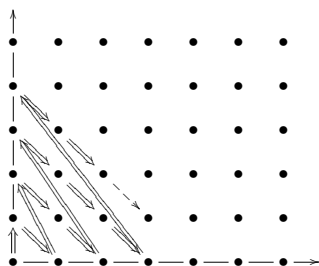
► $\bar{u}(m, n) = 2^m(2n+1)$ (różnowartościowa)

► $u(m, n) = 2^m(2n+1) - 1$ (bijekcja)

► $v(m, n) = \frac{(m+n)(m+n+1)}{2} + m$ (bijekcja)

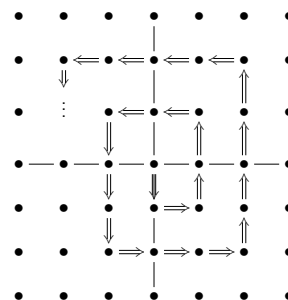
138

Przykład: $v(m, n) = \frac{(m+n)(m+n+1)}{2} + m$



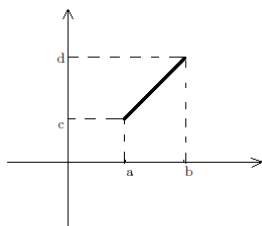
139

Przykład: Zbiory $\mathbb{Z} \times \mathbb{Z}$ i $\mathbb{N}$ są równoliczne.



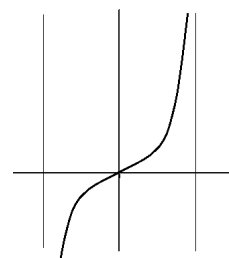
140

Przykład: Przedziały otwarte (a, b) i (c, d) są równoliczne, bo jeśli $f(x) = \frac{d-c}{b-a} \cdot x + \frac{bc-ad}{b-a}$, to $f : (a, b) \xrightarrow{1-1} (c, d)$.



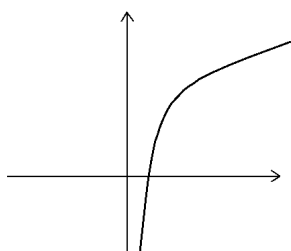
141

Przykład: Przedział $(-\frac{\pi}{2}, \frac{\pi}{2})$ (i każdy inny przedział otwarty) jest równoliczny z $\mathbb{R}$ (funkcja tangens).



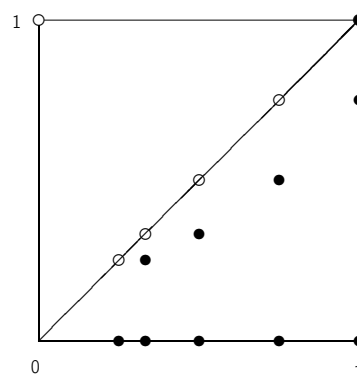
142

Przykład: Półprosta otwarta jest równoliczna z prostą (funkcja logarytm).



143

Przedziały $(0, 1]$ i $(0, 1)$ są równoliczne



144

Przykład: Przedziały $(0, 1]$ i $(0, 1)$ są równoliczne:

$$f(x) = \begin{cases} \frac{1}{n+1}, & \text{jeśli } x = \frac{1}{n}, \text{ dla pewnego } n \in \mathbb{N}; \\ x, & \text{w przeciwnym przypadku.} \end{cases}$$

Wtedy $f : (0, 1] \xrightarrow[\text{na}]{1-1} (0, 1)$.

145

Przykład:

Zbiór $P(\mathbb{N})$ jest równoliczny z produktem $P(\mathbb{N}) \times P(\mathbb{N})$.

Dowód: Już wiemy, że $\mathbb{N} \sim \mathcal{P}_r \sim \mathcal{N}_p$.

Z tego łatwo wynika, że $P(\mathbb{N}) \sim P(\mathcal{P}_r) \sim P(\mathcal{N}_p)$.

Ale ponieważ $\mathbb{N} = \mathcal{P}_r \cup \mathcal{N}_p$, więc mamy bijekcję:

$$F : P(\mathbb{N}) \xrightarrow[\text{na}]{1-1} P(\mathcal{P}_r) \times P(\mathcal{N}_p)$$

określoną tak: $F(A) = (A \cap \mathcal{P}_r, A \cap \mathcal{N}_p)$, dla $A \subseteq \mathbb{N}$.

Stąd $P(\mathbb{N}) \sim P(\mathcal{P}_r) \times P(\mathcal{N}_p) \sim P(\mathbb{N}) \times P(\mathbb{N})$.

147

Nie wszystkie zbiory nieskończone są równoliczne

Twierdzenie: Zbiór $\{0, 1\}^{\mathbb{N}}$ wszystkich nieskończonych ciągów zerojedynkowych nie jest równoliczny z $\mathbb{N}$.

Dowód: Przypuśćmy, że wszystkie ciągi zerojedynkowe można ustawić w ciąg nieskończony, np. tak:

$$\begin{aligned} r_0 &= 0110010101101\dots \\ r_1 &= 0101000001001\dots \\ r_2 &= 1000011101000\dots \\ r_3 &= 1101010110001\dots \end{aligned}$$

Ale ciąg 1010... na pewno tutaj nie ma.

□

149

Zbiory przeliczalne i nieprzelicalne

- Zbiór jest **przeliczalny**, gdy jest skończony lub równoliczny z $\mathbb{N}$.
- W przeciwnym razie zbiór jest **nieprzeliczalny**.

151

Proste obserwacje

- Jeśli $A \sim B$, to $P(A) \sim P(B)$.
- Jeśli $A \sim B$ i $C \sim D$, to $A \times C \sim B \times D$.

146

Przykład: $\overline{P(\mathbb{N})} = \overline{\{0, 1\}^{\mathbb{N}}} = \overline{\mathbb{N}} \rightarrow \{0, 1\}$.

Dowód: Bijekcja $F : P(\mathbb{N}) \xrightarrow[\text{na}]{1-1} (\mathbb{N} \rightarrow \{0, 1\})$ może być określona tak: $F(A) = \lambda n. \mathbb{N}. \text{if } n \in A \text{ then } 1 \text{ else } 0$.

Uwaga: Funkcja $F(A)$ to **funkcja charakterystyczna** zbioru A . Bywa oznaczana symbolem χ_A .

148

Nie wszystkie zbiory nieskończone są równoliczne

Twierdzenie: Zbiór $P(\mathbb{N})$ wszystkich podzbiorów zbioru $\mathbb{N}$ nie jest równoliczny z $\mathbb{N}$.

Dowód: Przypuśćmy, że wszystkie podzbiory $\mathbb{N}$ można ustawić w ciąg nieskończony, np. tak:

Zbiór	Funkcja charakterystyczna
$A_0 = \{1, 2, 5, 7, 9, 10, 12, \dots\}$	0110010101101...
$A_1 = \{1, 3, 9, 12, \dots\}$	0101000001001...
$A_2 = \{0, 5, 6, 7, 9, \dots\}$	1000011101000...
$A_3 = \{0, 1, 3, 5, 7, 8, 12, \dots\}$	1101010110001...
Jakiego zbioru brak? $B = \{0, 2, \dots\}$	$\chi_B = 1010\dots$
$n \in B \Leftrightarrow n \notin A_n$	

□

150

Nieprzeliczalność

Twierdzenie

Zbiór $P(\mathbb{N})$ nie jest równoliczny z $\mathbb{N}$.

Dowód: Przypuśćmy, że $P(\mathbb{N}) = \{A_n \mid n \in \mathbb{N}\}$. Niech

$$B = \{n \mid n \notin A_n\}.$$

Wtedy $B = A_k$, dla pewnego k .

Jeśli $k \in B$, to $k \notin A_k$, więc $k \notin B$, sprzeczność.

Jeśli $k \notin B$, to $\neg(k \notin A_k)$, czyli $k \in A_k = B$, sprzeczność. □

152

Twierdzenie (Cantora)

Dla dowolnego zbioru A zachodzi $\bar{A} \neq \overline{\bar{A}}$.

Dowód: Przypuśćmy, że $F : A \xrightarrow{1-1}_{na} P(A)$. Niech

$$B = \{x \in A \mid x \notin F(x)\}.$$

Istnieje takie $b \in A$, że $F(b) = B$.

Jeśli $b \in B$, to $b \notin F(b) = B$, sprzeczność.

Jeśli $b \notin B$, to $b \in F(b)$, sprzeczność. $\square$

153

Liczby kardynalne

Umowa: Zbiорom przypisujemy *liczby kardynalne*.

Liczbę kardynalną (moc) zbioru A oznaczamy przez $\bar{A}$.
Robimy to tak, aby zachodziła równoważność:

$$\bar{A} = \bar{B} \quad \text{wtedy i tylko wtedy, gdy} \quad A \sim B.$$

- ▶ Liczby kardynalne zbiorów skończonych to liczby naturalne.
- ▶ Moc zbioru $\mathbb{N}$ oznaczamy symbolem $\aleph_0$ („alef zero”).
- ▶ Moc zbioru $\mathbb{R}$ oznaczamy symbolem $\mathfrak{c}$ („continuum”).

Z poprzedniego wyniku, że $\overline{P(\mathbb{N})} \neq \aleph_0$.

Pokażemy później, że $\overline{P(\mathbb{N})} = \mathfrak{c}$.

155

Przeliczanie przeliczalnego

Elementy niepustych zbiorów przeliczalnych można numerować:

$$A = \{a_n \mid n \in \mathbb{N}\}$$

Nieskończone bez powtórzeń, skończone z powtórzeniami.

Inaczej:

Niepusty zbiór A jest przeliczalny wtedy i tylko wtedy, gdy istnieje surjekcja $g : \mathbb{N} \xrightarrow{na} A$.

157

Twierdzenie

Suma przeliczalnej rodziny zbiorów przeliczalnych jest przeliczalna.

Dowód: Niech $\mathcal{A}$ będzie przeliczalną rodziną zbiorów przeliczalnych. Załóżmy, że $\mathcal{A} \neq \emptyset$ oraz $\emptyset \notin \mathcal{A}$.

Elementy rodziny $\mathcal{A}$ można ponumerować: $\mathcal{A} = \{X_n \mid n \in \mathbb{N}\}$.

Elementy zbiorów X_n też można: $X_n = \{a_n^k \mid k \in \mathbb{N}\}$

Niech $G(n, k) = a_n^k$ dla $n, k \in \mathbb{N}$.

Funkcja $G : \mathbb{N} \times \mathbb{N} \rightarrow \bigcup_{n \in \mathbb{N}} X_n$ jest na $\bigcup_{n \in \mathbb{N}} X_n$.

Zatem $\bigcup_{n \in \mathbb{N}} X_n = \bigcup \mathcal{A}$ jest zbiorem przeliczalnym. $\square$

159

Fryzjerowi polecono golić tych, którzy się sami nie golą.

$$F : A \rightarrow P(A)$$

$$F(x) = \{y \mid x \text{ goli } y\}$$

To polecenie jest niewykonalne. Nie istnieje takie b , że:

$$\forall x (b \text{ goli } x \Leftrightarrow x \text{ nie goli } x)$$

$$\forall x (x \in F(b) \Leftrightarrow x \notin F(x))$$

$$b \in F(b) \Leftrightarrow b \notin F(b)$$

154

Zbiory przeliczalne

- ▶ Zbiór jest *przeliczalny*, gdy jest skończony lub mocy $\aleph_0$ (czyli równoliczny z $\mathbb{N}$).
- ▶ W przeciwnym razie zbiór jest *nieprzeliczalny*.

Przykłady:

- ▶ Zbiory $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \emptyset, \{0, 1, 6\}$ są przeliczalne.
- ▶ Zbiory $\mathbb{R}, P(\mathbb{N}), \mathbb{R}^2$ (płaszczyzna), $P(\mathbb{R}), \mathbb{N}^{\mathbb{R}}$ są nieprzeliczalne.

Uwaga: nie wszystkie zbiory nieprzeliczalne są równoliczne!

156

Własności zbiorów przeliczalnych

Fakt

- ▶ Podzbiór zbioru przeliczalnego jest przeliczalny.
- ▶ Jeśli zbiory A i B są przeliczalne, to zbiory $A \oplus B$, $A \cup B$ i $A \times B$ są przeliczalne.

Dowód: Ćwiczenie. (Podobne do dowodu, że $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ i $\mathbb{P}r \cup \mathbb{N}p \sim \mathbb{N}$. Trzeba wszystko ponumerować.) $\square$

158

Przykłady zbiorów przeliczalnych

- ▶ Zbiór $\mathbb{N} \times \mathbb{N}$ jest przeliczalny.
- ▶ Zbiór $\mathbb{Z}$ wszystkich liczb całkowitych jest przeliczalny.
- ▶ Zbiór $\mathbb{Q}$ wszystkich liczb wymiernych jest przeliczalny.
- ▶ Zbiór wszystkich punktów płaszczyzny o współrzędnych wymiernych jest przeliczalny.
- ▶ Zbiór skończonych ciągów (krotek) liczb naturalnych jest przeliczalny.

Bo to produkt zbiorów przeliczalnych.

Bo $f : \mathbb{N} \times \mathbb{N} \xrightarrow{na} \mathbb{Z}$, gdzie $f(m, n) = m - n$.

Bo $f : \mathbb{Z} \times (\mathbb{Z} - \{0\}) \xrightarrow{na} \mathbb{Q}$, gdzie $f(m, n) = \frac{m}{n}$.

Bo to po prostu $\mathbb{Q} \times \mathbb{Q}$.

Bo to w istocie przeliczalna suma $\bigcup \{\mathbb{N}^k \mid k \in \mathbb{N}\}$.

160

Jeszcze jeden przykład

Definicja

Liczby *algebraiczne* to pierwiastki rzeczywiste wielomianów o współczynnikach wymiernych.

Fakt

Zbiór wszystkich liczb algebraicznych jest przeliczalny.

Dowód: Wielomian jest wyznaczony przez skończony ciąg swoich współczynników. Zbiór wielomianów $\mathbb{Q}[x]$ jest więc równoliczny ze zbiorem skończonych ciągów (krotek) liczb wymiernych i też przeliczalny.

Wielomian ma skończenie wiele pierwiastków, więc zbiór liczb algebraicznych to przeliczalna suma zbiorów skończonych. $\square$

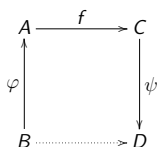
161

Poprawność definicji $\leq$

Lemat Jeżeli $\bar{A} = \bar{B} = m$ i $\bar{C} = \bar{D} = n$ oraz istnieje injekcja $f : A \xrightarrow{1-1} C$, to istnieje też injekcja $g : B \xrightarrow{1-1} D$.

Dowód: Istnieją bijekcje $\varphi : B \xrightarrow[na]{1-1} A$ oraz $\psi : C \xrightarrow[na]{1-1} D$.

Zatem $\psi \circ f \circ \varphi : B \xrightarrow{1-1} D$.



163

Najmniejsza moc nieskończona to $\aleph_0$.

Twierdzenie

Zbiór A jest nieskończony wtedy i tylko wtedy, gdy ma podzbiór mocy $\aleph_0$.

Szkic dowodu ($\Rightarrow$):

Zbiór nieskończony jest niepusty, więc jest jakieś $a_0 \in A$.

Zbiór $A - \{a_0\}$ też jest niepusty, więc jest jakieś $a_1 \in A - \{a_0\}$.

I tak dalej: mamy ciąg elementów a_n o własności

$$a_n \in A - \{a_0, \dots, a_{n-1}\}.$$

Te elementy tworzą zbiór mocy $\aleph_0$.

165

Wniosek

Zbiór A jest nieskończony wtedy i tylko wtedy, gdy jest równoliczny z pewnym swoim podzbiorem właściwym.

Dowód: ($\Leftarrow$) Wtedy istnieje funkcja $f : A \xrightarrow{1-1} A$, która nie jest na A . Zatem A nie jest skończony. $\square$

167

Nierówności

Mówimy, że moc zbioru A jest *mniejsza lub równa* mocy zbioru B (i piszemy $\bar{A} \leq \bar{B}$), wtedy i tylko wtedy, gdy istnieje injekcja $f : A \xrightarrow{1-1} B$.

Jeżeli $\bar{A} \leq \bar{B}$ ale zbiory A i B nie są równoliczne, to piszemy $\bar{A} < \bar{B}$ i mówimy, że zbiór A jest *mniejszy* niż zbiór B .

Przykład: $\bar{\mathbb{N}} < \overline{\mathbb{P}(\mathbb{N})}$.

162

Nierówności

► Jeśli $A \subseteq B$, to $\bar{A} \leq \bar{B}$.

► Dla dowolnej liczby naturalnej n zachodzi $n < \aleph_0$.

► Dla dowolnego zbioru A zachodzi $\bar{A} < \overline{\mathbb{P}(A)}$.

Istotnie, z jednej strony $\lambda a. \{a\} : A \xrightarrow{1-1} \mathbb{P}(A)$, a z drugiej strony mamy twierdzenie Cantora.

164

Wniosek

Zbiór A jest nieskończony wtedy i tylko wtedy, gdy jest równoliczny z pewnym swoim podzbiorem właściwym.

Dowód: ($\Rightarrow$) Zbiór A ma podzbiór B mocy $\aleph_0$. Mamy wtedy $B = \{f(n) \mid n \in \mathbb{N}\}$, gdzie $f : \mathbb{N} \xrightarrow[na]{1-1} B$.

Możemy określić $g : A \xrightarrow{1-1} A$:

$$g(x) = \begin{cases} f(n+1), & \text{jeśli } x = f(n) \in B; \\ x, & \text{w przeciwnym przypadku.} \end{cases}$$

Funkcja g nie jest na A , bo $f(0) \notin \text{Rg}(g)$.

Zatem $A \sim \text{Rg}(g) \subsetneq A$. $\square$

166

Nierówności

Fakt

Dla dowolnych niepustych zbiorów A, B następujące warunki są równoważne:

- 1) $\bar{A} \leq \bar{B}$;
- 2) Istnieje $g : B \xrightarrow{na} A$;
- 3) Zbiór A jest równoliczny z pewnym podzbiorem zbioru B .

168

Fakt

Dla dowolnych zbiorów A, B, C :

- ▶ $\overline{\overline{A}} \leq \overline{A}$;
- ▶ Jeśli $\overline{\overline{A}} \leq \overline{\overline{B}}$ i $\overline{\overline{B}} \leq \overline{\overline{C}}$, to $\overline{\overline{A}} \leq \overline{\overline{C}}$.

Czy jeśli $\overline{\overline{A}} \leq \overline{\overline{B}}$ i $\overline{\overline{B}} \leq \overline{\overline{A}}$, to $\overline{\overline{A}} = \overline{\overline{B}}$?

Twierdzenie (Cantora-Bernsteina)

Jeśli $\overline{\overline{A}} \leq \overline{\overline{B}}$ i $\overline{\overline{B}} \leq \overline{\overline{A}}$ to $\overline{\overline{A}} = \overline{\overline{B}}$.

Inaczej:

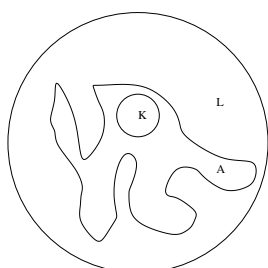
Jeśli $f : A \xrightarrow{1-1} B$ oraz $g : B \xrightarrow{1-1} A$,
to istnieje $h : A \xrightarrow{1-1}_{na} B$.

169

170

Przykład

Ponieważ $K \subseteq A \subseteq L \sim K$, więc wszystkie trzy zbiory są równoliczne.



171

Przykład

Przedziały $(0, 1)$ i $[0, 1]$ są równoliczne, bo

- ▶ $(0, 1) \subseteq [0, 1]$;
- ▶ $[0, 1] \subseteq (-1, 2) \sim (0, 1)$.

172

Dowód twierdzenia Cantora-Bernsteina

Założmy, że $\overline{\overline{A}} \leq \overline{\overline{B}} \leq \overline{\overline{A}}$.

Istnieją funkcje $f : A \xrightarrow{1-1} B$ oraz $g : B \xrightarrow{1-1} A$.

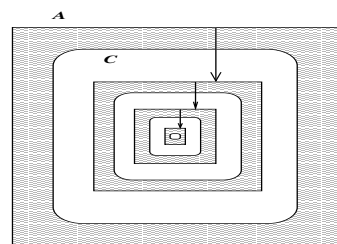
Niech $C = \text{Rg}(g)$. Wtedy $B \sim C$, oraz $g \circ f : A \xrightarrow{1-1} C$.

Wystarczy więc udowodnić:

Lemat: Jeśli $\varphi : A \xrightarrow{1-1} C \subseteq A$, to $C \sim A$.

Dowód twierdzenia Cantora-Bernsteina

Lemat: Jeśli $\varphi : A \xrightarrow{1-1} C \subseteq A$ to $C \sim A$.



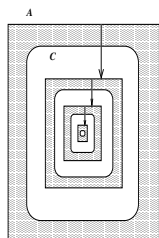
Pomysł: użyć φ tylko w częściach zakreskowanych.

173

174

Dowód twierdzenia Cantora-Bernsteina

Lemat: Jeśli $\varphi : A \xrightarrow{1-1} C \subseteq A$, to $A \sim C$.



$X_0 = A - C$
 $X_1 = \varphi(X_0)$
 $\dots$
 $X_{n+1} = \varphi(X_n)$
 $\dots$
 $\psi : A \xrightarrow{1-1}_{na} C$
 $\psi(x) = \begin{cases} \varphi(x), & \text{jeśli } x \in \bigcup_{n \in \mathbb{N}} X_n; \\ x, & \text{w przeciwnym przypadku.} \end{cases}$

Moc continuum

175

176

$$\overline{\overline{\mathbb{N} \rightarrow \{0,1\}}} \leq \overline{\mathbb{R}}$$

Definicja

Moc zbioru wszystkich liczb rzeczywistych nazywamy *continuum* i oznaczamy przez $\mathfrak{C}$.

Twierdzenie

$$\mathfrak{C} = \overline{\overline{\mathbb{P}(\mathbb{N})}} = \overline{\overline{\{0,1\}^{\mathbb{N}}}} = \overline{\overline{\mathbb{N} \rightarrow \{0,1\}}}.$$

Dowód: Część łatwa już była.

Dowód: Określamy funkcję $H : (\mathbb{N} \rightarrow \{0,1\}) \xrightarrow{1-1} [0,1]$:

$$H(f) = \sum_{i=0}^{\infty} \frac{f(i)}{10^{i+1}}$$

Na przykład $H(0110001110\dots) = 0,0110001110\dots$

Dwa różne ciągi f i g dają dwie różne liczby $H(f)$ i $H(g)$. Ale nie każda liczba z przedziału $[0,1]$ jest postaci $H(f)$.

177

178

$$\overline{\mathbb{R}} \leq \overline{\overline{\mathbb{P}(\mathbb{Q})}}$$

Dowód: Definiujemy $G : \mathbb{R} \xrightarrow{1-1} \mathbb{P}(\mathbb{Q})$:

$$G(r) = \mathbb{Q} \cap (-\infty, r)$$

Jeśli $r_1 < r_2$ to $r_1 < q < r_2$ dla pewnego $q \in \mathbb{Q}$.

Wtedy $q \in G(r_2) - G(r_1)$.

Dygresja:

Czy łańcuch zbiorów przeliczalnych musi być przeliczalny?

Nie.

Zbiory $G(r)$ są przeliczalne i tworzą nieprzeliczalny łańcuch!

$$\text{Morał: } \mathbb{P}(\mathbb{N}) \sim \mathbb{R}$$

Dowód:

Po pierwsze, $\overline{\mathbb{P}(\mathbb{N})} = \overline{\overline{\mathbb{N} \rightarrow \{0,1\}}} \leq \overline{\mathbb{R}} = \mathfrak{C}$.

Po drugie, $\mathfrak{C} = \overline{\mathbb{R}} \leq \overline{\overline{\mathbb{P}(\mathbb{Q})}} = \overline{\overline{\mathbb{P}(\mathbb{N})}}$.

Z twierdzenia Cantora-Bernsteina zbiory $\mathbb{P}(\mathbb{N})$ i $\mathbb{R}$ są równoliczne.

179

180

Arytmetyka liczb kardynalnych

Niech m, n to liczby kardynalne.

Suma $m + n$ to moc zbioru $A \oplus C$, gdzie $\overline{A} = m$ i $\overline{C} = n$.

Iloczyn $m \cdot n$ to moc zbioru $A \times C$, gdzie $\overline{A} = m$, $\overline{C} = n$.

Potęga m^n to moc zbioru A^C , gdzie $\overline{A} = m$, $\overline{C} = n$.

(Dla liczb naturalnych wychodzi to, co zwykle.)

Ale dlaczego te definicje są poprawne?

Przykłady:

► $\aleph_0 + \aleph_0 = \aleph_0$, bo $\mathbb{Z} \sim \mathbb{N}$.

► $\aleph_0 \cdot \aleph_0 = \aleph_0$, bo $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

► $2^{\aleph_0} = \mathfrak{C}$, bo $\mathbb{P}(\mathbb{N}) \sim \mathbb{R}$.

181

182

Fakt

Jeśli $m \geq \aleph_0$ to $m + \aleph_0 = m$.

Dowód: Niech $\overline{A} = m$ i $\overline{C} = \aleph_0$, a przy tym $A \cap C = \emptyset$. Wystarczy udowodnić, że $\overline{A \cup C} = \overline{A}$.

Istnieje podzbiór $B \subseteq A$, o mocy $\aleph_0$. Wtedy

$$A \cup C = (A - B) \cup (B \cup C) \sim (A - B) \cup B = A.$$

A zatem $m + \aleph_0 = \overline{A \cup C} = \overline{A} = m$.

Dodawanie i mnożenie:

- $m + 0 = m$;
- $m + n = n + m$;
- $(m + n) + p = m + (n + p)$;
- $m \cdot 1 = m$;
- $m \cdot 0 = 0$;
- $m \cdot n = n \cdot m$;
- $(m \cdot n) \cdot p = m \cdot (n \cdot p)$;
- $m \cdot (n + p) = m \cdot n + m \cdot p$.

Bo $A \oplus \emptyset \sim A$.

Bo $A \oplus B \sim B \oplus A$.

Bo $(A \oplus B) \oplus C \sim A \oplus (B \oplus C)$.

Bo $A \times \{c\} \sim A$.

Bo $A \times \emptyset = \emptyset$.

Bo $A \times B \sim B \times A$.

Bo $(A \times B) \times C \sim A \times (B \times C)$.

Bo $A \times (B \oplus C) \sim (A \times B) \oplus (A \times C)$.

183

184

Potęgowanie:

- ▶ $m^0 = 1$;
- ▶ $m^1 = m$;
- ▶ $1^m = 1$;
- ▶ $0^m = 0$ (o ile $m \neq 0$);
- ▶ $m^n \cdot m^p = m^{(n+p)}$;
- ▶ $m^n \cdot p^n = (m \cdot p)^n$;
- ▶ $(m^n)^p = m^{n \cdot p}$.

Bo tylko funkcja pusta należy do $A^\emptyset$.

Bo elementy $A^{\{0\}}$ to funkcje stałe.

Bo tylko $\lambda x. c$ należy do $\{c\}^A$.

Bo nie ma funkcji ze zbioru niepustego do $\emptyset$.

Bo $A^B \times A^C \sim A^{B \oplus C}$.

Bo $A^B \times C^B \sim (A \times C)^B$.

Bo $(A^B)^C \sim A^{B \times C}$. Czyli $C \rightarrow (B \rightarrow A) \sim C \times B \rightarrow A$.

185

Wnioski

- ▶ $\aleph_0 \cdot \mathfrak{C} = \mathfrak{C} \cdot \mathfrak{C} = \mathfrak{C}$. A więc $\mathbb{N} \times \mathbb{R} \sim \mathbb{R}^2 \sim \mathbb{R}$.
- ▶ $\aleph_0^{\aleph_0} = \mathfrak{C}^{\aleph_0} = \mathfrak{C}$; A więc $(\mathbb{N} \rightarrow \mathbb{N}) \sim (\mathbb{N} \rightarrow \mathbb{R}) \sim \mathbb{R}$.
- ▶ $2^{\mathfrak{C}} = \aleph_0^{\mathfrak{C}} = \mathfrak{C}^{\mathfrak{C}}$. A więc $(\mathbb{R} \rightarrow \mathbb{N}) \sim (\mathbb{R} \rightarrow \mathbb{R})$.

Bo $\mathfrak{C} = 1 \cdot \mathfrak{C} \leq \aleph_0 \cdot \mathfrak{C} \leq \mathfrak{C} \cdot \mathfrak{C} = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0} = \mathfrak{C}$.

Bo $\mathfrak{C} = 2^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq \mathfrak{C}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{C}$.

Bo $2^{\mathfrak{C}} \leq \aleph_0^{\mathfrak{C}} \leq \mathfrak{C}^{\mathfrak{C}} = (2^{\aleph_0})^{\mathfrak{C}} = 2^{\aleph_0 \cdot \mathfrak{C}} = 2^{\mathfrak{C}}$.

187

Alefy i bety

Niech $\beth_0 = \aleph_0$ i dalej $\beth_{n+1} = 2^{\beth_n}$.

Wtedy $\overline{\overline{P(\mathbb{N})}} = \overline{\mathbb{R}} = \beth_1$, $\overline{\overline{P(P(\mathbb{N}))}} = \beth_2$, itd.

Liczba $\aleph_1$ to najmniejsza nieprzeliczalna liczba kardynalna,
liczba $\aleph_2$ to najmniejsza liczba większa od $\aleph_1$, itd.

Hipoteza continuum: $\aleph_1 = \beth_1$.

Hipotezy continuum nie można ani udowodnić
ani obalić metodami teorii zbiorów.

Jest niezależna od aksjomatów teorii zbiorów.

189

Relacje

(dwuargumentowe)

Monotoniczność

Jeśli $m \leq n$ i $p \leq q$, to:

- ▶ $m + p \leq n + q$;
- ▶ $m \cdot p \leq n \cdot q$;
- ▶ $m^p \leq n^q$ (o ile $p \neq 0$).

186

Ostrzeżenie

Monotoniczność działań nie jest ścisła.

- ▶ $5 + \aleph_0 = \aleph_0 + \aleph_0 = \aleph_0$;
- ▶ $5 \cdot \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$;
- ▶ $2^{\aleph_0} = \aleph_0^{\aleph_0} = \mathfrak{C}$;
- ▶ $\mathfrak{C}^5 = \mathfrak{C}^{\aleph_0} = \mathfrak{C}$.

Nie zachodzą prawa skracania; liczb kardynalnych nie można odejmować, dzielić, pierwiastkować ani logarytmować.

188

Ostrzeżenie

Z tego, że $A \subseteq \mathbb{R}$ jest nieprzeliczalny. . .

nie wynika, że $\overline{\overline{A}} = \mathfrak{C}$!!

190

Relacje

Przypomnijmy, że:

Dowolny podzbiór r iloczynu kartezjańskiego $A \times B$ nazywamy
relacją z A do B . Jeśli $A = B$, to relacja jest w zbiorze A .

Jeśli $\langle x, y \rangle \in r$, to często piszemy $x r y$.

191

192

Relacja odwrotna do relacji $r \subseteq A \times B$ to zbiór

$$r^{-1} = \{\langle y, x \rangle \in B \times A \mid \langle x, y \rangle \in r\}.$$

Na przykład relacją odwrotną do relacji $\leq$ w zbiorze $\mathbb{N}$ jest relacja $\geq$. Można napisać $\leq^{-1} = \geq$.

193

Operacje na relacjach

Relacja identycznościowa w A to relacja

$$1_A = \{\langle a, a \rangle \mid a \in A\}.$$

Uwaga: $a 1_A b$ wtedy i tylko wtedy, gdy $a = b$.

195

Relacje przechodnie

Relacja r w A jest *przechodnia*, gdy

$$\forall x, y, z \in A (x r y \wedge y r z \rightarrow x r z)$$

Przykłady:

- ▶ Relacja $\leq$ w zbiorze liczb rzeczywistych.
- ▶ Relacja $\subseteq$ w zbiorze $P(A)$.
- ▶ Relacja równoległości prostych.

197

Relacje przechodnie

Ćwiczenie 1:

Relacja r jest przechodnia wtedy i tylko wtedy, gdy $r \cdot r \subseteq r$.

Dowód: $(\Leftarrow)$ Załóżmy, że $r \cdot r \subseteq r$. Mamy udowodnić, że r jest przechodnia, tj. że $\forall x, y, z. (x r y \wedge y r z \rightarrow x r z)$.

Przypuśćmy, że $x r y$ i $y r z$.

Wtedy $x(r \cdot r)z$.

A ponieważ $r \cdot r \subseteq r$, więc $x r z$.

199

Złożenie relacji $r \subseteq A \times B$ oraz $s \subseteq B \times C$ to relacja

$$r \cdot s = \{\langle x, y \rangle \in A \times C \mid \exists z (x r z \wedge z s y)\}$$

$$x(r \cdot s)y \text{ wtedy i tylko wtedy, gdy } \exists z (x r z \wedge z s y).$$

Przykład:

Jeśli znaki $\parallel$ i $\perp$ oznaczają odpowiednio równoległość i prostokątłość prostych na płaszczyźnie, to $\parallel \cdot \perp = \perp$. A co to jest $\perp \cdot \perp$?

194

Własności operacji składania

- ▶ $r \cdot (s \cdot p) = (r \cdot s) \cdot p$;
- ▶ $r \cdot (s \cup p) = r \cdot s \cup r \cdot p$;
- ▶ $(s \cup p) \cdot r = s \cdot r \cup p \cdot r$;
- ▶ $r \cdot 1_B = 1_A \cdot r = r$, gdy $r \subseteq A \times B$;
- ▶ Jeśli $r \subseteq r'$ i $s \subseteq s'$, to $r \cdot s \subseteq r' \cdot s'$.
- ▶ Uwaga: nie zawsze $r \cdot r^{-1} = 1$!

196

Relacje przechodnie

Ćwiczenie 1:

Relacja r jest przechodnia wtedy i tylko wtedy, gdy $r \cdot r \subseteq r$.

Dowód: $(\Rightarrow)$ Załóżmy, że r jest przechodnia i rozpatrzmy dowolny element złożenia $r \cdot r$. Zbiór $r \cdot r$ jest relacją, więc ten element musi być parą uporządkowaną. A więc:

Niech $\langle x, y \rangle \in r \cdot r$.

Z definicji $r \cdot r$ istnieje takie z , że $\langle x, z \rangle, \langle z, y \rangle \in r$.

Ponieważ jednak r jest przechodnia, więc $\langle x, y \rangle \in r$.

198

Relacje przechodnie

Ćwiczenie 2:

Iloczyn niepustej rodziny relacji przechodnich jest przechodni.

Dowód: Niech $\mathcal{R}$ będzie rodziną relacji przechodnich. Mamy wykazać, że iloczyn $\bigcap \mathcal{R}$ jest przechodni.

Przypuśćmy, że $\langle x, y \rangle, \langle y, z \rangle \in \bigcap \mathcal{R}$.

Pokażemy, że $\langle x, z \rangle \in \bigcap \mathcal{R}$,

tj., że $\langle x, z \rangle \in r$, dla wszystkich relacji $r \in \mathcal{R}$.

Niech $r \in \mathcal{R}$. Wtedy $\langle x, y \rangle, \langle y, z \rangle \in r$,

a ponieważ r przechodnia, więc $\langle x, z \rangle \in r$.

Z dowolności r wynika $\langle x, z \rangle \in \bigcap \mathcal{R}$.

200

Domknięcie przechodnie

Niech $r \subseteq A \times A$.

Relację r^+ nazywamy *domknięciem przechodnim* relacji r , gdy jest to *najmniejsza relacja przechodnia zawierająca r* , tj:

- ▶ r^+ jest przechodnia;
- ▶ $r \subseteq r^+$;
- ▶ jeśli $r \subseteq s$ i s przechodnia, to $r^+ \subseteq s$.

Fakt: Istnieje dokładnie jedna taka relacja r^+ .
Możemy ją zdefiniować tak:

$$r^+ = \bigcap \{s \subseteq A \times A \mid r \subseteq s \text{ oraz } s \text{ przechodnia}\}$$

201

$$r^+ = \bigcap \mathcal{R}, \text{ gdzie } \mathcal{R} = \{s \subseteq A \times A \mid r \subseteq s \text{ oraz } s \text{ przechodnia}\}$$

Własność 1: $r \subseteq r^+$

Dowód: Niech $\langle x, y \rangle \in r$.

Jeśli $s \in \mathcal{R}$, to $r \subseteq s$, więc $\langle x, y \rangle \in s$.

Z dowolności s wynika $\langle x, y \rangle \in \bigcap \mathcal{R} = r^+$.

203

$$r^+ = \bigcap \mathcal{R}, \text{ gdzie } \mathcal{R} = \{s \subseteq A \times A \mid r \subseteq s \text{ oraz } s \text{ przechodnia}\}$$

Własność 3: Jeśli $r \subseteq s$ i s przechodnia, to $r^+ \subseteq s$.

Dowód: Jeśli $r \subseteq s$ i s przechodnia, to $s \in \mathcal{R}$.

Zatem $r^+ = \bigcap \mathcal{R} \subseteq s$.

205

Przykłady

- ▶ Jeśli $r = \{\langle n, n+1 \rangle \mid n \in \mathbb{N}\}$, to $r^+ = \{\langle n, m \rangle \mid n < m\}$
- ▶ Relacja $\leq$ w zbiorze $\mathbb{N}$ jest swoim własnym domknięciem przechodnim.

207

$$r^+ = \bigcap \{s \subseteq A \times A \mid r \subseteq s \text{ oraz } s \text{ przechodnia}\}$$

Przyjmijmy oznaczenie:

$$\mathcal{R} = \{s \subseteq A \times A \mid r \subseteq s \text{ oraz } s \text{ przechodnia}\}$$

Wtedy $r^+ = \bigcap \mathcal{R}$.

Własność 0: Zbiór $\mathcal{R}$ jest niepustą rodziną relacji.

Dowód: Relacja $A \times A$ zawiera r i jest przechodnia, czyli $A \times A \in \mathcal{R}$.

202

$$r^+ = \bigcap \mathcal{R}, \text{ gdzie } \mathcal{R} = \{s \subseteq A \times A \mid r \subseteq s \text{ oraz } s \text{ przechodnia}\}$$

Własność 2: Relacja r^+ jest przechodnia.

Dowód: Ponieważ $\mathcal{R}$ jest rodziną relacji przechodnich, więc jej iloczyn jest przechodni.

204

$$r^+ = \bigcap \mathcal{R}, \text{ gdzie } \mathcal{R} = \{s \subseteq A \times A \mid r \subseteq s \text{ oraz } s \text{ przechodnia}\}$$

0. Zbiór $\mathcal{R}$ jest niepustą rodziną relacji.

1. $r \subseteq r^+$.

2. Relacja r^+ jest przechodnia.

3. Jeśli $r \subseteq s$ i s przechodnia, to $r^+ \subseteq s$.

Zatem r^+ jest

– dobrze określoną relacją (0),

– domknięciem przechodnim relacji r (1–3).

206

Domknięcie przechodnie inaczej

Dla ustalonej relacji r w zbiorze A , definiujemy ciąg relacji r_n :

- ▶ $r_0 = r$;
- ▶ $r_{n+1} = r_n \cup (r_n \cdot r_n)$.

Wreszcie niech $r_\omega = \bigcup_{n \in \mathbb{N}} r_n$.

Łatwy lemat: Jeśli $m \leq n$, to $r_m \subseteq r_n$.
(Indukcja ze względu na n .)

Fakt: $r_\omega = r^+$

Dowód: Zaczniemy od tego, że relacja r_ω jest przechodnia.

Bo tak: jeśli $\langle x, y \rangle, \langle y, z \rangle \in r_\omega$, to istnieją takie m, n , że $\langle x, y \rangle \in r_m$ i $\langle y, z \rangle \in r_n$. Wtedy obie pary należą do $r_{\max\{m, n\}}$, skąd $\langle x, z \rangle \in r_{\max\{m, n\}+1} \subseteq r_\omega$.

Ponieważ $r = r_0 \subseteq r_\omega$ i r_ω jest przechodnia, więc $r^+ \subseteq r_\omega$.

208

Domknięcie przechodnie inaczej

Dla ustalonej relacji r w zbiorze A , definiujemy ciąg relacji r_n :

- ▶ $r_0 = r$;
- ▶ $r_{n+1} = r_n \cup (r_n \cdot r_n)$.

Wreszcie niech $r_\omega = \bigcup_{n \in \mathbb{N}} r_n$.

Fakt: $r_\omega = r^+$

Dowód: Teraz trzeba pokazać, że $r_\omega \subseteq r^+$. W tym celu przez indukcję dowodzimy, że $r_n \subseteq r^+$ dla wszystkich $n \in \mathbb{N}$.

Po pierwsze, $r_0 = r \subseteq r^+$.

Po drugie, jeśli $r_n \subseteq r^+$, to

$$r_{n+1} = r_n \cup (r_n \cdot r_n) \subseteq r^+ \cup (r^+ \cdot r^+) \subseteq r^+ \cup r^+ = r^+.$$

209

Relacje zwrotne

Relacja $r \subseteq A \times A$ jest **zwrotna w A** wtedy i tylko wtedy, gdy $x r x$ dla wszystkich $x \in A$.

(Inaczej: r jest zwrotna, gdy $1_A \subseteq r$.)

Przykłady: 1_A , $\leq$, równoległość prostych.

210

Domknięcie przechodnio-zwrotne

Domknięcie przechodnio-zwrotne relacji r to najmniejsza relacja przechodnia i zwrotna zawierająca r , czyli relacja

$$r^* = 1_A \cup r^+.$$

Ćwiczenie: Sprawdzić, że to faktycznie ta relacja.

Przykłady

Niech $\rightarrow$ oznacza relację sąsiedztwa wierzchołków w pewnym grafie. Wtedy relacja $\rightarrow^*$ (oznaczana też przez $\twoheadrightarrow$) to relacja osiągalności w tym grafie.

Domknięciem przechodnim relacji następnika w $\mathbb{N}$ jest relacja $<$.

Relacja $\leq$ jest jej domknięciem przechodnio-zwrotnym.

211

212

Własności relacji

Relacja r w A jest

- | | | |
|-------------------|-----|--|
| zwrotna (w A), | gdy | $\forall x \in A (x r x)$; |
| symetryczna, | gdy | $\forall x, y \in A (x r y \rightarrow y r x)$; |
| przechodnia, | gdy | $\forall x, y, z \in A (x r y \wedge y r z \rightarrow x r z)$; |
| antysymetryczna, | gdy | $\forall x, y \in A (x r y \wedge y r x \rightarrow x = y)$; |
| spójna (w A), | gdy | $\forall x, y \in A (x r y \vee y r x)$. |

213

Relacje równoważności

Dwuargumentowa relacja r w zbiorze A jest **relacją równoważności** wtedy i tylko wtedy, gdy jest zwrotna, symetryczna i przechodnia:

- ▶ $\forall x \in A (x r x)$;
- ▶ $\forall x, y \in A (x r y \rightarrow y r x)$;
- ▶ $\forall x, y, z \in A (x r y \wedge y r z \rightarrow x r z)$.

Przykład: *Jądro* przekształcenia $f : A \rightarrow B$:

$$\langle x, y \rangle \in \ker(f) \Leftrightarrow f(x) = f(y).$$

Przykład: równoległość prostych

Jakie własności ma ta relacja?

Jest zwrotna, symetryczna i przechodnia.

Relacje równoważności

216

215

Przykład 1: Dwa punkty na prostej są w relacji r , wtedy i tylko wtedy, gdy ich odległość jest liczbą wymierną.

To jest relacja równoważności, bo:

- ▶ Każdy punkt jest w odległości zero sam od siebie;
- ▶ Punkt y jest w tej samej odległości od x , co x od y ;
- ▶ Odległość od x do z jest zawsze sumą lub różnicą odległości x od y i odległości y od z .

Przykład 2: Dwa punkty na płaszczyźnie są w relacji, r_2 wtedy i tylko wtedy, gdy ich odległość jest liczbą wymierną.

To **nie** jest relacja równoważności, bo nie jest przechodnia. Na przykład odległość od $\langle 1, 0 \rangle$ do $\langle 0, 0 \rangle$ i od $\langle 0, 0 \rangle$ do $\langle 0, 1 \rangle$ są wymierne, a odległość od $\langle 1, 0 \rangle$ do $\langle 0, 1 \rangle$ nie jest wymierna.

217

Jądro

Definicja: *Jądro* przekształcenia $f : A \rightarrow B$:

$$\langle x, y \rangle \in \ker(f) \Leftrightarrow f(x) = f(y).$$

Jądro jest zawsze relacją równoważności.

Przykład: Jądrem funkcji stałej jest relacja totalna.

Jądrem funkcji różnowartościowej jest relacja identycznościowa.

218

Przykład: Liczby całkowite x i y są w relacji $\equiv_3$ wtedy i tylko wtedy, gdy $3 \mid x - y$.

Inaczej:

$$x \equiv_3 y \text{ wtedy i tylko wtedy, gdy } x \bmod 3 = y \bmod 3.$$

To jest jądro funkcji $\lambda x. x \bmod 3$, a więc relacja równoważności.

219

Przykład

Relacja

$$\{ \langle f, g \rangle \in \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}} \mid \forall x (f(x) \neq g(x) \rightarrow x \bmod 3 \neq 0) \}$$

jest jądrem przekształcenia

$$\lambda f. f|_{\{x \mid x \bmod 3 = 0\}}$$

a zatem jest relacją równoważności.

220

Czy to jest ten sam tramwaj?



221

Zbiór (typ) ilorazowy

$$A/r = \{ a/r \mid a \in \text{Dom}(r) \}$$

$$a/r = b/r \text{ wtedy i tylko wtedy, gdy } a r b.$$

Klasy abstrakcji

$$[x]_r = \{ y \in A \mid y r x \}.$$

Uwaga: $x \in [x]_r \neq \emptyset$.

222

Przykład: $x \equiv_3 y$ wtedy i tylko wtedy, gdy $x \bmod 3 = y \bmod 3$.

Ta relacja ma 3 klasy abstrakcji: $[0]_{\equiv_3}$, $[1]_{\equiv_3}$, $[2]_{\equiv_3}$.

223

Def. $[x]_r = \{ y \in A \mid y r x \}.$

Fakt: Następujące warunki są równoważne:

- a) $[x]_r = [y]_r$;
- b) $x r y$;
- c) $x \in [y]_r$;
- d) $y \in [x]_r$;
- e) $[x]_r \cap [y]_r \neq \emptyset$;

Te implikacje są łatwe:

(a) $\Rightarrow$ (b), (b) $\Rightarrow$ (c), (c) $\Rightarrow$ (d) i (d) $\Rightarrow$ (e)

Sens implikacji (e) $\Rightarrow$ (a):

Klasy abstrakcji są albo równe albo rozłączne.

224

Fakt: Następujące warunki są równoważne:

- a) $[x]_r = [y]_r$.
- b) $x r y$;
- c) $x \in [y]_r$;
- d) $y \in [x]_r$;
- e) $[x]_r \cap [y]_r \neq \emptyset$;

Dowód (e) $\Rightarrow$ (a):

Skoro $[x]_r \cap [y]_r \neq \emptyset$, to jest takie z , że $z \in [x]_r \cap [y]_r$.
Wtedy $z r x$ oraz $z r y$.

Niech $v \in [x]_r$. Wtedy $v r x$, $x r z$, oraz $z r y$.

Z przechodności $v r y$, czyli $v \in [y]_r$.

Pokazaliśmy, że $[x]_r \subseteq [y]_r$.

Podobnie w przeciwną stronę, a więc $[x]_r = [y]_r$.

225

Przykład: Dwa punkty na prostej są w relacji r , wtedy i tylko wtedy, gdy ich odległość jest liczbą wymierną. Inaczej: dwie liczby rzeczywiste są w relacji, wtedy i tylko wtedy, gdy ich różnica jest liczbą wymierną.

Jakie klasy abstrakcji ma taka relacja r ?

Na przykład $[\frac{1}{2}]_r = \mathbb{Q} = [1]_r = [\frac{5}{4}]_r$, itd.

Ogólnie klasy są postaci $[a]_r = \{a + q \mid q \in \mathbb{Q}\}$.

Każda klasa to „przesunięta kopia” zbioru liczb wymiernych.

227

Zasada abstrakcji

Podział zbioru A to rodzina $P \subseteq \mathcal{P}(A)$ o własnościach:

- ▶ $\forall p(p \in P \rightarrow p \neq \emptyset)$;
- ▶ $\forall p, q(p, q \in P \rightarrow (p = q \vee p \cap q = \emptyset))$;
- ▶ $\bigcup P = A$, czyli $\forall x(x \in A \rightarrow \exists p(p \in P(x \in p)))$.

Twierdzenie (Zasada abstrakcji)

1) Jeżeli r jest relacją równoważności w A , to A/r jest podziałem zbioru A .

2) Jeżeli P jest podziałem zbioru A , to istnieje taka relacja równoważności r w A , że $P = A/r$.

229

Zasada abstrakcji: Każdy podział zbioru A jest postaci A/r .

Dowód: P – podział zbioru A .

$$r = \{\langle x, y \rangle \in A \times A \mid \exists p \in P(x \in p \wedge y \in p)\}$$

Wtedy:

1. r jest relacją równoważności;
- 2.

Zwrotność i symetria są łatwe.

Przechodność: Przypuśćmy, że $x r y$ i $y r z$. Wtedy są takie $p, q \in P$, że $x, y \in p$ oraz $y, z \in q$. Ale wtedy $p \cap q \neq \emptyset$, więc $p = q$. Skoro więc $x \in p$ i $z \in q = p$, to $x r z$.

231

Własności klas abstrakcji

1) $x \in [x]_r$.

2) Następujące warunki są równoważne:

- a) $x r y$;
- b) $x \in [y]_r$;
- c) $y \in [x]_r$;
- d) $[x]_r = [y]_r$;
- e) $[x]_r \cap [y]_r \neq \emptyset$.

Wniosek: $[x]_r = [y]_r \Leftrightarrow x/r = y/r$

Morał: Można uważać, że A/r to zbiór klas abstrakcji.

Czyli $[x]_r$ to to samo, co x/r .

$$A/r = \{[x]_r \mid x \in A\}$$

226

Przykład: Punkty płaszczyzny $\langle x_1, y_1 \rangle$ i $\langle x_2, y_2 \rangle$ są w relacji wtedy i tylko wtedy, gdy $x_1^2 + y_1^2 = x_2^2 + y_2^2$.

Klasy abstrakcji to okręgi o środku w $(0, 0)$ i dowolnych promieniach, oraz jeden singleton $\{(0, 0)\}$.

Te zbiory są rozłączne i pokrywają całą płaszczyznę.

228

Zanim przejdziemy do dowodu...

Ćwiczenie 1: Czy istnieje taka relacja równoważności r w zbiorze $\mathbb{N}$, która ma 22 klasy abstrakcji, a każda klasa abstrakcji ma 37 elementów?

Odpowiedź: Nie, bo suma wszystkich klas miałaby tylko 814 elementów, a liczb naturalnych jest więcej.

Ćwiczenie 2: Czy istnieje taka relacja równoważności r w zbiorze $\mathbb{R}$, której klasami abstrakcji są dokładnie zbiory: $(-\infty, -7], (-7, -5], [-5, 0], \{0, 1, \pi\}, (0, 1), (1, \pi), (\pi, \infty)$?

Odpowiedź: Tak, bo te zbiory tworzą podział prostej.

230

Zasada abstrakcji: Każdy podział zbioru A jest postaci A/r .

Dowód: P – podział zbioru A .

$$r = \{\langle x, y \rangle \in A \times A \mid \exists p \in P(x \in p \wedge y \in p)\}$$

Wtedy:

- 1.
2. jeśli $x \in p \in P$, to $[x]_r = p$.

$([x]_r \subseteq p)$ Niech $x \in p \in P$ i niech $t \in [x]_r$. Wtedy $x, t \in q$ dla pewnego $q \in P$. Ale $q = p$ bo $x \in p \cap q$. Zatem $t \in p$.

$(p \subseteq [x]_r)$ Jeśli $t \in p$, to $t r x$ (bo $x \in p$) więc $t \in [x]_r$.

232

Zasada abstrakcji: Każdy podział zbioru A jest postaci A/r .

Dowód: P – podział zbioru A .

$$r = \{ \langle x, y \rangle \in A \times A \mid \exists p \in P (x \in p \wedge y \in p) \}$$

Wtedy:

1. r jest relacją równoważności;
2. jeśli $x \in p \in P$, to $[x]_r = p$.

Pokażemy, że $P = A/r$.

($\subseteq$): Jeśli $p \in P$, to $p \neq \emptyset$, więc jest $x \in p$. Wtedy $p = [x]_r$ na mocy (2), więc $p \in A/r$.

($\supseteq$): Dla dowolnego $x \in A$ istnieje takie $p \in P$, że $x \in p$.

Wtedy $[x]_r = p$. A zatem każda klasa $[x]_r \in A/r$ należy do P .

233

Zasada abstrakcji

Podział zbioru A to rodzina $P \subseteq \mathcal{P}(A)$ o własnościach:

- ▶ $\forall p(p \in P \rightarrow p \neq \emptyset)$;
- ▶ $\forall p, q(p, q \in P \rightarrow (p = q \vee p \cap q = \emptyset))$;
- ▶ $\bigcup P = A$, czyli $\forall x(x \in A \rightarrow \exists p \in P (x \in p))$.

Twierdzenie (Zasada abstrakcji)

1) Jeżeli r jest relacją równoważności w A , to A/r jest podziałem zbioru A .

2) Jeżeli P jest podziałem zbioru A , to istnieje taka relacja równoważności r w A , że $P = A/r$.

234

Jeszcze kilka przykładów

Przykład: Jeśli V_0 jest podprzestrzenią przestrzeni liniowej V , to relacja $\sim$ w zbiorze V :

$$x \sim y \text{ wtedy i tylko wtedy, gdy } x - y \in V_0$$

jest relacją równoważności.

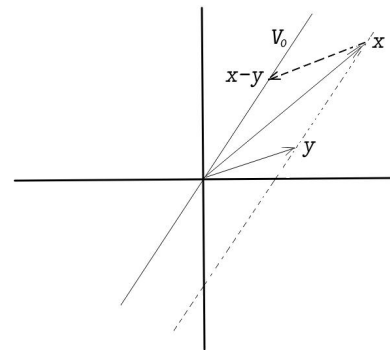
Jej klasy abstrakcji nazywamy *warstwami* podprzestrzeni V_0 .

Ta relacja jest jądrem pewnego homomorfizmu $h : V \rightarrow V'$, który ma tę własność, że $V_0 = h^{-1}(\{0\})$.

$$h(x) = h(y) \Leftrightarrow h(x - y) = 0$$

235

Podprzestrzeń i warstwa



236

Każda relacja równoważności jest jądrem

$$x \sim y \text{ wtedy i tylko wtedy, gdy } [x]_r = [y]_r$$

$$r = \ker(\lambda x. [x]_r)$$

237

Niech $\mathcal{Pr}$ oznacza zbiór wszystkich liczb parzystych

Ćwiczenie: Dwie relacje w zbiorze $\mathbb{N} \rightarrow \mathbb{N}$:

- ▶ $f \sim_r g$ wtedy i tylko wtedy, gdy $\forall x : \mathbb{N}. |f(x) - g(x)| \in \mathcal{Pr}$;
- ▶ $f \sim_s g$ wtedy i tylko wtedy, gdy $\forall x \in \mathcal{Pr}. f(x) = g(x)$.

Czy to są relacje równoważności? Może jądra?

Relacja r jest jądrem operacji $\lambda f. (\lambda x. f(x) \bmod 2)$.

Relacja s jest jądrem operacji $\lambda f. f|_{\mathcal{Pr}}$.

Jakie są klasy abstrakcji? Czy jest ich skończenie wiele?

238

Porządki

Relacje porządkujące

Relacja częściowego porządku to relacja zwrotna, antysymetryczna i przechodnia.

Relacja liniowego porządku to spójny częściowy porządek.

239

240

Przykłady porządków

- ▶ Relacja $\leq$ w $\mathbb{N}$ jest liniowym porządkiem.
- ▶ Relacja podzielności jest częściowym porządkiem:
 $m|n$ wtedy i tylko wtedy, gdy $\exists k:\mathbb{N}(k \cdot m = n)$.
- ▶ Inkluzja częściowo porządkuje $\mathcal{P}(A)$.
- ▶ Porządek *leksykograficzny* w zbiorze $\mathbb{N} \times \mathbb{N}$:
 $\langle x, y \rangle \leq \langle x', y' \rangle \Leftrightarrow x < x' \vee (x = x' \wedge y \leq y')$
jest porządkiem liniowym.

241

Definicje

Niech $\langle A, \leq \rangle$ będzie częściowym porządkiem.

1. Elementy $a, b \in A$ są *porównywalne*,
gdy $a \leq b$ lub $b \leq a$.
W przeciwnym razie a, b są *nieporównywalne*.
2. Jeśli każde dwa elementy zbioru $B \subseteq A$ są porównywalne
to mówimy, że B jest *łańcuchem* w A .
3. Jeśli każde dwa różne elementy zbioru B są
nieporównywalne, to B jest *antyłańcuchem* w A .

243

Definicje

Niech $\langle A, \leq \rangle$ będzie częściowym porządkiem i niech $a \in A$.
Mówimy, że element a jest w zbiorze A :

<i>największy</i> ,	gdy	$\forall x \in A (x \leq a)$;
<i>maksymalny</i> ,	gdy	$\forall x \in A (a \leq x \rightarrow a = x)$;
<i>najmniejszy</i> ,	gdy	$\forall x \in A (a \leq x)$;
<i>minimalny</i> ,	gdy	$\forall x \in A (x \leq a \rightarrow a = x)$.

Uwaga:

Element maksymalny w porządku liniowym jest największy.
Element minimalny w porządku liniowym jest najmniejszy.

245

Przykład

W zbiorze $\langle A \rightarrow B, \subseteq \rangle$ funkcji częściowych z A do B :

- ▶ Elementem najmniejszym jest funkcja pusta $\perp$,
która nigdzie nie jest określona.
- ▶ Elementami maksymalnymi są funkcje całkowite.
- ▶ Jeśli $A \neq \emptyset$ i B jest co najmniej dwuelementowy,
to nie istnieje element największy.

247

Przykład

W zbiorze $A \rightarrow B$ funkcji częściowych z A do B
definiujemy relację $\subseteq$:

$f \subseteq g$ wtedy i tylko wtedy, gdy

$$\text{Dom}(f) \subseteq \text{Dom}(g) \wedge \forall a (a \in \text{Dom}(f) \rightarrow f(a) = g(a)).$$

242

Przykłady

- ▶ W porządku $\langle \mathbb{N}, | \rangle$ potęgi dwójki tworzą łańcuch,
a liczby pierwsze tworzą antyłańcuch.
- ▶ Zbiór jednoelementowy jest zarówno łańcuchem
jak antyłańcuchem. Tak samo zbiór pusty.
- ▶ Zbiory dwuelementowe tworzą antyłańcuch w $\langle \mathcal{P}(\mathbb{N}), \subseteq \rangle$.
- ▶ Rodzina $\{(-x, 0) \mid x > 0\}$ jest łańcuchem w $\mathcal{P}(\mathbb{R})$.
- ▶ Rodzina $\{(x, \infty) \mid x > 0\}$ też.

244

Przykłady

- ▶ Zero jest elementem największym a 1 najmniejszym
w zbiorze $\mathbb{N}$ uporządkowanym przez podzielność.
- ▶ W porządku $\langle \mathbb{N} - \{0, 1\}, | \rangle$ nie ma elementu
najmniejszego ani żadnych elementów maksymalnych.
Elementami minimalnymi są liczby pierwsze.
- ▶ W zbiorze $\langle \mathbb{Z}, \leq \rangle$ nie ma żadnych elementów minimalnych
ani maksymalnych.
- ▶ W zbiorze $\langle \mathcal{P}(\mathbb{N}), \subseteq \rangle$ najmniejszy jest zbiór pusty,
a największy jest zbiór $\mathbb{N}$.
- ▶ W zbiorze $\langle \mathcal{P}(\mathbb{N}) - \{\emptyset\}, \subseteq \rangle$ nie ma elementu
najmniejszego, a minimalne są singletony.

246

Maksymalne i największe

Fakt: Element największy (najmniejszy) jest
jedynym elementem maksymalnym (minimalnym).

Dowód: Niech a będzie największy w A i niech $b \in A$.
Przypuśćmy, że $a \leq b$. Ponieważ a jest największy,
więc także $a \geq b$, skąd $a = b$.
Zatem a jest maksymalny.

Niech teraz c będzie dowolnym elementem maksymalnym.
Skoro $c \leq a$, to $a = c$ z maksymalności c . $\square$

248

Maksymalne i największe

Fakt: Element największy (najmniejszy) jest jedynym elementem maksymalnym (minimalnym).

Ale nie na odwrót:

Częściowy porządek $\langle \mathbb{Z} \oplus \{\omega\}, \preceq \rangle$, w którym:

$$x \preceq y \Leftrightarrow [(x, y \in \mathbb{Z}) \wedge (x \leq y)] \vee [x = y = \omega],$$

ma tylko jeden element minimalny ω ,
ale nie ma elementu najmniejszego.

... -4 -3 -2 -1 0 1 2 3 4
 ω

249

Izomorfizmy porządków

Jeśli dwa zbiory częściowo uporządkowane są izomorficzne i jeden z nich

- ▶ ma element najmniejszy, największy, maksymalny, minimalny;²
- ▶ jest liniowo uporządkowany;
- ▶ ma nieskończony antyłańcuch;
- ▶ ma jakąś inną własność *porządkową*,

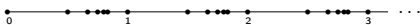
to ten drugi też.

²Niepotrzebne skreślić.

251

Przykład

Zbiór $B = \{m - \frac{1}{n} \mid m, n \in \mathbb{N} - \{0\}\}$



jest izomorficzny ze zbiorem $\mathbb{N} \times \mathbb{N}$ uporządkowanym leksykograficznie:

$\langle 0, 0 \rangle, \langle 0, 1 \rangle, \langle 0, 2 \rangle, \dots \langle 1, 0 \rangle, \langle 1, 1 \rangle, \langle 1, 2 \rangle, \dots \langle 2, 0 \rangle, \langle 2, 1 \rangle, \dots$

253

Przykład

W porządku $\langle \mathbb{N}, | \rangle$ podzbiór $\{18, 30\}$ jest ograniczony z dołu (np. przez 1 albo 3) i z góry (np. przez 180 lub 360).

255

Izomorfizmy porządków

Definicja

Mówimy, że zbiory częściowo uporządkowane $\langle A, \leq \rangle$ i $\langle B, \leq \rangle$ są *izomorficzne*, gdy istnieje taka bijekcja $f: A \xrightarrow[na]{1-1} B$, że

$$a \leq a' \Leftrightarrow f(a) \leq f(a'),$$

dla dowolnych $a, a' \in A$.

Piszemy $\langle A, \leq \rangle \approx \langle B, \leq \rangle$ lub $A \approx B$.

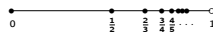
Funkcję f nazywamy *izomorfizmem*.

250

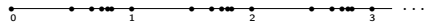
Przykład

Zbiór $\langle \mathbb{N}, \leq \rangle$ jest izomorficzny ze zbiorem

$$A = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$$



ale nie ze zbiorem $B = \{m - \frac{1}{n} \mid m, n \in \mathbb{N} - \{0\}\}$.



Zbiór B jest izomorficzny ze zbiorem $\mathbb{N} \times \mathbb{N}$ uporządkowanym leksykograficznie.

252

Ograniczenie górne i dolne

Niech $\langle A, \leq \rangle$ będzie porządkiem częściowym i niech $B \subseteq A$ i $a \in A$. Mówimy, że a jest *ograniczeniem górnym* zbioru B (oznaczenie $B \leq a$), gdy $b \leq a$ dla wszystkich $b \in B$.

Analogicznie definiujemy ograniczenia dolne:

($a \leq B$ oznacza, że $a \leq b$ dla wszystkich $b \in B$.)

Jeśli istnieje ograniczenie górne (odp. dolne), to mówimy, że zbiór jest *ograniczony z góry* (odp. *z dołu*).

254

Kresy

Element a jest *kresem górnym* zbioru B ($a = \sup B$), gdy jest najmniejszym ograniczeniem górnym B , czyli:

- ▶ $a \geq B$;
- ▶ dla dowolnego $c \in A$, jeśli $c \geq B$, to $c \geq a$.

Analogicznie, a jest *kresem dolnym* zbioru B ($a = \inf B$), gdy jest największym ograniczeniem dolnym B , czyli:

- ▶ $a \leq B$;
- ▶ dla dowolnego $c \in A$, jeśli $c \leq B$, to $c \leq a$.

256

Przykłady

- ▶ W porządku $\langle \mathbb{N}, | \rangle$ kresem górnym zbioru $\{18, 30\}$ jest liczba 90 a dolnym liczba 6.
- ▶ Ogólniej: w tym porządku kresem górnym zbioru liczb jest ich najmniejsza wspólna wielokrotność a kresem dolnym – największy wspólny dzielnik.
- ▶ W rodzinie $\langle \mathcal{P}(A), \subseteq \rangle$ kresem górnym dowolnej podrodziny $X \subseteq \mathcal{P}(A)$ jest suma $\bigcup X$.
- ▶ W szczególności $\sup\{B, C\} = B \cup C$.
Podobnie $\inf\{B, C\} = B \cap C$.

257

Przykłady

- ▶ Rodzina $\mathcal{R}$ funkcji częściowych jest *zgodna*, gdy dla dowolnych $f, g \in \mathcal{R}$ i dowolnego $x \in \text{Dom}(f) \cap \text{Dom}(g)$ zachodzi $f(x) = g(x)$.
- ▶ W zbiorze $\langle A \rightarrow B, \subseteq \rangle$ funkcji częściowych z A do B każda zgodna rodzina $\mathcal{R}$ ma kres górny, $\sup \mathcal{R} = \bigcup \mathcal{R}$, gdzie:
 - ▶ $\text{Dom}(\bigcup \mathcal{R}) = \bigcup \{\text{Dom}(f) \mid f \in \mathcal{R}\}$;
 - ▶ jeśli $f \in \mathcal{R}$ i $f(x)$ jest określone, to $(\bigcup \mathcal{R})(x) = f(x)$.

259

Przykłady

- ▶ W zbiorze liczb wymiernych $\mathbb{Q}$, zbiór $\{q \in \mathbb{Q} \mid q^2 < 2\}$ ma ograniczenia górne, ale nie ma kresu górnego.
- ▶ W zbiorze liczb rzeczywistych $\mathbb{R}$ każdy niepusty podzbiór ograniczony z góry ma kres górny (i analogicznie z dołu). Własność tę nazywamy *ciągłością*.

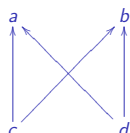
258

- ▶ Kres górny zbioru pustego to element najmniejszy.
- ▶ Kres dolny zbioru pustego to element największy.

260

Przykład

Podzbiór $\{c, d\}$ ma dwa ograniczenia górne...



ale nie ma kresu górnego.

261

Zasada minimum

262

Fakt

Każdy skończony i niepusty liniowy porządek ma element najmniejszy (i największy też).

Dowód: Indukcja ze względu na liczbę elementów. Dla zbioru pustego i zbiorów jednoelementowych oczywiste.

Założmy, że teza zachodzi dla zbiorów n -elementowych.

Niech $\langle A, \leq \rangle$ będzie liniowym porządkiem mocy $n + 1$.

Wtedy $A = B \cup \{a\}$, gdzie B ma n elementów.

Z założenia indukcyjnego B ma element najmniejszy b .

Jeśli teraz $b \leq a$, to b jest elementem najmniejszym w A .

A jeśli $a \leq b$, to elementem najmniejszym jest a . $\square$

263

Uogólnienie

Fakt

Każdy skończony i niepusty częściowy porządek ma element maksymalny i minimalny.

Dowód: Ćwiczenie. $\square$

(Co trzeba zmienić w poprzednim dowodzie?)

264

Fakt

Każdy niepusty podzbiór $A \subseteq \mathbb{N}$ ma element najmniejszy.

Dowód: Skoro A jest niepusty, to ma jakiś element n . Zbiór $B = \{m \in A \mid m \leq n\}$ jest podzbiorem $\overline{s(n)}$, więc jest skończony, a zatem ma element najmniejszy b , bo jest uporządkowany liniowo.

Liczba b jest elementem najmniejszym zbioru A . Istotnie, niech $m \in A$. Jeśli $m \leq n$, to $m \in B$, więc $b \leq m$. A jeśli $n < m$, to $b \leq n < m$, bo $n \in B$.

□

265

Trochę inna zasada indukcji

Wniosek

Jeśli $\forall n: \mathbb{N} (\forall m: \mathbb{N} (m < n \rightarrow W(m)) \rightarrow W(n))$,
to $\forall n: \mathbb{N}. W(n)$.

Dowód: Niech $A = \{n: \mathbb{N} \mid \neg W(n)\}$. Jeśli teza nie zachodzi, to zbiór A jest niepusty, ma więc element najmniejszy n . Wtedy $\forall m: \mathbb{N} (m < n \rightarrow W(m))$ ale nie jest spełniony warunek $W(n)$, co jest sprzeczne z założeniem. □

Morał: Aby udowodnić, że każda liczba naturalna ma własność W , wystarczy dla każdego n pokazać, że:

jeśli wszystkie liczby mniejsze od n mają własność W ,
to także n ma własność W

267

Zły przykład

Niefakt: W dowolnym skończonym zbiorze koni K wszystkie konie są tego samego koloru.

Niedowód: Jeśli zbiór K jest pusty, albo w zbiorze jest tylko jeden koń, to warunek jest spełniony.

Jeśli jest więcej koni, to wybierzmy jednego konia $k \in K$, a resztę zbioru K podzielmy na dwie mniejsze części A i B . Zbiory $A \cup \{k\}$ i $B \cup \{k\}$ są mniejsze niż zbiór K , więc konie w zbiorze $A \cup \{k\}$ są tego samego koloru i konie w zbiorze $B \cup \{k\}$ też.
No to wszystkie konie są tego samego koloru co koń k .

Gdzie jest błąd? To nie działa dla 2 koni.

269

Porządki dobrze ufundowane

Każdy niepusty podzbiór $A \subseteq \mathbb{N}$ ma element najmniejszy, tj. taki element $a \in A$, że $\forall b (b \in A \rightarrow a \leq b)$.

Oznaczenie: $a = \min A$

266

Przykład

Graf spójny, w którym nie ma cykli, nazywamy *drzewem*.

Fakt: Drzewo o $n \geq 1$ wierzchołkach ma $n - 1$ krawędzi.

Dowód: Indukcja ze względu na liczbę wierzchołków n .

Usuwaając jedną krawędź dostajemy dwa drzewa.

Jedno ma n_1 wierzchołków, drugie n_2 wierzchołków.

Razem jest $n_1 + n_2 = n$ wierzchołków.

Z założenia indukcyjnego, pierwsze drzewo ma $n_1 - 1$ krawędzi, a drugie $n_2 - 1$. Razem z tą usuniętą mamy dokładnie $n_1 - 1 + n_2 - 1 + 1 = n - 1$ krawędzi.

268

Poprzedni przykład jeszcze raz

Graf spójny, w którym nie ma cykli nazywamy *drzewem*.

Fakt: Drzewo o $n \geq 1$ wierzchołkach ma $n - 1$ krawędzi.

Dowód: Indukcja ze względu na liczbę wierzchołków n .

Jeśli drzewo nie ma krawędzi, to ma tylko 1 wierzchołek.

Warunek jest wtedy spełniony.

Dalej można założyć, że drzewo ma jakieś krawędzie.

Usuwaając jedną z nich dostajemy dwa drzewa...

270

Dobre ufundowanie

Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym.

Jeśli każdy niepusty podzbiór zbioru A ma element minimalny, to mówimy, że $\langle A, \leq \rangle$ jest *częściowym dobrym porządkiem*, lub, że A jest *dobrze ufundowany*.

Jeśli ponadto porządek $\langle A, \leq \rangle$ jest liniowy,

to jest to *dobry porządek*.

(Wtedy każdy niepusty podzbiór A ma element najmniejszy.)

271

272

Fakt

Zbiór $\langle A, \leq \rangle$ jest dobrze ufundowany wtedy i tylko wtedy, gdy nie istnieje w nim ciąg malejący, tj. taki podzbiór $\{a_i \mid i \in \mathbb{N}\}$, że $a_{i+1} < a_i$ dla dowolnego i .

Dowód: $(\Rightarrow)$ Gdyby taki istniał, to by nie miał elementu minimalnego.

$(\Leftarrow)$ Przypuśćmy, że niepusty podzbiór $B \subseteq A$ nie ma elementu minimalnego. Skoro B jest niepusty, to ma jakiś element b_0 . On oczywiście nie jest minimalny, więc jest takie $b_1 \in B$, że $b_1 < b_0$. I tak dalej: przez indukcję określamy ciąg malejący $b_0 > b_1 > b_2 > \dots$ $\square$

273

Definicja

W porządku częściowym $\langle A, \leq \rangle$ odcinkiem początkowym wyznaczonym przez element $x \in A$ nazwiemy zbiór:

$$\mathcal{O}_A(x) = \{y \in A \mid y < x\}.$$

Zasada indukcji

Niech $\langle A, \leq \rangle$ będzie dobrze ufundowany i niech $W \subseteq A$. Załóżmy, że dla dowolnego $a \in A$ zachodzi implikacja:

$$\mathcal{O}_A(a) \subseteq W \Rightarrow a \in W.$$

Wtedy $W = A$.

Dowód: Przypuśćmy, że $W \neq A$. Zbiór $A - W$ jest wtedy niepusty i ma element minimalny a . Z minimalności mamy jednak $\mathcal{O}_A(a) \subseteq W$, więc $a \in W$. $\square$

275

Przykład: funkcja Ackermanna-Sudana

Fakt: Następująca procedura rekurencyjna

```
A(n, m) = if n = 0 then m + 1
           else if m = 0 then A(n - 1, 1)
           else A(n - 1, A(n, m - 1))
```

zatrzymuje się dla dowolnej pary $\langle n, m \rangle \in \mathbb{N}^2$.

Dowód: Indukcja ze względu na porządek leksykograficzny w zbiorze $\mathbb{N}^2$. („Indukcja ze względu na dwa parametry”)

Dowodzimy, że: „ $A(n, m)$ jest określone”

przy założeniu: „ $A(i, j)$ jest określone dla wszystkich par $\langle i, j \rangle$ leksykograficznie mniejszych od $\langle n, m \rangle$ ”.

277

Funkcja Ackermanna-Sudana

```
A(n, m) = if n = 0 then m + 1
           else if m = 0 then A(n - 1, 1)
           else A(n - 1, A(n, m - 1))
```

Inaczej: $A(n, m) = A_n(m)$, gdzie

$$A_0(m) = m + 1 \text{ oraz } A_{n+1}(0) = A_n(1), \\ A_{n+1}(m + 1) = A_n(A_{n+1}(m)).$$

Czyli $A_{n+1}(m) = A_n^{m+1}(1)$.

279

- Każdy porządek skończony jest dobrze ufundowany.
- Zbiór $\mathbb{N}$ jest dobrze uporządkowany przez zwykłe $\leq$.
- Zbiór $\mathbb{N}$ jest dobrze ufundowany przez podzielność.
- Zbiór $\mathbb{N} \times \mathbb{N}$ jest dobrze uporządkowany leksykograficznie.
- Zbiory $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $[0, 1]$ nie są dobrze ufundowane.
- Zbiór $\mathcal{P}(\mathbb{N})$ nie jest dobrze ufundowany przez inkluzję...
...bo rodzina wszystkich zbiorów nieskończonych nie ma elementu minimalnego.

274

Morał

Można dowodzić przez indukcję (i definiować przez indukcję) ze względu na dowolny zbiór dobrze ufundowany.

276

Przykład: funkcja Ackermanna-Sudana

Fakt: Następująca procedura rekurencyjna

```
A(n, m) = if n = 0 then m + 1
           else if m = 0 then A(n - 1, 1)
           else A(n - 1, A(n, m - 1))
```

zatrzymuje się dla dowolnej pary $\langle n, m \rangle \in \mathbb{N}^2$.

Dowód: Indukcja ze względu na porządek leksykograficzny w zbiorze $\mathbb{N}^2$. („Indukcja ze względu na dwa parametry”)

Dla $n = 0$ teza jest oczywista.

Dla $n > 0$ i $m = 0$, użyjemy zał. indukcyjnego o $\langle n - 1, 1 \rangle$.

Jeśli $n > 0$ i $m > 0$, to z założenia indukcyjnego o $\langle n, m - 1 \rangle$ obliczenie $A(n, m - 1)$ zatrzymuje się z pewnym wynikiem a . Teraz używamy założenia indukcyjnego dla $\langle n - 1, a \rangle$.

278

$$A_0(m) = m + 1 \quad A_{n+1}(m) = A_n^{m+1}(1) \quad \text{Jak szybko to rośnie?}$$

Najpierw powoli, jak żółw ociężale...

$$A_1(m) = m + 2,$$

I biegu przyspiesza,...

$$A_2(m) = 2m + 3 > 2m$$

i gna coraz prędszej,...

$$A_3(m) > 2^m$$

$$A_4(m) = 2^{2^{\cdot^{\cdot^{\cdot}}}} m$$

A skądże to, jakże to, czemu tak gna?

Indukcja podwójna wprawiła to w ruch!

280

Można dowodzić przez indukcję (i definiować przez indukcję) ze względu na dowolny zbiór dobrze ufundowany.

Na przykład wtedy, kiedy sam zbiór jest skonstruowany przez indukcję – wtedy mamy indukcję *strukturalną*.

Dziedziny zdefiniowane przez indukcję nazywamy *typami indukcyjnymi*.

Słowa

281

282

Typ indukcyjny: słowa nad $\{a, b\}$

Naśladując Giuseppe Peana:

- ▶ Słowo puste ε jest słowem.
- ▶ Każde słowo w można przedłużyć, dopisując na końcu literę a lub b (oznaczenie wa , wb).
- ▶ Jeśli $wa = va$ lub $wb = vb$ to $w = v$;
- ▶ Słowa wa i vb są różne i niepuste;
- ▶ Zasada indukcji?

283

Zasada indukcji dla słów

Jeśli

- ▶ słowo puste ma własność X ,
- ▶ z tego, że słowo w ma własność X wynika, że słowa wa i wb też mają własność X ,

to

- ▶ każde słowo ma własność X .

$$X(\varepsilon) \wedge (\forall w: \{a, b\}^* (X(w) \rightarrow X(wa) \wedge X(wb))) \rightarrow \rightarrow \forall w: \{a, b\}^*. X(w).$$

284

Definiowanie przez indukcję

Długość słowa:

- ▶ $|\varepsilon| = 0$;
- ▶ $|wa| = |w| + 1$;
- ▶ $|wb| = |w| + 1$.

Składanie (konkatenacja) słów:

- ▶ $w \cdot \varepsilon = w$;
- ▶ $w \cdot va = (w \cdot v)a$;
- ▶ $w \cdot vb = (w \cdot v)b$.

Konkatenacja jest łączna:

$$\text{ein} \cdot (\text{und} \cdot \text{zwanzig}) = (\text{ein} \cdot \text{und}) \cdot \text{zwanzig} = \text{einundzwanzig}.$$

285

Dowodzenie przez indukcję

Fakt

Dla dowolnych słów v i w zachodzi $|w \cdot v| = |w| + |v|$.

Dowód: Udowodnimy, że każde słowo v ma własność

$$\forall w: \{a, b\}^*. |w \cdot v| = |w| + |v|.$$

Krok bazowy: Ponieważ $w \cdot \varepsilon = w$, więc $|w \cdot \varepsilon| = |w|$.

Krok indukcyjny: Niech $|w \cdot v| = |w| + |v|$ dla wszystkich w .

$$|w \cdot va| = |(w \cdot v)a| = |w \cdot v| + 1 = |w| + |v| + 1 = |w| + |va|.$$

Drugi przypadek jest analogiczny. $\square$

Ćwiczenie: Udowodnić, że $\forall w (\varepsilon \cdot w = w)$.

286

Porządek prefiksowy

Definicja: $w \subseteq v \Leftrightarrow \exists u (v = w \cdot u)$.

Fakt

Relacja $\subseteq$ jest częściowym porządkiem, na dodatek dobrze ufundowany.

Dowód: Zwrotność i przechodność są oczywiste.

Antysymetria: jeśli $w = vx$ i $v = wy$ to $w = wyx$.

Ale $|w| = |wyx| = |w| + |y| + |x|$, więc $x = y = \varepsilon$.

Ufundowanie: w malejącym ciągu słów maleje też długość. $\square$

287

Porządek leksykograficzny

Założmy, że alfabet A jest uporządkowany przez relację $\leq$. Dla $w, v \in A^*$, przyjmujemy, że $w \preceq v$, gdy:

- ▶ $w \subseteq v$, albo
- ▶ istnieje takie słowo u , że $ua \subseteq w$ i $ub \subseteq v$, dla pewnych $a, b \in A$ takich, że $a < b$.

Na przykład, jeśli $a < b$, to $\varepsilon \preceq ab \preceq aba \preceq baba \preceq bba$ (decyduje pierwsza różnica).

288

Fakt

Porządek leksykograficzny jest relacją częściowego porządku w zbiorze A^* . Jeśli alfabet jest liniowo uporządkowany, to porządek leksykograficzny też jest liniowy.

Dowód: Zwrotność wynika ze zwrotności relacji $\subseteq$.

Przechodność (przykłady)

agfr	agfr	agf ^r rtzj	agf ^r rtzj	agf ^r rtzj
agfr ^v sj	agfr ^v sj	ah	agg ^b ds	agf ^r zzj
agf ^r zg	ahf ^r vsj	ahgsfadr	aggb ^d va	anhg

Antysymetria

Żaden nietrywialny przypadek nie jest możliwy.

Spójność

Zawsze jest „pierwsza różnica” (lub walkower). $\square$

289

Porządek leksykograficzny

Uwaga: Jeśli w A są dwa elementy a, b , takie że $a < b$, to porządek leksykograficzny $\preceq$ nie jest dobrym ufundowaniem zbioru A^* .

Bo np. zbiór $\{a^n b \mid n \in \mathbb{N}\}$ nie ma elementu minimalnego. Istotnie, $a^n b > a^{n+1} b$, dla każdego n .

290

Typy indukcyjne

Co łączy ze sobą liczby naturalne i słowa?

- Definicja przez konstruktory;
- Indukcja.

Takie dziedziny nazywamy *typami indukcyjnymi*.

291

Typy indukcyjne

Obiekty typu indukcyjnego tworzone są przez *konstruktory*.

Każdy element można otrzymać tylko w jeden sposób, przez pewne złożenie konstruktorów.

Z typem indukcyjnym związane są

- ▶ swoista zasada indukcji;
- ▶ swoisty schemat definiowania przez indukcję.

292

Listy

Listy liczb naturalnych tworzą typ indukcyjny **list** generowany przez dwa konstruktory:

$\text{nil} : \text{list}$, oraz $\text{cons} : \mathbb{N} \times \text{list} \rightarrow \text{list}$.

Zamiast $\text{cons}(n, \ell)$ często piszemy $n :: \ell$.

Zasada indukcji:

$W(\text{nil}) \wedge \forall \ell : \text{list} (W(\ell) \rightarrow \forall n : \mathbb{N}. W(n :: \ell)) \rightarrow \forall \ell : \text{list}. W(\ell)$.

Schemat definiowania przez indukcję:

$f(\text{nil}, d) = g(d);$
 $f(n :: \ell, d) = h(\ell, n, d, f(\ell, d)).$

293

Inne typy indukcyjne

Drzewa binarne:

$\text{leaf} : \text{tree}$ $\text{node} : \text{tree} \times \text{tree} \rightarrow \text{tree}$

Omega-drzewa:

$\text{leaf} : \omega\text{-tree}$ $\text{node} : (\mathbb{N} \rightarrow \omega\text{-tree}) \rightarrow \omega\text{-tree}.$

294

Typy indukcyjne z trywialną indukcją

Suma prosta:

Suma prosta $A \oplus B$ ma dwa konstruktory
 $\text{in}_1 : A \rightarrow A \oplus B$, $\text{in}_2 : B \rightarrow A \oplus B$.

Dowodzenie przez indukcję sprowadza się do dwóch przypadków. (Nie ma założenia indukcyjnego.)

Iloczyn kartezjański:

Iloczyn $A \times B$ ma jeden konstruktor $\text{para} : A \rightarrow (B \rightarrow A \times B)$.

Typ jednostkowy:

Typ **Unit** ma jeden konstruktor $\bullet \in \text{Unit}$.

Typ Bool:

Typ wartości logicznych **Bool** to suma prosta $\text{Unit} \oplus \text{Unit}$.

295

Abstrakcyjna składnia

Wyrażenia algebraiczne (*termy*), w których występują (na przykład):

zmienne ze zbioru $V = \{x_i \mid i \in \mathbb{N}\}$,

stałe ze zbioru $\{0, 1\}$,

operacje $+$ oraz $*$,

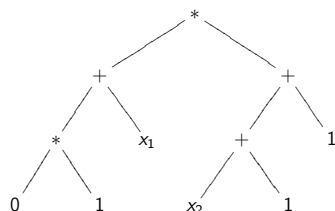
tworzą typ indukcyjny **WA** o konstruktorach:

$x : \mathbb{N} \rightarrow \text{WA}$,
 $0, 1 : \text{WA}$,
 $+, * : \text{WA} \times \text{WA} \rightarrow \text{WA}$.

296

Przykład: składnia abstrakcyjna

Wyrażenie algebraiczne (term) to w istocie drzewo, np. takie:



Taki term można zapisać tak:

$*(+(* (0, 1), x_1), +(+(x_2, 1), 1))$
albo tak: $((0 * 1) + x_1) * ((x_2 + 1) + 1)$.

297

Składnia konkretna

Składnia abstrakcyjna termu to jego faktyczna struktura. Term można sobie wyobrażać jako drzewo.

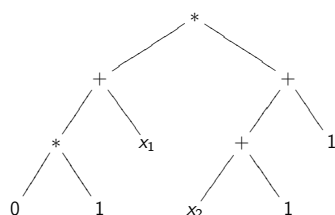
Składnia konkretna, to przedstawienie termu w postaci napisu. Może używać nawiasów, albo konwencji notacyjnych, na przykład określenia priorytetów:

- Mnożenie ma wyższy priorytet niż dodawanie,
- Dodawanie wykonujemy od lewej, itp.

Wtedy wyrażenie $((0 * 1) + x_1) * ((x_2 + 1) + 1)$ można zapisać w postaci $(0 * 1 + x_1) * (x_2 + 1 + 1)$.

298

Różne składnie konkretne



Taki term można zapisać tak: $(0 * 1 + x_1) * (x_2 + 1 + 1)$.

Albo tak: $*(+(* (0, 1), x_1), +(+(x_2, 1), 1))$.

Albo: $* + * 0 1 x_1 + + x_2 1 1$ (notacja polska).

Albo: $0 1 * x_1 + x_2 1 + 1 + *$ (notacja odwrotna polska).

299

Definiowanie przez indukcję

Wartościowanie zmiennych ze zbioru $V = \{x_i \mid i \in \mathbb{N}\}$ w zbiorze $\mathbb{N}$, to dowolna funkcja $v : V \rightarrow \mathbb{N}$.

Uówmy się, że znaki $+$, $*$, 0 i 1 interpretujemy jak zwykle.

Wartość termu t przy wartościowaniu v , ozn. $\llbracket t \rrbracket_v$, definiujemy przez indukcję:

$\llbracket x_i \rrbracket_v = v(x_i)$, $\llbracket 0 \rrbracket_v = 0$, $\llbracket 1 \rrbracket_v = 1$.

$\llbracket t + u \rrbracket_v = \llbracket t \rrbracket_v + \llbracket u \rrbracket_v$, $\llbracket t * u \rrbracket_v = \llbracket t \rrbracket_v * \llbracket u \rrbracket_v$.

Jeśli $v(x_1)=7$ i $v(x_2)=3$, to $\llbracket (0 * 1 + x_1) * (x_2 + 1 + 1) \rrbracket_v = 35$.

Ale możemy się umówić inaczej.

300

Logika formalna

(Klasyczny rachunek zdań)

Składnia (abstrakcyjna) rachunku zdań

- **Symbole** (zmienne) zdaniowe $(p, q, r, \dots)$, oraz stałe $\perp$ i $\top$ są formułami zdaniowymi.

- Jeśli α jest formułą zdaniową, to także $\neg \alpha$ jest formułą zdaniową.

- Jeśli α i β są formułami zdaniowymi to

$$\alpha \rightarrow \beta, \alpha \vee \beta, \alpha \wedge \beta$$

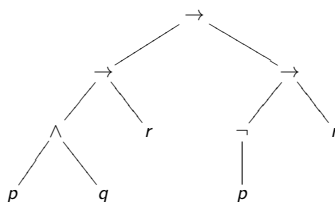
też są formułami zdaniowymi.

Inaczej: formuły zdaniowe tworzą typ indukcyjny, o konstruktorach $p, q, r, \dots, \perp, \top, \neg, \rightarrow, \vee, \wedge$

301

302

Przykład: składnia abstrakcyjna



Składnia konkretna: $(p \wedge q \rightarrow r) \rightarrow (\neg p \rightarrow r)$

Składnia konkretna

- Koniunkcja i alternatywa mają wyższy priorytet niż implikacja: zamiast $(p \wedge q) \rightarrow r$ piszemy $p \wedge q \rightarrow r$.
- Negacja ma najwyższy priorytet: napis $\neg p \rightarrow q$ oznacza implikację.
- Koniunkcja i alternatywa mają ten sam priorytet: napis $p \vee q \wedge r$ jest niepoprawny.
- Ale wielokrotną koniunkcję (alternatywę) piszemy bez nawiasów: napis $p \vee q \vee r$ oznacza $(p \vee q) \vee r$.

Przykłady:

$(p \wedge q \rightarrow r) \rightarrow (\neg p \rightarrow r)$

$p \wedge (q \rightarrow r) \rightarrow \neg(p \rightarrow r)$

303

304

- Napis $\alpha \leftrightarrow \beta$ jest skrótem napisu $(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$.

305

Przykład

Formuła $(p \wedge q \rightarrow r) \rightarrow (\neg p \rightarrow r)$ ma wartość jeden przy interpretacji ϱ , gdzie

$$\varrho(p) = \varrho(r) = 1 \quad \text{i} \quad \varrho(q) = 0.$$

Ta sama formuła ma wartość zero przy interpretacji μ , gdzie

$$\mu(p) = \mu(r) = 0 \quad \text{i} \quad \mu(q) = 1.$$

307

Spełnialność i prawdziwość

Jeśli $\llbracket \varphi \rrbracket_{\varrho} = 1$, to piszemy też $\varrho \models \varphi$ i mówimy, że formuła φ jest *spełniona* przez interpretację ϱ .

Formuła φ jest *spełnialna*, gdy $\varrho \models \varphi$ zachodzi dla pewnej interpretacji ϱ .

Formuła spełniona przy *każdej* interpretacji jest *prawdziwa* (jest *tautologią*). Piszemy $\models \varphi$.

309

Przykłady tautologii

- Prawo wyłączonego środka: $p \vee \neg p$.
- Prawo podwójnego przeczenia: $\neg \neg p \leftrightarrow p$.
- Prawa De Morgana:
 - $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$;
 - $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$.

311

Semantyka rachunku zdań

Interpretacja zdaniowa (inaczej: *wartościowanie zdaniowe*) to funkcja ϱ , która każdej zmiennej zdaniowej p przypisuje wartość logiczną $\varrho(p) \in \{0, 1\}$.

Wartość formuły przy interpretacji ϱ definiujemy (oczywiście) przez indukcję:

- $\llbracket \perp \rrbracket_{\varrho} = 0$ oraz $\llbracket \top \rrbracket_{\varrho} = 1$;
- $\llbracket p \rrbracket_{\varrho} = \varrho(p)$, gdy p jest symbolem zdaniowym;
- $\llbracket \neg \alpha \rrbracket_{\varrho} = 1 - \llbracket \alpha \rrbracket_{\varrho}$;
- $\llbracket \alpha \vee \beta \rrbracket_{\varrho} = \max\{\llbracket \alpha \rrbracket_{\varrho}, \llbracket \beta \rrbracket_{\varrho}\}$;
- $\llbracket \alpha \wedge \beta \rrbracket_{\varrho} = \min\{\llbracket \alpha \rrbracket_{\varrho}, \llbracket \beta \rrbracket_{\varrho}\}$;
- $\llbracket \alpha \rightarrow \beta \rrbracket_{\varrho} = 0$, gdy $\llbracket \alpha \rrbracket_{\varrho} = 1$ i $\llbracket \beta \rrbracket_{\varrho} = 0$;
- $\llbracket \alpha \rightarrow \beta \rrbracket_{\varrho} = 1$, w przeciwnym przypadku.

306

Równoważność i implikacja

- Co znaczy napis: $p \leftrightarrow q \leftrightarrow r$?
- Formuły $((p \leftrightarrow q) \leftrightarrow r)$ i $(p \leftrightarrow (q \leftrightarrow r))$ są równoważne.
- Ale żadna z nich **nie jest** równoważna formule $(p \leftrightarrow q) \wedge (q \leftrightarrow r)$.
- Zdania postaci $((p \rightarrow q) \rightarrow r)$ i $(p \rightarrow (q \rightarrow r))$ **nie są** równoważne.
- I żadne z nich **nie jest** równoważne zdaniu $(p \rightarrow q) \wedge (q \rightarrow r)$.
- Co znaczy napis $p \rightarrow q \rightarrow r$?
- Czasami znaczy $p \rightarrow (q \rightarrow r)$ (taka konwencja).

308

Wnioskowanie z przesłanek

Mówimy, że formuła φ jest *konsekwencją* zbioru założeń Γ i piszemy $\Gamma \models \varphi$, gdy dla dowolnej interpretacji zdaniowej ϱ , jeżeli $\llbracket \gamma \rrbracket_{\varrho} = 1$ dla każdego $\gamma \in \Gamma$, to także $\llbracket \varphi \rrbracket_{\varrho} = 1$.

Przykład: $\{\varphi \rightarrow \psi, \psi \rightarrow \vartheta\} \models \varphi \rightarrow \vartheta$.

(Można to napisać bez klamerek: $\varphi \rightarrow \psi, \psi \rightarrow \vartheta \models \varphi \rightarrow \vartheta$.)

Związek $\Gamma \models \varphi$ to ogólnie poprawny schemat wnioskowania.

310

Łączność i przemienność

- $(p \vee q) \vee r \leftrightarrow p \vee (q \vee r)$;
- $(p \wedge q) \wedge r \leftrightarrow p \wedge (q \wedge r)$;
- $(p \vee q) \leftrightarrow (q \vee p)$;
- $(p \wedge q) \leftrightarrow (q \wedge p)$.

Morał:
można pisać $p \vee q \vee r \vee \dots$ nie dbając o nawiasy i kolejność.

312

- ▶ $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$.
- ▶ $\neg(p \rightarrow q) \leftrightarrow (p \wedge \neg q)$.
- ▶ $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ (prawo kontrapozycji).
- ▶ $\neg p \leftrightarrow (p \rightarrow \perp)$.
- ▶ $p \wedge (p \rightarrow q) \rightarrow q$ (odrywanie, czyli modus ponens).

313

Normalizacja formuł

Literał to symbol zdaniowy lub negacja symbolu zdaniowego.

Formuła zdaniowa φ jest w **koniunkcyjnej postaci normalnej**, gdy φ jest koniunkcją alternatyw literałów, tj. wygląda tak:

$$(p_1^1 \vee \dots \vee p_1^{k_1}) \wedge \dots \wedge (p_r^1 \vee \dots \vee p_r^{k_r}),$$

gdzie wszystkie p_j^i są literałami.

Przykład: $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$

Uwaga: (1) Stała $\top$ to pusta koniunkcja ($r = 0$).
(2) Stała $\perp$ to jedna pusta alternatywa ($r = 1, k_1 = 0$).

315

Normalizacja formuł

Dana jest formuła, w której występują tylko $\vee, \wedge$ i $\neg$.
Jeśli ta formuła nie jest w postaci normalnej

$$(p_1^1 \vee \dots \vee p_1^{k_1}) \wedge \dots \wedge (p_r^1 \vee \dots \vee p_r^{k_r}),$$

to zawiera „podformułę” jednej z następujących postaci:

$$\begin{array}{ccccccc} \neg(\alpha \vee \beta), & \neg(\alpha \wedge \beta), & \neg\top, & \neg\perp, & \neg\neg\alpha, \\ \top \vee \alpha, & \top \wedge \alpha, & \perp \wedge \alpha, & \perp \vee \alpha \\ & & \alpha \vee (\beta \wedge \gamma) \end{array}$$

(z dokładnością do kolejności argumentów).

317

Przykład

Formułę $\neg(p \vee \neg q) \vee (r \wedge \top)$ przepisujemy do postaci:

$$\begin{array}{l} \neg(p \vee \neg q) \vee r \\ (\neg p \wedge \neg\neg q) \vee r \\ (\neg p \wedge q) \vee r \\ (\neg p \vee r) \wedge (q \vee r). \end{array}$$

Wszystkie te formuły są równoważne.
Ostatnia formuła jest w koniunkcyjnej postaci normalnej.

319

Koniunkcja i alternatywa

Alternatywa to najsilniejszy warunek, który wynika zarówno z p jak i q .

- ▶ $p \rightarrow (p \vee q), \quad q \rightarrow (p \vee q),$
- ▶ $(p \rightarrow r) \rightarrow ((q \rightarrow r) \rightarrow (p \vee q \rightarrow r)).$

Koniunkcja to najsłabszy warunek, z którego wynika zarówno p jak q .

- ▶ $(p \wedge q) \rightarrow p, \quad (p \wedge q) \rightarrow q,$
- ▶ $(r \rightarrow p) \rightarrow ((r \rightarrow q) \rightarrow (r \rightarrow p \wedge q)).$

Elementy wyróżnione:

- ▶ $p \vee \perp \leftrightarrow p, \quad p \vee \top \leftrightarrow \top,$
- ▶ $p \wedge \perp \leftrightarrow \perp, \quad p \wedge \top \leftrightarrow p.$

314

Normalizacja formuł

Twierdzenie: Dla każdej formuły zdaniowej istnieje równoważna jej formuła w koniunkcyjnej postaci normalnej.

Szkic dowodu:

Najpierw eliminujemy implikacje, stosując zasadę:

$$(\alpha \rightarrow \beta) \leftrightarrow (\neg\alpha \vee \beta).$$

Otrzymujemy formułę, w której występują tylko $\vee, \wedge$ i $\neg$.

316

Reguły przepisywania

Eliminujemy podwójne i trywialne negacje:

$$\neg\neg\alpha \Rightarrow \alpha \quad \neg\top \Rightarrow \perp \quad \neg\perp \Rightarrow \top$$

„Przesuwamy w dół” negacje z pomocą praw De Morgana:

$$\neg(\alpha \vee \beta) \Rightarrow (\neg\alpha \wedge \neg\beta) \quad \neg(\alpha \wedge \beta) \Rightarrow (\neg\alpha \vee \neg\beta)$$

Eliminujemy nadmiar stałych logicznych:

$$\begin{array}{ll} \top \vee \alpha \Rightarrow \top, & \top \wedge \alpha \Rightarrow \alpha, \\ \perp \wedge \alpha \Rightarrow \perp, & \perp \vee \alpha \Rightarrow \alpha. \end{array}$$

„Przesuwamy w dół” alternatywy:

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

318

Dlaczego ta procedura musi się zakończyć?

Każdej formule (bez $\rightarrow$) przypiszemy liczbową **wagę**:

- ▶ $waga(p) = 2$, gdy p jest atomem (w tym $\top, \perp$).
- ▶ $waga(\varphi \wedge \psi) = waga(\varphi) + waga(\psi) + 2$;
- ▶ $waga(\varphi \vee \psi) = 2 \cdot waga(\varphi) \cdot waga(\psi)$;
- ▶ $waga(\neg\varphi) = 2^{waga(\varphi)}$.

Fakt: Każda operacja zmniejsza wagę.

Weźmy na przykład $\neg(\alpha \vee \beta) \Rightarrow (\neg\alpha \wedge \neg\beta)$.

Niech $waga(\alpha) = a$ i $waga(\beta) = b$. Wtedy:

$$\begin{array}{l} waga(\neg(\alpha \vee \beta)) = 2^{waga(\alpha \vee \beta)} = 2^{2ab}; \\ waga(\neg\alpha \wedge \neg\beta) = 2^a + 2^b + 2 < 2^{2ab}. \end{array}$$

320

Operacja

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

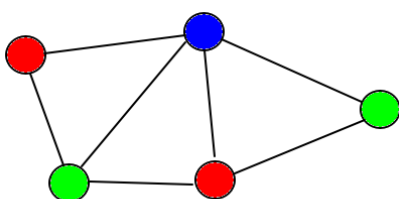
podwaja podformułę α . Wielokrotne poddawanie może wykładniczo zwiększyć rozmiary całej formuły.

Jakiej wielkości jest postać normalna tej formuły?

$$(p_1 \wedge q_1) \vee (p_2 \wedge q_2) \vee \dots \vee (p_n \wedge q_n)$$

321

Ten graf jest trójkolorowy



323

Kolorowanie grafu

Dany graf $\mathcal{G} = \langle G, r \rangle$. Określmy tak zbiór formuł $\Gamma_{\mathcal{G}}$, że:

$$\mathcal{G} \text{ jest trójkolorowy} \Leftrightarrow \Gamma_{\mathcal{G}} \text{ jest spełnialny.}$$

w ten sposób pytanie dotyczące grafu sprowadzimy do pytania o spełnialność. (Podobnie można robić z innymi pytaniami.)

Użyjemy do tego zmiennych zdaniowych postaci p_a^i , dla $a \in G$ oraz $i \in \{1, 2, 3\}$. (Sens: wierzchołek a ma kolor i .)

Każde wartościowanie zmiennych p_a^i odpowiada pewnemu powiązaniu kolorów z wierzchołkami grafu.

Warunki $\Gamma_{\mathcal{G}}$ mówią, że to powiązanie jest poprawne.

322

Rachunek predykatów

(pierwszego rzędu)

326

Kolorowanie grafu

Dany graf $\mathcal{G} = \langle G, r \rangle$. Określmy tak zbiór formuł $\Gamma_{\mathcal{G}}$, że:

$$\mathcal{G} \text{ jest trójkolorowy} \Leftrightarrow \Gamma_{\mathcal{G}} \text{ jest spełnialny.}$$

w ten sposób pytanie dotyczące grafu sprowadzimy do pytania o spełnialność. (Podobnie można robić z innymi pytaniami.)

Użyjemy do tego zmiennych zdaniowych postaci p_a^i , dla $a \in G$ oraz $i \in \{1, 2, 3\}$. (Sens: wierzchołek a ma kolor i .)

W zbiorze $\Gamma_{\mathcal{G}}$ są takie formuły:

$$\alpha_a = (p_a^1 \vee p_a^2 \vee p_a^3) \wedge \neg(p_a^1 \wedge p_a^2) \wedge \neg(p_a^1 \wedge p_a^3) \wedge \neg(p_a^2 \wedge p_a^3),$$

dla każdego $a \in G$. (Element a ma dokładnie jeden kolor.)

$$\beta_{ab} = \neg(p_a^1 \wedge p_b^1) \wedge \neg(p_a^2 \wedge p_b^2) \wedge \neg(p_a^3 \wedge p_b^3),$$

dla każdej pary $\langle a, b \rangle \in r$. (Elementy a i b są różnego koloru.)

325

Język logiki pierwszego rzędu

- ▶ Zmienne indywidualne, np. $x, y, \dots$
- ▶ Symbole relacyjne, np. $r, \leq$, itp.
- ▶ Symbole funkcyjne (w tym stałe), np. $+$, f , $\$$.

Symbole funkcyjne i relacyjne tworzą *sygnaturę*. (Taka sygnatura jest zwykle skończona.)

Na przykład sygnatura arytmetyki może być taka:

$$+, *, 0, 1, \leq.$$

327

Formuły pierwszego rzędu

- ▶ Formuły atomowe $r(t_1, \dots, t_n)$ są formułami, gdzie r to symbol relacyjny a $t_1, \dots, t_n$ to termy (wyrażenia algebraiczne). (Zwykle piszemy np. $t_1 + t_2$ zamiast $+(t_1, t_2)$.)

- ▶ Stałe logiczne $\perp$, $\top$ są formułami.

- ▶ Jeśli φ, ψ są formułami, to

$$\varphi \rightarrow \psi, \quad \varphi \vee \psi, \quad \varphi \wedge \psi, \quad \neg \varphi$$

są formułami.

- ▶ Jeśli φ jest formułą, a x zmienną indywidualną, to

$$\forall x \varphi, \quad \exists x \varphi$$

są formułami.

328

$FV(\varphi)$ to zbiór wszystkich *zmiennych wolnych* formuły φ :

$FV(r(t_1, \dots, t_n))$ to zbiór wszystkich zmiennych w $t_1, \dots, t_n$.

$FV(\alpha \vee \beta) = FV(\alpha \wedge \beta) = FV(\alpha \rightarrow \beta) = FV(\alpha) \cup FV(\beta)$,

$FV(\top) = FV(\perp) = \emptyset$,

$FV(\neg \alpha) = FV(\alpha)$,

$FV(\forall x \varphi) = FV(\exists x \varphi) = FV(\varphi) - \{x\}$.

Na przykład $FV(\forall x (r(x, x) \rightarrow r(x, y)) \vee \exists z r(x, z)) = \{x, y\}$.

329

Struktura relacyjna (także: *model*, *interpretacja*),

to niepusty zbiór wraz z odpowiednimi relacjami i funkcjami:

$$\mathcal{A} = \langle A, r_1^{\mathcal{A}}, \dots, r_n^{\mathcal{A}}, f_1^{\mathcal{A}}, \dots, f_m^{\mathcal{A}} \rangle$$

Wartościowanie w strukturze $\mathcal{A}$, to funkcja $v : V \rightarrow A$.

Znaczenie formuły φ przy wartościowaniu v

to jej wartość logiczna $\llbracket \varphi \rrbracket_v \in \{0, 1\}$.

330

Semantyka formuł

Znaczenie formuły φ przy wartościowaniu v

to jej wartość logiczna $\llbracket \varphi \rrbracket_v \in \{0, 1\}$.

Znaczenie formuły atomowej:

- ▶ $\llbracket \perp \rrbracket_v = 0$;
- ▶ $\llbracket \top \rrbracket_v = 1$;
- ▶ $\llbracket r(t_1, \dots, t_n) \rrbracket_v = 1$, gdy $\langle \llbracket t_1 \rrbracket_v, \dots, \llbracket t_n \rrbracket_v \rangle \in r^{\mathcal{A}}$;
- ▶ $\llbracket r(t_1, \dots, t_n) \rrbracket_v = 0$, w przeciwnym przypadku.

331

Znaczenie formuł złożonych

- ▶ $\llbracket \neg \alpha \rrbracket_v = 1 - \llbracket \alpha \rrbracket_v$;
- ▶ $\llbracket \alpha \vee \beta \rrbracket_v = \max\{\llbracket \alpha \rrbracket_v, \llbracket \beta \rrbracket_v\}$;
- ▶ $\llbracket \alpha \wedge \beta \rrbracket_v = \min\{\llbracket \alpha \rrbracket_v, \llbracket \beta \rrbracket_v\}$;
- ▶ $\llbracket \alpha \rightarrow \beta \rrbracket_v = 0$, gdy $\llbracket \alpha \rrbracket_v = 1$ i $\llbracket \beta \rrbracket_v = 0$;
- ▶ $\llbracket \alpha \rightarrow \beta \rrbracket_v = 1$, w przeciwnym przypadku.

332

Znaczenie formuł z kwantyfikatorami

Poniżej, $v[x \mapsto a]$ oznacza takie wartościowanie, że

$v[x \mapsto a](x) = a$ oraz $v[x \mapsto a](y) = v(y)$.

- ▶ $\llbracket \forall x \varphi \rrbracket_v = \min\{\llbracket \varphi \rrbracket_{v[x \mapsto a]} \mid a \in A\}$;
- ▶ $\llbracket \exists x \varphi \rrbracket_v = \max\{\llbracket \varphi \rrbracket_{v[x \mapsto a]} \mid a \in A\}$.

333

Przykład

Znaczeniem formuły $\exists z(x < z \wedge z < y)$ w strukturze $\langle \mathbb{Q}, < \rangle$,

- przy wartościowaniu $v(x) = 1$, $v(y) = 2$ jest 1,
- przy wartościowaniu $v(x) = 3$, $v(y) = 2$ jest 0.

Znaczeniem tej samej formuły w strukturze $\langle \mathbb{Z}, < \rangle$,

- przy wartościowaniu $v(x) = 1$, $v(y) = 2$ jest 0,
- przy wartościowaniu $v(x) = 1$, $v(y) = 7$ jest 1.

334

Ważny fakt:

Znaczenie formuły zależy tylko od wartości jej zmiennych wolnych. Ścisłej:

Jeśli $v(x) = w(x)$ dla każdego $x \in FV(\varphi)$, to $\llbracket \varphi \rrbracket_v = \llbracket \varphi \rrbracket_w$

(Dowód: indukcja ze względu na budowę formuły.)

Zdanie, to formuła, która nie ma zmiennych wolnych.

Na przykład formuła $\exists x \forall y (x \leq y)$ jest zdaniem, a formuła $\forall y (x \leq y \wedge y \leq z)$ nie jest zdaniem.

W ustalonej strukturze zdanie jest albo prawdziwe albo fałszywe (niezależnie od wartościowania).

335

Spełnialność i prawdziwość

Formuła jest *spełnialna* (*spełnialna w $\mathcal{A}$*) jeśli jest spełniona w pewnym modelu (w modelu $\mathcal{A}$) przez pewne wartościowanie.

Formuła φ jest *prawdziwa w $\mathcal{A}$* (piszemy $\mathcal{A} \models \varphi$), jeżeli jest spełniona w $\mathcal{A}$ przez wszystkie wartościowania.

Formuła φ jest *prawdziwa* (jest *tautologią*), jeżeli jest prawdziwa w każdym modelu $\mathcal{A}$. Wtedy piszemy $\models \varphi$.

336

Przykład

Zdanie $\forall x(P(x) \vee Q(x)) \rightarrow \forall x P(x) \vee \forall x Q(x)$
nie jest tautologią, ale jest spełnialne.

Interpretacja pierwsza: zbiór liczb naturalnych, gdzie $P(x)$ oznacza parzystość, a $Q(x)$ nieparzystość liczby x .

Interpretacja druga: zbiór liczb naturalnych, gdzie $P(x)$ oznacza podzielność przez 3, a $Q(x)$ podzielność przez 7.

337

Zadanie: Czy to jest tautologia?

$$(\exists y P(y) \rightarrow \forall z Q(z)) \rightarrow \forall y (P(y) \rightarrow Q(y))$$

Rozwiązanie: Przesłanka $\exists y P(y) \rightarrow \forall z Q(z)$
jest równoważna każdej z formuł:

$$\neg \exists y P(y) \vee \forall z Q(z);$$

$$\forall y \neg P(y) \vee \forall z Q(z);$$

$$\forall y (\neg P(y) \vee \forall z Q(z));$$

$$\forall y \forall z (\neg P(y) \vee Q(z));$$

$$\forall y \forall z (P(y) \rightarrow Q(z)).$$

Zatem całość jest równoważna oczywistej tautologii:

$$\forall y \forall z (P(y) \rightarrow Q(z)) \rightarrow \forall y (P(y) \rightarrow Q(y)).$$

339

Ćwiczenie

Napisać zdanie prawdziwe w strukturze $\langle \{a, b\}^*, \cdot, \varepsilon, = \rangle$
słów nad alfabetem $\{a, b\}^*$ z konkatenacją i słowem pustym,
ale nieprawdziwe w strukturze $\langle \{a, b, c\}^*, \cdot, \varepsilon, = \rangle$.

Rozwiązanie:

$$\exists x_1 \exists x_2 \forall y (\forall z_1 \forall z_2 (y = z_1 \cdot z_2 \rightarrow y = z_1 \vee y = z_2) \rightarrow y = x_1 \vee y = x_2 \vee y = \varepsilon)$$

Powyższe zdanie *rozdziela* te dwie struktury.

341

Jak ustalić, że formuła jest tautologią?

Można ją *udowodnić*.

343

Tautologie z kwantyfikatorami

$$\neg \forall x A(x) \leftrightarrow \exists x \neg A(x);$$

$$\neg \exists x A(x) \leftrightarrow \forall x \neg A(x);$$

$$\forall x (A(x) \wedge B(x)) \leftrightarrow \forall x A(x) \wedge \forall x B(x);$$

$$\exists x (A(x) \vee B(x)) \leftrightarrow \exists x A(x) \vee \exists x B(x);$$

Poniżej, zmienna x nie jest wolna w A :

$$\forall x (A \vee B(x)) \leftrightarrow A \vee \forall x B(x);$$

$$\exists x (A \wedge B(x)) \leftrightarrow A \wedge \exists x B(x).$$

338

Ćwiczenie

Symbole relacyjne R, S są jednoargumentowe,
symbol funkcyjny f jest dwuargumentowy.

Napisać zdanie prawdziwe dokładnie w tych modelach

$$\mathcal{A} = \langle A, f^A, R^A, S^A \rangle,$$

w których obraz zbioru $R^A \times S^A$ przy przekształceniu f^A
zawiera się w zbiorze $R^A \cap S^A$.

Rozwiązanie:

$$\forall x \forall y (R(x) \wedge S(y) \rightarrow R(f(x, y)) \wedge S(f(x, y)))$$

340

Jak ustalić, że formuła jest tautologią?

Złe wiadomości:

- ▶ Formuła zdaniowa z n symbolami zdaniowymi ma 2^n różnych interpretacji. Może tylko jedna jest zła?
Sprawdzenie wszystkich stanowczo trwa zbyt długo.
- ▶ **Nie istnieje** żadna algorytmiczna metoda sprawdzania czy dana formuła pierwszego rzędu jest tautologią.

342

Stanisław Jaśkowski, Gerhard Gentzen



344

- Reguły *wprowadzania* spójników logicznych: jak można udowodnić formułę danej postaci?
- Reguły *eliminacji* spójników: jak można wykorzystać formułę tej postaci do udowodnienia innej?

345

Eliminacja koniunkcji

$$\begin{array}{c} A \wedge B \\ \vdots \\ \text{Ponieważ } A \wedge B, \text{ więc } A. \\ A \wedge B \\ \vdots \\ \text{Ponieważ } A \wedge B, \text{ więc } B. \end{array}$$

Reguły wnioskowania $E\wedge$:

$$\frac{A \wedge B}{A} \quad \frac{A \wedge B}{B}$$

347

Eliminacja implikacji (odrywanie)

$$\begin{array}{c} A \\ \vdots \\ A \rightarrow B \\ \vdots \\ \text{Ponieważ } A \text{ oraz } A \rightarrow B, \text{ więc } B. \end{array}$$

Reguła *modus ponens*:

$$\frac{A \quad A \rightarrow B}{B}$$

349

Wprowadzanie implikacji

$\begin{array}{c} \text{Założmy } A. \\ \vdots \\ \text{Zatem } B. \end{array}$	$\begin{array}{c} (\text{Cel: } B) \\ \\ (\text{Cel osiągnięty}) \end{array}$
---	---

Zatem $A \rightarrow B$.

Jaką tu mamy regułę?

$$\frac{A \vdash B}{A \rightarrow B}$$

Aby udowodnić $A \rightarrow B$, dowodzimy B przy założeniu A .

351

$$\begin{array}{c} \vdots \\ A \\ \vdots \\ B \end{array}$$

Ponieważ A oraz B , więc $A \wedge B$.

Zapisujemy to jako *regułę wnioskowania* $W\wedge$:

$$\frac{A \quad B}{A \wedge B} \quad \text{albo tak:} \quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B},$$

gdzie „ $\Gamma \vdash$ ” oznacza: „przy założeniach Γ ”

346

Eliminacja koniunkcji

$$\begin{array}{c} A \wedge B \\ \vdots \\ \text{Ponieważ } A \wedge B, \text{ więc } A. \\ A \wedge B \\ \vdots \\ \text{Ponieważ } A \wedge B, \text{ więc } B. \end{array}$$

Reguły wnioskowania $E\wedge$:

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

348

Eliminacja implikacji (odrywanie)

$$\begin{array}{c} A \\ \vdots \\ A \rightarrow B \\ \vdots \\ \text{Ponieważ } A \text{ oraz } A \rightarrow B, \text{ więc } B. \end{array}$$

Reguła *modus ponens*:

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A \rightarrow B}{\Gamma \vdash B} (E \rightarrow)$$

350

Wprowadzanie implikacji

$\begin{array}{c} \text{Założmy } A. \\ \vdots \\ \text{Zatem } B. \end{array}$	$\begin{array}{c} (\text{Cel: } B) \\ \\ (\text{Cel osiągnięty}) \end{array}$
---	---

Zatem $A \rightarrow B$.

Jaką tu mamy regułę?

$$\frac{\Gamma \cup \{A\} \vdash B}{\Gamma \vdash A \rightarrow B}$$

Aby udowodnić $A \rightarrow B$, dodajemy założenie A i dowodzimy B .

352

Wprowadzanie implikacji

Założmy A .	(Cel: B)
⋮	
Zatem B .	(Cel osiągnięty)

Zatem $A \rightarrow B$.

Jaką tu mamy regułę?

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} (W \rightarrow)$$

Aby udowodnić $A \rightarrow B$, dodajemy założenie A i dowodzimy B .

353

Przykład

Założmy p	(Cel 1: $q \rightarrow p$)
Założmy q	(Cel 2: p)
Z założenia mamy p	(Cel 2 osiągnięty)
Zatem $q \rightarrow p$	(Cel 1 osiągnięty)

Zatem $p \rightarrow (q \rightarrow p)$

Spróbujemy to zapisać zwięźle.

354

Przykład

p	(Cel 1: $q \rightarrow p$)
p, q	(Cel 2: p)
$\vdash p$	(Cel 2 osiągnięty)
$p \vdash q \rightarrow p$	(Cel 1 osiągnięty)

$\vdash p \rightarrow (q \rightarrow p)$

Jeszcze zwięźlej:

$p, q \vdash p$
$p \vdash q \rightarrow p$
$\vdash p \rightarrow (q \rightarrow p)$

Bez ramek:

$$\frac{p, q \vdash p}{p \vdash q \rightarrow p} (W \rightarrow)$$

$$\frac{p \vdash q \rightarrow p}{\vdash p \rightarrow (q \rightarrow p)} (W \rightarrow)$$

355

Naturalna dedukcja: formalizacja w stylu Gentzena

- ▶ Rozważamy *osądy* postaci $\Gamma \vdash \varphi$, gdzie Γ jest zbiorem formuł (założeń), a φ to formuła (teza). Zamiast $\emptyset \vdash \varphi$ piszemy po prostu $\vdash \varphi$.
- ▶ Reguły w stylu Gentzena służą do wyprowadzania osądów (z innych osądów). Zapisujemy je tak:

$$\frac{\Gamma_1 \vdash \varphi_1, \dots, \Gamma_n \vdash \varphi_n}{\Delta \vdash \psi}$$

Na górze są przesłanki, na dole konkluzja.

Uwaga: Naturalna dedukcja w stylu Gentzena, to *co innego* niż „rachunek sekwentów Gentzena”!

356

Przykład dowodu

$$\frac{\frac{(p \rightarrow p) \rightarrow q, p \vdash p}{(p \rightarrow p) \rightarrow q \vdash p \rightarrow p} (W \rightarrow) \quad (p \rightarrow p) \rightarrow q \vdash (p \rightarrow p) \rightarrow q}{\frac{(p \rightarrow p) \rightarrow q \vdash q}{\vdash ((p \rightarrow p) \rightarrow q) \rightarrow q} (W \rightarrow)} (E \rightarrow)$$

Dowód formalny to drzewo, którego korzeń (u dołu!), to udowodniony osąd.

A liście (u góry)?

357

Trzeba od czegoś zacząć

Poniższa reguła nie ma przesłanek.

$$\frac{}{\Gamma \cup \{\varphi\} \vdash \varphi} (Ax)$$

Nazywamy ją *aksjomatem naturalnej dedukcji* i zwykle zapisujemy tak:

$$\Gamma, \varphi \vdash \varphi (Ax)$$

(Najprostszy dowód polega na przywołaniu założenia.)

358

Wprowadzanie negacji

Założmy A	(Cel: $\perp$)
⋮	
Zatem $\perp$ (sprzeczność).	

Zatem $\neg A$.

$$\frac{\Gamma, A \vdash \perp}{\Gamma \vdash \neg A} (W \neg)$$

359

Eliminacja negacji

A
⋮
 $\neg A$
⋮

Ponieważ A oraz $\neg A$ więc $\perp$ (sprzeczność).

$$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \perp} (E \neg)$$

360

$\vdots$
 $\perp$
 $\vdots$
 Ponieważ $\perp$, więc A

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} (E\perp)$$

361

Jeszcze jedna reguła bez przesłanek:

$$\frac{}{\Gamma \vdash \top} (W\top)$$

362

Wprowadzanie alternatywy

A
 $\vdots$
 Ponieważ A , więc $A \vee B$.

B
 $\vdots$
 Ponieważ B , więc $A \vee B$.

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \quad (W\vee) \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

363

Eliminacja alternatywy

$A \vee B$
 $\vdots$
 Załóżmy A . (Cel 1: C)
 $\vdots$
 Zatem C .

Załóżmy B . (Cel 2: C)
 $\vdots$
 Zatem C .

Ponieważ $A \vee B$, więc C .

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} (E\vee)$$

364

Wnioskowanie przez zaprzeczenie

Załóżmy $\neg A$. (Cel: $\perp$)
 $\vdots$
 Zatem $\perp$.

Zatem A .

$$\frac{\Gamma, \neg A \vdash \perp}{\Gamma \vdash A}$$

365

„Nienaturalny wyjątek”

$$\frac{\Gamma, \neg A \vdash \perp}{\Gamma \vdash A} (E\neg\neg)$$

Ta reguła to jakby eliminacja podwójnej negacji:

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$$

366

Przykład: *Tertium non datur*

Załóżmy $\neg(p \vee \neg p)$ $\vdots$ Załóżmy p . Ponieważ p , więc $p \vee \neg p$. Ponieważ $p \vee \neg p$ oraz $\neg(p \vee \neg p)$, więc sprzeczność. Zatem $\neg p$. Ponieważ $\neg p$, więc $p \vee \neg p$. Ponieważ $p \vee \neg p$ oraz $\neg(p \vee \neg p)$, więc $\perp$.	(Cel 1: $\perp$) (Cel 2: $p \vee \neg p$) (Cel 3: $\neg p$) (Cel 4: $\perp$) (Cel 4 osiągnięty) (Cel 3 osiągnięty) (Cel 2 osiągnięty) (Cel 1 osiągnięty)
--	---

Zatem $p \vee \neg p$.

367

To samo w notacji Gentzena:

$$\frac{\neg(p \vee \neg p), p \vdash p}{\neg(p \vee \neg p), p \vdash p \vee \neg p} \quad \frac{\neg(p \vee \neg p), p \vdash p \vee \neg p}{\neg(p \vee \neg p), p \vdash \perp}$$

$$\frac{\neg(p \vee \neg p), p \vdash \perp}{\neg(p \vee \neg p) \vdash \neg p} \quad \frac{\neg(p \vee \neg p) \vdash \neg p}{\neg(p \vee \neg p) \vdash p \vee \neg p}$$

$$\frac{\neg(p \vee \neg p) \vdash p \vee \neg p \quad \neg(p \vee \neg p) \vdash \neg(p \vee \neg p)}{\neg(p \vee \neg p) \vdash \perp}$$

$$\frac{\neg(p \vee \neg p) \vdash \perp}{\vdash p \vee \neg p}$$

Uwaga: Istotą naturalnej dedukcji jest wprowadzanie i eliminacja spójników. Pudełka, drzewa itp. to tylko sposoby prezentacji.

368

$$\Gamma, \varphi \vdash \varphi \text{ (Ax)}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \text{ (W}\wedge\text{)}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \text{ (W}\rightarrow\text{)}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A \rightarrow B}{\Gamma \vdash B} \text{ (E}\rightarrow\text{)}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \text{ (E}\wedge\text{)}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \text{ (E}\wedge\text{)}$$

369

370

Reguły dla alternatywy

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \text{ (W}\vee\text{)}$$

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \text{ (W}\vee\text{)}$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \text{ (E}\vee\text{)}$$

371

Reguły dla prawdy, fałszu i negacji

$$\frac{}{\Gamma \vdash \top} \text{ (W}\top\text{)}$$

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} \text{ (E}\perp\text{)}$$

$$\frac{\Gamma, A \vdash \perp}{\Gamma \vdash \neg A} \text{ (W}\neg\text{)}$$

$$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \perp} \text{ (E}\neg\text{)}$$

$$\frac{\Gamma, \neg A \vdash \perp}{\Gamma \vdash A} \text{ (E}\neg\neg\text{)}$$

372

Dowód formalny

Dowód formalny osądu $\Gamma \vdash \varphi$ w naturalnej dedukcji, to drzewo skończone, w którym każdemu wierzchołkowi przypisano pewien osąd. Przy tym:

- ▶ Korzeniowi drzewa przypisano osąd $\Gamma \vdash \varphi$.
- ▶ Osąd przypisany dowolnemu wierzchołkowi powstaje z osądów przypisanych jego dzieciom poprzez zastosowanie jednej z reguł wnioskowania.
- ▶ Liściom przypisano osądy postaci $\Delta, \alpha \vdash \alpha$.

Dowód osądu $\vdash \varphi$ nazywamy *dowodem formuły* φ .

373

Przykład : $\neg\beta \vdash \neg(\beta \wedge \gamma)$

$$\frac{\neg\beta, \beta \wedge \gamma \vdash \neg\beta \quad \frac{\neg\beta, \beta \wedge \gamma \vdash \beta \wedge \gamma}{\neg\beta, \beta \wedge \gamma \vdash \beta} \text{ (E}\wedge\text{)}}{\neg\beta, \beta \wedge \gamma \vdash \perp} \text{ (E}\neg\text{)}$$

$$\frac{\neg\beta, \beta \wedge \gamma \vdash \perp}{\neg\beta \vdash \neg(\beta \wedge \gamma)} \text{ (W}\neg\text{)}$$

◦

374

Poprawność i pełność (dla rachunku zdań)

Twierdzenie (o pełności)

- ▶ System naturalnej dedukcji jest *poprawny*: Jeśli formuła ma dowód (jest *twierdzeniem*) to jest tautologią.
- ▶ System naturalnej dedukcji jest *pełny*: Każda tautologia ma dowód.

375

Przypomnienie notacji

Piszemy $\varrho \models \Gamma$, gdy $\llbracket \gamma \rrbracket_{\varrho} = 1$, dla każdego $\gamma \in \Gamma$.

Piszemy $\Gamma \models \varphi$, gdy dla dowolnej interpretacji zdaniowej ϱ : jeżeli $\varrho \models \Gamma$, to także $\llbracket \varphi \rrbracket_{\varrho} = 1$.

Jeśli osąd $\Gamma \vdash \varphi$ ma dowód, to piszemy po prostu " $\Gamma \vdash \varphi$ ".

376

Poprawność

Twierdzenie: Jeśli osąd $\Gamma \vdash \alpha$ ma dowód, to $\Gamma \models \alpha$.

Dowód: Dowód jest przez indukcję ze względu na wielkość... dowodu $\Gamma \vdash \alpha$.

Rozważamy kilka przypadków, zależnie od ostatniej użytej reguły.

Przypadek 1: Osąd $\Gamma \vdash \alpha$ jest aksjomatem, tj. $\Gamma = \Gamma', \alpha$. Wtedy teza jest oczywista.

Przypadek 2: Osąd $\Gamma \vdash \alpha$ otrzymano przez $(E \rightarrow)$ z osądów $\Gamma \vdash \beta \rightarrow \alpha$ i $\Gamma \vdash \beta$. Z założenia indukcyjnego $\Gamma \models \beta \rightarrow \alpha$ oraz $\Gamma \models \beta$, bo te dowody mają mniejsze rozmiary. Jeśli więc $\varrho \models \Gamma$, to ϱ spełnia obie formuły $\beta \rightarrow \alpha$ i β . Wtedy ϱ musi też spełniać α .

377

Jeśli $\Gamma \vdash \alpha$, to $\Gamma \models \alpha$

Przypadek 4: Osąd $\Gamma \vdash \alpha$ otrzymano przez $(E \perp)$ z $\Gamma \vdash \perp$. Z założenia indukcyjnego dostajemy $\Gamma \models \perp$, co oznacza, że nie istnieje interpretacja zdaniowa spełniająca Γ .

A więc $\Gamma \models \alpha$, walkowerem.

Przypadek 5: Osąd $\Gamma \vdash \alpha$ otrzymano z pomocą reguły $(E \neg \neg)$ z osądu $\Gamma, \neg \alpha \vdash \perp$. Wtedy $\Gamma, \neg \alpha \models \perp$ z założenia indukcyjnego, czyli nie istnieje interpretacja zdaniowa spełniająca $\Gamma, \neg \alpha$. Znaczy to dokładnie tyle, że każda interpretacja zdaniowa spełniająca Γ musi spełniać α .

379

Pełność: Jeśli $\models \alpha$, to $\vdash \alpha$

(1) $\beta, \gamma \vdash \beta \wedge \gamma$

$$\frac{\beta, \gamma \vdash \beta \quad \beta, \gamma \vdash \gamma}{\beta, \gamma \vdash \beta \wedge \gamma} (W \wedge)$$

383

Jeśli $\Gamma \vdash \alpha$, to $\Gamma \models \alpha$

Przypadek 3: Osąd $\Gamma \vdash \alpha$ otrzymano przez $(W \rightarrow)$. Wtedy $\alpha = \beta \rightarrow \gamma$ oraz $\Gamma, \beta \vdash \gamma$ ma dowód mniejszych rozmiarów, zatem $\Gamma, \beta \models \gamma$, z założenia indukcyjnego.

Założmy, że $\varrho \models \Gamma$. Jeśli $\llbracket \beta \rrbracket_{\varrho} = 1$, to $\varrho \models \Gamma, \beta$, więc $\llbracket \gamma \rrbracket_{\varrho} = 1$, skąd $\llbracket \beta \rightarrow \gamma \rrbracket_{\varrho} = 1$. A jeśli $\llbracket \beta \rrbracket_{\varrho} = 0$, to tym bardziej $\llbracket \beta \rightarrow \gamma \rrbracket_{\varrho} = 1$.

378

Jeśli $\Gamma \vdash \alpha$, to $\Gamma \models \alpha$

Przypadek 6: Osąd $\Gamma \vdash \alpha$ otrzymano z pomocą reguły $(E \vee)$ z trzech osądów: $\Gamma \vdash \beta \vee \gamma$, $\Gamma, \beta \vdash \alpha$, $\Gamma, \gamma \vdash \alpha$. Z założenia indukcyjnego wiemy, że $\Gamma \models \beta \vee \gamma$.

Jeśli więc $\varrho \models \Gamma$, to $\llbracket \beta \rrbracket_{\varrho} = 1$ lub $\llbracket \gamma \rrbracket_{\varrho} = 1$, skąd ϱ spełnia jeden ze zbiorów Γ, β , lub Γ, γ . W obu przypadkach z założenia indukcyjnego wynika, że $\llbracket \alpha \rrbracket_{\varrho} = 1$.

Przypadki 7–14: Podobnie.

380

Lemat 1:

Następujące osądy mają dowody w naturalnej dedukcji:

1. $\beta, \gamma \vdash \beta \wedge \gamma$;
2. $\beta, \neg \gamma \vdash \neg(\beta \rightarrow \gamma)$;
3. $\neg \beta, \neg \gamma \vdash \neg(\beta \vee \gamma)$;
4. $\neg \beta \vdash \neg(\beta \wedge \gamma)$ oraz $\neg \gamma \vdash \neg(\beta \wedge \gamma)$;
5. $\neg \beta \vdash \beta \rightarrow \gamma$;
6. $\gamma \vdash \beta \rightarrow \gamma$;
7. $\vdash \neg \neg$;
8. $\vdash \alpha \vee \neg \alpha$;
9. $\beta \vdash \neg \neg \beta$.

381

(2) $\beta, \neg \gamma \vdash \neg(\beta \rightarrow \gamma)$

Oznaczenie: $\Gamma = \{\beta, \neg \gamma, \beta \rightarrow \gamma\}$

$$\frac{\frac{\frac{\Gamma \vdash \beta \quad \Gamma \vdash \beta \rightarrow \gamma}{\Gamma \vdash \gamma} (E \rightarrow)}{\Gamma \vdash \neg \gamma} (E \neg)}{\Gamma \vdash \perp} (W \neg)$$

$$\frac{\Gamma \vdash \perp}{\beta, \neg \gamma \vdash \neg(\beta \rightarrow \gamma)} (W \neg)$$

384

$$(3) \quad \neg\beta, \neg\gamma \vdash \neg(\beta \vee \gamma)$$

Oznaczenie: $\Gamma = \{\neg\beta, \neg\gamma, \beta \vee \gamma\}$

$$\frac{\frac{\frac{\Gamma, \beta \vdash \beta \quad \Gamma, \beta \vdash \neg\beta}{\Gamma, \beta \vdash \perp} (E\neg) \quad \frac{\Gamma, \gamma \vdash \gamma \quad \Gamma, \gamma \vdash \neg\gamma}{\Gamma, \gamma \vdash \perp} (E\vee)}{\Gamma \vdash \perp} (E\perp) \quad \frac{}{\neg\beta, \neg\gamma \vdash \neg(\beta \vee \gamma)} (E\perp)$$

385

$$(5) \quad \neg\beta \vdash \beta \rightarrow \gamma$$

$$\frac{\frac{\neg\beta, \beta \vdash \neg\beta \quad \neg\beta, \beta \vdash \beta}{\neg\beta, \beta \vdash \perp} (E\neg) \quad \frac{}{\neg\beta, \beta \vdash \gamma} (E\perp)}{\neg\beta \vdash \beta \rightarrow \gamma} (W\rightarrow)$$

386

$$(6) \quad \gamma \vdash \beta \rightarrow \gamma$$

$$\frac{\gamma, \beta \vdash \gamma}{\gamma \vdash \beta \rightarrow \gamma} (W\rightarrow)$$

387

$$(7) \quad \vdash \neg\perp$$

$$\frac{\perp \vdash \perp}{\vdash \neg\perp} (W\neg)$$

388

$$(9) \quad \beta \vdash \neg\neg\beta$$

$$\frac{\frac{\beta, \neg\beta \vdash \beta \quad \beta, \neg\beta \vdash \neg\beta}{\beta, \neg\beta \vdash \perp} (E\neg) \quad \frac{}{\beta \vdash \neg\neg\beta} (W\neg)}$$

389

Pełność: *Jeśli* $\models \alpha$, *to* $\vdash \alpha$

Lemat 2 (Osłabianie): Jeśli $\Gamma \vdash \alpha$ to także $\Gamma \cup \Delta \vdash \alpha$.

Dowód: We wszystkich osądach występujących w dowodzie $\Gamma \vdash \alpha$ dopisujemy Δ po lewej stronie. (Porządnym dowód jest przez indukcję.)

390

Lemat 3 (Reguła cięcia):

Jeśli $\Gamma \vdash \alpha$ oraz $\Gamma, \alpha \vdash \beta$, to $\Gamma \vdash \beta$.

Dowód:

$$\frac{\frac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \rightarrow \beta} (W\rightarrow) \quad \Gamma \vdash \alpha}{\Gamma \vdash \beta} (E\rightarrow)$$

Wniosek:

Jeśli $\Gamma \vdash \alpha_1, \dots, \Gamma \vdash \alpha_n$, oraz $\Gamma, \alpha_1, \dots, \alpha_n \vdash \beta$, to $\Gamma \vdash \beta$.

391

Lemat 4: Jeśli $\Gamma, \gamma \vdash \alpha$ oraz $\Gamma, \neg\gamma \vdash \alpha$, to $\Gamma \vdash \alpha$.

Dowód: Ponieważ $\vdash \gamma \vee \neg\gamma$, więc $\Gamma \vdash \gamma \vee \neg\gamma$ (osłabianie). Teraz należy zastosować regułę eliminacji alternatywy:

$$\frac{\Gamma \vdash \gamma \vee \neg\gamma \quad \Gamma, \gamma \vdash \alpha \quad \Gamma, \neg\gamma \vdash \alpha}{\Gamma \vdash \alpha}$$

392

Lemat Kalmára

Oznaczenie: Dla dowolnej interpretacji zdaniowej ϱ i dowolnej formuły α przyjmijmy, że

$$\alpha^{\varrho} = \begin{cases} \alpha, & \text{jeśli } \llbracket \alpha \rrbracket_{\varrho} = 1; \\ \neg \alpha, & \text{w przeciwnym przypadku.} \end{cases}$$

Na przykład jeśli $\varrho(p) = 0$ i $\varrho(q) = 1$, to $q^{\varrho} = q$, $p^{\varrho} = \neg p$ oraz $((p \rightarrow q) \rightarrow p)^{\varrho} = \neg((p \rightarrow q) \rightarrow p)$.

Lemat Kalmára: Niech $p_1, \dots, p_n$ będą wszystkimi symbolami zdaniowymi występującymi w formule α . Wówczas $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \alpha^{\varrho}$, dla dowolnego ϱ .

Czyli na przykład $q, \neg p \vdash \neg((p \rightarrow q) \rightarrow p)$.

393

Dowód lematu Kalmára

Przypadek 3: Niech $\alpha = \beta \rightarrow \gamma$.

Jeśli $\llbracket \alpha \rrbracket_{\varrho} = 0$ to $\llbracket \beta \rrbracket_{\varrho} = 1$ i $\llbracket \gamma \rrbracket_{\varrho} = 0$. Formuły β i γ są krótsze od α , więc $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \beta$ oraz $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg \gamma$ z założenia indukcyjnego. Z lematu 1(2) wiadomo, że $\beta, \neg \gamma \vdash \neg(\beta \rightarrow \gamma)$. Używając osłabiania i reguły cięcia dostaniemy $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg(\beta \rightarrow \gamma)$.

Jeśli $\llbracket \alpha \rrbracket_{\varrho} = 1$, to albo $\llbracket \beta \rrbracket_{\varrho} = 0$ albo $\llbracket \gamma \rrbracket_{\varrho} = 1$. W pierwszym przypadku z założenia indukcyjnego wiemy, że $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg \beta$, a w drugim, że $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \gamma$. W obu przypadkach potrafimy udowodnić $\beta \rightarrow \gamma$ z lematu 1(5,6).

395

Dowód lematu Kalmára

Przypadek 5: Niech $\alpha = \beta \wedge \gamma$

Jeśli $\llbracket \alpha \rrbracket_{\varrho} = 1$, to $\llbracket \beta \rrbracket_{\varrho} = \llbracket \gamma \rrbracket_{\varrho} = 1$ i mamy dowody osądów $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \beta$ i $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \gamma$. Pozostaje zastosować regułę ($W\wedge$).

Jeśli $\llbracket \alpha \rrbracket_{\varrho} = 0$, to jedna z wartości $\llbracket \beta \rrbracket_{\varrho}$, $\llbracket \gamma \rrbracket_{\varrho}$ jest zerem, istnieje więc dowód osądu $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg \beta$ lub dowód osądu $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg \gamma$. Można teraz skorzystać z tego, że $\neg \beta \vdash \neg(\beta \wedge \gamma)$ oraz $\neg \gamma \vdash \neg(\beta \wedge \gamma)$.

397

Pełność rachunku zdań

Twierdzenie (o pełności): Każda tautologia ma dowód.

Dowód: Niech α będzie tautologią zdaniową. Wtedy $\alpha^{\varrho} = \alpha$ dla dowolnej interpretacji ϱ .

Niech $p_1, \dots, p_n$ będą wszystkimi symbolami zdaniowymi w formule α . Udowodnimy, że dla dowolnego $m \leq n$ i dowolnego ϱ zachodzi $p_1^{\varrho}, \dots, p_m^{\varrho} \vdash \alpha$. Przyjmując $m = 0$ otrzymamy $\vdash \alpha$.

Dowód przebiega przez indukcję ze względu na $n - m$. Dla $m = n$ teza wynika z lematu Kalmára.

399

Lemat Kalmára

Jeśli w formule α występują tylko symbole $p_1, \dots, p_n$, to $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \alpha^{\varrho}$.

Dowód: Indukcja ze względu na długość formuły α .

Przypadek 1: Jeśli $\alpha = p_i$, to $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash p_i^{\varrho}$ jest aksjomatem.

Przypadek 2: Jeśli $\alpha = \perp$, to $\alpha^{\varrho} = \neg \perp$. A skoro $\vdash \neg \perp$, to także $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg \perp$ (osłabianie).

Podobnie dla $\alpha = \top$.

394

Dowód lematu Kalmára

Przypadek 4: Załóżmy, że $\alpha = \beta \vee \gamma$ i niech $\llbracket \alpha \rrbracket_{\varrho} = 1$. Zatem $\llbracket \beta \rrbracket_{\varrho} = 1$ lub $\llbracket \gamma \rrbracket_{\varrho} = 1$. Wtedy jedna z formuł β , γ ma dowód przy założeniach $p_1^{\varrho}, \dots, p_n^{\varrho}$ i stosując regułę wprowadzania alternatywy od razu dostajemy $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \beta \vee \gamma$.

Jeśli natomiast $\llbracket \alpha \rrbracket_{\varrho} = 0$, to z założenia indukcyjnego wynika, że mamy dowody dla osądu $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg \gamma$ oraz dla osądu $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg \beta$. Ale z lematu 1(3) mamy $\neg \beta, \neg \gamma \vdash \neg(\beta \vee \gamma)$, skąd wynika $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg(\beta \vee \gamma)$.

396

Dowód lematu Kalmára

Przypadek 6: Niech $\alpha = \neg \beta$.

Jeśli $\llbracket \alpha \rrbracket_{\varrho} = 1$, to $\llbracket \beta \rrbracket_{\varrho} = 0$ i z założenia indukcyjnego $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg \beta$.

W przeciwnym razie, $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \beta$, a skoro $\beta \vdash \neg \neg \beta$ (lemat 1(9)), to też $p_1^{\varrho}, \dots, p_n^{\varrho} \vdash \neg \alpha$.

398

Krok indukcyjny

Założenie indukcyjne:
 $p_1^{\varrho}, \dots, p_m^{\varrho}, p_{m+1}^{\varrho} \vdash \alpha$, dla dowolnego ϱ .

Teza:
 $p_1^{\varrho}, \dots, p_m^{\varrho} \vdash \alpha$, dla dowolnego ϱ .

Weźmy dowolne ϱ . Z założenia indukcyjnego wynika, że

$$p_1^{\varrho}, \dots, p_m^{\varrho}, p_{m+1}^{\varrho} \vdash \alpha \quad \text{oraz} \quad p_1^{\varrho}, \dots, p_m^{\varrho}, \neg p_{m+1}^{\varrho} \vdash \alpha$$

Pozostaje skorzystać z lematu 4

(Jeśli $\Gamma, \gamma \vdash \alpha$ oraz $\Gamma, \neg \gamma \vdash \alpha$, to $\Gamma \vdash \alpha$.)

400

Twierdzenie (łatwe) Dla dowolnej formuły φ i dowolnego skończonego zbioru formuł Γ zachodzi równoważność:

$$\Gamma \models \varphi \quad \text{wtw, gdy} \quad \Gamma \vdash \varphi$$

Twierdzenie uogólnione: Dla dowolnej formuły φ i dowolnego zbioru formuł Γ zachodzi równoważność:

$$\Gamma \models \varphi \quad \text{wtw, gdy} \quad \Gamma \vdash \varphi$$

Albo co znaczy $\Gamma \vdash \varphi$, jeśli Γ jest zbiorem nieskończonym?

Że istnieje taki skończony zbiór $\Gamma_0 \subseteq \Gamma$, że $\Gamma_0 \vdash \varphi$.

401

Zwartość

Twierdzenie (o zwartości): Jeżeli $\Gamma \models \varphi$, to istnieje taki skończony podzbiór $\Gamma_0 \subseteq \Gamma$, że $\Gamma_0 \models \varphi$.

Wniosek: Jeżeli każdy skończony podzbiór zbioru Γ jest spełnialny, to cały zbiór Γ jest spełnialny.

Dowód: Jeśli Γ nie jest spełnialny, to $\Gamma \models \perp$. Z twierdzenia o zwartości istnieje więc skończony niespełnialny podzbiór.

403

Twierdzenie uogólnione: Dla dowolnej formuły φ i dowolnego zbioru formuł Γ zachodzi równoważność:

$$\Gamma \models \varphi \quad \text{wtw, gdy} \quad \text{istnieje taki skończony zbiór } \Gamma_0 \subseteq \Gamma, \text{ że } \Gamma_0 \vdash \varphi.$$

Twierdzenie (o zwartości): Jeżeli $\Gamma \models \varphi$, to istnieje taki skończony podzbiór $\Gamma_0 \subseteq \Gamma$, że $\Gamma_0 \models \varphi$.

402

Przykład: kolorowanie nieskończonego grafu

Niech G będzie nieskończonym zbiorem, w którym określono symetryczną relację r .

(Myślimy o G jak o zbiorze wierzchołków nieskończonego grafu i o relacji r jak o zbiorze krawędzi tego grafu.)

Relacja r jest **trójkolorowa**, gdy istnieje taki podział zbioru G na trzy składowe, że żadne dwa elementy zbioru G , należące do jednej składowej, nie są w relacji r .

(Wierzchołki połączone krawędziami są różnych kolorów.)

Relacja r jest **trójkolorowa w podzbiorze** $H \subseteq G$, gdy trójkolorowa jest relacja $r \cap (H \times H)$ w zbiorze H .

404

Kolorowanie nieskończonego grafu

Twierdzenie: Jeśli relacja r jest trójkolorowa w każdym skończonym podzbiorze zbioru G , to jest trójkolorowa w G .

Dowód: Zdefiniujemy pewien nieskończony zbiór Γ formuł rachunku zdań. Użyjemy do tego (nieskończenie wielu) zmiennych zdaniowych postaci p_a^i , dla $a \in G$ oraz $i \in \{1, 2, 3\}$.

Intuicja: p_a^i czytamy „wierzchołek a ma kolor i ”.

W zbiorze Γ są takie formuły:

$$\alpha_a = (p_a^1 \vee p_a^2 \vee p_a^3) \wedge \neg(p_a^1 \wedge p_a^2) \wedge \neg(p_a^1 \wedge p_a^3) \wedge \neg(p_a^2 \wedge p_a^3),$$

dla każdego $a \in G$. (Element a ma dokładnie jeden kolor.)

$$\beta_{ab} = \neg(p_a^1 \wedge p_b^1) \wedge \neg(p_a^2 \wedge p_b^2) \wedge \neg(p_a^3 \wedge p_b^3),$$

dla każdej pary $\langle a, b \rangle \in r$. (Elementy a i b są różnego koloru.)

405

Kolorowanie nieskończonego grafu

$$\alpha_a = (p_a^1 \vee p_a^2 \vee p_a^3) \wedge \neg(p_a^1 \wedge p_a^2) \wedge \neg(p_a^1 \wedge p_a^3) \wedge \neg(p_a^2 \wedge p_a^3)$$

$$\beta_{ab} = \neg(p_a^1 \wedge p_b^1) \wedge \neg(p_a^2 \wedge p_b^2) \wedge \neg(p_a^3 \wedge p_b^3)$$

$$\Gamma_H = \{\alpha_a \mid a \in H\} \cup \{\beta_{ab} \mid \langle a, b \rangle \in r \cap (H \times H)\}, \text{ dla } H \subseteq G.$$

$$\Gamma = \Gamma_G.$$

Zbiór Γ_H jest spełnialny wtw, gdy relacja r jest trójkolorowa w podzbiorze H . A tak jest dla wszystkich skończonych H .

Niech $\Gamma' \subseteq \Gamma$ będzie skończony. Wtedy $\Gamma' \subseteq \Gamma_H$ dla pewnego skończonego $H \subseteq G$. Zatem Γ' jest spełnialny.

Z twierdzenia o zwartości cały zbiór Γ jest spełnialny, czyli relacja r jest trójkolorowa.

406

Naturalna dedukcja pierwszego rzędu

(Dygresja fakultatywna)

Wprowadzanie $\forall$

Weźmy dowolne y . $\vdots$ Zatem $A(y)$.	(Cel: $A(y)$)
---	----------------

Zatem $\forall x A(x)$.

$$\frac{\Gamma \vdash A(y)}{\Gamma \vdash \forall x A(x)} \quad y \notin FV(\Gamma)$$

407

408

Eliminacja $\forall$

$\vdots$
 $\forall x A(x)$
 $\vdots$

Ponieważ $\forall x A(x)$, więc $A(t)$.

gdzie t jest dowolnym termem (także zmienną).

$$\frac{\Gamma \vdash \forall x A(x)}{\Gamma \vdash A(t)}$$

409

Wprowadzanie $\exists$

$\vdots$
 $A(t)$
 $\vdots$

Ponieważ $A(t)$, więc $\exists x A(x)$

gdzie t jest dowolnym termem.

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x A(x)}$$

410

Eliminacja $\exists$

$\exists x A(x)$
 $\vdots$

Niech y będzie takie, że $A(y)$ (Cel: B)
 $\vdots$
Zatem B .

Ponieważ $\exists x A(x)$, więc B .

$$\frac{\Gamma \vdash \exists x A(x) \quad \Gamma, A(y) \vdash B}{\Gamma \vdash B} \quad (y \notin \text{FV}(\Gamma) \cup \text{FV}(B))$$

411

Przykład: $\forall x(P(x) \rightarrow C), \exists y P(y) \vdash C$

Założmy, że $\forall x(P(x) \rightarrow C)$ oraz $\exists y P(y)$ (Cel 1: C)
Niech y będzie takie, że $P(y)$. (Cel 2: C)
Ponieważ $\forall x(P(x) \rightarrow C)$, więc $P(y) \rightarrow C$.
Ponieważ $P(y)$ oraz $P(y) \rightarrow C$, więc C .

Ponieważ $\exists y P(y)$, więc C

Oznaczenie: $\Gamma = \{\forall x(P(x) \rightarrow C), \exists y P(y)\}$

$$\frac{\Gamma, P(y) \vdash \forall x(P(x) \rightarrow C) \quad \Gamma, P(y) \vdash P(y) \rightarrow C \quad \Gamma, P(y) \vdash P(y)}{\Gamma \vdash \exists y P(y) \quad \Gamma, P(y) \vdash C} \quad \Gamma \vdash C$$

412

Przykład: $\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$

Założmy $\exists x \forall y P(x, y)$ (Cel: $\forall y \exists x P(x, y)$)
Weźmy dowolne $\bar{y}$. (Cel: $\exists x P(x, \bar{y})$)
Niech $\bar{x}$ będzie takie, że $\forall y P(\bar{x}, y)$. (Cel: $\exists x P(x, \bar{y})$)
Ponieważ $\forall y P(\bar{x}, y)$, więc $P(\bar{x}, \bar{y})$.
Ponieważ $P(\bar{x}, \bar{y})$, więc $\exists x P(x, \bar{y})$.
Ponieważ $\exists x \forall y P(x, y)$, więc $\exists x P(x, \bar{y})$.
Zatem $\forall y \exists x P(x, y)$.

Zatem $\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$.

Ćwiczenie: Napisać dowód formalny.

413

Twierdzenie o pełności

- Następujące warunki są równoważne:
- ▶ Formuła φ jest prawdziwa w dowolnej interpretacji.
 - ▶ Osąd $\vdash \varphi$ ma dowód.

414

Silniejsza wersja twierdzenia o pełności

Twierdzenie: Dla dowolnej formuły φ i dowolnego zbioru formuł Γ zachodzi równoważność:
 $\Gamma \models \varphi$ wtedy i tylko wtedy, gdy $\Gamma \vdash \varphi$

Co to znaczy?
 $\Gamma \vdash \varphi$ wtedy i tylko wtedy, gdy istnieje taki skończony podzbiór $\Gamma_0 \subseteq \Gamma$, że $\Gamma_0 \vdash \varphi$.

Twierdzenie (o zwartości): Jeżeli $\Gamma \models \varphi$, to istnieje taki skończony podzbiór $\Gamma_0 \subseteq \Gamma$, że $\Gamma_0 \models \varphi$.

415

Zwartość logiki pierwszego rzędu

Twierdzenie (o zwartości): Jeżeli $\Gamma \models \varphi$, to istnieje taki skończony podzbiór $\Gamma_0 \subseteq \Gamma$, że $\Gamma_0 \models \varphi$.

Wniosek: Jeżeli każdy skończony podzbiór zbioru Γ jest spełnialny, to cały zbiór Γ jest spełnialny.

Dowód: Jeśli Γ nie jest spełnialny, to $\Gamma \models \perp$. Z twierdzenia o zwartości istnieje więc skończony niespełnialny podzbiór.

416

Zastosowanie twierdzenia o zwartości

Fakt: Nie istnieje formuła φ spełnialna dokładnie w tych modelach, gdzie interpretacją symbolu relacyjnego r jest relacja dobrego porządku.

Dowód: Załóżmy, że takie φ istnieje. Zdefiniujmy formuły

$$\begin{aligned}\alpha_n = & r(x_2, x_1) \wedge \neg r(x_1, x_2) \wedge \\ & r(x_3, x_2) \wedge \neg r(x_2, x_3) \wedge \\ & \dots \\ & r(x_n, x_{n-1}) \wedge \neg r(x_{n-1}, x_n)\end{aligned}$$

(Sens: wartości $x_1, x_2, \dots, x_n$ tworzą skończony ciąg malejący.)

Zbiór $\Gamma = \{\alpha_n \mid n > 1\} \cup \{\varphi\}$ jest niespełnialny.

Ale każdy jego skończony podzbiór Γ_0 jest spełnialny, na przykład w $\langle \mathbb{N}, \leq \rangle$. Sprzeczność.

417

Jeszcze o relacjach równoważności

Przypomnienie

Dwuargumentowa relacja r w zbiorze A jest *relacją równoważności* wtedy i tylko wtedy, gdy jest zwrotna, symetryczna i przechodnia:

- ▶ $\forall x \in A (x r x)$;
- ▶ $\forall x, y \in A (x r y \rightarrow y r x)$;
- ▶ $\forall x, y, z \in A (x r y \wedge y r z \rightarrow x r z)$.

Przykład: *Jądro* przekształcenia $f : A \rightarrow B$:

$$\langle x, y \rangle \in \ker(f) \Leftrightarrow f(x) = f(y).$$

419

Przykład: alfa-konwersja

Formuły $\exists x(x + 1 = y)$ i $\exists z(z + 1 = y)$ znaczą dokładnie to samo (mają zawsze tę samą wartość), bo różnią się tylko wyborem zmiennej związanej.

Mówimy, że między tymi formułami zachodzi relacja alfa-konwersji. Często *utożsamiamy* takie formuły.

418

Konstrukcje ilorazowe

Nowe typy można definiować jako ilorazy.

421

Liczby całkowite

Chcemy odejmować liczby naturalne, tj. mieć działanie odwrotne do dodawania: chcemy, żeby „ $3 - 5$ ” + $5 = 3$. Inaczej: chcemy rozwiązać równanie $x + 5 = 3$.

Pomysł: implementować „ $3 - 5$ ” jako parę $\langle 3, 5 \rangle$.

Ale wtedy „ $3 - 5$ ” + $4 + 1 = 2 + 1$, skąd „ $3 - 5$ ” + $4 = 2$. Zatem „ $3 - 5$ ” = „ $2 - 4$ ”. Tak jest dlatego, że $3 + 4 = 2 + 5$. A więc niektóre różnice muszą być równe:

$$\langle m, n \rangle \sim \langle m', n' \rangle \Leftrightarrow m + n' = m' + n$$

To jest relacja równoważności w $\mathbb{N} \times \mathbb{N}$. Liczby całkowite to jej abstrakty (pary liczb naturalnych „z dokładnością do $\sim$ ”).

Morał: Można definiować $\mathbb{Z}$ jako $\mathbb{N} \times \mathbb{N} / \sim$.

422

Liczby wymierne

Liczby wymierne (ułamki) to pary liczb całkowitych z dokładnością do (częściowej) relacji równoważności

$$\langle x, y \rangle \approx \langle u, v \rangle \Leftrightarrow (y, v \neq 0 \wedge x \cdot v = u \cdot y)$$

Oczywiście zamiast $[(x, y)]_{\approx}$ piszemy $\frac{x}{y}$.

423

Liczby rzeczywiste

Ciąg Cauchy'ego to taki ciąg f liczb (wymiernych), że

$$\forall \varepsilon: \mathbb{Q} (\varepsilon > 0 \rightarrow \exists n \forall k: \mathbb{N} (k \geq n \rightarrow |f(n) - f(k)| < \varepsilon))$$

Liczby rzeczywiste to ciągi Cauchy'ego liczb wymiennych z dokładnością do relacji równoważności $\equiv$:

$f \equiv g$ wtedy i tylko wtedy, gdy

$$\forall \varepsilon: \mathbb{Q} (\varepsilon > 0 \rightarrow \exists n \forall k (k \geq n \rightarrow |f(k) - g(k)| < \varepsilon)).$$

424

- Kanoniczna surjekcja $\kappa : A \rightarrow A/\sim$ (jest jedna taka)
 $\kappa(a) = [a]_r$
- Funkcja wyboru $\sigma : A/\sim \rightarrow A$ (mogą być różne takie)
 $\sigma([a]_r) \in [a]_r$

425

Pewnik wyboru inaczej

Zbiór $S \subseteq \bigcup \mathcal{R}$ jest *selektorem* dla rodziny $\mathcal{R}$,
 gdy S ma dokładnie po jednym elemencie wspólnym
 z każdym zbiorem rodziny $\mathcal{R}$, tj.:

$$\forall a \in \mathcal{R} \exists t \in a (S \cap a = \{t\}).$$

Wierzimy, że dla dowolnej rodziny niepustych zbiorów
 istnieje funkcja wyboru.

Wniosek

Dla dowolnej rodziny niepustych zbiorów parami rozłącznych
 istnieje selektor.

Dowód: Selektorem jest zbiór wartości funkcji wyboru. $\square$

427

Produkt uogólniony

Produkt uogólniony rodziny indeksowanej $\{A_t\}_{t \in T}$
 podzbiorów $\mathcal{D}$, to zbiór

$$\prod_{t \in T} A_t = \{f : T \rightarrow \mathcal{D} \mid \forall t \in T. f(t) \in A_t\}$$

$$f \in \prod_{t \in T} A_t \Leftrightarrow \text{Dom}(f) = T \wedge \forall t \in T. f(t) \in A_t.$$

Uwaga:

Jeśli $A_t = A$, dla wszystkich $t \in T$, to $\prod_{t \in T} A_t = A^T$.

429

Niepustość produktu

Twierdzenie

Jeśli $\{A_t\}_{t \in T}$ jest rodziną indeksowaną zbiorów niepustych,
 to produkt $\prod_{t \in T} A_t$ jest niepusty.

Dowód: Niech φ będzie funkcją wyboru dla $\{A_t \mid t \in T\}$,
 i niech $f(t) = \varphi(A_t)$, dla $t \in T$. Wtedy $f \in \prod_{t \in T} A_t$. $\square$

431

Pewnik wyboru

Definicja

Funkcja wyboru dla rodziny zbiorów $\mathcal{R}$: taka funkcja f , że
 $f(X) \in X$, gdy $X \in \mathcal{R}$.

Czy funkcja wyboru (dla rodziny $\mathcal{R}$ zbiorów niepustych)
 zawsze istnieje?

Zakładamy, że tak.

To założenie nazywamy pewnikiem (aksjomatem) wyboru.

426

Iloczyn kartezjański

Iloczyn kartezjański $A \times B$ składa się z par. Para to obiekt
 wyznaczony przez jeden element A i jeden element B .

Iloczyn kartezjański trzech zbiorów składa się z trójek.

Ogólnie, iloczyn postaci $A_1 \times \dots \times A_n$ składa się z krotek
 postaci $\langle a_1, \dots, a_n \rangle$. Czyli z ciągów skończonych.

Jak zdefiniować iloczyn kartezjański
 nieskończenie wielu zbiorów?

Jeśli te zbiory A_i są numerowane liczbami naturalnymi $i \in \mathbb{N}$,
 to elementami iloczynu kartezjańskiego powinny być ciągi
 nieskończone postaci $\{a_i\}_{i \in \mathbb{N}}$.

A co zrobić z dowolną *rodziną indeksowaną* $\{A_t\}_{t \in T}$?

428

Ćwiczenie

- Zbiory $\prod_{t \in T} (A_t \cap B_t)$ i $\prod_{t \in T} A_t \cap \prod_{t \in T} B_t$ są równe.

- Zbiory $\prod_{t \in T} (A_t \cup B_t)$ i $\prod_{t \in T} A_t \cup \prod_{t \in T} B_t$
 niekoniecznie.

Na przykład dla $T = \mathbb{N}$, $A_t = \{0\}$, $B_t = \{1\}$,
 do pierwszego zbioru należą wszystkie ciągi
 zerojedynkowe, do drugiego tylko ciągi stałe.

- Por. $\forall t (A(t) \vee B(t))$ vs. $\forall t A(t) \vee \forall t B(t)$

430

Twierdzenie

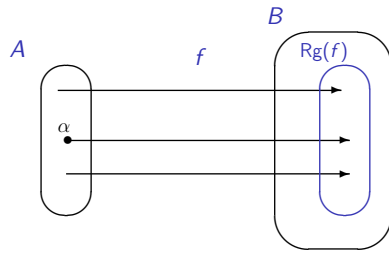
Jeśli $A \neq \emptyset$, to następujące warunki są równoważne:

- 1) Istnieje funkcja $f : A \xrightarrow{1-1} B$;
- 2) Istnieje funkcja $g : B \xrightarrow{\text{na}} A$.

Implikacja $(1) \Rightarrow (2)$ jest oczywista.
 Implikacja odwrotna niekoniecznie.

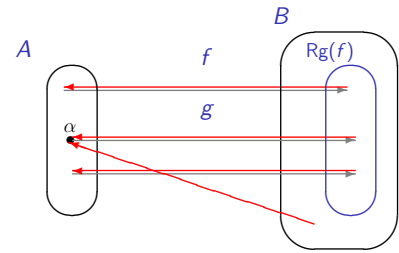
432

Jeśli $A \neq \emptyset$ i $f : A \xrightarrow{1-1} B$ to istnieje takie $g : B \xrightarrow{na} A$, że $g \circ f = id_A$.



433

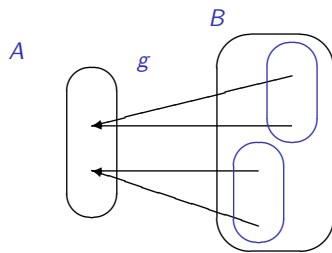
Jeśli $A \neq \emptyset$ i $f : A \xrightarrow{1-1} B$ to istnieje takie $g : B \xrightarrow{na} A$, że $g \circ f = id_A$.



$$g(b) = \text{if } b \in \text{Rg}(f) \text{ then } f^{-1}(b) \text{ else } \alpha$$

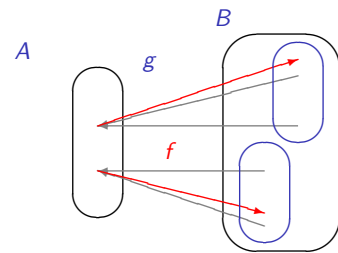
434

Jeśli $g : B \xrightarrow{na} A$ to istnieje takie $f : A \xrightarrow{1-1} B$, że $g \circ f = id_A$.



435

Jeśli $g : B \xrightarrow{na} A$ to istnieje takie $f : A \xrightarrow{1-1} B$, że $g \circ f = id_A$.



$$f \in \prod_{a \in A} g^{-1}(\{a\}) \neq \emptyset$$

436

Twierdzenie

Suma przeliczalnej rodziny zbiorów przeliczalnych
jest przeliczalna.

Dowód: Niech $\mathcal{A}$ będzie przeliczalną rodziną zbiorów przeliczalnych. Załóżmy, że $\mathcal{A} \neq \emptyset$ oraz $\emptyset \notin \mathcal{A}$. Wtedy:

- Istnieje funkcja $F : \mathbb{N} \xrightarrow{na} \mathcal{A}$.
- Istnieją funkcje $f_m : \mathbb{N} \xrightarrow{na} F(m)$.

Każde $a \in \bigcup \mathcal{A}$ należy do pewnego $F(m)$.
Zatem każde $a \in \bigcup \mathcal{A}$ jest postaci $f_m(n)$.

Niech $G(m, n) = f_m(n)$, dla $m, n \in \mathbb{N}$. **Ale które f_m ?**
Funkcja $G : \mathbb{N} \times \mathbb{N} \rightarrow \bigcup \mathcal{A}$ jest na $\bigcup \mathcal{A}$.

Zatem $\bigcup \mathcal{A}$ jest zbiorem przeliczalnym. □

437

Twierdzenie

Suma przeliczalnej rodziny zbiorów przeliczalnych
jest przeliczalna.

Dowód: Niech $\mathcal{A}$ będzie przeliczalną rodziną zbiorów przeliczalnych. Załóżmy, że $\mathcal{A} \neq \emptyset$ oraz $\emptyset \notin \mathcal{A}$. Wtedy:

- Istnieje funkcja $F : \mathbb{N} \xrightarrow{na} \mathcal{A}$.
- Istnieją funkcje $f : \mathbb{N} \xrightarrow{na} F(m)$.

Niech $F_m = \{f : \mathbb{N} \xrightarrow{na} F(m)\}$ i niech φ będzie funkcją wyboru dla rodziny $\{F_m \mid m \in \mathbb{N}\}$.

Teraz $G(m, n) = \varphi(F_m)(n)$, dla $m, n \in \mathbb{N}$.

Funkcja $G : \mathbb{N} \times \mathbb{N} \rightarrow \bigcup \mathcal{A}$ jest na $\bigcup \mathcal{A}$.

Zatem $\bigcup \mathcal{A}$ jest zbiorem przeliczalnym. □

438

Mniej oczywisty skutek pewnika wyboru: lemat Kuratowskiego-Zorna

Twierdzenie

Niech $\langle Z, \leq \rangle$ będzie zbiorem częściowo uporządkowanym, spełniającym następujący warunek:

(*) Każdy łańcuch ma w Z ograniczenie górne.

Wtedy w Z istnieje element maksymalny.

Tymczasem, w przestrzeni liniowej...

Podzbiór A przestrzeni liniowej V jest *liniowo niezależny*, jeśli z warunku $k_1 v_1 + \dots + k_n v_n = 0$, gdzie $v_1, \dots, v_n \in A$, wynika $k_1 = \dots = k_n = 0$.

Zbiór A jest *bazą* przestrzeni V , wtedy i tylko wtedy, gdy jest liniowo niezależny, oraz każdy element przestrzeni V jest kombinacją liniową elementów zbioru A .

Wniosek

Baza to maksymalny zbiór liniowo niezależny, czyli maksymalny element rodziny

$Z = \{A \subseteq V \mid A \text{ jest liniowo niezależny}\}$
uporządkowanej przez inkluzję.

439

440

Twierdzenie: Każda przestrzeń liniowa ma bazę

Dowód: Niech $Z = \{A \subseteq V \mid A \text{ jest liniowo niezależny}\}$.

Wykażemy, że $\langle Z, \subseteq \rangle$ ma element maksymalny.

Sprawdzamy czy każdy łańcuch ma w Z ograniczenie górne.

Niech $\mathcal{L}$ będzie łańcuchem w Z i niech $B = \bigcup \mathcal{L}$.

Pokażemy, że zbiór B jest liniowo niezależny.

Przypuśćmy $k_1 v_1 + \dots + k_n v_n = 0$, gdzie $v_1, \dots, v_n \in B$.

Wtedy $v_1 \in A_1, \dots, v_n \in A_n$ dla pewnych $A_1, \dots, A_n \in \mathcal{L}$.

Któryś zbiór A_i jest największy; wtedy $v_1, \dots, v_n \in A_i$.

Skoro A_i jest liniowo niezależny oraz $k_1 v_1 + \dots + k_n v_n = 0$, to $k_1 = \dots = k_n = 0$.

Zatem zbiór $B = \bigcup \mathcal{L}$ jest liniowo niezależny, tj. $B \in Z$.

Oczywiście B jest ograniczeniem górnym dla $\mathcal{L}$.

A więc każdy łańcuch ma ograniczenie górne. (*)

Pokazaliśmy, że spełniony jest warunek (*).

Zatem $\langle Z, \subseteq \rangle$ ma element maksymalny. $\square$

441

Każda przestrzeń liniowa ma bazę

Cel 1: Każdy łańcuch jest ograniczony z góry.

Założmy, że $\mathcal{L}$ jest łańcuchem. Cel 2: $B = \bigcup \mathcal{L}$ ogranicza $\mathcal{L}$ w Z .

Cel 3: $B \in Z$

Niech $k_1 v_1 + \dots + k_n v_n = 0 \dots$ Cel 4: $k_1 = \dots = k_n = 0$.

...

Zatem $k_1 = \dots = k_n = 0$ (Cel 4 osiągnięty)

Zatem B jest liniowo niezależny, tj. $B \in Z$ (Cel 3 osiągnięty)

Łatwo widzieć, że $\forall A \in \mathcal{L} \rightarrow A \subseteq B$

Zatem B jest ograniczeniem $\mathcal{L}$ w Z (Cel 2 osiągnięty)

Zatem każdy łańcuch ma ograniczenie górne (Cel 1 osiągnięty)

Z lematu Kuratowskiego-Zorna istnieje element maksymalny.

442

Jeszcze jeden przykład

Niech A, B - dowolne zbiory i niech $\mathcal{F} = \{f \mid f: A \xrightarrow{1-1} B\}$.

$\langle \mathcal{F}, \subseteq \rangle$ spełnia założenia lematu Kuratowskiego-Zorna.

Niech L - łańcuch.

To jest rodzina zgodna, więc $\bigcup L: A \rightarrow B$.

Czy ta suma jest różnowartościowa?

Przypuśćmy, że $(\bigcup L)(a_1) = (\bigcup L)(a_2) = b$.

Są takie $f_1, f_2 \in L$, że $f_1(a_1) = b$ i $f_2(a_2) = b$.

Ale to jest łańcuch, więc np. $f_1 \subseteq f_2$.

Wtedy $f_2(a_1) = f_2(a_2)$, skąd $a_1 = a_2$.

443

Porównywanie liczb kardynalnych

Niech A, B - dowolne zbiory i niech $\mathcal{F} = \{f \mid f: A \xrightarrow{1-1} B\}$.

$\langle \mathcal{F}, \subseteq \rangle$ spełnia założenia lematu Kuratowskiego-Zorna.

Zatem istnieje element maksymalny $f: A \xrightarrow{1-1} B$.

Z maksymalności:

- albo $\text{Dom}(f) = A$ i mamy $f: A \xrightarrow{1-1} B$, skąd $\bar{A} \leq \bar{B}$.

- albo $\text{Rg}(f) = B$ i mamy $f^{-1}: B \xrightarrow{1-1} A$, skąd $\bar{B} \leq \bar{A}$.

Wniosek: Zawsze $\bar{A} \leq \bar{B}$ lub $\bar{B} \leq \bar{A}$.

444

Paradoksalny skutek pewnika wyboru:
twierdzenie Banacha-Tarskiego

Twierdzenie

Niech K oznacza kulę w $\mathbb{R}^3$ o promieniu 1.

Istnieje taki podział K na skończenie wiele części

$C_1, C_2, \dots, C_n$, oraz takie izometrie $\varphi_1, \dots, \varphi_n$,

że $\varphi_1(C_1) \cup \dots \cup \varphi_1(C_n) = K_1 \cup K_2$,

gdzie K_1 i K_2 to rozłączne kule o promieniu 1..

Uwaga: Nie każdy zbiór ma „objętość”.

Istnieją zbiory niemierzalne.

Dowód: <https://www.youtube.com/watch?v=s86-Z-CbaHA>

445

Jeszcze o porządkach częściowych

Fakt

W kracie zupełnej istnieje element najmniejszy $\perp$ i największy $\top$.

Fakt

W kracie zupełnej każdy podzbiór ma kres dolny.

Dowód: Niech $\langle A, \leq \rangle$ będzie kratą zupełną i niech $B \subseteq A$.

Rozpatrzmy zbiór $C = \{x \in A \mid x \leq b\}$. Istnieje $\sup C$.

Jeśli $b \in B$, to $b \geq c$, więc dla $c = \sup C$ mamy $b \geq c$.

Zatem c jest ograniczeniem dolnym zbioru B .

Ponadto c jest kresem dolnym, bo $x \leq B$ implikuje $x \leq c$. $\square$

446

Przypomnijmy sobie, że:

Element a jest *kresem górnym* zbioru B ($a = \sup B$),
gdy jest najmniejszym ograniczeniem górnym B , czyli:

- ▶ $a \geq b$;
- ▶ dla dowolnego $c \in A$, jeśli $c \geq b$, to $c \geq a$.

Analogicznie, a jest *kresem dolnym* zbioru B ($a = \inf B$),
gdy jest największym ograniczeniem dolnym B , czyli:

- ▶ $a \leq b$;
- ▶ dla dowolnego $c \in A$, jeśli $c \leq b$, to $c \leq a$.

447

448

Niech $\langle A, \leq \rangle$ i $\langle B, \leq \rangle$ będą porządkami częściowymi.

- Funkcja $f : A \rightarrow B$ jest *monotoniczna*, gdy $x \leq y$ implikuje $f(x) \leq f(y)$.
- Jeśli $f : A \rightarrow A$ oraz $f(a) = a$, to mówimy, że a jest *punktem stałym* funkcji f .

449

Twierdzenie o punkcie stałym (Tarski-Knaster)

Jeśli $\langle A, \leq \rangle$ jest kratą zupełną, to każda monotoniczna funkcja $f : A \rightarrow A$ ma najmniejszy punkt stały.

Dowód: Niech $B = \{x \in A \mid f(x) \leq x\}$; niech $a = \inf B$. Pokażemy, że a jest najmniejszym punktem stałym funkcji f .

Dla dowolnego $x \in B$ mamy $a \leq x$, więc $f(a) \leq f(x) \leq x$. Zatem $f(a)$ jest ograniczeniem dolnym zbioru B , skąd $f(a) \leq a$, bo a jest kresem dolnym.

Ale skoro $f(a) \leq a$, to także $f(f(a)) \leq f(a)$, więc $f(a) \in B$. Zatem $a \leq f(a)$ i mamy równość.

Ponieważ wszystkie punkty stałe funkcji f muszą należeć do B , więc a jest najmniejszym punktem stałym. $\square$

451

Przykład

Niech V będzie przestrzenią liniową nad $\mathbb{R}$. Ustalmy $Z \subseteq V$ i niech $F : P(V) \rightarrow P(V)$ będzie taką funkcją, że $F(W) = Z \cup \{u + w \mid u, w \in W\} \cup \{s \cdot w \mid s \in \mathbb{R} \wedge w \in W\}$.

Punkty stałe operacji F , to podprzestrzenie przestrzeni V zawierające zbiór Z .

Najmniejszym punktem stałym operacji F jest podprzestrzeń rozpięta na zbiorze Z .

453

Motywujący przykład

Rozpatrzmy program (definicję funkcji):

$$f(m, n) = \text{if } m = n \text{ then } 0 \text{ else } f(m + 3, n) + 3.$$

Mamy tu w istocie równanie postaci $f = \Phi(f)$.

Znaczeniem tego programu jest funkcja $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, która jest punktem stałym przekształcenia

$$\Phi : (\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}) \rightarrow (\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z})$$

$$\Phi(f)(m, n) = \text{if } m = n \text{ then } 0 \text{ else } f(m + 3, n) + 3.$$

455

Przykład

Niech $f : P(\mathbb{N}) \rightarrow P(\mathbb{N})$ będzie taka, że $f(A) = A \cup \{1, 3, 7\}$.

To jest funkcja monotoniczna.

Punkty stałe przekształcenia f to wszystkie te zbiory A , do których należą liczby 1, 3, 7.

Zbiór $\{1, 3, 7\}$ jest najmniejszym punktem stałym funkcji f .

Piszemy $\{1, 3, 7\} = \text{lfp}(f)$. (Least fixed point)

450

Przykład: domknięcie przechodnie relacji

(Przypomnijmy, że relacja s jest przechodnia wtedy i tylko wtedy, gdy $s \cdot s \subseteq s$.)

Niech $r \subseteq A \times A$ niech $\varphi : P(A \times A) \rightarrow P(A \times A)$ będzie taka:

$$\varphi(s) = r \cup s \cup (s \cdot s).$$

Punkty stałe funkcji φ to relacje przechodnie zawierające r . Inaczej: rozwiązania równania $s = r \cup s \cup (s \cdot s)$.

Najmniejszy punkt stały φ to domknięcie przechodnie relacji r .

452

Najmniejsze punkty stałe

Rozwiązanie równania $X = F(X)$ to punkt stały przekształcenia $\lambda X. F(X)$.

Jeśli równanie $X = F(X)$ stanowi rekurencyjną definicję X , to szukamy *najmniejszego* punktu stałego.

454

Motywujący przykład

Przekształcenie $\Phi : (\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}) \rightarrow (\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z})$

$$\Phi(f)(m, n) = \text{if } m = n \text{ then } 0 \text{ else } f(m + 3, n) + 3$$

ma różne punkty stałe, na przykład:

- $f_1(m, n) = n - m$;
- $f_2(m, n) = \text{if } 3 \mid (n - m) \text{ then } n - m \text{ else } 7 - m$;
- $f_0(m, n) = \text{if } n \geq m \wedge 3 \mid (n - m) \text{ then } n - m \text{ else } \perp$.

Nas interesuje *najmniejszy* punkt stały f_0 . Dlaczego?

456

Motywujący przykład

Najmniejszym rozwiązaniem równania

$$f(m, n) = \text{if } m = n \text{ then } 0 \text{ else } f(m + 3, n) + 3$$

jest funkcja

$$f_0(m, n) = \text{if } n \geq m \wedge 3|(n - m) \text{ then } n - m \text{ else } \perp.$$

Jest to kres górny ciągu przybliżeń:

$$\text{if } m = n \text{ then } 0 \text{ else } \perp;$$

$$\text{if } m = n \text{ then } 0 \text{ else if } m + 3 = n \text{ then } 0 + 3 \text{ else } \perp;$$

i tak dalej.

457

niestety...

- Zbiór funkcji częściowych $\langle A \rightarrow B, \subseteq \rangle$ nie jest kratą zupełną (o ile B ma co najmniej dwa elementy).

Na szczęście:

- W zbiorze $\langle A \rightarrow B, \subseteq \rangle$ funkcji częściowych z A do B każda zgodna rodzina $\mathcal{R}$ ma kres górny $\sup \mathcal{R} = \bigcup \mathcal{R}$.

(Rodzina $\mathcal{R}$ funkcji częściowych jest *zgodna*, gdy dla dowolnych $f, g \in \mathcal{R}$ i dowolnego $x \in \text{Dom}(f) \cap \text{Dom}(g)$ zachodzi $f(x) = g(x)$.)

459

Przykłady

- Każda krata zupełna jest zupełnym porządkiem częściowym.
- Zbiór funkcji częściowych $\langle \mathbb{N} \rightarrow \mathbb{N}, \subseteq \rangle$ nie jest kratą zupełną, ale jest zupełnym porządkiem częściowym. (Uwaga: nie każda rodzina zgodna jest skierowana, ale każda skierowana jest zgodna.)

461

Nie mówcie tego na analizie

Definicja

Niech $\langle A, \leq \rangle$ i $\langle B, \leq \rangle$ będą porządkami częściowymi. Jeśli $\langle A, \leq \rangle$ i $\langle B, \leq \rangle$ są cpo, to $f : A \rightarrow B$ jest *ciągła*, gdy $f(\sup X) = \sup f(X)$ dla skierowanych i niepustych X .

Fakt

Każda funkcja ciągła jest monotoniczna.

Dowód: Niech $x \leq y$. Wtedy zbiór $\{x, y\}$ jest skierowany, a jego kresem górnym jest y . Zatem $f(y)$ jest kresem górnym zbioru $\{f(x), f(y)\}$, czyli $f(x) \leq f(y)$. $\square$

463

Uogólnienie: Semantyka denotacyjna

Znaczeniem programu:

$$f(m, n) = \text{if } m = n \text{ then } 0 \text{ else } f(m + 3, n) + 3$$

jest $f_0 : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, która jest najmniejszym punktem stałym przekształcenia

$$\Phi : (\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}) \rightarrow (\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z})$$

$$\Phi(f)(m, n) = \text{if } m = n \text{ then } 0 \text{ else } f(m + 3, n) + 3.$$

Fakt: To przekształcenie jest monotoniczne: jeśli $g \subseteq h$ to $\Phi(g) \subseteq \Phi(h)$.

ale...

458

Porządki zupełne

Niech $\langle A, \leq \rangle$ będzie porządkiem częściowym.

- Podzbiór B zbioru A jest *skierowany*, gdy dla dowolnych $a, b \in B$ istnieje takie $c \in B$, że $a, b \leq c$.
- Zbiór A jest *zupełnym* porządkiem częściowym (cpo) wtedy i tylko wtedy, gdy każdy jego skierowany podzbiór ma kres górny.

Uwaga: Każde cpo ma najmniejszy element $\perp = \sup \emptyset$.

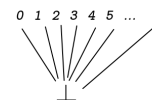
Fakt: Każdy łańcuch jest zbiorem skierowanym.

A zatem w każdym cpo istnieją kresy wszystkich łańcuchów.

460

Przykłady

- Zbiór $\mathbb{N}_\perp = \mathbb{N} \cup \{\perp\}$ uporządkowany w ten sposób, że
 - nowy element $\perp$ jest najmniejszy;
 - różne liczby naturalne są nieporównywalne,
 jest zupełnym porządkiem częściowym.



462

Twierdzenie o punkcie stałym (Kleene)

Jeśli $\langle A, \leq \rangle$ jest cpo, to każda funkcja ciągła $f : A \rightarrow A$ ma najmniejszy punkt stały, którym jest $\sup\{f^n(\perp) \mid n \in \mathbb{N}\}$.

Dowód: Oczywiście $\perp \leq f(\perp)$. Ponieważ f jest monotoniczna, więc ciąg $f^n(\perp)$ jest wstępujący (indukcja):

$$\perp \leq f(\perp) \leq f^2(\perp) \leq f^3(\perp) \leq \dots$$

Zbiór $\{f^n(\perp) \mid n \in \mathbb{N}\}$ jest więc skierowany i z ciągłości:

$$f(\sup\{f^n(\perp) \mid n \in \mathbb{N}\}) = \sup\{f^{n+1}(\perp) \mid n \in \mathbb{N}\} = \sup\{f^n(\perp) \mid n \in \mathbb{N}\},$$

czyli $a = \sup\{f^n(\perp) \mid n \in \mathbb{N}\}$ jest punktem stałym.

Jeśli b jest innym punktem stałym, to z nierówności $\perp \leq b$ wynika przez indukcję $f^n(\perp) \leq f^n(b) = b$, skąd $a \leq b$. $\square$

464

Przykład: domknięcie przechodnie

(Przypomnijmy, że relacja s jest przechodnia wtedy i tylko wtedy, gdy $s \cdot s \subseteq s$.)

Niech $r \subseteq A \times A$ niech $f : P(A \times A) \rightarrow P(A \times A)$ będzie taka:
 $\varphi(s) = r \cup s \cup (s \cdot s)$.

Punkty stałe funkcji φ to relacje przechodnie zawierające r .

Najmniejszy punkt stały φ to domknięcie przechodnie relacji r .

Otrzymujemy go jako sumę ciągu przybliżeń:

$$\emptyset \subseteq \varphi(\emptyset) \subseteq \varphi^2(\emptyset) \subseteq \dots$$

Uwaga: $\varphi(\emptyset) = r_0 = r$, $\varphi^2(\emptyset) = r_1 = r \cup (r \cdot r)$, i tak dalej.

465

Wracamy do naszego przykładu

Rozpatrzmy program (definicję funkcji):

$$f(m, n) = \text{if } m = n \text{ then } 0 \text{ else } f(m + 3, n) + 3$$

Znaczeniem tego programu jest funkcja $f_0 : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, która jest najmniejszym punktem stałym przekształcenia

$$\Phi : (\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}) \rightarrow (\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z})$$

$$\Phi(f)(m, n) = \text{if } m = n \text{ then } 0 \text{ else } f(m + 3, n) + 3.$$

Fakt: To przekształcenie jest ciągłe: jeśli $\mathcal{R}$ jest skierowaną rodziną funkcji częściowych, to $\Phi(\sup \mathcal{R}) = \sup \Phi(\mathcal{R})$.

466

Semantyka denotacyjna

Najmniejszym rozwiązaniem równania

$$f(m, n) = \text{if } m = n \text{ then } 0 \text{ else } f(m + 3, n) + 3$$

jest funkcja

$$f_0(m, n) = \text{if } n \geq m \wedge 3|(n - m) \text{ then } n - m \text{ else } \perp.$$

Jest to kres górny ciągu przybliżeń:

$$\perp(m, n) = \perp;$$

$$\Phi(\perp)(m, n) = \text{if } m = n \text{ then } 0 \text{ else } \perp$$

$$\Phi^2(\perp)(m, n) =$$

$$\text{if } m = n \text{ then } 0 \text{ else if } m + 3 = n \text{ then } 0 + 3 \text{ else } \perp$$

i tak dalej.

467

Jeszcze jeden przykład punktu stałego: palindromy

adapannapocałowanawoławocannapada

napotkałtazapytałaktopan

468

Gramatyka dla palindromów

Palindromy nad alfabetem $\{a, b\}$:

$$X ::= \varepsilon \mid a \mid b \mid aXa \mid bXb$$

- ▶ Słowo puste i słowa jednoliterowe są palindromami.
- ▶ Jeśli X jest palindromem, to aXa jest palindromem.
- ▶ Jeśli X jest palindromem, to bXb jest palindromem.
- ▶ Nie ma innych palindromów.

Zbiór $\mathcal{P}$ wszystkich palindromów spełnia warunek

$$\mathcal{P} = \{\varepsilon, a, b\} \cup \{aXa \mid X \in \mathcal{P}\} \cup \{bXb \mid X \in \mathcal{P}\}.$$

Jest to jedyny zbiór o tej własności.

469

Palindromy: $X ::= \varepsilon \mid a \mid b \mid aXa \mid bXb$

Zbiór $\mathcal{P}$ to najmniejszy (bo jedyny) punkt stały przekształcenia

$$F : P(\{a, b\}^*) \rightarrow P(\{a, b\}^*):$$

$$F(B) = \{\varepsilon, a, b\} \cup \{aXa \mid X \in B\} \cup \{bXb \mid X \in B\}.$$

Jest to suma ciągu przybliżeń $F^n(\emptyset)$:

$$\emptyset,$$

$$F(\emptyset) = \{\varepsilon, a, b\},$$

$$F(\{\varepsilon, a, b\}) = \{\varepsilon, a, b, aa, bb, aaa, bab, aba, bbb\},$$

$$F(\{\varepsilon, a, b, aa, bb, aaa, bab, aba, bbb\}) = \{\varepsilon, a, b, aaa, bab, aba, bbb, aaaaa, \dots\}$$

470

Wyrażenia nawiasowe

Rozważamy słowa zbudowane z symboli $(,)$.

Gramatyka pierwsza: $X ::= \varepsilon \mid X \cdot X \mid (X)$.

Ta gramatyka odpowiada przekształceniu

$$F = \lambda X. \{\varepsilon\} \cup \{xy \mid x, y \in X\} \cup \{(x) \mid x \in X\},$$

które ma wiele punktów stałych. Najmniejszy z nich, to zbiór *poprawnych wyrażeń nawiasowych*. A inne?

Gramatyka druga: $X ::= \varepsilon \mid (X)X$.

Ćwiczenie: ile rozwiązań ma równanie

$$X = \{\varepsilon\} \cup \{(x)y \mid x, y \in X\}?$$

471

Dobre ufundowanie

472

Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Jeśli każdy niepusty podzbiór zbioru A ma element minimalny, to mówimy, że $\langle A, \leq \rangle$ jest *częściowym dobrym porządkiem*, lub, że A jest *dobrze ufundowany*.

Jeśli ponadto porządek $\langle A, \leq \rangle$ jest liniowy, to jest to *dobry porządek*.

(Wtedy każdy niepusty podzbiór A ma element najmniejszy.)

473

Przykłady

- Relacja porządku prefiksowego jest dobrym ufundowaniem zbioru A^* .
- Jeśli w A są dwa elementy a, b , takie że $a < b$, to porządek leksykograficzny $\preceq$ nie jest dobrym ufundowaniem zbioru A^* .

Zbiór $\{a^n b \mid n \in \mathbb{N}\}$ nie ma elementu minimalnego:
 $b \succ ab \succ aab \succ aaab \succ \dots$

- Dla dowolnego k , zbiór $\mathbb{N}^k$, złożony z k -krotek liczb naturalnych (słów długości k) jest dobrze uporządkowany przez porządek leksykograficzny.

475

Fakt

Zbiór $\langle A, \leq \rangle$ jest dobrze ufundowany wtedy i tylko wtedy, gdy nie istnieje w nim ciąg malejący, tj. taki podzbiór $\{a_i \mid i \in \mathbb{N}\}$, że $a_{i+1} < a_i$ dla dowolnego i .

474

Odcinki początkowe

Podzbiór B zbioru częściowo uporządkowanego A nazywamy *odcinkiem początkowym* w A , gdy

$$\forall x, y \in A (x \in B \wedge y \leq x \rightarrow y \in B).$$

Szczególny przypadek odcinka początkowego, to odcinek wyznaczony przez element $x \in A$:

$$\mathcal{O}_A(x) = \{y \in A \mid y < x\}.$$

476

Dendrologia

Zbiór częściowo uporządkowany $\langle T, \leq \rangle$ nazywamy *drzewem*, gdy spełnia on następujące warunki:

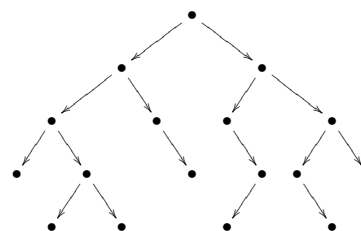
- 1) Istnieje element najmniejszy.
- 2) Każdy odcinek $\mathcal{O}_T(x)$ jest skończonym łańcuchem.

Jeśli łańcuch $\mathcal{O}_T(x)$ ma n elementów, to powiemy, że x jest wierzchołkiem o *wysokości* n . Element najmniejszy, nazywany *korzeniem*, ma wysokość zerową.

Fakt: każde drzewo jest dobrze ufundowane.

477

Drzewa rosną z góry na dół.



478

Drzewo słów

Niepusty podzbiór T zbioru A^* nazywamy *drzewem słów*, gdy jest on odcinkiem początkowym w $\langle A^*, \preceq \rangle$, czyli gdy

$$\forall w, u \in A^* (w \cdot u \in T \rightarrow w \in T).$$

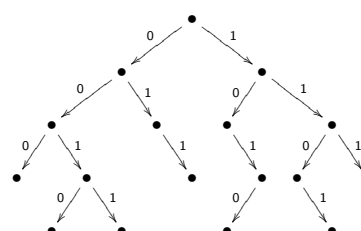
Przykład: $\{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 011, 101, 110, 111, 0010, 0011, 1010, 1101\}$.

Drzewa słów nad alfabetem dwuliterowym to *drzewa binarne*. Zbiór $\{0, 1\}^*$ to *pełne nieskończone drzewo binarne*.

Uwaga: w ogólności alfabet może być także nieskończony.

479

Każde drzewo jest izomorficzne z pewnym drzewem słów.

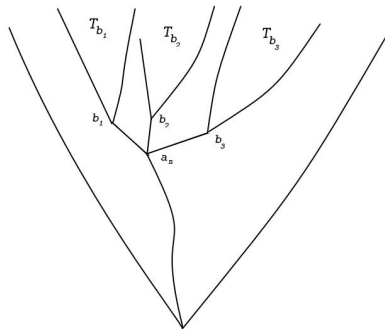


$\{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 011, 101, 110, 111, 0010, 0011, 1010, 1101\}$

480

- ▶ **Gałąź** w drzewie T nazywamy dowolny ciąg postaci $\varepsilon = a_0, a_1, a_2, \dots$ (skończony lub nieskończony) gdzie każde a_{i+1} jest bezpośrednim następnikiem a_i .
- ▶ Mówimy, że T jest drzewem **o skończonym rozgałęzieniu**, jeśli każdy element T ma skończenie wiele bezpośrednich następników.

481



483

Przykład: Niech $f: \mathbb{N} \rightarrow \{0, 1\}$. Liczba $c \in \mathbb{N}$ jest **świadkiem pitagorejskim** dla funkcji f , gdy istnieją takie liczby $a, b < c$, że $f(a) = f(b) = f(c)$ oraz $a^2 + b^2 = c^2$.

0	1	2	3	4	5	6	7	8	9	10	11	12
0	1	0	1	1	0	0	1	0	1	0	1	0
13	14	15	16	17	18	19	20	21	22	23	24	25
1	0	0	0	0	1	0	0	0	1	1	1	1

Twierdzenie (M. Heule, O. Kullmann, W. Marek):
Dla każdego $f: \mathbb{N} \rightarrow \{0, 1\}$ istnieje świadek pitagorejski.

485

www.nature.com/news/two-hundred-terabyte-maths-proof-is-largest-ever-1.19990

nature
International weekly journal of science

Home | News & Comment | Research | Careers & Jobs | Current issue | Archive | Audio & Video | Feedback

Archive > Volume 534 > Issue 7605 > News > Article

NATURE | NEWS

Two-hundred-terabyte maths proof is largest ever
A computer cracks the Boolean Pythagorean triples problem — but is it really maths?
Evelyn Lamb

MATHS
Maths proof smashes size record
Supercomputer produces a 200-terabyte proof — but is it really mathematics?

BY EVELYN LAMB

Computer-assisted proofs too large to be directly verifiable by humans have become common, as have computers that solve problems in combinatorics — the study of finite discrete structures — by checking through unproven individual cases. Still, “200 terabytes is unbelievable”, says Ronald Graham, a mathematician at the University of California, San Diego. The previous record-holder is thought to be a 13-gigabyte proof, published in 2014. The puzzle that required the 200-terabyte proof, called the Boolean Pythagorean triples problem, has troubled mathematicians for decades. In the 1980s, Graham offered a prize of US\$100 for anyone who could solve it. (He presented the challenge to one of the three computer scientists, Marijn Heule of the University of Texas at Austin, last month.) The problem asks whether it is possible to colour each positive integer either red or blue, so that no trio of integers a, b and c that satisfy Pythagoras’ famous equation $a^2 + b^2 = c^2$ are all the same colour. For example, for the Pythagorean triple 3, 4 and 5, if 3 and 5 were blue, 4 would have to be red. ▶

487

Jeśli T jest nieskończonym drzewem o skończonym rozgałęzieniu, to w T jest gałąź nieskończona.

Dowód: Dla $a \in T$ niech $T_a = \{b \in T \mid a \leq b\}$.

Przez indukcję konstruujemy gałąź $\varepsilon = a_0, a_1, a_2, \dots$ tak, aby każde T_{a_i} było nieskończone.

Krok bazowy jest poprawny, bo $T_\varepsilon = T$.

482

Lemat Königa

Jeśli T jest nieskończonym drzewem o skończonym rozgałęzieniu to w T jest gałąź nieskończona.

Dowód: Dla $a \in T$ niech $T_a = \{b \in T \mid a \leq b\}$.

Przez indukcję konstruujemy gałąź $\varepsilon = a_0, a_1, a_2, \dots$ tak, aby każde T_{a_i} było nieskończone.

Krok bazowy jest poprawny, bo $T_\varepsilon = T$.

Niech T_{a_n} będzie nieskończony i niech $b_1, \dots, b_k$ będą bezpośrednimi następnikami a_n . Ponieważ

$$T_{a_n} = \{a_n\} \cup T_{b_1} \cup \dots \cup T_{b_k},$$

więc któreś T_{b_i} jest nieskończone.

Można przyjąć $a_{n+1} = b_i$.

□

484

Przykład: Niech $f: \mathbb{N} \rightarrow \{0, 1\}$. Liczba $c \in \mathbb{N}$ jest **świadkiem pitagorejskim** dla funkcji f , gdy istnieją takie liczby $a, b < c$, że $f(a) = f(b) = f(c)$ oraz $a^2 + b^2 = c^2$.

Twierdzenie (M. Heule, O. Kullmann, W. Marek):
Dla każdego $f: \mathbb{N} \rightarrow \{0, 1\}$ istnieje świadek pitagorejski.

Wniosek: Istnieje taka stała N , że każda funkcja ma świadka pitagorejskiego mniejszego od N .

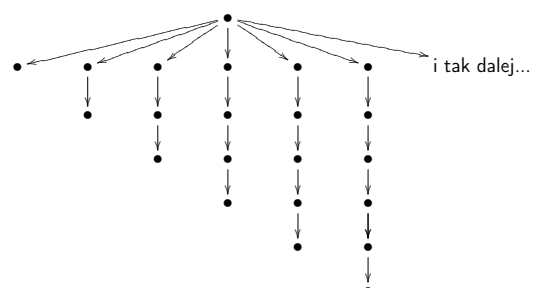
Dowód: Funkcje $f: \mathbb{N} \rightarrow \{0, 1\}$ to nieskończone gałęzie w pełnym drzewie binarnym. Na każdej gałęzi jest świadek pitagorejski. Jeśli usuniemy z drzewa wszystkie potomki świadków pitagorejskich, to otrzymamy drzewo binarne bez gałęzi nieskończonej. Z lematu Königa to drzewo musi być skończone, ma więc skończoną wysokość.

Rekord świata: W istocie wystarczy $N = 7826$.

Dowód komputerowy ma 200... **terabajtów**.

486

Drzewo o nieskończonym rozgałęzieniu



488

Uporządkowanie dobre

czyli liniowe dobre ufundowanie

489

Zadziwiająca twierdzenie

Twierdzenie (E. Zermelo)

Każdy zbiór można dobrze uporządkować.

Wniosek: No to można dobrze uporządkować na przykład zbiór liczb rzeczywistych.

Ale jak ?? Tego nikt nie wie... I się nie dowie!

Uwaga: Twierdzenie Zermela, lemat Kuratowskiego-Zorna i aksjomat wyboru są wzajemnie równoważne.

491

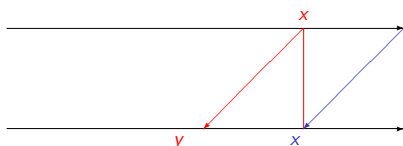
Własności dobrych porządków (łatwe)

Fakt:

- ▶ Niepusty zbiór dobrze uporządkowany ma element najmniejszy.
Ale $[0, 1]$ też ma.
- ▶ W zbiorze dobrze uporządkowanym każdy element oprócz ostatniego ma bezpośredni następnik.
Ale w zbiorze $\mathbb{Z}$ też.
- ▶ Dobry porządek jest liniowy i każdy właściwy odcinek początkowy jest postaci $\mathcal{O}_A(x)$.
I na odwrót.

493

Twierdzenie

Jeśli A jest zbiorem dobrze uporządkowanym, to A nie jest izomorficzny z żadnym swoim właściwym odcinkiem początkowym.**Dowód:** Przypuśćmy przeciwnie. Rozpatrzmy najmniejsze takie x , że $A \approx \mathcal{O}_A(x)$. Skoro $\mathcal{O}_A(x) \subsetneq A$... to $\mathcal{O}_A(x) \approx \mathcal{O}_A(y)$, dla pewnego $y < x$.

495

Przykłady dobre:

- ▶ Zbiór liczb naturalnych $\mathbb{N}$;
- ▶ Każdy skończony liniowy porządek;
- ▶ Zbiór $\mathbb{N}^k$ uporządkowany leksykograficznie.

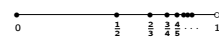
Przykłady nie-dobre:

- ▶ Zbiór liczb całkowitych $\mathbb{Z}$;
- ▶ Odcinek $[0, 1]$;
- ▶ Zbiór $\mathbb{N}^*$ uporządkowany leksykograficznie.

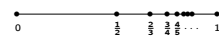
490

Następujące nieizomorficzne podzbiory $\mathbb{R}$ są dobrze uporządkowane

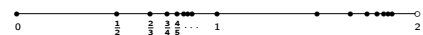
- ▶ $A = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$;



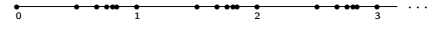
- ▶ $A' = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\} \cup \{1\}$;



- ▶ $A'' = A \cup \{2 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$;



- ▶ $B = \{m - \frac{1}{n} \mid m, n \in \mathbb{N} - \{0\}\}$.



492

Własności dobrych porządków (trudniejsze)

- ▶ Jeśli A jest zbiorem dobrze uporządkowanym, to A nie jest izomorficzny z żadnym swoim właściwym odcinkiem początkowym.
- ▶ Jeśli A i B są dobrze uporządkowane, to jeden z nich jest izomorficzny z odcinkiem początkowym drugiego.

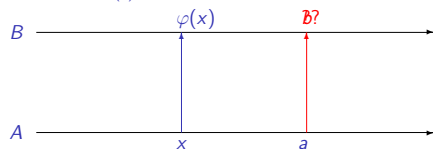
494

Twierdzenie

Jeśli A i B są dobrze uporządkowane, to jeden z nich jest izomorficzny z odcinkiem początkowym drugiego.**Dowód:** Przypuśćmy, że zbiór B nie jest izomorficzny z żadnym właściwym odcinkiem w A .Przez indukcję definiujemy takie $\varphi: A \xrightarrow{1-1} B$, że dla każdego $x \in A$ funkcja $\varphi|_{\mathcal{O}_A(x)}: \mathcal{O}_A(x) \rightarrow \mathcal{O}_B(\varphi(x))$ jest izomorfizmem.Takie φ będzie izomorfizmem A i odcinka $\text{Rg}(\varphi)$.

496

Przez indukcję definiujemy takie $\varphi : A \xrightarrow{1-1} B$, że dla $x \in A$ funkcja $\varphi|_{\mathcal{O}_A(x)} : \mathcal{O}_A(x) \rightarrow \mathcal{O}_B(\varphi(x))$ jest izomorfizmem.



Założmy, że dla wszystkich $x < a$ już zdefiniowano $\varphi(x)$.

Czyli mamy włożenie $\varphi|_{\mathcal{O}_A(a)} : \mathcal{O}_A(a) \xrightarrow{1-1} B$.

Obraz tego włożenia jest odcinkiem początkowym w B (i to właściwym), więc ma postać $\mathcal{O}_B(b)$.

Można wziąć $\varphi(a) = b$.

497

Liczby porządkowe

Konwencja: Każdemu dobremu porządkowi A przypisujemy jego *liczbę porządkową*, oznaczaną przez $\bar{A}$. Robimy to tak, aby zachodziła równoważność:

$$\bar{A} = \bar{B} \quad \text{wtedy i tylko wtedy, gdy} \quad A \approx B.$$

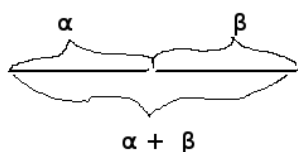
Piszemy $\bar{A} \leq \bar{B}$, gdy A jest izomorficzny z pewnym odcinkiem początkowym w B .

- Liczby porządkowe zbiorów skończonych to liczby naturalne.
- Liczba porządkowa zbioru $\mathbb{N}$ to ω .

498

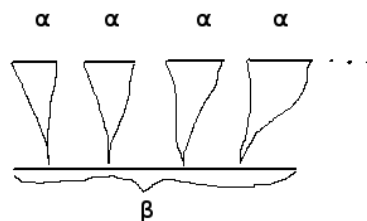
Działania na liczbach porządkowych

Dodawanie



499

$$\alpha \cdot \beta$$



500

Działania na liczbach porządkowych

Niech $\bar{A} = \alpha$ i $\bar{B} = \beta$.

- Suma $\alpha + \beta$ to liczba porządkowa zbioru $A \oplus B$ uporządkowanego tak:

$$\langle x \rangle_i \leq \langle y \rangle_j \Leftrightarrow i < j, \text{ lub } i = j \text{ oraz } x \leq y.$$

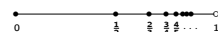
- Iloczyn $\alpha \cdot \beta$ to liczba porządkowa zbioru $A \times B$ uporządkowanego „antyleksykograficznie”:

$$\langle a, b \rangle \leq \langle a', b' \rangle \Leftrightarrow b < b', \text{ lub } b = b' \text{ oraz } a \leq a'.$$

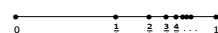
501

Przykłady

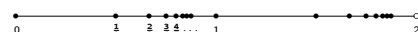
$$\text{► } A = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}; \quad (\omega)$$



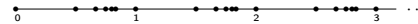
$$\text{► } A' = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\} \cup \{1\}; \quad (\omega + 1)$$



$$\text{► } A'' = A \cup \{2 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}; \quad (\omega + \omega = \omega \cdot 2)$$



$$\text{► } B = \{m - \frac{1}{n} \mid m, n \in \mathbb{N} - \{0\}\}. \quad (\omega \cdot \omega)$$



502

Działania na liczbach porządkowych

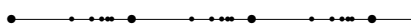
- $1 + \omega = \omega \neq \omega + 1$;
- $2 \cdot \omega = \omega \neq \omega + \omega = \omega \cdot 2$;
- $\alpha^2 := \alpha \cdot \alpha$;
- $\alpha^{k+1} := \alpha \cdot \alpha^k$;
- $\alpha^\omega :=$ najmniejsza liczba większa od wszystkich α^k .
- $2^\omega = \omega$.

503

Porządkowanie zbioru $\mathbb{N}^k$

Zwykły porządek $\leq$ w zbiorze $\mathbb{N}$ jest typu ω .

Porządek leksykograficzny w $\mathbb{N}^2$ jest typu $\omega \cdot \omega = \omega^2$:



$$\langle 0, 0 \rangle < \langle 0, 1 \rangle < \langle 0, 2 \rangle < \dots < \langle 1, 0 \rangle < \langle 1, 1 \rangle < \dots < \langle 2, 1 \rangle < \dots$$

Porządek leksykograficzny w $\mathbb{N}^3$ jest typu $\omega^2 \cdot \omega = \omega^3$:

$$\langle 0, 0, 0 \rangle \dots \langle 0, m, n \rangle \dots \langle 1, m, n \rangle \dots \langle 2, m, n \rangle \dots$$

Porządek leksykograficzny w $\mathbb{N}^k$ jest typu ω^k .

504

Multizbiór to „zbiór z powtórzeniami” (funkcja $M : A \rightarrow \mathbb{N}$).

Na przykład $\{1, 2, 2, 3, 4, 4, 4\}$ to taka funkcja M , że

$$M(1) = M(3) = 1, M(2) = 2 \text{ i } M(4) = 3.$$

Dla $x \neq 1, 2, 3, 4$ przyjmujemy $M(x) = 0$.

505

Porównujemy skończone multizbiory

Niech M_1, M_2 to skończone multizbiory.

Przyjmujemy, że $M_1 \leq M_2$, gdy $M_1 = M_2$ albo

$$\exists k (M_1(k) < M_2(k) \wedge \forall n > k. M_1(n) = M_2(n))$$

Przykłady:

$$\{0, 0, 0, 0, 0, 1, 1, 1, 2\} \leq \{0, 1, 1, 2, 3, 3\} \leq \{0, 1, 3, 6\}$$

$$\{0, 0, 0, 0, 1, 2, 3, 3\} \leq \{0, 1, 1, 2, 3, 3\} \leq \{1, 2, 2, 3, 3\}$$

507

Dwóch graczy: Klient i Bank.

Klient ma na początku pewną sumę pieniędzy w polskiej gotówce. Zasoby Banku są nieograniczone.

W każdej fazie gry, Klient oddaje Bankowi jeden banknot lub jedną monetę.

Może żądać w zamian dowolnej kwoty, ale wypłaconej w nominałach niższych niż ten oddany Bankowi.

Przykład 1: Klient oddaje Bankowi banknot 200zł i dostaje w zamian 3 miliony setkami.

Przykład 2: Klient oddaje Bankowi monetę 1gr i... nic nie dostaje.

509

Multizbiór M jest *skończony*, jeśli zbiór $\{n \mid M(n) > 0\}$ jest skończony.

Taki multizbiór można utożsamiać z krotką liczb naturalnych, np. $\{1, 2, 2, 3, 4, 4, 4\}$ można zapisać jako $\langle 0, 1, 2, 1, 3 \rangle$.

(Zero zer, jedna jedynka, dwie dwójki, jedna trójka, trzy czwórki.)

506

Porównujemy skończone multizbiory

$$\{0, 0, 0, 0, 0, 1, 1, 1, 2\} \leq \{0, 1, 1, 2, 3, 3\} \leq \{0, 1, 3, 6\}$$

$$\{0, 0, 0, 0, 1, 2, 3, 3\} \leq \{0, 1, 1, 2, 3, 3\} \leq \{1, 2, 2, 3, 3\}$$

Zapiszmy to jako krotki liczb:

$$\langle 5, 3, 1, 0, 0, 0, 0 \rangle \leq \langle 1, 2, 1, 2, 0, 0, 0 \rangle \leq \langle 1, 1, 0, 1, 0, 0, 1 \rangle$$

$$\langle 4, 1, 1, 2 \rangle \leq \langle 1, 2, 1, 2 \rangle \leq \langle 0, 1, 2, 2 \rangle$$

Fakt: To jest dobre uporządkowanie typu ω^ω .

508

Dwóch graczy: Klient i Bank.

Klient ma na początku pewną sumę pieniędzy w polskiej gotówce. Zasoby Banku są nieograniczone.

W każdej fazie gry, Klient oddaje Bankowi jeden banknot lub jedną monetę.

Może żądać w zamian dowolnej kwoty, ale wypłaconej w nominałach niższych niż ten oddany Bankowi.

Twierdzenie: Klient zawsze zgra się do zera.

Dowód: To jest porządek dobry o liczbie ω^{15} , bo w Polsce mamy 9 monet i 6 banknotów.

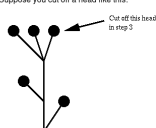
Ćwiczenie: Co się zmienia, jeśli nominały są dowolne?

510

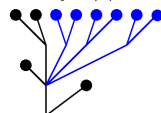
Achilles i hydra, czyli: Może być gorzej niż ω^ω

A hydra is a finite tree, with a root at the bottom. The object of the game is to cut down the hydra to its root. At each step, you can cut off one of the heads, after which the hydra grows new heads according to the following rules:

- If you cut off a head growing out of the root, the hydra does not grow any new heads.
- Suppose you cut off a head like this:



Delete the head and its neck. Descend down by 1 from the node at which the neck was attached. Look at the subtree growing from the connection through which you just discarded. Pick a natural number,



say 3, and grow that many copies of that subtree, like this:

511

Indukcja pozaskończona

512

Twierdzenie (E. Zermelo)

Każdy zbiór można dobrze uporządkować.

Dowód (szkie): Niech $A \neq \emptyset$ i niech:

$\Gamma = \{\alpha \mid \alpha \text{ jest liczbą porządkową}$
 jakiegoś podzbioru zbioru A
 dobrze uporządkowanego przez jakąś relację.}

Wtedy $\Gamma = \{\alpha \mid \alpha < \gamma\}$, gdzie $\gamma = \bar{\Gamma}$.

Niech φ będzie funkcją wyboru dla $P(A) - \{\emptyset\}$.

Definiujemy ciąg pozaskończony $\{a_\alpha\}_{\alpha < \gamma}$ elementów A :

$a_\alpha = \begin{cases} a_0, & \text{jeśli } A = \{a_\beta \mid \beta < \alpha\}; \\ \varphi(A - \{a_\beta \mid \beta < \alpha\}), & \text{w przeciwnym przypadku.} \end{cases}$

Na przykład $a_0 = \varphi(A)$, $a_\omega = \varphi(A - \{a_n \mid n \in \mathbb{N}\})$.

513

Dowód, ciąg dalszy

$\Gamma = \{\alpha \mid \alpha \text{ jest liczbą porządkową jakiegoś podzbioru } A\}$

$\Gamma = \{\alpha \mid \alpha < \gamma\}$.

Ciąg pozaskończony

$a_\alpha = \begin{cases} a_0, & \text{jeśli } A = \{a_\beta \mid \beta < \alpha\}; \\ \varphi(A - \{a_\beta \mid \beta < \alpha\}), & \text{w przeciwnym przypadku,} \end{cases}$

jest dobrze określony dla $\alpha < \gamma$. Jeśli $A = \{a_\beta \mid \beta < \alpha\}$, dla pewnego α , to A można dobrze uporządkować relacją:

$$a_\delta \leq a_\beta \Leftrightarrow \delta \leq \beta.$$

W przeciwnym razie ciąg $\{a_\alpha\}_{\alpha < \gamma}$ jest różnowartościowy, zatem zbiór $Z = \{a_\alpha \mid \alpha < \gamma\} \subseteq A$ można dobrze uporządkować w liczbę γ . A to niemożliwe, bo $\gamma \notin \Gamma$.

514

Lemat Kuratowskiego-Zorna

Niech $(Z, \leq)$ będzie zbiorem częściowo uporządkowanym, spełniającym następujący warunek:

(*) Każdy łańcuch ma w Z ograniczenie górne.

Wtedy w Z istnieje element maksymalny.

Dowód: Zbiór Z można dobrze uporządkować, tj. można przyjąć, że $Z = \{a_\alpha \mid \alpha < \gamma\}$, dla pewnego γ .

Budujemy ciąg pozaskończony $\{b_\alpha\}_{\alpha < \gamma}$, biorąc

$b_\alpha = \begin{cases} a_\alpha, & \text{jeśli } a_\alpha \text{ ogranicza z góry zbiór } \{b_\beta \mid \beta < \alpha\}; \\ a_0, & \text{w przeciwnym przypadku.} \end{cases}$

Zbiór $L = \{b_\alpha \mid \alpha < \gamma\}$ jest łańcuchem, więc ma ograniczenie górne $d \in Z$. Pokażemy, że ten element d jest maksymalny.

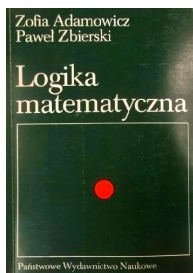
Istotnie, jeśli $d \leq a_\alpha$, dla jakiegoś $a_\alpha \in Z$, to z definicji b_α mamy $b_\alpha = a_\alpha$, czyli $a_\alpha \in L$. Stąd $a_\alpha \leq d$, a więc $a_\alpha = d$.

515

Literatura dla dociekliwych

516

Logika i teoria zbiorów



517

Logika i teoria obliczeń



518