Podstawy matematyki dla informatyków

Semestr zimowy 2023/24

Wykładowcy/koordynatorzy

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

Ogólnodostępna strona przedmiotu

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

- Skrypt: pomat.pdf
- Zadania: zadania23.pdf
- Obrazki: slajdy231.pdf

Moodle

https://moodle.mimuw.edu.pl/course/view.php?id=1862

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

Konsultacje

Wszyscy prowadzący zajęcia odbywają w ustalonych godzinach konsultacje dla studentów.

Konsultacje P. Urzyczyna: czwartki, 19:00 - 20:30, zdalnie:

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

Konsultacje J. Chrząszcza: czwartki 14:15 – 15:45, pok. 5710

Uwaga: te terminy mogą ulegać zmianom.

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.

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.

Klasówka

Klasówka będzie w czwartek 14 grudnia
(zamiast wykładu)

Zagadki-niespodzianki

W najbliższym czasie będzie udostępniony na Moodlu „quiz” sprawdzający znajomość podstawowych definicji.

Należy go rozwiązać przed poniedziałkowymi ćwiczeniami (do niedzieli, godz. 23:59).

Takich niespodzianek będzie jeszcze kilka.

Egzamin zerowy

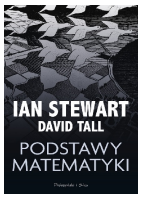
Do egzaminu zerowego (przed sesją zimową) mogą przystąpić osoby, które:

- uzyskały z kolokwium co najmniej 90% punktów,
- mają zaliczone prace domowe,
- zgłoszą gotowość do egzaminu najpóźniej 7 stycznia.

Tryb egzaminu (ustny/pisemny) zależnie od liczby chętnych.

Różne książki dla dociekliwych

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



Books in English

- 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*

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, . . .

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)

Spójniki zdaniowe

Koniunkcja: napis $\alpha \wedge \beta$ czytamy „α i β";
Alternatywa: napis $\alpha \vee \beta$ czytamy „α lub β";
Implikacja: napis $\alpha \to \beta$ 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 $\bot$, *prawdę* symbolem $\top$.

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*.

Przemienność i łączność

Wieloczłonowe 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 $p \vee (q \wedge r)$

Implikacja materialna

α	β	$\alpha \to \beta$
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 $\alpha \to \beta$ znaczy to samo, co $\neg\alpha \vee \beta$

Które z następujących zdań jest materialnie prawdziwe?

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

Kwantyfikatory

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 $W(x)$".

Kwantyfikatory ograniczone

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.

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*.

Które zmienne są tu wolne, a które związane?

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

Zasięg kwantyfikatora obejmuje tylko zielone x.

Jak to lepiej zapisać?

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

„Odpowiednie dać rzeczy – słowo" [1]

W matematyce posługujemy się językiem naturalnym.

Róbmy to w sposób precyzyjny i jednoznaczny.

I pamiętajmy o różnicach pomiędzy językami.

[1] Norwid też.

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:

$\mathit{Pierwsze}(m) \wedge \mathit{Pierwsze}(n)$.

Drugie zdanie mówi o związku między liczbami:

$\mathit{Względnie\_pierwsze}(m, n)$.

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.

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 $\exists x.\, \neg W(x)$.

Ćwiczenie

Jak brzmi zaprzeczenie zdania

Żaden pies nie goni każdego kota?

Najpierw zastanówmy się, co dokładnie mówi to zdanie.
Możemy je zapisać tak:

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

bo zwrot „żaden. . . nie" oznacza tyle, co „$\forall \ldots \neg$".
Negacją tego zdania będzie więc:

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

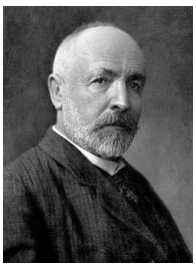
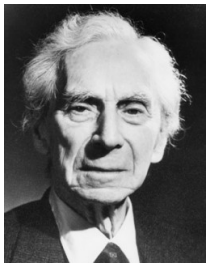
$\exists x : \mathit{Pies}.\, \forall y : \mathit{Kot}.\, \mathit{Goni}(x, y)$,

co po polsku powiemy tak:

Pewien pies goni każdego kota.

Teoria zbiorów

Georg Cantor, Bertrand Russell

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.

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

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

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 $R \in R$!

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:

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

Definiowanie zbiorów: wycinanie

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

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

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

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

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

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:
  - $\{x_1, \ldots, x_n\}$;
  - $\{x_1, x_2, x_3, \ldots\}$.

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 $y \in (-1, 2)$.

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.

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

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

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. □

Zbiór pusty oznaczamy symbolem $\varnothing$.

Zawieranie (inkluzja):

$$A \subseteq B \qquad \Leftrightarrow \qquad \forall z(z \in A \to z \in B).$$

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

Notacja:

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

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

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

Zbiór potęgowy:

Elementami zbioru $\mathrm{P}(A)$ są wszystkie podzbiory zbioru A

$$X \in \mathrm{P}(A) \qquad \Leftrightarrow \qquad X \subseteq A$$

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

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

Przykład: $\mathrm{P}(\{0, 1\}) = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}$
$\mathrm{P}(\varnothing) = \{\varnothing\}$, $\mathrm{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$.

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 $\mathcal{D} - A$).

Złote myśli

$$
\begin{aligned}
x \in A \cup B &\quad\Leftrightarrow\quad x \in A \vee x \in B \\
x \in A \cap B &\quad\Leftrightarrow\quad x \in A \wedge x \in B \\
x \in A - B &\quad\Leftrightarrow\quad x \in A \wedge x \notin B \\
x \in -A &\quad\Leftrightarrow\quad x \notin A
\end{aligned}
$$

Złote myśli

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

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 $\mathcal{R}$:

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

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

Złote myśli:

$$
\begin{aligned}
x \in \bigcup \mathcal{R} &\quad\Leftrightarrow\quad \exists A(A \in \mathcal{R} \wedge x \in A). \\
x \in \bigcap \mathcal{R} &\quad\Leftrightarrow\quad \forall A(A \in \mathcal{R} \to x \in A).
\end{aligned}
$$

Ćwiczenie (prawo De Morgana)

- Dla dowolnych A, B zachodzi równość:
  $$-(A \cup B) = -A \cap -B.$$

  Dowód: Bo *dla dowolnego* x mamy równoważność:
  $$x \notin A \cup B \quad\leftrightarrow\quad x \notin A \wedge x \notin B,$$
  czyli
  $$\forall x\,(x \in -(A \cup B) \;\leftrightarrow\; x \in -A \cap -B).$$

- Dla dowolnych A i B zachodzi równość:
  $$-(A \cap B) = -A \cup -B.$$

Nie zawsze jest tak łatwo

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

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

Nie zawsze jest tak łatwo

Jak udowodnić, że $A \subseteq B$?

Najpierw trzeba zapytać: co to znaczy?

Odpowiedź: $A \subseteq B$ znaczy, że $\forall x(x \in A \to x \in B)$.
„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 wiecej o nim nie wiadomo).

„Rozpatrzmy dowolne $x \in A$. Wtedy ....
... ... Zatem $x \in B$."

Ćwiczenie:

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

Załóżmy, 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 $\forall x(x \in A - B \to x \in C - B)$,
czyli $A - B \subseteq C - B$. *(Cel 1 osiągnięty)*
Zatem jeśli $A \cup B \subseteq C$, to $A - B \subseteq C - B$.

Ćwiczenie:

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

Załóżmy, 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 $\forall x(x \in A - B \to x \in C - B)$, czyli $A - B \subseteq C - B$. *(Cel 1 osiągnięty)*

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

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

Załóżmy, że $A - B = \varnothing$. *(Cel 1: $A \subseteq B$)*
- Rozpatrzmy dowolne $x \in A$. *(Cel 2: $x \in B$)*
- Załóżmy, że $x \notin B$. *(Cel 3: sprzeczność)*
- Skoro $x \in A$ i $x \notin B$, to $x \in A - B$.
- Ale $A - B = \varnothing$, więc $x \in \varnothing$, sprzeczność. *(Cel 3 osiągnięty)*
- Zatem $x \in B$. *(Cel 2 osiągnięty)*

Zatem $\forall x(x \in A \to x \in B)$, czyli $A \subseteq B$. *(Cel 1 osiągnięty)*

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

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

Załóżmy, że $A - B = \varnothing$. *(Cel 1: $A \subseteq B$)*
- Rozpatrzmy dowolne $x \in A$. *(Cel 2: $x \in B$)*
  - Załóżmy, że $x \notin B$. *(Cel 3: sprzeczność)*
  - Skoro $x \in A$ i $x \notin B$, to $x \in A - B$.
  - Ale $A - B = \varnothing$, więc $x \in \varnothing$, sprzeczność. *(Cel 3 osiągnięty)*
- Zatem $x \in B$. *(Cel 2 osiągnięty)*

Zatem $\forall x(x \in A \to x \in B)$, czyli $A \subseteq B$. *(Cel 1 osiągnięty)*

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

To samo, krócej:
Niech $A - B = \varnothing$ oraz $x \in A$. Gdyby $x \notin B$, to $x \in A - B = \varnothing$, sprzeczność. Zatem $x \in B$.

Wnioskowanie przez zaprzeczenie

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

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

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

$$(\neg p \to \bot) \to p.$$

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

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

Załóżmy, 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 $\forall x(x \in A \to x \in B \cup C)$. *(Cel 1 osiągnięty)*

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

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:

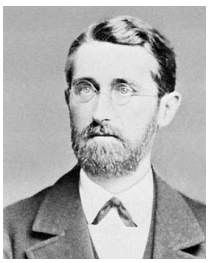
$$(p \vee q) \wedge (p \to r) \wedge (q \to r) \to r.$$

Najczęściej stosujemy go tak:

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

Liczby naturalne

Giuseppe Peano, Richard Dedekind



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.

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. Jeśli $s(n) = s(m)$, to $n = m$.
  4. Zawsze $s(n) \neq 0$.
  5. Jeśli $W(0)$ oraz $\forall n{:}\mathbb{N}(W(n) \to W(s(n)))$, to $\forall n{:}\mathbb{N}.\, W(n)$.

Wnioskowanie przez indukcję

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

Należy udowodnić, że:

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

Przykład dowodu przez indukcję

Twierdzenie: $\forall n : \mathbb{N}.\, s(n) \neq n$.

Dowód: Stosujemy schemat indukcji do warunku

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

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

(1) Krok bazowy $s(0) \neq 0$ wynika z aksjomatu $\forall m.\, s(m) \neq 0$.

(2) Krok indukcyjny: $\forall n : \mathbb{N}\,(s(n) \neq n \to s(s(n)) \neq s(n))$.

Rozpatrzmy dowolne $n \in \mathbb{N}$ i załóżmy, 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 $s(s(n)) \neq s(n)$.

Wnioskowanie przez indukcję

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

Należy udowodnić, że:

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

Wnioskowanie przez indukcję:
Cel: $\forall n{:}\mathbb{N}\, W(n)$

⋮
Zatem $W(0)$. *(Krok bazowy wykonany)*

Niech $n \in \mathbb{N}$ *(Cel 1:* $W(n) \to W(s(n))$*)*

Załóżmy, że $W(n)$. *(Cel 2:* $W(s(n))$*)*

⋮
Zatem $W(s(n))$. *(Cel 2 osiągnięty)*

Zatem $W(n) \to W(s(n))$. *(Cel 1 osiągnięty)*

Zatem $\forall n{:}\mathbb{N}(W(n) \to W(s(n)))$. *(Krok indukcyjny wykonany)*

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

Definiowanie przez indukcję: przykład

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

$$\overline{0} = \varnothing \qquad \overline{s(n)} = \overline{n} \cup \{n\}.$$

Co jest sumą wszystkich takich odcinków?

Coś takiego: $\overline{0} \cup \overline{1} \cup \overline{2} \ldots$?

Lepiej tak to napisać: $\bigcup_{n\in\mathbb{N}} \overline{n}$. Albo tak: $\bigcup\{\overline{n} \mid n \in \mathbb{N}\}$.

Teraz widać po co nam potrzebne sumy uogólnione.

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 $\mathcal{R}$:

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

Na przykład jeśli $\overline{0} = \varnothing$ oraz $\overline{s(n)} = \overline{n} \cup \{n\}$, to:

$$\bigcup\{\overline{n} \mid n \in \mathbb{N}\} = \bigcup_{n\in\mathbb{N}} \overline{n} = \mathbb{N}$$
$$\bigcap\{\overline{n} \mid n \in \mathbb{N}\} = \bigcap_{n\in\mathbb{N}} \overline{n} = \varnothing.$$

Dlaczego?

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 $\mathcal{R}$:

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

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

$$\bigcup\{A_t \mid t \in \mathbb{R}\} = \mathbb{R}^2 = \bigcup_{t\in\mathbb{R}} A_t$$
$$\bigcap\{A_t \mid t \in \mathbb{R}\} = \{\langle 0, 0\rangle\} = \bigcap_{t\in\mathbb{R}} A_t.$$

Dlaczego?

Złote myśli:

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

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

Łatwe ćwiczenia

- Jeśli $A \in \mathcal{R}$, to $\bigcap \mathcal{R} \subseteq A \subseteq \bigcup \mathcal{R}$.
- Jeśli $\mathcal{R} \neq \varnothing$, to $\bigcap \mathcal{R} \subseteq \bigcup \mathcal{R}$.
- Jeśli $\mathcal{R} = \varnothing$, to $\bigcup \mathcal{R} = \varnothing$.
- Jeśli $\varnothing \in \mathcal{R}$, to $\bigcap \mathcal{R} = \varnothing$.

Dygresja: fałszywi przyjaciele

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

  $\exists A \in \mathcal{R}.\, x \in A$, albo tak: $\exists A(A \in \mathcal{R} \wedge x \in A)$.
- Stwierdzenie „dla każdego $A \in \mathcal{R}$ zachodzi $x \in A$” zapisujemy tak:

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

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

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

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

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

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

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

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

Zatem $a \in \bigcup \mathrm{P}(A)$.

Jak używamy założenia egzystencjalnego?

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

Ustalmy więc takie $\alpha \in \mathrm{P}(A)$*, 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 $\alpha \in \mathrm{P}(A)$ oraz $a \in \alpha$.

Częsty błąd: „*nie to samo* x”

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

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

Skoro $B \neq \varnothing$, 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.

Częsty błąd: „*nie to samo* x”

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

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

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

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

Para uporządkowana

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

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

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

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 $x\, r\, y$.

Ćwiczenie

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

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

Niech $a \in A$. Ponieważ $B \neq \varnothing$, 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 $B = \varnothing$, to $A \times B = \varnothing$ dla każdego A.
Wtedy np. $\{1, 2\} \times \varnothing = \varnothing \subseteq \{3, 4\} \times \{5\}$, chociaż
$\{1, 2\} \not\subseteq \{3, 4\}$.

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!

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

Funkcje

Definiowanie funkcji

Definicja wprost:

$$f(x) = x + y \qquad \lambda x.\, x + y$$

Definicja warunkowa:

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

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

Definiowanie funkcji

Definicja implicite:

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

Napis $\imath x.\, W(x)$ czytamy: „jedyne x o własności $W(x)$"

Definicja indukcyjna: $f(0) = 0, \quad f(s(n)) = s(s(f(n)))$.

Ćwiczenie: Co to za funkcja? A jak to udowodnić?
Przez indukcję!

Funkcje całkowite i częściowe

Napis $f : A \to B$ 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 $A \to B$.

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

Dziedzina funkcji:

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

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

Funkcje

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

Przy tej definicji przeciwdziedzina zależy od kontekstu.

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

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

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

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

Równość funkcji

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

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

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

Wykres funkcji:

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

Funkcje o tym samym wykresie są równe.

Ćwiczenie

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

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

Własności funkcji

$f : A \to B$

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

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

Przykłady

Funkcja identycznościowa $\mathrm{id}_A : A \to A$ jest bijekcją.

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

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

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

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

Niech $in_1 : A \to A \oplus B$ i $in_2 : B \to A \oplus B$ będą okreslone tak:

$$in_1(a) = \langle a\rangle_1, \qquad in_2(b) = \langle b\rangle_2$$

Te funkcje (*włożenia*) są różnowartościowe.

Ćwiczenie

Niech $f : \mathrm{P}(\mathbb{N}) \times \mathrm{P}(\mathbb{N}) \to \mathrm{P}(\mathbb{N})$ *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

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

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

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

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

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.*

Operacje na funkcjach

Obcięcie

Obcięcie funkcji $f : A \to B$ do podzbioru $C \subseteq A$,
to taka funkcja $f\restriction_C : C \to B$, że $f\restriction_C(a) = f(a)$ dla $a \in C$.

Wtedy $\mathrm{Dom}(f\restriction_C) = C$.

Funkcja odwrotna

Funkcja odwrotna do $f : A \xrightarrow[\text{na}]{1-1} B$ to funkcja $f^{-1} : B \rightarrowtail\!\!\!\!\circ\; A$

$$f^{-1}(y) = \imath x \in A.\, f(x) = y.$$

Jest określona tylko dla funkcji różnowartościowej. Wtedy:

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

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

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

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

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

Ostatecznie:

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

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

Wniosek:

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

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

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

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

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

Złożenie funkcji

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

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

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

Własności operacji składania

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

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

Fakt

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

Własności operacji składania

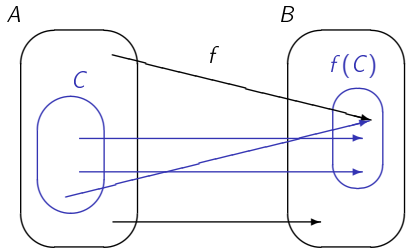
Niech $f : A \to B$ oraz $g : B \to C$. *Złożeniem funkcji f i g*
nazywamy funkcję $g \circ f : A \to C$ określoną równaniem

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

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 $g \circ f : A \xrightarrow{\text{na}} C$.*

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



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

Obraz

Niech $f : A \rightarrowtail\!\!\!\!\circ\; B$. *Obraz* zbioru $C \subseteq A$ przy przekształceniu f to zbiór

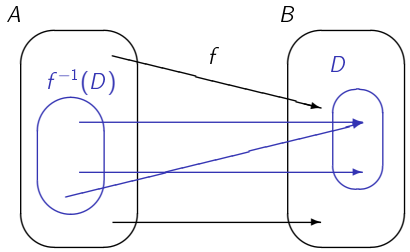
$$f(C) = \{b \in B \mid \exists a \in \mathrm{Dom}(f)\,(a \in C \wedge f(a) = b)\}.$$

W skrócie:

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

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

Przeciwobraz zbioru $D \subseteq B$ przy przekształceniu $f : A \to B$



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

Przeciwobraz

Przeciwobraz zbioru $D \subseteq B$ przy $f : A \rightarrowtail\!\!\!\!\circ\; B$ to zbiór:

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

Dla funkcji całkowitej to po prostu:

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

Ćwiczenie

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

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

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

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

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

Ćwiczenie

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

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

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

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

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

Istotnie:

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

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

Funkcje wieloargumentowe

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

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

Na przykład dodawanie liczb naturalnych to funkcja typu

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

No zaraz, ale co to w ogóle jest dodawanie?

Czy dodawanie można zdefiniować
z pomocą samej operacji następnika?

Można.
Jak?
Przez indukcję!

Definiowanie funkcji przez indukcję

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

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

Mnożenie:

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

Dwa razy dwa

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

$2 \cdot 2 = 1 \cdot 2 + 2 = (0 \cdot 2 + 2) + 2 =$
$(0 + 2) + 2 = 2 + 2 = s(1 + 2) =$
$s(s(0 + 2)) = s(s(2)) = s(s(s(s(0)))) = 4.$

Schemat definiowania przez indukcję

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

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

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...

Dowodzenie przez indukcję

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

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, ze 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
$s(m) + (k + l) = s(m + (k + l)) = s((m + k) + l) =$
$s(m + k) + l = (s(m) + k) + l$ i dobrze. □

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 $n + 0 = n$.

Przykład

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

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

To też szczególny przypadek schematu

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

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

Ćwiczenie:

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

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).

Własności nierówności

Trzy łatwe ćwiczenia:

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

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

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

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

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

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

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

Własności relacji nierówności

- *Zwrotność:* $\forall n \in \mathbb{N}.\, n \leq n$.
- *Przechodniość:* $\forall nmk \in \mathbb{N}.\, n \leq m \wedge m \leq k \to n \leq k$.
- *Antysymetria:* $\forall nm \in \mathbb{N}.\, n \leq m \wedge m \leq n \to n = m$.
- *Spójność:* $\forall nm \in \mathbb{N}.\, n \leq m \vee m \leq n$.

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

Własności relacji nierówności

- *Zwrotność:* $\forall n \in \mathbb{N}.\, n \leq n$.
- *Przechodniość:* $\forall nmk \in \mathbb{N}.\, n \leq m \wedge m \leq k \to n \leq k$.
- *Antysymetria:* $\forall nm \in \mathbb{N}.\, n \leq m \wedge m \leq n \to n = m$.
- *Spójność:* $\forall nm \in \mathbb{N}.\, n \leq m \vee m \leq n$.

Dowody opuszczamy z braku czasu.

Wróćmy do funkcji

Ćwiczenie

Ćwiczenie: *Niech* $\varphi : \mathrm{P}(A \times B) \to \mathrm{P}(A)^B$, *gdzie:*

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

dla dowolnego $\Delta \in \mathrm{P}(A \times B)$ *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 $b = y$.

Ćwiczenie: *Niech* $\varphi : \mathrm{P}(A \times B) \to \mathrm{P}(A)^B$, *gdzie:*

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

dla dowolnego $\Delta \in \mathrm{P}(A \times B)$ *i dowolnego* $b \in B$.
Pokazać, że ta funkcja jest na $\mathrm{P}(A)^B$.

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

Rozpatrzmy więc dowolną funkcję $F : B \to \mathrm{P}(A)$.
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: $\langle a, b\rangle \in \Delta \quad \Leftrightarrow \quad a \in F(b)$.

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

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

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 $\overline{\overline{A}} = \overline{\overline{B}}$.

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

Zbiory $\mathrm{P}(A \times B)$ i $\mathrm{P}(A)^B$ są równoliczne.

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 $A \sim \varnothing$, to $A = \varnothing$.

Zbiory skończone

Zbiory skończone

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

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

Pytanie: Czy tylko z jednym takim?

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 $B \neq \varnothing$, surjekcja $f : A \cup \{a\} \xrightarrow{\text{na}} B \cup \{b\}$ istnieje wtedy i tylko wtedy, gdy istnieje surjekcja $g : A \xrightarrow{\text{na}} B$.
- $A \cup \{a\} \sim B \cup \{b\}$ wtedy i tylko wtedy, gdy $A \sim B$.

Fakt

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

Dowód jest przez indukcję ze względu na m.

Szczegóły opuszczamy.

Fakt

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

Wniosek

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

Wniosek

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

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

Mówimy, ze zbiór A jest *n-elementowy* i piszemy $\overline{\overline{A}} = n$.

Fakt

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

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 $\{0, 1, \ldots, 13\}$ *wybierzemy* 8 *różnych liczb, to dwie z nich różnią się o* 7.

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

Fakt

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

Wniosek

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

Wniosek

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

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

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 $A - B \neq \varnothing$.
- Jeśli A jest skończony i $f : B \xrightarrow{1-1} A$, to B jest skończony.
- Jeśli A jest skończony i $f : A \xrightarrow{\text{na}} B$, 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 $A \sim \overline{n}$ 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 $B \sim \mathrm{Rg}(f) \subseteq A$.
Bo wtedy istnieje $g : B \xrightarrow{1-1} A$.
Indukcja (ćwiczenie).

Jeszcze o zbiorach skończonych

Twierdzenie
Jeśli A jest skończony, oraz $f : A \to A$, 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 $f : A \to A$, jeśli $\overline{\overline{A}} = n$, to:
f *jest różnowartościowa* $\Rightarrow$ f *jest na* A.

Jeśli $A = \varnothing$, 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 $f\restriction_{A'} : A' \to A$ jest różnowartościowa. . . ale to nie jest funkcja z A' do A' i założenie indukcyjne nie pasuje!
Co robić? Wzmocnić tezę!

Udowodnimy silniejsze twierdzenie.

Twierdzenie
Jeśli zbiory skończone A i B są równoliczne oraz $f : A \to B$, to:
f *jest różnowartościowa* $\Leftrightarrow$ f *jest na* B.

Wniosek
Jeśli A jest skończony oraz $f : A \to A$, to:
f *jest różnowartościowa* $\Leftrightarrow$ f *jest na* A.

Twierdzenie
Jeśli zbiory skończone A i B są równoliczne oraz $f : A \to B$, to:
f *jest różnowartościowa* $\Leftrightarrow$ f *jest na* B.

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

Jeśli $A = \varnothing$, 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 $\overline{\overline{B'}} = n$.

Funkcja $f\restriction_{A'} : A' \to B'$ jest różnowartościowa i z założenia indukcyjnego jest na B'.

Zatem „cała" funkcja f jest na B.

Twierdzenie
Jeśli zbiory skończone A i B są równoliczne oraz $f : A \to B$, to:
f *jest różnowartościowa* $\Leftrightarrow$ f *jest na* B.

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

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

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

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

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

Zatem funkcja f jest też różnowartościowa.

Zbiory nieskończone

Motywujący przykład:

Niech

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

Zbiory P i N są równoliczne, bo mamy funkcję

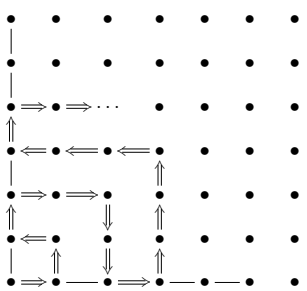
$$\lambda n.\, n + 1 : P \xrightarrow[\text{na}]{1-1} N.$$

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

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

Zatem „połowa" może być równoliczna z całością.

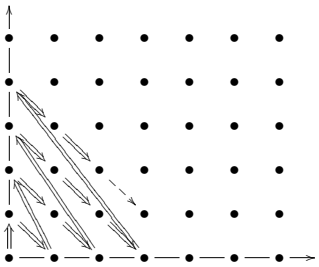
Przykład: Zbiory $\mathbb{N} \times \mathbb{N}$ i $\mathbb{N}$ są równoliczne.



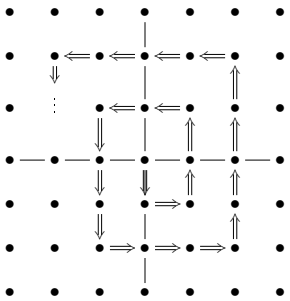
Funkcje pary z $\mathbb{N} \times \mathbb{N}$ do $\mathbb{N}$

- $t(m,n) = 2^m 3^n$ (różnowartościowa)
- $\overline{u}(m,n) = 2^m(2n+1)$ (różnowartościowa)
- $u(m,n) = 2^m(2n+1) - 1$ (bijekcja)
- $v(m,n) = \frac{(m+n)(m+n+1)}{2} + m$ (bijekcja)

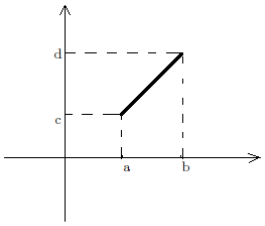
Przykład: $v(m,n) = \frac{(m+n)(m+n+1)}{2} + m$



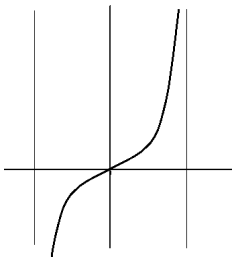
Przykład: Zbiory $\mathbb{Z} \times \mathbb{Z}$ i $\mathbb{N}$ są równoliczne.



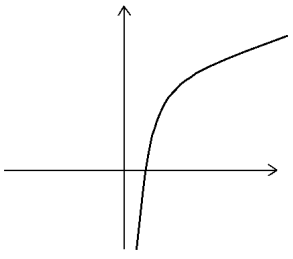
Przykład: Przedziały otwarte (a,b) i (c,d) są równoliczne, bo jeśli $f(x) = \frac{d-c}{b-a} \cdot x + \frac{bc-ad}{b-a}$, to $f : (a,b) \xrightarrow[\text{na}]{1-1} (c,d)$.



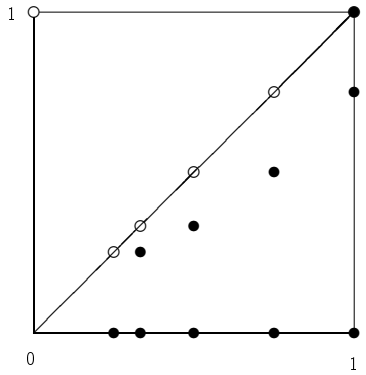
Przykład: Przedział $(-\frac{\pi}{2}, \frac{\pi}{2})$ (i każdy inny przedział otwarty) jest równoliczny z $\mathbb{R}$ (funkcja tangens).



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



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



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

Proste obserwacje

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

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

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

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

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

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

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

Stąd $\mathrm{P}(\mathbb{N}) \sim \mathrm{P}(N) \times \mathrm{P}(P) \sim \mathrm{P}(\mathbb{N}) \times \mathrm{P}(\mathbb{N})$.

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

Dowód: Bijekcja $F : \mathrm{P}(\mathbb{N}) \xrightarrow[\text{na}]{1-1} (\mathbb{N} \to \{0,1\})$ 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.

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:*

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

Ale ciągu $1010\ldots$ *na pewno tutaj nie ma.* □

Nie wszystkie zbiory nieskończone są równoliczne

Twierdzenie: *Zbiór $\mathrm{P}(\mathbb{N})$ 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	=	$\{1,2,5,7,9,10,12,\ldots\}$	$0110010101101\ldots$
A_1	=	$\{1,3,9,12,\ldots\}$	$0101000001001\ldots$
A_2	=	$\{0,5,6,7,9,\ldots\}$	$1000011101000\ldots$
A_3	=	$\{0,1,3,5,7,8,12,\ldots\}$	$1101010110001\ldots$

Jakiego zbioru brak? $B = \{0,2,\ldots\}$ $\quad \chi_B = 1010\ldots$

$$n \in B \quad \Leftrightarrow \quad n \notin A_n,$$

□

Nieprzeliczalność

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

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

Uogólnienie:

Twierdzenie (Cantora)
Dla dowolnego zbioru A zachodzi $\overline{\overline{A}} \neq \overline{\overline{\mathrm{P}(A)}}$.

Dowód: Przypuśćmy, że $F : A \xrightarrow[\text{na}]{1-1} \mathrm{P}(A)$. 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. □

Paradoks fryzjera

Fryzjerowi polecono golić tych, którzy się sami nie golą.

$$F : A \to \mathrm{P}(A)$$
$$F(x) = \{y \mid x \text{ goli } y\}$$

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

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

Liczby kardynalne

Umowa: Zbiorom przypisujemy *liczby kardynalne*.
Liczbę kardynalna (*moc*) zbioru A oznaczamy przez $\overline{\overline{A}}$.
Robimy to tak, aby zachodziła równoważność:

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

- 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 wynika, że $\overline{\overline{\mathrm{P}(\mathbb{N})}} \neq \aleph_0$.
Pokażemy później, że $\overline{\overline{\mathrm{P}(\mathbb{N})}} = \mathfrak{c}$.

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

Uwaga: nie wszystkie zbiory nieprzeliczalne są równoliczne!

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 $g : \mathbb{N} \xrightarrow{\text{na}} A$.

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 $\mathbb{N} \times \mathbb{N}$ i $P \cup N$ są przeliczalne. Trzeba wszystko ponumerować.) □

Twierdzenie

Suma przeliczalnej rodziny zbiorów przeliczalnych jest przeliczalna.

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

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

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

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 $f : \mathbb{N} \times \mathbb{N} \xrightarrow{\text{na}} \mathbb{Z}$, gdzie $f\langle m, n\rangle = m - n$.
Bo $f : \mathbb{Z} \times (\mathbb{Z} - \{0\}) \xrightarrow{\text{na}} \mathbb{Q}$, gdzie $f\langle m, n\rangle = \frac{m}{n}$.
Bo to po prostu $\mathbb{Q} \times \mathbb{Q}$.
Bo to w istocie przeliczalna suma $\bigcup\{\mathbb{N}^k \mid k \in \mathbb{N}\}$.

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. □

Nierówności

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

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

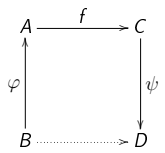
Przykład: $\overline{\overline{\mathbb{N}}} < \overline{\overline{\mathrm{P}(\mathbb{N})}}$.

Poprawność definicji $\leq$

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

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

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



Nierówności

- Jeśli $A \subseteq B$, to $\overline{\overline{A}} \leq \overline{\overline{B}}$.
- Dla dowolnej liczby naturalnej n zachodzi $n < \aleph_0$.
- Dla dowolnego zbioru A zachodzi $\overline{\overline{A}} < \overline{\overline{\mathrm{P}(A)}}$.
  Istotnie, z jednej strony $\lambda a.\, \{a\} : A \xrightarrow{1-1} \mathrm{P}(A)$, a z drugiej strony mamy twierdzenie Cantora.

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

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

Te elementy tworzą zbiór mocy $\aleph_0$.

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 $f : \mathbb{N} \xrightarrow[\text{na}]{1-1} B$.

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 $f(0) \notin \mathrm{Rg}(g)$.
Zatem $A \sim \mathrm{Rg}(g) \subsetneq A$. □

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. □

Nierówności

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

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

Nierówności

Fakt
Dla dowolnych zbiorów A, B, C:

- $\overline{\overline{A}} \leq \overline{\overline{A}}$;
- *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 $\overline{\overline{A}} = \overline{\overline{B}}$?

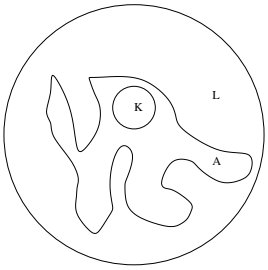
Twierdzenie (Cantora-Bernsteina)
Jeśli $\overline{\overline{A}} \leq \overline{\overline{B}}$ *i* $\overline{\overline{B}} \leq \overline{\overline{A}}$ *to* $\overline{\overline{A}} = \overline{\overline{B}}$.

Inaczej:

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

Przykład

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



Przykład

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

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

Dowód twierdzenia Cantora-Bernsteina

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

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

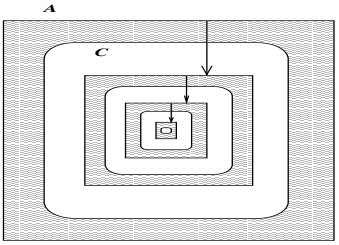
Niech $C = \mathrm{Rg}(g)$. Wtedy $B \sim C$, oraz $g \circ f : A \xrightarrow{1-1} C$.

Wystarczy więc udowodnić:

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

Dowód twierdzenia Cantora-Bernsteina

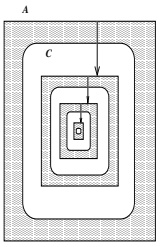
Lemat: Jeśli $\varphi : A \xrightarrow{1-1} C \subseteq A$ to $C \sim A$.



Pomysł: użyć φ tylko w cześciach zakreskowanych.

Dowód twierdzenia Cantora-Bernsteina

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



$X_0 = A - C$
$X_1 = \varphi(X_0)$
...
$X_{n+1} = \varphi(X_n)$
...

$\psi : A \xrightarrow[\text{na}]{1-1} C$

$$\psi(x) = \begin{cases} \varphi(x), & \text{jeśli } x \in \bigcup_{n\in\mathbb{N}} X_n; \\ x, & \text{w przeciwnym przypadku.} \end{cases}$$

Moc continuum

Definicja

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

Twierdzenie

$$\mathfrak{c} = \overline{\overline{\mathrm{P}(\mathbb{N})}} = \overline{\overline{\{0,1\}^{\mathbb{N}}}} = \overline{\overline{\mathbb{N} \to \{0,1\}}}.$$

Dowód: Część łatwa już była.

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

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

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

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

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 $H(f)$.

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

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

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

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!

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

Dowód:

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

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

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

Działania na liczbach kardynalnych

Arytmetyka liczb kardynalnych

Niech $\mathfrak{m}$, $\mathfrak{n}$ to liczby kardynalne.

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

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

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

(Dla liczb naturalnych wychodzi to, co zwykle.)

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 $\mathrm{P}(\mathbb{N}) \sim \mathbb{R}$.

Fakt
Jeśli $\mathfrak{m} \geq \aleph_0$ *to* $\mathfrak{m} + \aleph_0 = \mathfrak{m}$.

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

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

Dodawanie i mnożenie:

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

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

Potęgowanie:

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

Bo tylko funkcja pusta należy do $A^{\varnothing}$.
Bo elementy $A^{\{0\}}$ to funkcje stałe.
Bo tylko $\lambda x.\, c$ należy do $\{c\}^A$.
Bo nie ma funkcji ze zbioru niepustego do $\varnothing$.
Bo $A^B \times A^C \sim A^{B \oplus C}$.
Bo $A^B \times C^B \sim (A \times C)^B$.
Bo $(A^B)^C \sim A^{B \times C}$.

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 $p \neq 0$).

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 $(\mathbb{N} \to \mathbb{N}) \sim (\mathbb{N} \to \mathbb{R}) \sim \mathbb{R}$.
- $2^{\mathfrak{c}} = \aleph_0^{\mathfrak{c}} = \mathfrak{c}^{\mathfrak{c}}$. A więc $(\mathbb{R} \to \mathbb{N}) \sim (\mathbb{R} \to \mathbb{R})$.

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

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.

Alefy i bety

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

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

Ostrzeżenie

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

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

Relacje

(dwuargumentowe)

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 $x\, r\, y$.

Operacje na relacjach

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 $\leq^{-1} = \geq$.

Operacje na relacjach

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

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

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

Przykład:
Jeśli znaki $\|$ i $\perp$ oznaczają odpowiednio równoległość i prostopadłość prostych na płaszczyźnie, to $\| \cdot \perp = \perp$.
A co to jest $\perp \cdot \perp$?

Operacje na relacjach

Relacja identycznościowa w A to relacja

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

Uwaga: $a\,\mathbf{1}_A\,b$ wtedy i tylko wtedy, gdy $a = b$.

Własności operacji składania

- $r \cdot (s \cdot p) = (r \cdot s) \cdot p$;
- $r \cdot (s \cup p) = r \cdot s \ \cup \ r \cdot p$;
- $(s \cup p) \cdot r = s \cdot r \ \cup \ p \cdot r$;
- $r \cdot \mathbf{1}_B = \mathbf{1}_A \cdot r = r$, gdy $r \subseteq A \times B$;
- Jeśli $r \subseteq r'$ i $s \subseteq s'$, to $r \cdot s \subseteq r' \cdot s'$.

Relacje przechodnie

Relacja r w A jest *przechodnia*, gdy

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

Przykłady:

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

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

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 $\forall x\,y\,z.\,(x\,r\,y \wedge y\,r\,z \to x\,r\,z)$.*

Przypuśćmy, że $x\,r\,y$ i $y\,r\,z$.
Wtedy $x\,(r \cdot r)\,z$.
A ponieważ $r \cdot r \subseteq r$, więc $x\,r\,z$.

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

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:

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

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

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 $A \times A \in \mathcal{R}$.

$r^+ = \bigcap \mathcal{R}$, *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 $\langle x, y\rangle \in \bigcap \mathcal{R} = r^+$.

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

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

$r^+ = \bigcap \mathcal{R}$, *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).

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.

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: Zacznijmy 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 $r^+ \subseteq r_\omega$.

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

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

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 $\mathbf{1}_A \subseteq r$.)

Przykłady: $\mathbf{1}_A$, $\leq$, równoległość prostych.

Domknięcie przechodnio-zwrotne

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

$$r^* = \mathbf{1}_A \cup r^+.$$

Ćwiczenie: Sprawdzić, że to faktycznie ta relacja.

Przykłady

Niech $\to$ oznacza relację sąsiedztwa wierzchołków w pewnym grafie. Wtedy relacja $\to^*$ (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.

Własności relacji

Relacja r w A jest

zwrotna (*w* A),	gdy	$\forall x{\in}A\,(x\,r\,x)$;
symetryczna,	gdy	$\forall x, y{\in}A\,(x\,r\,y \to y\,r\,x)$;
przechodnia,	gdy	$\forall x, y, z{\in}A\,(x\,r\,y \wedge y\,r\,z \to x\,r\,z)$;
antysymetryczna,	gdy	$\forall x, y{\in}A\,(x\,r\,y \wedge y\,r\,x \to x = y)$;
spójna (*w* A),	gdy	$\forall x, y{\in}A\,(x\,r\,y \vee y\,r\,x)$.

Relacje równoważności

Przykład: równoległość prostych

Jakie własności ma ta relacja?

Jest zwrotna, symetryczna i przechodnia.

Relacje równoważności

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

- $\forall x{\in}A\,(x\,r\,x)$;
- $\forall x, y{\in}A\,(x\,r\,y \to y\,r\,x)$;
- $\forall x, y, z{\in}A(x\,r\,y \wedge y\,r\,z \to x\,r\,z)$.

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

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

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

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

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

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 odległości 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.

Jądro

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

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

Jądro jest zawsze relacją równoważności.

Przykład: Relacja

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

jest jądrem przekształcenia

$$\lambda f.\, f\restriction_{\{x \mid x \bmod 3 = 0\}}$$

a zatem jest relacją równoważności.

Czy to jest ten sam tramwaj?

Zbiór (typ) ilorazowy

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

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

Klasy abstrakcji

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

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

Przykład: $x \equiv_3 y$ wtedy i tylko wtedy, gdy

$$x \bmod 3 = y \bmod 3.$$

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

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) $[x]_r \cap [y]_r \neq \varnothing$;

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.

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) $[x]_r \cap [y]_r \neq \varnothing$;

Dowód (e) $\Rightarrow$ (a):

Skoro $[x]_r \cap [y]_r \neq \varnothing$, 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 przechodniości $v\, r\, y$, czyli $v \in [y]_r$.
Pokazaliśmy, że $[x]_r \subseteq [y]_r$.

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

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) $[x]_r \cap [y]_r \neq \varnothing$.

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

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

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

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

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.

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 $\{\langle 0,0\rangle\}$.

Te zbiory są rozłączne i pokrywają całą płaszczyznę.

Zasada abstrakcji

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

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

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 $P = A/_r$.

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.

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.

Przechodniość: 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 $p \cap q \neq \varnothing$, więc $p = q$. Skoro więc $x \in p$ i $z \in q = p$, to $x\,r\,z$.

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 $t \in [x]_r$.

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 $p \neq \varnothing$, 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.

Zasada abstrakcji

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

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

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 $P = A/_r$.

Jeszcze kilka przykładów

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

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

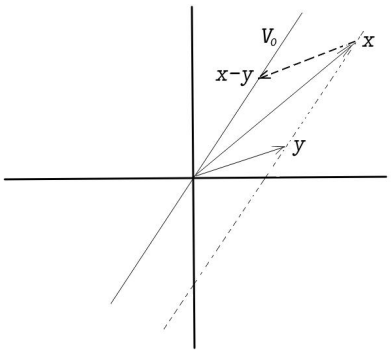
jest relacją równoważności.

Jej klasy abstrakcji nazywamy *warstwami* podprzestrzeni V_0.

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

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

Podprzestrzeń i warstwa



Każda relacja równoważności jest jądrem

$x \; r \; y$ wtedy i tylko wtedy, gdy $[x]_r = [y]_r$

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

Niech $\mathbb{P}\mathrm{r}$ oznacza zbiór wszystkich liczb parzystych

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

- $f \; r \; g$ wtedy i tylko wtedy, gdy $\forall x : \mathbb{N}.\, |f(x) - g(x)| \in \mathbb{P}\mathrm{r}$;
- $f \; s \; g$ wtedy i tylko wtedy, gdy $\forall x \in \mathbb{P}\mathrm{r}.\, f(x) = g(x)$.

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 $\lambda f.\, f|_{\mathbb{P}\mathrm{r}}$.

Jakie są klasy abstrakcji? Czy jest ich skończenie wiele?

Porządki

Relacje porządkujące

Relacja częściowego porządku to relacja zwrotna, antysymetryczna i przechodnia.

Relacja liniowego porządku to spójny częściowy porządek.

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 $\mathrm{P}(A)$.
- Porządek *leksykograficzny* w zbiorze $\mathbb{N} \times \mathbb{N}$:

  $\langle x, y\rangle \leq \langle x', y'\rangle \quad \Leftrightarrow \quad x < x' \vee (x = x' \wedge y \leq y')$

  jest porządkiem liniowym.

Przykład

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

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

$\mathrm{Dom}(f) \subseteq \mathrm{Dom}(g) \wedge \forall a\, (a \in \mathrm{Dom}(f) \to f(a) = g(a))$.

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.

Przykłady

- W porządku $\langle \mathbb{N}, \mid \rangle$ 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 $\langle \mathrm{P}(\mathbb{N}), \subseteq \rangle$.
- Rodzina $\{(-x, 0) \mid x > 0\}$ jest łańcuchem w $\mathrm{P}(\mathbb{R})$.
- Rodzina $\{(x, \infty) \mid x > 0\}$ też.

Definicje

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

największy,	gdy	$\forall x \in A\,(x \leq a)$;
maksymalny,	gdy	$\forall x \in A\,(a \leq x \to a = x)$;
najmniejszy,	gdy	$\forall x \in A\,(a \leq x)$;
minimalny,	gdy	$\forall x \in A\,(x \leq a \to a = x)$.

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

Przykłady

- Zero jest elementem największym a 1 najmniejszym w zbiorze $\mathbb{N}$ uporządkowanym przez podzielność.
- W porządku $\langle \mathbb{N} - \{0, 1\}, \mid \rangle$ 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 $\langle \mathrm{P}(\mathbb{N}), \subseteq \rangle$ najmniejszy jest zbiór pusty, a największy jest zbiór $\mathbb{N}$.
- W zbiorze $\langle \mathrm{P}(\mathbb{N}) - \{\varnothing\}, \subseteq \rangle$ nie ma elementu najmniejszego, a minimalne są singletony.

Przykład

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

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

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. □

Maksymalne i największe

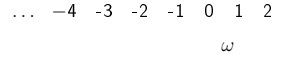
Fakt: *Element największy (najmniejszy) jest jedynym elementem maksymalnym (minimalnym).*

Ale nie na odwrót:

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

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

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



Izomorfizmy porządków

Definicja

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

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

dla dowolnych $a, a' \in A$. Piszemy $\langle A, \leq \rangle \approx \langle B, \leq \rangle$ lub $A \approx B$.
Funkcję f nazywamy *izomorfizmem*.

Izomorfizmy porządków

Jeśli dwa zbiory częściowo uporządkowane są izomorficzne i jeden z nich

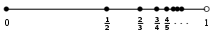
- ma element najmniejszy, największy, maksymalny, minimalny;[2]
- jest liniowo uporządkowany;
- ma nieskończony antyłańcuch;
- ma jakąś inną własność *porządkową*,

to ten drugi też.

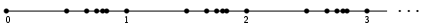
[2] Niepotrzebne skreślić.

Przykład

Zbiór $\langle \mathbb{N}, \leq \rangle$ jest izomorficzny ze zbiorem $A = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$



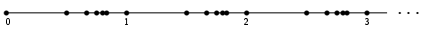
ale nie ze zbiorem $B = \{m - \frac{1}{n} \mid m, n \in \mathbb{N} - \{0\}\}$.



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

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:

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

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*).

Przykład

W porządku $\langle \mathbb{N}, \mid \rangle$ podzbiór $\{18, 30\}$ jest ograniczony

z dołu (np. przez 1 albo 3)

i z góry (np. przez 180 lub 360).

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 $c \leq a$.

Przykłady

- W porządku $\langle \mathbb{N}, \mid \rangle$ 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 $\langle \mathsf{P}(A), \subseteq \rangle$ kresem górnym dowolnej podrodziny $X \subseteq \mathsf{P}(A)$ jest suma $\bigcup X$.
- W szczególności $\sup\{B, C\} = B \cup C$. Podobnie $\inf\{B, C\} = B \cap C$.

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*.

Przykłady

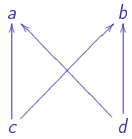
- Rodzina $\mathcal{R}$ funkcji częściowych jest *zgodna*, gdy dla dowolnych $f, g \in \mathcal{R}$ i dowolnego $x \in \mathrm{Dom}(f) \cap \mathrm{Dom}(g)$ zachodzi $f(x) = g(x)$.
- W zbiorze $\langle A \multimap B, \subseteq \rangle$ funkcji częściowych z A do B każda zgodna rodzina $\mathcal{R}$ ma kres górny, $\sup \mathcal{R} = \bigcup \mathcal{R}$, gdzie:
  - $\mathrm{Dom}(\bigcup \mathcal{R}) = \bigcup \{\mathrm{Dom}(f) \mid f \in \mathcal{R}\}$;
  - jeśli $f \in \mathcal{R}$ i $f(x)$ jest określone, to $(\bigcup \mathcal{R})(x) = f(x)$.

Przykłady

- Kres górny zbioru pustego to element najmniejszy.
- Kres dolny zbioru pustego to element największy.

Przykład

Podzbiór $\{c, d\}$ ma dwa ograniczenia górne...



ale nie ma kresu górnego.

Zadanie: Jakiej mocy jest zbiór $\mathcal{P}$ wszystkich porządków częściowych w $\mathbb{R}$?

Rozwiązanie: Po pierwsze każdy porządek częściowy jest relacją w $\mathbb{R}$, więc $\overline{\overline{\mathcal{P}}} \leq \overline{\overline{\mathrm{P}(\mathbb{R} \times \mathbb{R})}} = 2^{\mathfrak{c}}$.

Po drugie pokażemy, że $2^{\mathfrak{c}} \leq \overline{\overline{\mathcal{P}}}$.

Pierwszy pomysł: Spróbujmy pokazać, że $\overline{\overline{\mathrm{P}(\mathbb{R})}} \leq \overline{\overline{\mathcal{P}}}$.
Jeśli $X \subseteq \mathbb{R}$, to określmy taką relację $\leq_X$, że dla $x, y \in \mathbb{R}$:

$x \leq_X y$ wtw, gdy albo $x = y$, albo $x \in X$ i $y \notin X$.

Tak otrzymamy funkcję $\lambda X.\leq_X : \mathrm{P}(\mathbb{R}) \to \mathcal{P}$.

Dlaczego to jest niedobrze i jak to poprawić?

Jest niedobrze, bo $\leq_\varnothing$ i $\leq_\mathbb{R}$ to ta sama relacja.
Zatem $\lambda X.\leq_X$ nie jest injekcją.
Trzeba się pozbyć np. $\mathbb{R}$...

Zadanie: Jakiej mocy jest zbiór $\mathcal{P}$ wszystkich porządków częściowych w $\mathbb{R}$?

Rozwiązanie c.d. Pokażemy, że $\overline{\overline{\mathrm{P}(\mathbb{R}_+)}} \leq \overline{\overline{\mathcal{P}}}$.
Jeśli $X \subseteq \mathbb{R}_+$, to określmy taką relację $\leq_X$, że dla $x, y \in \mathbb{R}$:

$x \leq_X y$ wtw, gdy albo $x = y$, albo $x \in X$ i $y \notin X$.

Tak otrzymamy injekcję $\lambda X.\leq_X : \mathrm{P}(\mathbb{R}_+) \xrightarrow{1-1} \mathcal{P}$.

Ale dlaczego to jest injekcja?

Bo jeśli $X \neq Y$, np. $a \in X - Y$, to $a \leq_X -1$, ale $a \not\leq_Y -1$.

Wnioski: Ponieważ $\mathbb{R}_+ \sim \mathbb{R}$, więc $\mathrm{P}(\mathbb{R}_+) \sim \mathrm{P}(\mathbb{R})$.

A zatem $\overline{\overline{\mathcal{P}}} \leq \overline{\overline{\mathrm{P}(\mathbb{R}_+)}} = 2^{\mathfrak{c}}$...
i z twierdzenia Cantora-Bernsteina $\overline{\overline{\mathcal{P}}} = 2^{\mathfrak{c}}$.

Zasada minimum

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.

Załóżmy, że teza zachodzi dla zbiorów n-elementowych.
Niech $\langle A, \leq \rangle$ będzie liniowym porządkiem mocy $s(n)$.
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. □

Uogólnienie

Fakt

Każdy skończony i niepusty częściowy porządek ma element maksymalny i minimalny.

Dowód: Ćwiczenie.
(Co trzeba zmienić w poprzednim dowodzie?) □

Zasada minimum

Fakt
Każdy niepusty podzbiór $A \subseteq \mathbb{N}$ ma element najmniejszy, tj. taki element $a \in A$, że $\forall b\,(b \in A \to a \leq b)$.

Dowód: Skoro A jest niepusty, to ma jakiś element n. Zbiór $B = \{m \in A \mid m \leq n\}$ jest podzbiorem $s(n)$, 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 $n \in B$.

□

Zasada minimum

Każdy niepusty podzbiór $A \subseteq \mathbb{N}$ ma element najmniejszy, tj. taki element $a \in A$, że $\forall b\,(b \in A \to a \leq b)$.

Oznaczenie: $a = \min A$

Trochę inna zasada indukcji

Wniosek
Jeśli $\forall n{:}\mathbb{N}(\forall m{:}\mathbb{N}(m < n \to W(m)) \to W(n))$,
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 $\forall m{:}\mathbb{N}(m < n \to W(m))$ 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

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.

Usuwając 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.

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.

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.
Usuwając jedną z nich dostajemy dwa drzewa...

Porządki dobrze ufundowane

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.)

Przykłady

- 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.

Inna definicja dobrego ufundowania

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 $b_0 > b_1 > b_2 > \cdots$ □

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 $a \in W$. □

Przykład: funkcja Ackermanna-Sudana

Fakt: Następująca procedura rekurencyjna

$$\begin{aligned} A(n,m) = \texttt{if } n = 0 \texttt{ then } & m+1 \\ \texttt{else if } m = 0 \texttt{ then } & A(n-1,1) \\ \texttt{else } & A(n-1, A(n, m-1)) \end{aligned}$$

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 $\langle n, m \rangle$.*

Przykład: funkcja Ackermanna-Sudana

Fakt: Następująca procedura rekurencyjna

$$\begin{aligned} A(n,m) = \texttt{if } n = 0 \texttt{ then } & m+1 \\ \texttt{else if } m = 0 \texttt{ then } & A(n-1,1) \\ \texttt{else } & A(n-1, A(n, m-1)) \end{aligned}$$

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 $\langle n-1, a \rangle$.

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 $W = A$.

Morał

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*.

Słowa

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?

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.

$$X(\varepsilon) \wedge (\forall w{:}\{a,b\}^*(X(w) \to X(wa) \wedge X(wb))) \to \\ \to \forall w{:}\{a,b\}^*.\, X(w).$$

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:
$ein \cdot (und \cdot zwanzig) = (ein \cdot und) \cdot zwanzig = einundzwanzig$.

Dowodzenie przez indukcję

Fakt
Dla dowolnych słów w i v 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. □

Ćwiczenie: Udowodnić, że $\forall w\,(\varepsilon \cdot w = w)$.

Porządek prefiksowy

Definicja: $w \subseteq v \quad \Leftrightarrow \quad \exists u\,(v = w \cdot u)$.

Fakt
Relacja $\subseteq$ jest częściowym porządkiem, na dodatek dobrze ufundowanym.

Dowód: Zwrotność i przechodniość 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. □

Porządek leksykograficzny

Załóżmy, 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).

Fakt (ćwiczenie)

Porządek leksykograficzny jest relacją częściowego porządku w zbiorze A^*. Jeśli alfabet jest liniowo uporządkowany, to porządek leksykograficzny też jest liniowy.

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.

Typy indukcyjne

Co łączy ze sobą liczby naturalne i słowa?

- Definicja przez konstruktory;
- Indukcja.

Takie dziedziny nazywamy *typami indukcyjnymi*.

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.

Listy

Listy liczb naturalnych tworzą typ indukcyjny list generowany przez dwa konstruktory:

$\mathsf{nil} : \mathsf{list}, \quad$ oraz $\quad \mathsf{cons} : \mathbb{N} \times \mathsf{list} \to \mathsf{list}.$

Zamiast $\mathsf{cons}(n, \ell)$ często piszemy $n :: \ell$.

Zasada indukcji:

$$W(\mathsf{nil}) \ \wedge \ \forall \ell : \mathsf{list}(W(\ell) \to \forall n : \mathbb{N}.\, W(n :: \ell)) \ \to \ \forall \ell : \mathsf{list}.\, W(\ell).$$

Schemat definiowania przez indukcję:

$$\begin{aligned} f(\mathsf{nil}, d) &= g(d); \\ f(n :: \ell, d) &= h(\ell, n, d, f(\ell, d)). \end{aligned}$$

Inne typy indukcyjne

Drzewa binarne:

$\mathsf{leaf} : \mathsf{tree} \qquad \mathsf{node} : \mathsf{tree} \times \mathsf{tree} \to \mathsf{tree}$

Omega-drzewa:

$\mathsf{leaf} : \omega\text{-tree} \qquad \mathsf{node} : (\mathbb{N} \to \omega\text{-tree}) \to \omega\text{-tree}.$

Typy indukcyjne z trywialną indukcją

Suma prosta:

Suma prosta $A \oplus B$ ma dwa konstruktory
$in_1 : A \to A \oplus B, \quad in_2 : B \to A \oplus B.$

Dowodzenie przez indukcję sprowadza się do dwóch przypadków. (Nie ma założenia indukcyjnego.)

Iloczyn kartezjański:

Iloczyn $A \times B$ ma jeden konstruktor $para : A \to (B \to A \times B)$.

Typ jednostkowy:

Typ Unit ma jeden konstruktor $\bullet \in \mathsf{Unit}$.

Typ Bool:

Typ wartości logicznych Bool to suma prosta $\mathsf{Unit} \oplus \mathsf{Unit}$.

Abstrakcyjna składnia

Wyrażenia algebraiczne (*termy*), w których występują (na przykład):

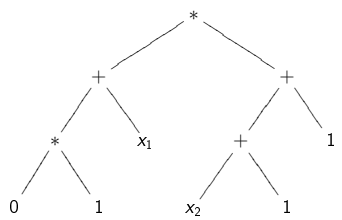
zmienne ze zbioru $V = \{x_i \mid i \in \mathbb{N}\}$,
stałe ze zbioru $\{0, 1\}$,
operacje $+$ oraz $*$,

tworzą typ indukcyjny WA o konstruktorach:

$x : \mathbb{N} \to \mathrm{WA}$,
$0, 1 : \mathrm{WA}$,
$+, * : \mathrm{WA} \times \mathrm{WA} \to \mathrm{WA}$.

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: $((0 * 1) + x_1) * ((x_2 + 1) + 1)$.

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 $(0 * 1 + x_1) * (x_2 + 1 + 1)$.

Definiowanie przez indukcję

Wartościowanie zmiennych ze zbioru $V = \{x_i \mid i \in \mathbb{N}\}$ w zbiorze $\mathbb{N}$ to dowolna funkcja $v : V \to \mathbb{N}$.

Umówmy się, że znaki $+$, $*$, 0 i 1 interpretujemy jak zwykle.

Wartość termu t przy wartościowaniu v, ozn. $[\![t]\!]_v$, definiujemy przez indukcję:

$[\![x_i]\!]_v = v(x_i)$, $\quad [\![0]\!]_v = 0$, $\quad [\![1]\!]_v = 1$.

$[\![t+u]\!]_v = [\![t]\!]_v + [\![u]\!]_v$, $\quad [\![t*u]\!]_v = [\![t]\!]_v * [\![u]\!]_v$

Jeśli $v(x_1)$=7 i $v(x_2)$=3, to $[\![(0*1+x_1)*(x_2+1+1)]\!]_v = 35$.

Ale możemy się umówić inaczej.

Wartość termu, ogólniej

Wartościowanie zmiennych ze zbioru $V = \{x_i \mid i \in \mathbb{N}\}$ w zbiorze A to dowolna funkcja $v : V \to A$.

Ustalamy pewne funkcje $a, m : A \times A \to A$ i stałe $z, j \in A$.

Umówmy się, że $+$, $*$, 0 i 1 interpretujemy jako a, m, z, j.

Wartość termu t przy wartościowaniu v definiujemy przez indukcję:

$[\![x_i]\!]_v = v(x_i)$, $\quad [\![0]\!]_v = z$, $\quad [\![1]\!]_v = j$.

$[\![t+u]\!]_v = a([\![t]\!]_v, [\![u]\!]_v)$, $\quad [\![t*u]\!]_v = m([\![t]\!]_v, [\![u]\!]_v)$

Wtedy $[\![(0*1+x_1)*(x_2+1+1)]\!]_v$ jest jakimś elementem A.

Wartość termu, przykład

Przyjmijmy $A = \mathrm{P}(\mathbb{R})$, $z = \varnothing$, $j = \mathbb{Q}$ i niech $a(u,v) = u \cup v$, $\quad m(u,v) = u - v$.

Jeśli v jest takie, że $v(x_1) = \mathbb{R}$ i $v(x_2) = \{0, \pi\}$, to

$[\![(0*1+x_1)*(x_2+1+1)]\!]_v =$

$((\varnothing - \mathbb{Q}) \cup \mathbb{R}) - (((\{0,\pi\} \cup \mathbb{Q}) \cup \mathbb{Q}) =$

$\mathbb{R} - (\mathbb{Q} \cup \{\pi\}) = \mathbb{IQ} - \{\pi\}$,

gdzie $\mathbb{IQ}$ to zbiór wszystkich liczb niewymiernych.

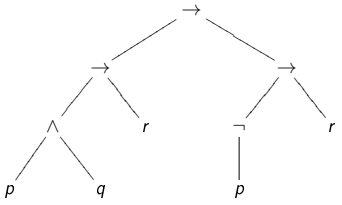
Przerwa na reklamę

Składnia (abstrakcyjna) rachunku zdań

- *Symbole* (zmienne) zdaniowe ($p, q, r, \ldots$), oraz stałe $\bot$ 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
  $$\alpha \to \beta, \quad \alpha \vee \beta, \quad \alpha \wedge \beta$$
  też są formułami zdaniowymi.

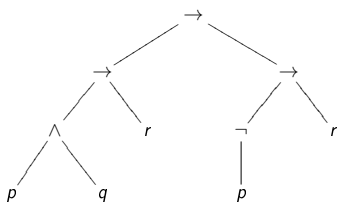
Inaczej: formuły zdaniowe tworzą typ indukcyjny, o konstruktorach $p, q, r, \ldots, \bot, \top, \neg, \to, \vee, \wedge$

Przykład: składnia abstrakcyjna



Składnia konkretna: $(((p \wedge q) \to r) \to ((\neg p) \to r))$

Przykład: składnia abstrakcyjna



Składnia konkretna: $(p \wedge q \to r) \to (\neg p \to r)$

Składnia konkretna

- Koniunkcja i alternatywa mają wyższy priorytet niż implikacja: zamiast $(p \wedge q) \to r$ piszemy $p \wedge q \to r$.
- Negacja ma najwyższy priorytet: napis $\neg p \to q$ 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:

$(p \wedge q \to r) \to (\neg p \to r)$ $\qquad$ $p \wedge (q \to r) \to \neg(p \to r)$

Równoważność

- Napis $\alpha \leftrightarrow \beta$ jest skrótem napisu $(\alpha \to \beta) \wedge (\beta \to \alpha)$.

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:

- $[\![\bot]\!]_\varrho = 0$ oraz $[\![\top]\!]_\varrho = 1$;
- $[\![p]\!]_\varrho = \varrho(p)$, gdy p jest symbolem zdaniowym;
- $[\![\neg\alpha]\!]_\varrho = 1 - [\![\alpha]\!]_\varrho$;
- $[\![\alpha \vee \beta]\!]_\varrho = \max\{[\![\alpha]\!]_\varrho, [\![\beta]\!]_\varrho\}$;
- $[\![\alpha \wedge \beta]\!]_\varrho = \min\{[\![\alpha]\!]_\varrho, [\![\beta]\!]_\varrho\}$;
- $[\![\alpha \to \beta]\!]_\varrho = 0$, gdy $[\![\alpha]\!]_\varrho = 1$ i $[\![\beta]\!]_\varrho = 0$;
- $[\![\alpha \to \beta]\!]_\varrho = 1$, w przeciwnym przypadku.

Przykład

Formuła $(p \wedge q \to r) \to (\neg p \to r)$ 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

$$\mu(p) = \mu(r) = 0 \quad \text{i} \quad \mu(q) = 1.$$

Spełnialność i prawdziwość

Jeśli $[\![\varphi]\!]_\varrho = 1$, 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 $\models \varphi$.

Równoważność i implikacja

- Formuły $((p \leftrightarrow q) \leftrightarrow r)$ i $(p \leftrightarrow (q \leftrightarrow r))$
  są równoważne.
- Ale żadna z nich nie jest równoważna
  formule $(p \leftrightarrow q) \wedge (q \leftrightarrow r)$.
- Co znaczy napis: $p \leftrightarrow q \leftrightarrow r$?
- Zdania postaci $((p \to q) \to r)$ i $(p \to (q \to r))$
  nie są równoważne.
- I żadne z nich nie jest równoważne
  zdaniu $(p \to q) \wedge (q \to r)$.
- Co znaczy napis $p \to q \to r$?

Przykłady tautologii

- Prawo wyłączonego środka: $p \vee \neg p$.
- Prawo podwójnego przeczenia: $\neg\neg p \leftrightarrow p$.
- Prawa De Morgana:
  - $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$;
  - $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$.

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 $p \vee q \vee r \vee \ldots$ nie dbając o nawiasy i kolejność.

Ważne schematy z implikacją

- $(p \to q) \leftrightarrow (\neg p \vee q)$.
- $\neg(p \to q) \leftrightarrow (p \wedge \neg q)$.
- $(p \to q) \leftrightarrow (\neg q \to \neg p)$ (prawo kontrapozycji).
- $\neg p \leftrightarrow (p \to \bot)$.
- $p \wedge (p \to q) \to q$ (odrywanie, czyli modus ponens).

Ważne schematy z implikacją

- $(p \to q) \leftrightarrow (\neg p \vee q)$.
- $\neg(p \to q) \leftrightarrow (p \wedge \neg q)$.
- $(p \to q) \leftrightarrow (\neg q \to \neg p)$ (prawo kontrapozycji).
- $\neg p \leftrightarrow (p \to \bot)$.
- $p \wedge (p \to q) \to q$ (odrywanie, czyli modus ponens).

Koniunkcja i alternatywa

- $p \to (p \vee q)$, $q \to (p \vee q)$,
- $(p \to r) \to ((q \to r) \to (p \vee q \to r))$;
- $(p \wedge q) \to p$, $(p \wedge q) \to q$,
- $(r \to p) \to ((r \to q) \to (r \to p \wedge q))$;
- $p \vee \bot \leftrightarrow p$, $p \vee \top \leftrightarrow \top$;
- $p \wedge \bot \leftrightarrow \bot$, $p \wedge \top \leftrightarrow p$.

Wnioskowanie z przesłanek

Mówimy, że formuła φ jest *konsekwencją* zbioru założeń Γ i piszemy $\Gamma \models \varphi$, gdy dla dowolnej interpretacji zdaniowej ϱ,

jeżeli $[\![\gamma]\!]_\varrho = 1$ dla każdego $\gamma \in \Gamma$, to także $[\![\varphi]\!]_\varrho = 1$.

Przykład: $\{\varphi \to \psi, \psi \to \vartheta\} \models \varphi \to \vartheta$.

(Można to napisać bez klamerek: $\varphi \to \psi, \psi \to \vartheta \models \varphi \to \vartheta$.)

Związek $\Gamma \models \varphi$ to ogólnie poprawny schemat wnioskowania.

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:

- $[\![\bot]\!]_\varrho = 0$ oraz $[\![\top]\!]_\varrho = 1$;
- $[\![p]\!]_\varrho = \varrho(p)$, gdy p jest symbolem zdaniowym;
- $[\![\neg\alpha]\!]_\varrho = 1 - [\![\alpha]\!]_\varrho$;
- $[\![\alpha \vee \beta]\!]_\varrho = \max\{[\![\alpha]\!]_\varrho, [\![\beta]\!]_\varrho\}$;
- $[\![\alpha \wedge \beta]\!]_\varrho = \min\{[\![\alpha]\!]_\varrho, [\![\beta]\!]_\varrho\}$;
- $[\![\alpha \to \beta]\!]_\varrho = 0$, gdy $[\![\alpha]\!]_\varrho = 1$ i $[\![\beta]\!]_\varrho = 0$;
- $[\![\alpha \to \beta]\!]_\varrho = 1$, w przeciwnym przypadku.

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:

$$(p_1^1 \vee \cdots \vee p_1^{k_1}) \wedge \cdots \wedge (p_r^1 \vee \cdots \vee p_r^{k_r}),$$

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) Pusta koniunkcja ($r = 0$) to stała $\top$.
(2) Pusta alternatywa ($k_i = 0$) to stała $\bot$.

Normalizacja formuł

Twierdzenie: Dla każdej formuły zdaniowej istnieje równoważna jej formuła w koniunkcyjnej postaci normalnej.

Szkic dowodu:

Najpierw eliminujemy implikacje, stosując zasadę:

$$(\alpha \to \beta) \leftrightarrow (\neg\alpha \vee \beta).$$

Otrzymujemy formułę, w której występują tylko $\vee$, $\wedge$ i $\neg$.

Normalizacja formuł

Dana jest formuła, w której występują tylko $\vee$, $\wedge$ i $\neg$.
Jeśli ta formuła nie jest w postaci normalnej

$$(p_1^1 \vee \cdots \vee p_1^{k_1}) \wedge \cdots \wedge (p_r^1 \vee \cdots \vee p_r^{k_r}),$$

to zawiera „podformułę" jednej z następujących postaci:

$$\neg(\alpha \vee \beta), \quad \neg(\alpha \wedge \beta), \quad \neg\top, \quad \neg\bot, \quad \neg\neg\alpha,$$
$$\top \vee \alpha, \quad \top \wedge \alpha, \quad \bot \wedge \alpha, \quad \bot \vee \alpha$$
$$\alpha \vee (\beta \wedge \gamma)$$

(z dokładnością do kolejności argumentów).

Reguły przepisywania

Eliminujemy podwójne i trywialne negacje:

$$\neg\neg\alpha \Rightarrow \alpha \qquad \neg\top \Rightarrow \bot \qquad \neg\bot \Rightarrow \top$$

„Przesuwamy w dół" negacje z pomocą praw De Morgana:

$$\neg(\alpha \vee \beta) \Rightarrow (\neg\alpha \wedge \neg\beta) \qquad \neg(\alpha \wedge \beta) \Rightarrow (\neg\alpha \vee \neg\beta)$$

Eliminujemy nadmiar stałych logicznych:

$$\top \vee \alpha \Rightarrow \top, \qquad \top \wedge \alpha \Rightarrow \alpha,$$
$$\bot \wedge \alpha \Rightarrow \bot, \qquad \bot \vee \alpha \Rightarrow \alpha.$$

„Przesuwamy w dół" alternatywy:

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

Przykład

Formułę $\neg(p \vee \neg q) \vee (r \wedge \top)$ przepisujemy do postaci:

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

$(\neg p \wedge \neg\neg q) \vee r$

$(\neg p \wedge q) \vee r$

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

Wszystkie te formuły są równoważne.
Ostatnia formuła jest w koniunkcyjnej postaci normalnej.

Dlaczego ta procedura musi się zakończyć?

Każdej formule (bez $\rightarrow$) przypiszemy liczbową *wagę*:

- $waga(p) = 2$, gdy p jest atomem (w tym $\top, \bot$).
- $waga(\varphi \wedge \psi) = waga(\varphi) + waga(\psi) + 2$;
- $waga(\varphi \vee \psi) = 2 \cdot waga(\varphi) \cdot waga(\psi)$;
- $waga(\neg\varphi) = 2^{waga(\varphi)}$.

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:

$waga(\neg(\alpha \vee \beta)) = 2^{waga(\alpha \vee \beta)} = 2^{2ab}$;
$waga(\neg\alpha \wedge \neg\beta) = 2^a + 2^b + 2 < 2^{2ab}$.

Rozmiar postaci normalnej

Operacja

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

podwaja podformułę α. Wielokrotne podwajanie może wykładniczo zwiększyć rozmiary całej formuły.

Jakiej wielkości jest postać normalna tej formuły?

$$(p_1 \wedge q_1) \vee (p_2 \wedge q_2) \vee \cdots \vee (p_n \wedge q_n)$$

Siła wyrazu rachunku zdań

Kolorowanie grafu

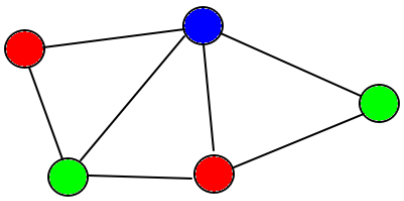
Niech G będzie (skończonym) zbiorem, w którym określono symetryczną relację r. Parę $\mathcal{G} = \langle G, r\rangle$ nazwiemy *grafem*.

(*Myślimy o G jak o zbiorze wierzchołków grafu, a o relacji r jak o zbiorze krawędzi tego grafu.*)

Graf $\mathcal{G} = \langle G, r\rangle$ jest *trójkolorowy*, gdy istnieje taki podział zbioru G na trzy rozłączne części, że żadne dwa elementy zbioru G, należące do jednej składowej, nie są w relacji r.

(*Wierzchołki połączone krawędziami są różnych kolorów.*)

Ten graf jest trójkolorowy



Kolorowanie grafu

Dany graf $\mathcal{G} = \langle G, r\rangle$. Określimy tak zbiór formuł $\Gamma_{\mathcal{G}}$, że:

$\mathcal{G}$ jest trójkolorowy $\quad\Leftrightarrow\quad$ $\Gamma_{\mathcal{G}}$ 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^i_a, dla $a \in G$ oraz $i \in \{1, 2, 3\}$. (Sens: wierzchołek a ma kolor i.)

W zbiorze $\Gamma_{\mathcal{G}}$ są takie formuły:

$\alpha_a = (p^1_a \vee p^2_a \vee p^3_a) \wedge \neg(p^1_a \wedge p^2_a) \wedge \neg(p^1_a \wedge p^3_a) \wedge \neg(p^3_a \wedge p^2_a)$,

dla każdego $a \in G$. (*Element a ma dokładnie jeden kolor.*)

$\beta_{ab} = \neg(p^1_a \wedge p^1_b) \wedge \neg(p^2_a \wedge p^2_b) \wedge \neg(p^3_a \wedge p^3_b)$,

dla każdej pary $\langle a, b\rangle \in r$. (*Elementy a i b są różnego koloru.*)

Rachunek predykatów

(pierwszego rzędu)

Język logiki pierwszego rzędu

- Zmienne indywiduowe, np. $x, y, \ldots$
- 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:

$$+, *, 0, 1, \leq.$$

Formuły pierwszego rzędu

- Formuły atomowe $r(t_1, \ldots, t_n)$ są formułami, gdzie r to symbol relacyjny a $t_1, \ldots, t_n$ to termy (wyrażenia algebraiczne).
  (Zwykle piszemy np. $t_1 + t_2$ zamiast $+(t_1, t_2)$.)
- Stałe logiczne $\bot$, $\top$ są formułami.
- Jeśli φ, ψ są formułami, to
  $$\varphi \to \psi, \quad \varphi \vee \psi, \quad \varphi \wedge \psi, \quad \neg\varphi$$
  są formułami.
- Jeśli φ jest formułą, a x zmienną indywiduową, to
  $$\forall x \varphi, \quad \exists x \varphi$$
  są formułami.

Zmienne wolne

$\mathrm{FV}(\varphi)$ to zbiór wszystkich *zmiennych wolnych* formuły φ:

$\mathrm{FV}(r(t_1, \ldots, t_n))$ to zbiór wszystkich zmiennych w $t_1, \ldots, t_n$.
$\mathrm{FV}(\alpha \vee \beta) = \mathrm{FV}(\alpha \wedge \beta) = \mathrm{FV}(\alpha \to \beta) = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta)$,
$\mathrm{FV}(\top) = \mathrm{FV}(\bot) = \varnothing$,
$\mathrm{FV}(\neg\alpha) = \mathrm{FV}(\alpha)$,
$\mathrm{FV}(\forall x\, \varphi) = \mathrm{FV}(\exists x\, \varphi) = \mathrm{FV}(\varphi) - \{x\}$.

Na przykład $\mathrm{FV}(\forall x\, (r(x, x) \to r(x, y)) \vee \exists z\, r(x, z)) = \{x, y\}$.

Semantyka formuł

Struktura relacyjna (także: *model, interpretacja*),
to niepusty zbiór wraz z odpowiednimi relacjami i funkcjami:
$$\mathcal{A} = \langle A, r_1^{\mathcal{A}}, \ldots, r_n^{\mathcal{A}}, f_1^{\mathcal{A}}, \ldots, f_m^{\mathcal{A}} \rangle$$

Wartościowanie w strukturze $\mathcal{A}$, to funkcja $v : V \to A$.

Znaczenie formuły φ przy wartościowaniu v
to jej wartość logiczna $[\![\varphi]\!]_v \in \{0, 1\}$.

Semantyka formuł

Znaczenie formuły φ przy wartościowaniu v
to jej wartość logiczna $[\![\varphi]\!]_v \in \{0, 1\}$.

Znaczenie formuły atomowej:

- $[\![\bot]\!]_v = 0$;
- $[\![\top]\!]_v = 1$;
- $[\![r(t_1, \ldots, t_n)]\!]_v = 1$, gdy $\langle [\![t_1]\!]_v, \ldots, [\![t_n]\!]_v \rangle \in r^{\mathcal{A}}$;
- $[\![r(t_1, \ldots, t_n)]\!]_v = 0$, w przeciwnym przypadku.

Znaczenie formuł złożonych

- $[\![\neg\alpha]\!]_v = 1 - [\![\alpha]\!]_v$;
- $[\![\alpha \vee \beta]\!]_v = \max\{[\![\alpha]\!]_v, [\![\beta]\!]_v\}$;
- $[\![\alpha \wedge \beta]\!]_v = \min\{[\![\alpha]\!]_v, [\![\beta]\!]_v\}$;
- $[\![\alpha \to \beta]\!]_v = 0$, gdy $[\![\alpha]\!]_v = 1$ i $[\![\beta]\!]_v = 0$;
- $[\![\alpha \to \beta]\!]_v = 1$, w przeciwnym przypadku.

Znaczenie formuł z kwantyfikatorami

Poniżej, $v[x \mapsto a]$ oznacza takie wartościowanie, że
$v[x \mapsto a](x) = a$ oraz $v[x \mapsto a](y) = v(y)$.

- $[\![\forall x \varphi]\!]_v = \min\{[\![\varphi]\!]_{v[x \mapsto a]} \mid a \in A\}$;
- $[\![\exists x \varphi]\!]_v = \max\{[\![\varphi]\!]_{v[x \mapsto a]} \mid a \in A\}$.

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.

Ważny fakt:

Znaczenie formuły zależy tylko od wartości jej zmiennych wolnych. Ściślej:
Jeśli $v(x) = w(x)$ dla każdego $x \in \mathrm{FV}(\varphi)$, to $[\![\varphi]\!]_v = [\![\varphi]\!]_w$

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).

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 $\models \varphi$.

Przykład

Zdanie $\forall x(P(x) \vee Q(x)) \to \forall x\, P(x) \vee \forall x\, Q(x)$
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.

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:

- $\forall x(A \vee B(x)) \leftrightarrow A \vee \forall x B(x)$;
- $\exists x(A \wedge B(x)) \leftrightarrow A \wedge \exists x B(x)$.

Zadanie: Czy to jest tautologia?

$$(\exists y P(y) \to \forall z Q(z)) \to \forall y(P(y) \to Q(y))$$

Rozwiązanie: Przesłanka $\exists y P(y) \to \forall z Q(z)$ jest równoważna każdej z formuł:

$$\neg\exists y\, P(y) \vee \forall z\, Q(z);$$
$$\forall y\, \neg P(y) \vee \forall z\, Q(z);$$
$$\forall y(\neg P(y) \vee \forall z\, Q(z));$$
$$\forall y \forall z(\neg P(y) \vee Q(z));$$
$$\forall y \forall z(P(y) \to Q(z)).$$

Zatem całość jest równoważna oczywistej tautologii:

$$\forall y \forall z(P(y) \to Q(z)) \to \forall y(P(y) \to Q(y)).$$

Ćwiczenie

Symbole relacyjne R, S są jednoargumentowe, symbol funkcyjny f jest dwuargumentowy.

Napisać zdanie prawdziwe dokładnie w tych modelach

$$\mathcal{A} = \langle A, f^{\mathcal{A}}, R^{\mathcal{A}}, S^{\mathcal{A}} \rangle,$$

w których obraz zbioru $R^{\mathcal{A}} \times S^{\mathcal{A}}$ przy przekształceniu $f^{\mathcal{A}}$ zawiera się w zbiorze $R^{\mathcal{A}} \cap S^{\mathcal{A}}$.

Rozwiązanie:

$$\forall x \forall y(R(x) \wedge S(y) \to R(f(x,y)) \wedge S(f(x,y))$$

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:

$$\exists x_1 \exists x_2 \forall y(\forall z_1 \forall z_2(y = z_1 \cdot z_2 \to y = z_1 \vee y = z_2) \to y = x_1 \vee y = x_2 \vee y = \varepsilon)$$

Powyższe zdanie zdanie *rozróżnia* te dwie struktury.

Złe wiadomości

Jak ustalić, że formuła jest tautologią?

- 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.

Jak ustalić, że formuła jest tautologią?

Można ją *udowodnić*.

Naturalna dedukcja

Stanisław Jaśkowski, Gerhard Gentzen


Naturalna dedukcja

- Reguły *wprowadzania* spójników logicznych: jak można udowodnić formułę danej postaci?
- Reguły *eliminacji* spójników: jak można wykorzystać formułę tej postaci do udowodnienia innej?

Wprowadzanie koniunkcji

$$\begin{array}{c} \vdots \\ A \\ \vdots \\ B \end{array}$$

Ponieważ A oraz B, więc $A \wedge B$.

Zapisujemy to jako *regułę wnioskowania* $\mathrm{W}\wedge$:

$$\frac{A \quad B}{A \wedge B} \qquad \text{albo tak :} \quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B},$$

gdzie „$\Gamma \vdash$” oznacza: „przy założeniach Γ”

Eliminacja koniunkcji

$$\begin{array}{c} A \wedge B \\ \vdots \end{array}$$

Ponieważ $A \wedge B$, więc A.

$$\begin{array}{c} A \wedge B \\ \vdots \end{array}$$

Ponieważ $A \wedge B$, więc B.

Reguły wnioskowania $\mathrm{E}\wedge$:

$$\frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B}$$

Eliminacja koniunkcji

$$\begin{array}{c} A \wedge B \\ \vdots \end{array}$$

Ponieważ $A \wedge B$, więc A.

$$\begin{array}{c} A \wedge B \\ \vdots \end{array}$$

Ponieważ $A \wedge B$, więc B.

Reguły wnioskowania $\mathrm{E}\wedge$:

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

Eliminacja implikacji (odrywanie)

$$\begin{array}{c} A \\ \vdots \\ A \to B \\ \vdots \end{array}$$

Ponieważ A oraz $A \to B$, więc B.

Reguła *modus ponens:*

$$\frac{A \quad A \to B}{B}$$

Eliminacja implikacji (odrywanie)

$$\begin{array}{c} A \\ \vdots \\ A \to B \\ \vdots \end{array}$$

Ponieważ A oraz $A \to B$, więc B.

Reguła *modus ponens:*

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A \to B}{\Gamma \vdash B} \ (\mathrm{E}\to)$$

Wprowadzanie implikacji

Załóżmy A.	*(Cel: B)*
⋮	
Zatem B.	*(Cel osiągnięty)*

Zatem $A \to B$.

Jaką tu mamy regułę?

$$\frac{A \vdash B}{A \to B}$$

Aby udowodnić $A \to B$, dowodzimy B przy założeniu A.

Wprowadzanie implikacji

Załóżmy A.	*(Cel: B)*
⋮	
Zatem B.	*(Cel osiągnięty)*

Zatem $A \to B$.

Jaką tu mamy regułę?

$$\frac{\Gamma \cup \{A\} \vdash B}{\Gamma \vdash A \to B}$$

Aby udowodnić $A \to B$, dodajemy założenie A i dowodzimy B.

Wprowadzanie implikacji

Załóżmy A.	*(Cel: B)*
⋮	
Zatem B.	*(Cel osiągnięty)*

Zatem $A \to B$.

Jaką tu mamy regułę?

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ (\mathrm{W}\to)$$

Aby udowodnić $A \to B$, dodajemy założenie A i dowodzimy B.

Przykład

Załóżmy p	*(Cel 1: $q \to p$)*
Załóżmy q	*(Cel 2: p)*
Z założenia mamy p	*(Cel 2 osiągnięty)*
Zatem $q \to p$	*(Cel 1 osiągnięty)*

Zatem $p \to (q \to p)$

Spróbujemy to zapisać zwięźlej.

Przykład

p	*(Cel 1: $q \to p$)*
$p, q \vdash p$	*(Cel 2: p)*
	(Cel 2 osiągnięty)
$p \vdash q \to p$	*(Cel 1 osiągnięty)*

$\vdash p \to (q \to p)$

Jeszcze zwięźlej:

$p, q \vdash p$
$p \vdash q \to p$
$\vdash p \to (q \to p)$

Bez ramek:

$$\frac{\dfrac{p, q \vdash p}{p \vdash q \to p}\,(\mathrm{W}\to)}{\vdash p \to (q \to p)}\,(\mathrm{W}\to)$$

Naturalna dedukcja: formalizacja w stylu Gentzena

- Rozważamy *osądy* postaci $\Gamma \vdash \varphi$, gdzie Γ jest zbiorem formuł (założeń), a φ to formuła (teza). Zamiast $\varnothing \vdash \varphi$ piszemy po prostu $\vdash \varphi$.
- Reguły w stylu Gentzena służą do wyprowadzania osądów (z innych osądów). Zapisujemy je tak:

$$\frac{\Gamma_1 \vdash \varphi_1, \ldots, \Gamma_n \vdash \varphi_n}{\Delta \vdash \psi}$$

Na górze są przesłanki, na dole konkluzja.

Uwaga: Naturalna dedukcja w stylu Gentzena, to *co innego* niż „rachunek sekwentów Gentzena"!

Przykład dowodu

$$\dfrac{\dfrac{\dfrac{(p\to p)\to q,\ p \vdash p}{(p\to p)\to q \vdash p\to p}\,(\mathrm{W}\to) \qquad (p\to p)\to q \vdash (p\to p)\to q}{(p\to p)\to q \vdash q}\,(\mathrm{E}\to)}{\vdash ((p\to p)\to q) \to q}\,(\mathrm{W}\to)$$

Dowód formalny to drzewo, którego korzeń (u dołu!), to udowodniony osąd.

A liście (u góry)?

Trzeba od czegoś zacząć

Poniższa reguła nie ma przesłanek.

$$\frac{}{\Gamma \cup \{\varphi\} \vdash \varphi}\,(\mathrm{Ax})$$

Nazywamy ją *aksjomatem naturalnej dedukcji* i zwykle zapisujemy tak:

$$\Gamma, \varphi \vdash \varphi\ \ (\mathrm{Ax})$$

(Najprostszy dowód polega na przywołaniu założenia.)

Wprowadzanie negacji

Załóżmy A (*Cel:* $\bot$)
⋮
Zatem $\bot$ (*sprzeczność*).

Zatem $\neg A$.

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\,(\mathrm{W}\neg)$$

Eliminacja negacji

A
⋮
$\neg A$
⋮
Ponieważ A oraz $\neg A$ więc $\bot$ (sprzeczność).

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,(\mathrm{E}\neg)$$

Eliminacja fałszu: *ex falso quodlibet*

⋮
$\bot$
⋮
Ponieważ $\bot$, więc A

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,(\mathrm{E}\bot)$$

Wprowadzanie prawdy

Jeszcze jedna reguła bez przesłanek:

$$\frac{}{\Gamma \vdash \top}\,(\mathrm{W}\top)$$

Wprowadzanie alternatywy

A
⋮
Ponieważ A, więc $A \vee B$.

B
⋮
Ponieważ B, więc $A \vee B$.

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,(\mathrm{W}\vee)\qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

Eliminacja alternatywy

$A \vee B$
⋮
Załóżmy A. (*Cel 1:* C)
⋮
Zatem C.

Załóżmy B. (*Cel 2:* C)
⋮
Zatem C.

Ponieważ $A \vee B$, więc C.

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\,(\mathrm{E}\vee)$$

Wnioskowanie przez zaprzeczenie

Załóżmy $\neg A$. (*Cel:* $\bot$)
⋮
Zatem $\bot$.

Zatem A.

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}$$

„Nienaturalny wyjątek"

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\,(\mathrm{E}\neg\neg)$$

Ta reguła to jakby eliminacja podwójnej negacji:

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$$

Przykład: *Tertium non datur*

Załóżmy $\neg(p \vee \neg p)$ *(Cel 1: $\bot$)*
(Cel 2: $p \vee \neg p$)
(Cel 3: $\neg p$)

> Załóżmy p. *(Cel 4: $\bot$)*
> Ponieważ p, więc $p \vee \neg p$.
> Ponieważ $p \vee \neg p$ oraz $\neg(p \vee \neg p)$, więc sprzeczność.
> *(Cel 4 osiągnięty)*

Zatem $\neg p$. *(Cel 3 osiągnięty)*
Ponieważ $\neg p$, więc $p \vee \neg p$. *(Cel 2 osiągnięty)*
Ponieważ $p \vee \neg p$ oraz $\neg(p \vee \neg p)$, więc $\bot$. *(Cel 1 osiągnięty)*

Zatem $p \vee \neg p$.

To samo w notacji Gentzena:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\neg(p \vee \neg p), p \vdash p}{\neg(p \vee \neg p), p \vdash p \vee \neg p} \quad \neg(p \vee \neg p), p \vdash \neg(p \vee \neg p)}{\neg(p \vee \neg p), p \vdash \bot}}{\neg(p \vee \neg p) \vdash \neg p}}{\neg(p \vee \neg p) \vdash p \vee \neg p} \quad \neg(p \vee \neg p) \vdash \neg(p \vee \neg p)}{\neg(p \vee \neg p) \vdash \bot}}{\vdash p \vee \neg p}$$

Uwaga: Istotą naturalnej dedukcji jest wprowadzanie i eliminacja spójników. Pudełka, drzewa itp. to tylko sposoby prezentacji.

Podsumowanie: aksjomat i implikacja

$$\Gamma, \varphi \vdash \varphi \ \ (\mathrm{Ax})$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ (\mathrm{W}\to) \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash A \to B}{\Gamma \vdash B}\ (\mathrm{E}\to)$$

Reguły dla koniunkcji

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\mathrm{W}\wedge)$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ (\mathrm{E}\wedge) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ (\mathrm{E}\wedge)$$

Reguły dla alternatywy

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\mathrm{W}\vee) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (\mathrm{W}\vee)$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ (\mathrm{E}\vee)$$

Reguły dla prawdy, fałszu i negacji

$$\frac{}{\Gamma \vdash \top}\ (\mathrm{W}\top) \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ (\mathrm{E}\bot)$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ (\mathrm{W}\neg) \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\ (\mathrm{E}\neg)$$

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (\mathrm{E}\neg\neg)$$

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.

Przykład : $\neg\beta \vdash \neg(\beta \wedge \gamma)$

$$\dfrac{\dfrac{\neg\beta,\ \beta \wedge \gamma\ \vdash\ \neg\beta \qquad \dfrac{\neg\beta,\ \beta \wedge \gamma\ \vdash\ \beta \wedge \gamma}{\neg\beta,\ \beta \wedge \gamma\ \vdash\ \beta}\,(\mathrm{E}\wedge)}{\neg\beta, \beta \wedge \gamma\ \vdash\ \bot}\,(\mathrm{E}\neg)}{\neg\beta\ \vdash\ \neg(\beta \wedge \gamma)}\,(\mathrm{W}\neg)$$

∘

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.*

Przypomnienie notacji

Piszemy $\varrho \models \Gamma$, gdy $[\![\gamma]\!]_\varrho = 1$, dla każdego $\gamma \in \Gamma$.

Piszemy $\Gamma \models \varphi$, gdy dla dowolnej interpretacji zdaniowej ϱ:
jeżeli $\varrho \models \Gamma$, to także $[\![\varphi]\!]_\varrho = 1$.

Jeśli osąd $\Gamma \vdash \varphi$ ma dowód, to piszemy po prostu "$\Gamma \vdash \varphi$".

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$\to$) z osądów $\Gamma \vdash \beta \to \alpha$ i $\Gamma \vdash \beta$. Z założenia indukcyjnego $\Gamma \models \beta \to \alpha$ oraz $\Gamma \models \beta$, bo te dowody mają mniejsze rozmiary. Jeśli więc $\varrho \models \Gamma$, to ϱ spełnia obie formuły $\beta \to \alpha$ i β. Wtedy ϱ musi też spełniać α.

Jeśli $\Gamma \vdash \alpha$, to $\Gamma \models \alpha$

Przypadek 3: Osąd $\Gamma \vdash \alpha$ otrzymano przez (W$\to$). Wtedy $\alpha = \beta \to \gamma$ oraz $\Gamma, \beta \vdash \gamma$ ma dowód mniejszych rozmiarów, zatem $\Gamma, \beta \models \gamma$, z założenia indukcyjnego.

Załóżmy, że $\varrho \models \Gamma$. Jeśli $[\![\beta]\!]_\varrho = 1$, to $\varrho \models \Gamma, \beta$, więc $[\![\gamma]\!]_\varrho = 1$, skąd $[\![\beta \to \gamma]\!]_\varrho = 1$. A jeśli $[\![\beta]\!]_\varrho = 0$, to tym bardziej $[\![\beta \to \gamma]\!]_\varrho = 1$.

Jeśli $\Gamma \vdash \alpha$, to $\Gamma \models \alpha$

Przypadek 4: Osąd $\Gamma \vdash \alpha$ otrzymano przez (E$\bot$) z $\Gamma \vdash \bot$. Z założenia indukcyjnego dostajemy $\Gamma \models \bot$, 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 $\Gamma, \neg\alpha \vdash \bot$. Wtedy $\Gamma, \neg\alpha \models \bot$ 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.

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 $[\![\beta]\!]_\varrho = 1$ lub $[\![\gamma]\!]_\varrho = 1$, skąd ϱ spełnia jeden ze zbiorów Γ, β, lub Γ, γ. W obu przypadkach z założenia indukcyjnego wynika, że $[\![\alpha]\!]\varrho = 1$.

Przypadki 7–14: Podobnie.

Pełność: *Jeśli $\models \alpha$, to $\vdash \alpha$*

Lemat 1:
Następujące osądy mają dowody w naturalnej dedukcji:

1. $\beta, \gamma \vdash \beta \wedge \gamma$;
2. $\beta, \neg\gamma \vdash \neg(\beta \to \gamma)$;
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. $\neg\beta \vdash \beta \to \gamma$;
6. $\gamma \vdash \beta \to \gamma$;
7. $\vdash \neg\bot$;
8. $\vdash \alpha \vee \neg\alpha$;
9. $\beta \vdash \neg\neg\beta$.

(1) $\beta, \gamma \vdash \beta \wedge \gamma$

$$\frac{\beta, \gamma \vdash \beta \qquad \beta, \gamma \vdash \gamma}{\beta, \gamma \vdash \beta \wedge \gamma}\,(\mathrm{W}\wedge)$$

(2) $\beta, \neg\gamma \vdash \neg(\beta \to \gamma)$

Oznaczenie: $\Gamma = \{\beta, \neg\gamma, \beta \to \gamma\}$

$$\dfrac{\dfrac{\Gamma \vdash \neg\gamma \qquad \dfrac{\Gamma \vdash \beta \qquad \Gamma \vdash \beta \to \gamma}{\Gamma \vdash \gamma}\,(\mathrm{E}\to)}{\Gamma \vdash \bot}\,(\mathrm{E}\neg)}{\beta, \neg\gamma \vdash \neg(\beta \to \gamma)}\,(\mathrm{W}\neg)$$

(3) $\neg\beta, \neg\gamma \vdash \neg(\beta \vee \gamma)$

Oznaczenie: $\Gamma = \{\neg\beta, \neg\gamma, \beta \vee \gamma\}$

$$\dfrac{\dfrac{\Gamma \vdash \beta \vee \gamma \qquad \dfrac{\Gamma, \beta \vdash \beta \quad \Gamma, \beta \vdash \neg\beta}{\Gamma, \beta \vdash \bot}\,(\mathrm{E}\neg) \qquad \dfrac{\Gamma, \gamma \vdash \gamma \quad \Gamma, \gamma \vdash \neg\gamma}{\Gamma, \gamma \vdash \bot}}{\Gamma \vdash \bot}\,(\mathrm{E}\vee)}{\neg\beta, \neg\gamma \vdash \neg(\beta \vee \gamma)}\,(\mathrm{E}\bot)$$

(5) $\neg\beta \vdash \beta \to \gamma$

$$\dfrac{\dfrac{\dfrac{\neg\beta, \beta \vdash \neg\beta \qquad \neg\beta, \beta \vdash \beta}{\neg\beta, \beta \vdash \bot}\,(\mathrm{E}\neg)}{\neg\beta, \beta \vdash \gamma}\,(\mathrm{E}\bot)}{\neg\beta \vdash \beta \to \gamma}\,(\mathrm{W}\to)$$

(6) $\gamma \vdash \beta \to \gamma$

$$\frac{\gamma, \beta \vdash \gamma}{\gamma \vdash \beta \to \gamma}\,(\mathrm{W}\to)$$

(7) $\vdash \neg\bot$

$$\frac{\bot \vdash \bot}{\vdash \neg\bot}\,(\mathrm{W}\neg)$$

(9) $\beta \vdash \neg\neg\beta$

$$\dfrac{\dfrac{\beta, \neg\beta \vdash \beta \qquad \beta, \neg\beta \vdash \neg\beta}{\beta, \neg\beta \vdash \bot}\,(\mathrm{E}\neg)}{\beta \vdash \neg\neg\beta}\,(\mathrm{W}\neg)$$

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. (Porządny dowód jest przez indukcję.)

Lemat 3 (Reguła cięcia):

Jeśli $\Gamma \vdash \alpha$ oraz $\Gamma, \alpha \vdash \beta$, to $\Gamma \vdash \beta$.

Dowód:

$$\dfrac{\dfrac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \to \beta}\,(\mathrm{W}\to) \qquad \Gamma \vdash \alpha}{\Gamma \vdash \beta}\,(\mathrm{E}\to)$$

Wniosek:
Jeśli $\Gamma \vdash \alpha_1, \ldots, \Gamma \vdash \alpha_n$, oraz $\Gamma, \alpha_1 \ldots, \alpha_n \vdash \beta$, to $\Gamma \vdash \beta$.

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:

$$\dfrac{\Gamma \vdash \gamma \vee \neg\gamma \qquad \Gamma, \gamma \vdash \alpha \qquad \Gamma, \neg\gamma \vdash \alpha}{\Gamma \vdash \alpha}$$

Lemat Kalmára

Oznaczenie: Dla dowolnej interpretacji zdaniowej ϱ i dowolnej formuły α przyjmijmy, że

$$\alpha^{\varrho} = \begin{cases} \alpha, & \text{jeśli } [\![\alpha]\!]_{\varrho} = 1; \\ \neg\alpha, & \text{w przeciwnym przypadku.} \end{cases}$$

Na przykład jeśli $\varrho(p) = 0$ i $\varrho(q) = 1$, to $q^{\varrho} = q$, $p^{\varrho} = \neg p$ oraz $((p \to q) \to p)^{\varrho} = \neg((p \to q) \to p)$.

Lemat Kalmára: *Niech $p_1, \ldots, p_n$ będą wszystkimi symbolami zdaniowymi występującymi w formule α. Wówczas $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \alpha^{\varrho}$, dla dowolnego ϱ.*

Czyli na przykład $q, \neg p \vdash \neg((p \to q) \to p)$.

Lemat Kalmára

Jeśli w formule α występują tylko symbole $p_1, \ldots, p_n$, to $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \alpha^{\varrho}$.

Dowód: Indukcja ze względu na długość formuły α.

Przypadek 1: Jeśli $\alpha = p_i$, to $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash p_i^{\varrho}$ jest aksjomatem.

Przypadek 2: Jeśli $\alpha = \bot$, to $\alpha^{\varrho} = \neg\bot$. A skoro $\vdash \neg\bot$, to także $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg\bot$ (osłabianie).

Podobnie dla $\alpha = \top$.

Dowód lematu Kalmára

Przypadek 3: Niech $\alpha = \beta \to \gamma$.

Jeśli $[\![\alpha]\!]_{\varrho} = 0$ to $[\![\beta]\!]_{\varrho} = 1$ i $[\![\gamma]\!]_{\varrho} = 0$. Formuły β i γ są krótsze od α, więc $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \beta$ oraz $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg\gamma$ z założenia indukcyjnego. Z lematu 1(2) wiadomo, że $\beta, \neg\gamma \vdash \neg(\beta \to \gamma)$. Używając osłabiania i reguły cięcia dostaniemy $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg(\beta \to \gamma)$.

Jeśli $[\![\alpha]\!]_{\varrho} = 1$, to albo $[\![\beta]\!]_{\varrho} = 0$ albo $[\![\gamma]\!]_{\varrho} = 1$.
W pierwszym przypadku z założenia indukcyjnego wiemy, że $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg\beta$, a w drugim, że $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \gamma$. W obu przypadkach potrafimy udowodnić $\beta \to \gamma$ z lematu 1(5,6).

Dowód lematu Kalmára

Przypadek 4: Załóżmy, że $\alpha = \beta \vee \gamma$ i niech $[\![\alpha]\!]_{\varrho} = 1$. Zatem $[\![\beta]\!]_{\varrho} = 1$ lub $[\![\gamma]\!]_{\varrho} = 1$. Wtedy jedna z formuł β, γ ma dowód przy założeniach $p_1^{\varrho}, \ldots, p_n^{\varrho}$ i stosując regułę wprowadzania alternatywy od razu dostajemy $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \beta \vee \gamma$.

Jeśli natomiast $[\![\alpha]\!]_{\varrho} = 0$, to z założenia indukcyjnego wynika, że mamy dowody dla osądu $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg\gamma$ oraz dla osądu $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg\beta$. Ale z lematu 1(3) mamy $\neg\beta, \neg\gamma \vdash \neg(\beta \vee \gamma)$, skąd wynika $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg(\beta \vee \gamma)$.

Dowód lematu Kalmára

Przypadek 5: Niech $\alpha = \beta \wedge \gamma$

Jeśli $[\![\alpha]\!]_{\varrho} = 1$, to $[\![\beta]\!]_{\varrho} = [\![\gamma]\!]_{\varrho} = 1$ i mamy dowody osądów $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \beta$ i $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \gamma$. Pozostaje zastosować regułę (W$\wedge$).

Jeśli $[\![\alpha]\!]_{\varrho} = 0$, to jedna z wartości $[\![\beta]\!]_{\varrho}$, $[\![\gamma]\!]_{\varrho}$ jest zerem, istnieje więc dowód osądu $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg\beta$ lub dowód osądu $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg\gamma$. Można teraz skorzystać z tego, że $\neg\beta \vdash \neg(\beta \wedge \gamma)$ oraz $\neg\gamma \vdash \neg(\beta \wedge \gamma)$.

Dowód lematu Kalmára

Przypadek 6: Niech $\alpha = \neg\beta$.

Jeśli $[\![\alpha]\!]_{\varrho} = 1$, to $[\![\beta]\!]_{\varrho} = 0$
i z założenia indukcyjnego $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg\beta$.

W przeciwnym razie, $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \beta$, a skoro $\beta \vdash \neg\neg\beta$ (lemat 1(9)), to też $p_1^{\varrho}, \ldots, p_n^{\varrho} \vdash \neg\alpha$.

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 $p_1, \ldots, p_n$ będą wszystkimi symbolami zdaniowymi w formule α. Udowodnimy, że dla dowolnego $m \leq n$ i dowolnego ϱ zachodzi $p_1^\varrho, \ldots, p_m^\varrho \vdash \alpha$.
Przyjmując $m = 0$ otrzymamy $\vdash \alpha$.

Dowód przebiega przez indukcję ze względu na $n - m$.
Dla $m = n$ teza wynika z lematu Kalmára.

Krok indukcyjny

Założenie indukcyjne:
$p_1^\varrho, \ldots, p_m^\varrho, p_{m+1}^\varrho \vdash \alpha$, dla dowolnego ϱ.

Teza:
$p_1^\varrho, \ldots, p_m^\varrho, \vdash \alpha$, dla dowolnego ϱ.

Weźmy dowolne ϱ. Z założenia indukcyjnego wynika, że

$p_1^\varrho, \ldots, p_m^\varrho, p_{m+1} \vdash \alpha$ oraz $p_1^\varrho, \ldots, p_m^\varrho, \neg p_{m+1} \vdash \alpha$

Pozostaje skorzystać z lematu 4

(*Jeśli* $\Gamma, \gamma \vdash \alpha$ *oraz* $\Gamma, \neg\gamma \vdash \alpha$, *to* $\Gamma \vdash \alpha$.)

Nieco silniejsza wersja twierdzenia o pełności

Twierdzenie (łatwe) *Dla dowolnej formuły φ i dowolnego skończonego zbioru formuł Γ zachodzi równoważność:*

$\Gamma \models \varphi$ *wtw, gdy* $\Gamma \vdash \varphi$

Twierdzenie uogólnione: *Dla dowolnej formuły φ i dowolnego zbioru formuł Γ zachodzi równoważność:*

$\Gamma \models \varphi$ *wtw, gdy* $\Gamma \vdash \varphi$

Ale co znaczy $\Gamma \vdash \varphi$, jeśli Γ jest zbiorem nieskończonym?

Że istnieje taki skończony zbiór $\Gamma_0 \subseteq \Gamma$, że $\Gamma_0 \vdash \varphi$.

Nieco silniejsza wersja twierdzenia o pełności

Twierdzenie uogólnione: *Dla dowolnej formuły φ i dowolnego zbioru formuł Γ zachodzi równoważność:*

$\Gamma \models \varphi$ *wtw, gdy istnieje taki skończony zbiór* $\Gamma_0 \subseteq \Gamma$, *że* $\Gamma_0 \vdash \varphi$.

Twierdzenie (o zwartości): *Jeżeli $\Gamma \models \varphi$, to istnieje taki skończony podzbiór $\Gamma_0 \subseteq \Gamma$, że $\Gamma_0 \models \varphi$.*

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 $\Gamma \models \bot$. Z twierdzenia o zwartości istnieje więc skończony niespełnialny podzbiór.

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.

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:

$\alpha_a = (p_a^1 \vee p_a^2 \vee p_a^3) \wedge \neg(p_a^1 \wedge p_a^2) \wedge \neg(p_a^1 \wedge p_a^3) \wedge \neg(p_a^3 \wedge p_a^2)$,
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.*)

Kolorowanie nieskończonego grafu

$\alpha_a = (p_a^1 \vee p_a^2 \vee p_a^3) \wedge \neg(p_a^1 \wedge p_a^2) \wedge \neg(p_a^1 \wedge p_a^3) \wedge \neg(p_a^3 \wedge p_a^2)$

$\beta_{ab} = \neg(p_a^1 \wedge p_b^1) \wedge \neg(p_a^2 \wedge p_b^2) \wedge \neg(p_a^3 \wedge p_b^3)$

$\Gamma_H = \{\alpha_a \mid a \in H\} \cup \{\beta_{ab} \mid \langle a, b\rangle \in r \cap H \times H\}$, 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.

Naturalna dedukcja pierwszego rzędu

(Dygresja fakultatywna)

Wprowadzanie ∀

Weźmy dowolne y.	(*Cel:* $A(y)$)
⋮	
Zatem $A(y)$.	

Zatem $\forall x\, A(x)$.

$$\frac{\Gamma \vdash A(y)}{\Gamma \vdash \forall x\, A(x)} \quad y \notin \mathrm{FV}(\Gamma)$$

Eliminacja ∀

⋮
$\forall x\, A(x)$
⋮
Ponieważ $\forall x\, A(x)$, więc $A(t)$.

gdzie t jest dowolnym termem (także zmienną).

$$\frac{\Gamma \vdash \forall x\, A(x)}{\Gamma \vdash A(t)}$$

Wprowadzanie ∃

⋮
$A(t)$
⋮
Ponieważ $A(t)$, więc $\exists x\, A(x)$

gdzie t jest dowolnym termem.

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x\, A(x)}$$

Eliminacja ∃

$\exists x\, A(x)$
⋮

Niech y będzie takie, że $A(y)$	(*Cel:* B)
⋮	
Zatem B.	

Ponieważ $\exists x\, A(x)$, więc B.

$$\frac{\Gamma \vdash \exists x\, A(x) \quad \Gamma, A(y) \vdash B}{\Gamma \vdash B} \quad (y \notin \mathrm{FV}(\Gamma) \cup \mathrm{FV}(B))$$

Przykład: $\forall x(P(x) \to C),\ \exists y\, P(y) \vdash C$

Załóżmy, że $\forall x(P(x) \to C)$ oraz $\exists y\, P(y)$	(*Cel 1:* C)
Niech y będzie takie, że $P(y)$.	(*Cel 2:* C)
Ponieważ $\forall x(P(x) \to C)$, więc $P(y) \to C$.	
Ponieważ $P(y)$ oraz $P(y) \to C$, więc C.	

Ponieważ $\exists y\, P(y)$, więc C

Oznaczenie: $\Gamma = \{\forall x(P(x) \to C), \exists y\, P(y)\}$

$$\dfrac{\Gamma \vdash \exists y\, P(y) \qquad \dfrac{\dfrac{\Gamma, P(y) \vdash \forall x(P(x) \to C)}{\Gamma, P(y) \vdash P(y) \to C} \qquad \Gamma, P(y) \vdash P(y)}{\Gamma, P(y) \vdash C}}{\Gamma \vdash C}$$

Przykład: $\exists x \forall y\, P(x,y) \to \forall y \exists x\, P(x,y)$

Załóżmy $\exists x \forall y\, P(x,y)$	(*Cel:* $\forall y \exists x\, P(x,y)$)
Weźmy dowolne $\overline{y}$.	(*Cel:* $\exists x\, P(x,\overline{y})$)
Niech $\overline{x}$ będzie takie, że $\forall y\, P(\overline{x},y)$.	(*Cel:* $\exists x\, P(x,\overline{y})$)
Ponieważ $\forall y\, P(\overline{x},y)$, więc $P(\overline{x},\overline{y})$.	
Ponieważ $P(\overline{x},\overline{y})$, więc $\exists x\, P(x,\overline{y})$.	
Ponieważ $\exists x \forall y\, P(x,y)$, więc $\exists x\, P(x,\overline{y})$.	
Zatem $\forall y \exists x\, P(x,y)$.	

Zatem $\exists x \forall y\, P(x,y) \to \forall y \exists x\, P(x,y)$.

Ćwiczenie: Napisać dowód formalny.

Twierdzenie o pełności

Następujące warunki są równoważne:

- Formuła φ jest prawdziwa w dowolnej interpretacji.
- Osąd $\vdash \varphi$ ma dowód.

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 $\Gamma_0 \models \varphi$.*

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 $\Gamma \models \bot$. Z twierdzenia o zwartości istnieje więc skończony niespełnialny podzbiór.

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

$$\begin{aligned}\alpha_n = \; & r(x_2, x_1) \wedge \neg r(x_1, x_2) \wedge \\ & r(x_3, x_2) \wedge \neg r(x_2, x_3) \wedge \\ & \ldots \\ & r(x_n, x_{n-1}) \wedge \neg r(x_{n-1}, x_n)\end{aligned}$$

(Sens: wartości $x_1, x_2, \ldots, x_n$ 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.

Jeszcze o porządkach

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 $c \leq a$.

Kraty zupełne

Zbiór uporządkowany $\langle A, \leq \rangle$ jest *kratą zupełną* wtedy i tylko wtedy, gdy każdy podzbiór A ma kres górny.

- Zbiór potęgowy $\mathrm{P}(X)$ jest kratą zupełną (dla każdego X). Kresem dolnym niepustej rodziny zbiorów jest iloczyn, a kresem górnym suma.
- Zbiór wypukłych podzbiorów płaszczyzny jest kratą zupełną. Kresem dolnym niepustej rodziny zbiorów jest iloczyn, a kresem górnym?
- Zbiór funkcji częściowych $\langle \mathbb{N} \rightharpoonup \mathbb{N}, \subseteq \rangle$ nie jest kratą zupełną.

Fakt

W kracie zupełnej istnieje element najmniejszy $\bot$ 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 $x \leq c$. $\square$

Punkty stałe

Niech $\langle A, \leq \rangle$ i $\langle B, \leq \rangle$ będą porządkami częściowymi.

- Funkcja $f : A \to B$ jest *monotoniczna*, gdy $x \leq y$ implikuje $f(x) \leq f(y)$.
- Jeśli $f : A \to A$ oraz $f(a) = a$, to mówimy, że a jest *punktem stałym* funkcji f.

Przykład

Niech $f : \mathrm{P}(\mathbb{N}) \to \mathrm{P}(\mathbb{N})$ 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 $\{1, 3, 7\} = \mathrm{lfp}(f)$.

Twierdzenie o punkcie stałym (Tarski-Knaster)

Jeśli $\langle A, \leq \rangle$ jest kratą zupełną, to każda monotoniczna funkcja $f : A \to A$ 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. □

Przykład

Niech $f : \mathrm{P}(\mathbb{N}) \to \mathrm{P}(\mathbb{N})$ będzie taką funkcją, że dla $X \subseteq \mathbb{N}$:

$$f(X) = \{0\} \cup (X \cap \{1, 2\}).$$

Wtedy:

$B = \{X \in \mathrm{P}(\mathbb{N}) \mid f(X) \subseteq X\} = \{X \subseteq \mathbb{N} \mid 0 \in X\}$,

$\mathrm{lfp}(f) = \{0\}$

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 $\varphi : \mathrm{P}(A \times A) \to \mathrm{P}(A \times A)$ będzie taka:

$$\varphi(s) = r \cup s \cup (s \cdot s).$$

Punkty stałe funkcji φ to relacje przechodnie zawierające r. Inaczej: rozwiązania równania $s = r \cup s \cup (s \cdot s)$. (Ćwiczenie)

Najmniejszy punkt stały φ to domknięcie przechodnie relacji r.

Przykład

Niech V będzie przestrzenią liniową nad $\mathbb{R}$. Ustalmy $Z \subseteq V$ i niech $F : \mathrm{P}(V) \to \mathrm{P}(V)$ 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.

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.

Motywujący przykład

Rozpatrzmy program (definicję funkcji):

$$f(m, n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } f(m + 3, n) + 3.$$

Mamy tu w istocie równanie postaci $f = \Phi(f)$.

Znaczeniem tego programu jest funkcja $f : \mathbb{Z} \times \mathbb{Z} \rightharpoonup \mathbb{Z}$, która jest punktem stałym przekształcenia

$$\Phi : (\mathbb{Z} \times \mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \times \mathbb{Z} \rightharpoonup \mathbb{Z})$$
$$\Phi(f)(m, n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } f(m + 3, n) + 3.$$

Motywujący przykład

Przekształcenie $\Phi : (\mathbb{Z} \times \mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \times \mathbb{Z} \rightharpoonup \mathbb{Z})$

$$\Phi(f)(m, n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } f(m + 3, n) + 3$$

ma różne punkty stałe, na przykład:

- $f_1(m, n) = n - m$;
- $f_2(m, n) = \texttt{if } 3|(n - m) \texttt{ then } n - m \texttt{ else } 7 - m$;
- $f_0(m, n) = \texttt{if } n \geq m \wedge 3|(n - m) \texttt{ then } n - m \texttt{ else } \bot$.

Nas interesuje *najmniejszy* punkt stały f_0. Dlaczego?

Motywujący przykład

Najmniejszym rozwiązaniem równania

$$f(m,n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } f(m+3,n)+3$$

jest funkcja

$$f_0(m,n) = \texttt{if } n \geq m \wedge 3|(n-m) \texttt{ then } n-m \texttt{ else } \bot.$$

Jest to kres górny ciągu przybliżeń:

$\texttt{if } m = n \texttt{ then } 0 \texttt{ else } \bot$;

$\texttt{if } m = n \texttt{ then } 0 \texttt{ else if } m+3 = n \texttt{ then } 0+3 \texttt{ else } \bot$;

i tak dalej.

Motywujący przykład: Semantyka denotacyjna

Znaczeniem programu:

$$f(m,n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } f(m+3,n)+3$$

jest $f_0 : \mathbb{Z}\times\mathbb{Z} \rightharpoonup \mathbb{Z}$, która jest najmniejszym punktem stałym przekształcenia

$$\Phi : (\mathbb{Z}\times\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z}\times\mathbb{Z} \rightharpoonup \mathbb{Z})$$

$$\Phi(f)(m,n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } f(m+3,n)+3.$$

Fakt: To przekształcenie jest monotoniczne:
jeśli $g \subseteq h$ to $\Phi(g) \subseteq \Phi(h)$.

ale...

niestety...

- Zbiór funkcji częściowych $\langle A \rightharpoonup B, \subseteq\rangle$ nie jest kratą zupełną (o ile B ma co najmniej dwa elementy).

Na szczęście:

- W zbiorze $\langle A \rightharpoonup B, \subseteq\rangle$ 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 $x \in \mathrm{Dom}(f) \cap \mathrm{Dom}(g)$ zachodzi $f(x) = g(x)$.)

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 $\bot = \sup\varnothing$.

Fakt: Każdy łańcuch jest zbiorem skierowanym.
A zatem w każdym cpo istnieją kresy wszystkich łańcuchów.

Przykłady

- Każda krata zupełna jest zupełnym porządkiem częściowym.
- Zbiór funkcji częściowych $\langle \mathbb{N} \rightharpoonup \mathbb{N}, \subseteq\rangle$ nie jest kratą zupełną, ale jest zupełnym porządkiem częściowym. (Uwaga: nie każda rodzina zgodna jest skierowana, ale każda skierowana jest zgodna.)
- Zbiór $\mathbb{N}_\bot = \mathbb{N} \cup \{\bot\}$ uporządkowany w ten sposób, że
  - nowy element $\bot$ jest najmniejszy;
  - różne liczby naturalne są nieporównywalne,

  jest zupełnym porządkiem częściowym.

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 $f : A \to B$ 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 $f(x) \leq f(y)$. □

Twierdzenie o punkcie stałym (Kleene)

Jeśli $\langle A, \leq\rangle$ jest cpo, to każda funkcja ciągła $f : A \to A$ ma najmniejszy punkt stały, którym jest $\sup\{f^n(\bot) \mid n \in \mathbb{N}\}$.

Dowód: Oczywiście $\bot \leq f(\bot)$. Ponieważ f jest monotoniczna, więc ciąg $f^n(\bot)$ jest wstępujący (indukcja):

$$\bot \leq f(\bot) \leq f^2(\bot) \leq f^3(\bot) \leq \cdots$$

Zbiór $\{f^n(\bot) \mid n \in \mathbb{N}\}$ jest więc skierowany i z ciągłości:

$$f(\sup\{f^n(\bot) \mid n \in \mathbb{N}\}) = \sup\{f^{n+1}(\bot) \mid n \in \mathbb{N}\} = \sup\{f^n(\bot) \mid n \in \mathbb{N}\},$$

czyli $a = \sup\{f^n(\bot) \mid n \in \mathbb{N}\}$ jest punktem stałym.

Jeśli b jest innym punktem stałym, to z nierówności $\bot \leq b$ wynika przez indukcję $f^n(\bot) \leq f^n(b) = b$, skąd $a \leq b$. □

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 $f : \mathrm{P}(A\times A) \to \mathrm{P}(A\times A)$ 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:

$$\varnothing \subseteq \varphi(\varnothing) \subseteq \varphi^2(\varnothing) \subseteq \ldots$$

Uwaga: $\varphi(\varnothing) = r_0 = r$, $\varphi^2(\varnothing) = r_1 = r \cup (r \cdot r)$, i tak dalej.

Wracamy do naszego przykładu

Rozpatrzmy program (definicję funkcji):

$$f(m,n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } f(m+3,n)+3$$

Znaczeniem tego programu jest funkcja $f_0 : \mathbb{Z}\times\mathbb{Z} \multimap \mathbb{Z}$, która jest najmniejszym punktem stałym przekształcenia

$$\Phi : (\mathbb{Z}\times\mathbb{Z} \multimap \mathbb{Z}) \to (\mathbb{Z}\times\mathbb{Z} \multimap \mathbb{Z})$$

$$\Phi(f)(m,n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } f(m+3,n)+3.$$

Fakt: To przekształcenie jest ciągłe: jeśli $\mathcal{R}$ jest skierowaną rodziną funkcji częściowych, to $\Phi(\sup\mathcal{R}) = \sup\Phi(\mathcal{R})$.

Semantyka denotacyjna

Najmniejszym rozwiązaniem równania

$$f(m,n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } f(m+3,n)+3$$

jest funkcja

$$f_0(m,n) = \texttt{if } n \geq m \wedge 3|(n-m) \texttt{ then } n-m \texttt{ else } \bot.$$

Jest to kres górny ciągu przybliżeń:

$\bot(m,n) = \bot$;

$\Phi(\bot)(m,n) = \texttt{if } m = n \texttt{ then } 0 \texttt{ else } \bot$

$\Phi^2(\bot)(m,n) =$
$\texttt{if } m = n \texttt{ then } 0 \texttt{ else if } m+3 = n \texttt{ then } 0+3 \texttt{ else } \bot$

i tak dalej.

Jeszcze jeden przykład punktu stałego: palindromy

adapannapocałowanawołacopannapada

napotkałatypazapytałaktopan

Gramatyka dla palindromów

Palindromy nad alfabetem $\{a,b\}$:

$$X ::= \varepsilon \mid a \mid b \mid a\,X\,a \mid b\,X\,b$$

- Słowo puste i słowa jednoliterowe są palindromami.
- Jeśli X jest palindromem, to $a\,X\,a$ jest palindromem.
- Jeśli X jest palindromem, to $b\,X\,b$ 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.

Palindromy: $X ::= \varepsilon \mid a \mid b \mid a\,X\,a \mid b\,X\,b$

Zbiór $\mathcal{P}$ to najmniejszy (bo jedyny) punkt stały przekształcenia

$$F : \mathrm{P}(\{a,b\}^*) \to \mathrm{P}(\{a,b\}^*):$$

$$F(B) = \{\varepsilon, a, b\} \cup \{aXa \mid X \in B\} \cup \{bXb \mid X \in B\}.$$

Jest to suma ciągu przybliżeń $F^n(\varnothing)$:

$\varnothing$,

$F(\varnothing) = \{\varepsilon, a, b\}$,

$F(\{\varepsilon, a, b\}) = \{\varepsilon, a, b, aa, bb, aaa, bab, aba, bbb\}$,

$F(\{\varepsilon, a, b, aa, bb, aaa, bab, aba, bbb\}) =$
$= \{\varepsilon, a, b, aaa, bab, aba, bbb, aaaaa, \dots\}$

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

$$X = \{\varepsilon\} \cup \{(x)y \mid x,y \in X\}?$$

Relacje równoważności

Przypomnienie

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

- $\forall x{\in}A\,(x\,r\,x)$;
- $\forall x,y{\in}A\,(x\,r\,y \to y\,r\,x)$;
- $\forall x,y,z{\in}A\,(x\,r\,y \wedge y\,r\,z \to x\,r\,z)$.

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

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

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.

Konstrukcje ilorazowe

Nowe typy można definiować jako ilorazy.

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:

$$\langle m,n\rangle \sim \langle m',n'\rangle \quad\Leftrightarrow\quad m+n'=m'+n$$

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 $\mathbb{N}\times\mathbb{N}/_\sim$.

Liczby wymierne

Liczby wymierne (ułamki) to pary liczb całkowitych z dokładnością do (częściowej) relacji równoważności

$$\langle x,y\rangle \approx \langle u,v\rangle \quad\Leftrightarrow\quad (y,v\neq 0 \ \wedge\ x\cdot v = u\cdot y)$$

Oczywiście zamiast $[\langle x,y\rangle]_\approx$ piszemy $\frac{x}{y}$.

Liczby rzeczywiste

Ciąg Cauchy'ego to taki ciąg f liczb (wymiernych), że

$$\forall\varepsilon{:}\mathbb{Q}\,(\varepsilon>0\to\exists n{:}\mathbb{N}\,\forall k{:}\mathbb{N}(k\geq n\to|f(n)-f(k)|<\varepsilon))$$

Liczby rzeczywiste to ciągi Cauchy'ego liczb wymiernych z dokładnością do relacji równoważności $\equiv$:

$f\equiv g$ wtedy i tylko wtedy, gdy
$\forall\varepsilon{:}\mathbb{Q}\,(\varepsilon>0\to\exists n\,\forall k\,(k\geq n\to|f(k)-g(k))|<\varepsilon))$.

Dwa naturalne przekształcenia

- *Kanoniczna surjekcja* $\kappa : A\to A/_\mathsf{r}$ (jest jedna taka)
  $$\kappa(a)=[a]_r$$
- *Funkcja wyboru* $\sigma : A/_\mathsf{r}\to A$ (mogą być różne takie)
  $$\sigma([a]_r)\in[a]_r$$

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.

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.:

$$\forall a\in\mathcal{R}\,\exists t\in a\,(S\cap a=\{t\}).$$

Wierzymy, 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. □

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 $A_1 \times \cdots \times A_n$ składa się z krotek postaci $\langle a_1, \ldots, a_n \rangle$. 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* $\{A_t\}_{t \in T}$?

Produkt uogólniony

Produkt uogólniony rodziny indeksowanej $\{A_t\}_{t \in T}$ podzbiorów $\mathcal{D}$, to zbiór

$$\prod_{t \in T} A_t = \{f : T \to \mathcal{D} \mid \forall t \in T. f(t) \in A_t\}$$

$$f \in \prod_{t \in T} A_t \quad \Leftrightarrow \quad \mathrm{Dom}(f) = T \quad \wedge \quad \forall t \in T.\, f(t) \in A_t.$$

Uwaga:
Jeśli $A_t = A$, dla wszystkich $t \in T$, to $\prod_{t \in T} A_t = A^T$.

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. $\forall t\, A(t) \vee \forall t\, B(t)$

Niepustość produktu

Twierdzenie
Jeśli $\{A_t\}_{t \in T}$ jest rodziną indeksowaną zbiorów niepustych, to produkt $\Pi_{t \in T} A_t$ 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 $f \in \prod_{t \in T} A_t$. □

Twierdzenie

Załóżmy, że $A \neq \varnothing$. Wtedy:

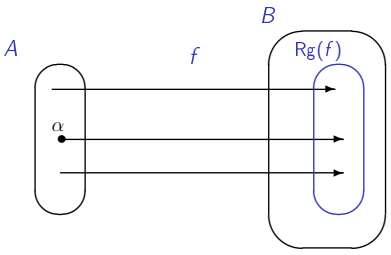
1) *Jeśli $f : A \xrightarrow{1-1} B$ to istnieje $g : B \xrightarrow{\text{na}} A$, że $g \circ f = \mathrm{id}_A$.*
2) *Jeśli $g : B \xrightarrow{\text{na}} A$ to istnieje $f : A \xrightarrow{1-1} B$, że $g \circ f = \mathrm{id}_A$.*

Wniosek

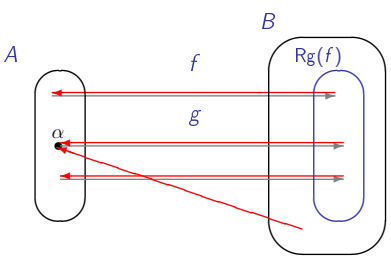
Jeśli $A \neq \varnothing$, to następujące warunki są równoważne:

1) *Istnieje funkcja $f : A \xrightarrow{1-1} B$;*
2) *Istnieje funkcja $g : B \xrightarrow{\text{na}} A$.*

Jeśli $A \neq \varnothing$ i $f : A \xrightarrow{1-1} B$ to istnieje takie $g : B \xrightarrow{\text{na}} A$, że $g \circ f = \mathrm{id}_A$.

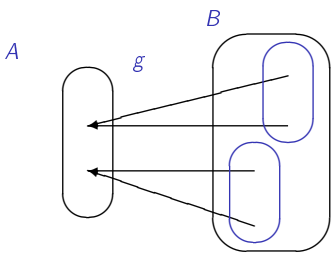


Jeśli $A \neq \varnothing$ i $f : A \xrightarrow{1-1} B$ to istnieje takie $g : B \xrightarrow{\text{na}} A$, że $g \circ f = \mathrm{id}_A$.

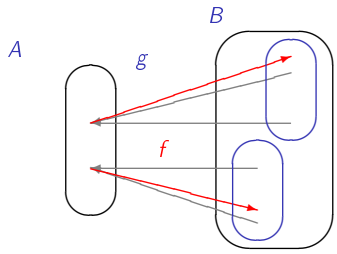


$$g(b) = \texttt{if } b \in \mathrm{Rg}(f) \texttt{ then } f^{-1}(b) \texttt{ else } \alpha$$

Jeśli $g : B \xrightarrow{\text{na}} A$ to istnieje takie $f : A \xrightarrow{1-1} B$, że $g \circ f = \mathrm{id}_A$.



Jeśli $g : B \xrightarrow{\text{na}} A$ to istnieje takie $f : A \xrightarrow{1-1} B$, że $g \circ f = \mathrm{id}_A$.



$$f \in \prod_{a \in A} g^{-1}(\{a\}) \neq \varnothing$$

Twierdzenie
Suma przeliczalnej rodziny zbiorów przeliczalnych jest przeliczalna.

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

- Istnieje funkcja $F : \mathbb{N} \xrightarrow{\text{na}} \mathcal{A}$.
- Istnieją funkcje $f_m : \mathbb{N} \xrightarrow{\text{na}} F(m)$.

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 $G : \mathbb{N} \times \mathbb{N} \to \bigcup \mathcal{A}$ jest na $\bigcup \mathcal{A}$.

Zatem $\bigcup \mathcal{A}$ jest zbiorem przeliczalnym. □

Twierdzenie
Suma przeliczalnej rodziny zbiorów przeliczalnych jest przeliczalna.

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

- Istnieje funkcja $F : \mathbb{N} \xrightarrow{\text{na}} \mathcal{A}$.
- Istnieją funkcje $f : \mathbb{N} \xrightarrow{\text{na}} F(m)$.

Niech $F_m = \{f \mid f : \mathbb{N} \xrightarrow{\text{na}} F(m)\}$ 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 $G : \mathbb{N} \times \mathbb{N} \to \bigcup \mathcal{A}$ jest na $\bigcup \mathcal{A}$.

Zatem $\bigcup \mathcal{A}$ jest zbiorem przeliczalnym. □

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 $k_1 v_1 + \cdots + k_n v_n = 0$, gdzie $v_1, \ldots, v_n \in A$, wynika $k_1 = \cdots = k_n = 0$.

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.

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 $Ł$ będzie łańcuchem w Z i niech $B = \bigcup Ł$.
Pokażemy, że zbiór B jest liniowo niezależny.
Przypuśćmy $k_1 v_1 + \cdots + k_n v_n = 0$, gdzie $v_1, \ldots, v_n \in B$.
Wtedy $v_1 \in A_1, \ldots, v_n \in A_n$ dla pewnych $A_1, \ldots, A_n \in Ł$.
Któryś zbiór A_i jest największy; wtedy $v_1, \ldots, v_n \in A_i$.
Skoro A_i jest liniowo niezależny oraz $k_1 v_1 + \cdots + k_n v_n = 0$, to $k_1 = \cdots = k_n = 0$.
Zatem zbiór $B = \bigcup Ł$ jest liniowo niezależny, tj. $B \in Z$.
Oczywiście B jest ograniczeniem górnym dla $Ł$.
A więc każdy łańcuch ma ograniczenie górne. (*)

Pokazaliśmy, że spełniony jest warunek (*).
Zatem $\langle Z, \subseteq \rangle$ ma element maksymalny. □

Każda przestrzeń liniowa ma bazę

Cel 1: Każdy łańcuch jest ograniczony z góry.
Załóżmy, że $Ł$ jest łańcuchem. *Cel 2: $B = \bigcup Ł$ ogranicza $Ł$ w Z.*
Cel 3: $B \in Z$
Niech $k_1 v_1 + \cdots + k_n v_n = 0 \ldots$ *Cel 4: $k_1 = \cdots = k_n = 0$.*
⋮
Zatem $k_1 = \cdots = k_n = 0$ *(Cel 4 osiągnięty)*
Zatem B jest liniowo niezależny, tj. $B \in Z$ *(Cel 3 osiągnięty)*
Łatwo widzieć, że $\forall A. A \in Ł \to A \subseteq B$
Zatem B jest ograniczeniem $Ł$ w Z *(Cel 2 osiągnięty)*
Zatem każdy łańcuch ma ograniczenie górne *(Cel 1 osiągnięty)*
Z lematu Kuratowskiego-Zorna istnieje element maksymalny.

Zadanie

Niech A będzie ustalonym podzbiorem płaszczyzny, który ma przynajmniej dwa elementy. Udowodnić, że istnieje podzbiór $B \subseteq A$, o takich własnościach:

- Żadne trzy różne punkty zbioru B nie są współliniowe;
- Każdy punkt zbioru $A - B$ leży na pewnej prostej wyznaczonej przez dwa różne punkty ze zbioru B.

Jeśli A jest całą płaszczyzną, to wystarczy dowolny okrąg.

Ale jeśli A jest jakimś dziwnym zbiorem?

Zadanie

Niech A będzie podzbiorem płaszczyzny. Udowodnić, że istnieje zbiór $B \subseteq A$, o takich własnościach:

1. Żadne trzy różne punkty zbioru B nie są współliniowe;
2. Każdy punkt zbioru $A - B$ leży na pewnej prostej wyznaczonej przez dwa różne punkty ze zbioru B.

Potrzebujemy zbioru $B \subseteq A$ o własności (1), którego nie da się już powiększyć, bez utraty tej własności.

Czyli *maksymalnego* zbioru o własności (1).

Rozwiązanie

A – jakiś podzbiór płaszczyzny.

$\mathcal{W} = \{X \subseteq A \mid \text{żadne trzy punkty w } X \text{ nie są współliniowe}\}$.

Nasze B to element maksymalny w porządku $\langle \mathcal{W}, \subseteq \rangle$.
Czy taki element istnieje?

Użyjemy lematu Kuratowskiego-Zorna. Sprawdzamy warunek

(*) Każdy łańcuch ma w $\langle \mathcal{W}, \subseteq \rangle$ ograniczenie górne.

Rozwiązanie

$\mathcal{W} = \{X \subseteq A \mid \text{żadne trzy punkty w } X \text{ nie są współliniowe}\}$.

Sprawdzamy warunek

(*) Każdy łańcuch ma w $\langle \mathcal{W}, \subseteq \rangle$ ograniczenie górne.

Niech więc $Ł$ będzie łańcuchem w $\mathcal{W}$ i niech $S = \bigcup Ł$.

Wtedy $S \in \mathcal{W}$. Istotnie, jeśli $a, b, c \in S = \bigcup Ł$, to każdy z tych punktów należy do pewnego zbioru z łańcucha $Ł$. Jeden z tych trzech zbiorów zawiera pozostałe (bo $Ł$ jest łańcuchem) więc punkty a, b, c nie mogą być współliniowe.

Skoro $S = \bigcup Ł \in \mathcal{W}$, to S jest szukanym ograniczeniem łańcucha $Ł$. Sprawdziliśmy warunek (*).

Rozwiązanie

A – jakiś podzbiór płaszczyzny.

$\mathcal{W} = \{X \subseteq A \mid \text{żadne trzy punkty w } X \text{ nie są współliniowe}\}$.

Nasze B to element maksymalny w porządku $\langle \mathcal{W}, \subseteq \rangle$.
Czy taki element istnieje?

Tak, na mocy lematu Kuratowskiego-Zorna, bo zachodzi warunek

(*) Każdy łańcuch ma w $\langle \mathcal{W}, \subseteq \rangle$ ograniczenie górne.

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 $C_1, C_2, \ldots C_n$, oraz takie izometrie $\varphi_1, \ldots, \varphi_n$,
że $\varphi_1(C_1) \cup \cdots \cup \varphi_1(C_n) = K_1 \cup K_2$,
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

Dobre ufundowanie

Przypomnijmy:

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.)

Inna definicja dobrego ufundowania

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.

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:
  $$b \succ ab \succ aab \succ aaab \succ \cdots$$
- Dla dowolnego k, zbiór $\mathbb{N}^k$, złożony z k-krotek liczb naturalnych (słów długości k) jest dobrze uporządkowany przez porządek leksykograficzny.

Odcinki początkowe

Podzbiór B zbioru częściowo uporządkowanego A nazywamy *odcinkiem początkowym* w A, gdy
$$\forall x, y \in A\,(x \in B \wedge y \leq x \to y \in B).$$

Szczególny przypadek odcinka początkowego, to odcinek wyznaczony przez element $x \in A$:
$$\mathcal{O}_A(x) = \{y \in A \mid y < x\}.$$

Dendrologia

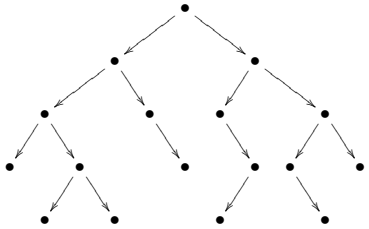
Zbiór częściowo uporządkowany $\langle T, \leq \rangle$ nazywamy *drzewem*, gdy spełnia on następujące warunki:

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.

Drzewa rosną z góry na dół.



Drzewo słów

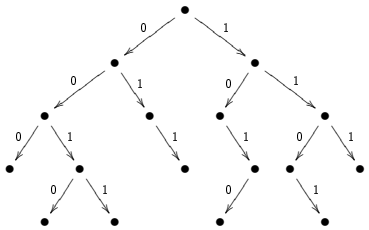
Niepusty podzbiór T zbioru A^* nazywamy *drzewem słów*, gdy jest on odcinkiem początkowym w $\langle A^*, \subseteq \rangle$, czyli gdy
$$\forall w, u \in A^*\,(w \cdot u \in T \to w \in T).$$

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.

Każde drzewo jest izomorficzne z pewnym drzewem słów.



$\{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 011,$
$101, 110, 111, 0010, 0011, 1010, 1101\}$

Definicje

- *Gałęzią* w drzewie T nazywamy dowolny ciąg postaci $\varepsilon = a_0, a_1, a_2, \ldots$ (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.

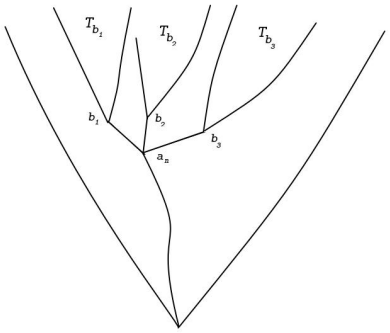
Lemat Königa

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 $\varepsilon = a_0, a_1, a_2, \ldots$ tak, aby każde T_{a_i} było nieskończone.

Krok bazowy jest poprawny, bo $T_\varepsilon = T$.



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 $\varepsilon = a_0, a_1, a_2, \ldots$ tak, aby każde T_{a_i} było nieskończone.

Krok bazowy jest poprawny, bo $T_\varepsilon = T$.

Niech T_{a_n} będzie nieskończony i niech $b_1, \ldots, b_k$ będą bezpośrednimi następnikami a_n. Ponieważ

$$T_{a_n} = \{a_n\} \cup T_{b_1} \cup \cdots \cup T_{b_k},$$

więc któreś T_{b_i} jest nieskończone.
Można przyjąć $a_{n+1} = b_i$. □

Przykład: Niech $f : \mathbb{N} \to \{0,1\}$. 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 $f : \mathbb{N} \to \{0,1\}$ istnieje świadek pitagorejski.

Przykład: Niech $f : \mathbb{N} \to \{0,1\}$. 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 $f : \mathbb{N} \to \{0,1\}$ istnieje świadek pitagorejski.

Wniosek: Istnieje taka stała N, że każda funkcja ma świadka pitagorejskiego mniejszego od N.

Dowód: Funkcje $f : \mathbb{N} \to \{0,1\}$ 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.


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

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

MATHEMATICS

Maths proof smashes size record

Supercomputer produces a 200-terabyte proof — but is it really mathematics?

BY EVELYN LAMB

Three computer scientists have announced the largest-ever mathematical proof: a file that comes in at a whopping 200 terabytes, equivalent to all the digitized text held by the US Library of Congress. The researchers have created[1] a 68-gigabyte compressed version of their solution — which would allow anyone with about 30,000 hours of spare processor time to download, reconstruct and verify it — but a human could never hope to read through it.

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 umpteen 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[2], 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 cheque 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.

Przykład: silna normalizacja

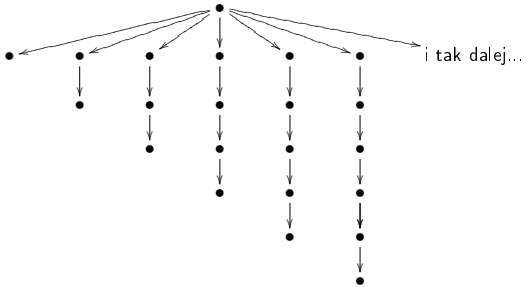
Definicja: Relacja $\to$ w zbiorze A ma własność *SN*, gdy nie istnieje ciąg nieskończony postaci

$$a_0 \to a_1 \to a_2 \to \cdots$$

Fakt: Załóżmy, że $\to$ ma własność SN, i że dla każdego a zbiór $\{b \mid a \to b\}$ jest skończony. Wtedy dla każdego a zbiór $\{b \in A \mid a \to^* b\}$ elementów osiągalnych z a jest skończony.

Dowód: Drzewo słów:
$T_a = \{a_0 a_1 \ldots a_k \mid a = a_0 \to a_1 \to a_2 \to \cdots \to a_k\}$
jest drzewem o skończonym rozgałęzieniu, ale nie ma nieskończonej gałęzi. Zatem musi być skończone.

Drzewo o nieskończonym rozgałęzieniu



Uporządkowanie dobre

czyli liniowe dobre ufundowanie

Dobre porządki

Przykłady dobre:

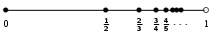
- Zbiór liczb naturalnych $\mathbb{N}$;
- Każdy skończony liniowy porządek;
- Zbiór $\mathbb{N}^k$ uporządkowany leksykograficznie.

Przykłady nie-dobre:

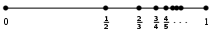
- Zbiór liczb całkowitych $\mathbb{Z}$;
- Odcinek $[0, 1]$;
- Zbiór $\mathbb{N}^*$ uporządkowany leksykograficznie.

Następujące nieizomorficzne podzbiory $\mathbb{R}$ są dobrze uporządkowane

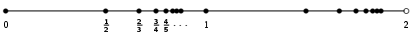
- $A = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$;



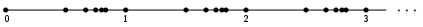
- $A' = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\} \cup \{1\}$;



- $A'' = A \cup \{2 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$;



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



Własności dobrych porządków

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.

Własności dobrych porządków

- *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.*

Liczby porządkowe

Konwencja: Każdemu dobremu porządkowi A przypisujemy jego *liczbę porządkową*, oznaczaną przez $\overline{A}$. Robimy to tak, aby zachodziła równoważność:

$\overline{A} = \overline{B}$ wtedy i tylko wtedy, gdy $A \approx B$.

Piszemy $\overline{A} \leq \overline{B}$, gdy A jest izomorficzny z pewnym odcinkiem początkowym w B.

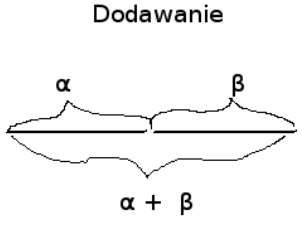
- Liczby porządkowe zbiorów skończonych to liczby naturalne.
- Liczba porządkowa zbioru $\mathbb{N}$ to ω.

Działania na liczbach porządkowych

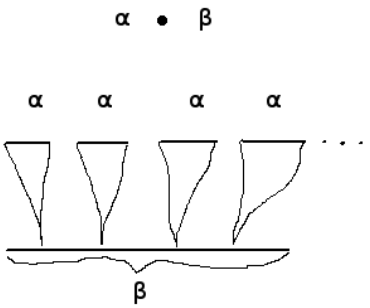
Niech $\overline{A} = \alpha$ i $\overline{B} = \beta$.

- Suma $\alpha + \beta$ to liczba porządkowa zbioru $A \oplus B$ uporządkowanego tak:
  $\langle x \rangle_i \leq \langle y \rangle_j \quad \Leftrightarrow \quad i < j$, lub $i = j$ oraz $x \leq y$.
- Iloczyn $\alpha \cdot \beta$ to liczba porządkowa zbioru $A \times B$ uporządkowanego „antyleksykograficznie”:
  $\langle a, b \rangle \leq \langle a', b' \rangle \quad \Leftrightarrow \quad b < b'$, lub $b = b'$ oraz $a \leq a'$.

Działania na liczbach porządkowych

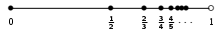


Mnożenie

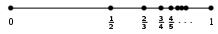


Przykłady

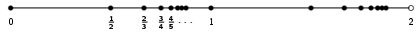
- $A = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$; (ω)



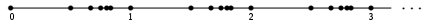
- $A' = \{1 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\} \cup \{1\}$; $(\omega + 1)$



- $A'' = A \cup \{2 - \frac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$; $(\omega + \omega = \omega \cdot 2)$



- $B = \{m - \frac{1}{n} \mid m, n \in \mathbb{N} - \{0\}\}$. $(\omega \cdot \omega)$



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.
- $2^\omega = \omega$.

Porządkowanie zbioru $\mathbb{N}^k$

Zwykły porządek $\leq$ w zbiorze $\mathbb{N}$ jest typu ω.

Porządek leksykograficzny w $\mathbb{N}^2$ jest typu $\omega \cdot \omega = \omega^2$:

$\langle 0,0\rangle < \langle 0,1\rangle < \langle 0,2\rangle < \cdots < \langle 1,0\rangle < \langle 1,1\rangle < \cdots < \langle 2,1\rangle < \ldots$

Porządek leksykograficzny w $\mathbb{N}^3$ jest typu $\omega^2 \cdot \omega = \omega^3$:

$\langle 0,0,0\rangle \ldots \langle 0,m,n\rangle \ldots \langle 1,m,n\rangle \ldots \langle 2,m,n\rangle \ldots$

Porządek leksykograficzny w $\mathbb{N}^k$ jest typu ω^k.

Multizbiory

Multizbiór to „zbiór z powtórzeniami" (funkcja $M : A \to \mathbb{N}$).

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 $M(x) = 0$.

Multizbiory skończone

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.)

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:

$\{0,0,0,0,0,1,1,1,2\} \leq \{0,1,1,2,3,3\} \leq \{0,1,3,6\}$

$\{0,0,0,0,1,2,3,3\} \leq \{0,1,1,2,3,3\} \leq \{1,2,2,3,3\}$

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.*

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.

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.

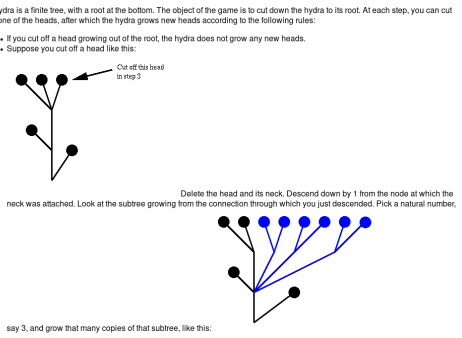
Może żądać w zamian dowolnej kwoty, ale wypłaconej w nominałach niższych niż ten oddany Bankowi.

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?

Achilles i hydra, czyli: *Może być gorzej niż ω^ω*



http://math.andrej.com/2008/02/02/the-hydra-game/

Jeszcze o liczbach porządkowych

Liczby porządkowe

Fakt: Jeśli α jest liczbą porządkową zbioru A, to

- Liczba β jest liczbą porządkową odcinka właściwego w A wtedy i tylko wtedy, gdy $\beta < \alpha$.
- A jest izomorficzny z $\{\beta \mid \beta < \alpha\}$.

Fakt: Każdy zbiór liczb porządkowych jest dobrze uporządkowany.

Dowód: Ciąg postaci $\alpha_0 > \alpha_1 > \cdots$ miałby swój odpowiednik w zbiorze uporządkowanym w liczbę $\alpha_0 + 1$.

Liczby porządkowe

Fakt: Każdy zbiór Γ liczb porządkowych o własności

$$\forall \alpha\beta(\alpha < \beta \in \Gamma \to \alpha \in \Gamma)$$

ma postać $\{\alpha \mid \alpha < \gamma\}$, dla pewnego γ.

Dowód: Liczba γ to liczba porządkowa zbioru Γ.

Twierdzenie (E. Zermelo)

Każdy zbiór można dobrze uporządkować.

Dowód: Niech $A \neq \varnothing$ i niech:

$\Gamma = \{\alpha \mid \alpha$ jest liczbą porządkową
jakiegoś podzbioru zbioru A
dobrze uporządkowanego przez jakąś relację.$\}$

Wtedy $\Gamma = \{\alpha \mid \alpha < \gamma\}$, gdzie $\gamma = \overline{\Gamma}$.

Niech φ będzie funkcją wyboru dla $\mathrm{P}(A) - \{\varnothing\}$.
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 $a_0 = \varphi(A)$, $a_\omega = \varphi(A - \{a_n \mid n \in \mathbb{N}\})$.

Dowód, ciąg dalszy

$\Gamma = \{\alpha \mid \alpha$ 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:

$$a_\delta \leq a_\beta \quad \Leftrightarrow \quad \delta \leq \beta.$$

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 $\gamma \notin \Gamma$.

Lemat Kuratowskiego-Zorna

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.

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

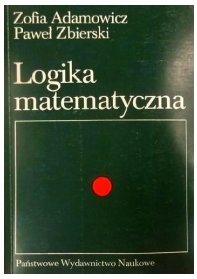
$$b_\alpha = \begin{cases} a_\alpha, & \text{jeśli } a_\alpha \text{ ogranicza z góry zbiór } \{b_\beta \mid \beta < \alpha\}; \\ a_0, & \text{w przeciwnym przypadku.} \end{cases}$$

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 $a_\alpha = d$.

Literatura dla dociekliwych

Logika i teoria zbiorów



Logika i teoria obliczeń