Jak upolować żywego lwa? Logika dla informatyków

(How to hunt a live lion? Logic for Computer Scientists)

Kamil Matuszewski

Praca magisterska

Promotor: dr Piotr Wieczorek

Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Informatyki

11 października 2021

Streszczenie

„Logika dla Informatyków" jest jednym z pierwszych przedmiotów obowiązkowych z którymi musi sobie poradzić każdy student informatyki na Uniwersytecie Wrocławskim. Mimo, że przedmiot nie jest trudny, to od wielu lat sprawia problemy studentom. Przez to, że logika znacznie różni się od poznanej w szkole średniej matematyki, niektórzy studenci mają problemy z opanowaniem początkowych tematów, a niezrozumienie poprzednich tematów jeszcze bardziej utrudnia zrozumienie dalszego materiału. Składająca się z części pisemnej i części audiowizualnej praca stanowi próbę stworzenia poradnika, który mógłby pomóc studentom pierwszego roku lepiej poradzić sobie z logiką i w efekcie mieć większe szanse by ukończyć studia na Uniwersytecie Wrocławskim.

„Logic for Computer Scientists" is one of the first mandatory classes that every computer science student at the University of Wrocław has to deal with. Although the subject is not difficult, it has been causing problems for students for many years. The fact that for many students logic is something completely different from the math they have learned in high school makes it difficult for them to master the starting material, and not understanding the first few topics makes it very difficult to understand the rest of the material. Consisting of a written part and an audiovisual part, the work is an attempt to create a guide that could help first-year students better cope with logic and, as a result, have a better chance of graduating from the University of Wrocław.

Spis treści

Rozdział 1.

Wprowadzenie

1.1. Wstęp

Przedmiot „Logika dla Informatyków" jest przedmiotem obowiązkowym, z którym każdy student Informatyki na Uniwersytecie Wrocławskim musi zdać już na pierwszym semestrze studiów. Choć z perspektywy czasu jest to przedmiot dość prosty, to co roku pojawiają się studenci, którzy nie potrafią sobie z nim samodzielnie poradzić. Wynika to głównie z tego, że jego tematyka różni się znacząco od treści nauczanych w szkołach średnich.

Poniższa praca jest szkicem podręcznika, który każdy student pierwszego roku mógłby przeczytać, w celu lepszego zrozumienia poszczególnych działów przedmiotu „Logika dla Informatyków". Podręcznik ten miałby być przystępny dla osób ze znajomością matematyki na poziomie szkoły średniej, jednak nie posiadających wiedzy z zakresu logiki matematycznej. Jako, że stworzenie obszernego podręcznika jest zadaniem wykraczającym poza wymagania pracy magisterskiej, praca ta jest jedynie koncepcją, przedstawiającą kilka wybranych zagadnień.

Praca powstała w oparciu o materiały ze skryptu do przedmiotu „Logkia dla Infomratyków" [1], a także skrypt „Wstęp do teorii mnogości i logiki" [2].

Oprócz części pisemnej, do pracy została załączona część audiowizualna, na której autor pracy, w formie „wykładu online" opowiada o wybranych zagadnieniach.

1.2. Część pisemna

Część pisemna pracy pisana była w oparciu o „Materiały do zajęć" i składa się z czterech tematów.

1. „Techniki dowodowe" jest rozdziałem wprowadzającym, w którym czytelnik zapozna się z pojęciem dowodu. Przedstawione w nim zostaną, na przykła-

dzie kilku prostych twierdzeń, popularne techniki dowodowe, dzięki którym czytelnik lepiej zrozumie czym jest dowód i jak powinno się przedstawiać tok rozumowania. Dzięki temu kolejne rozdziały, a także tematyka samego przedmiotu, powinny być bardziej przystępne.

2. „Indukcja Matematyczna" jest rozdziałem opisującym pierwszy temat, z którym spotykają się studenci na przedmiocie „Logika dla Informatyków". W tym rozdziale opisana jest indukcja matematyczna, wraz z podstawowymi definicjami a także przykładami użycia, dzięki którym czytelnik lepiej zrozumie czym jest indukcja matematyczna oraz jak powinno się jej używać.

3. Kolejny rozdział „Zbiory" zaczyna się od przedstawienia podstawowych definicji zbioru oraz operacji na zbiorach, następnie omawia tematykę rodzin zbiorów, na koniec skupiając się na zbiorach nieskończonych i operacjach na zbiorach nieskończonych. W tym rozdziale znajdują się także przykłady zadań, które pomogą zrozumieć definicje i ich zastosowanie.

4. W rozdziale „Relacje" zawarte są definicje pary, relacji, operacji na relacjach a także relacyjny rachunek dziedzin, oraz przykładowe zadania związane z tymi definicjami.

5. Ostatni rozdział, „Zakończenie" oprócz podsumowania pracy, przedstawia również jak można zastosować niektóre z przedstawionych wyżej tematów w praktyce. Pierwszy przykład pokaże, jak można użyć rozumowania indukcyjnego do udowodnienia czegoś o pewnym popularnym algorytmie, natomiast drugi przykład pokazuje, jak można przełożyć zapytanie w relacyjnym rachunku dziedzin na zapytanie w języku SQL.

1.3. Część audiowizualna

W skład części audiowizualnej wchodzi 28 filmików, o łącznej długości około 4 godzin. Na tych materiałach autor pracy opowiada o wybranych zagadnieniach przedmiotu „Logika dla Informatyków".

Część audiowizualna jest niezależna od części pisemnej: nie trzeba zapoznawać się z jedną, żeby zrozumieć drugą.

Materiały te stanowiły część projektu, w ramach którego na kanale „Logika dla Informatyków UWr" na portalu YouTube co tydzień przez 9 tygodni publikowane było omówienie materiału z danego tygodnia. Materiały, tworzone przez Kamila Matuszewskiego, Bartosza Bednarczyka oraz Annę Karykowską, udostępniane były następnie studentom.

Materiały czasem mogą wspominać części które tworzone były przez współautorów kanału „Logika dla informatyków UWr", zakładają też zrozumienie poprzednich materiałów w celu zrozumienia kolejnych.

Poniżej znajduje się spis materiałów, w kolejności, w której były one publikowane. W nawiasach dopisane zostały numery wykładów, oraz numer części którą dany materiał stanowił, jako część wszystkich materiałów opublikowanych w danym tygodniu.

- „Dowody Niekonstruktywne” (Wykład 0, część 3)
- „Silniejsza indukcja” 1, 2 i 3 (Wykład 1, część 5, 6 i 7)
- „Silna indukcja” 1 i 2 (Wykład 1, część 8 i 9)
- „Wstęp do rachunku zdań” 1 i 2 (Wykład 2, część 1 i 2)
- „Wartościowanie zmiennych i wartościowanie formuł” (Wykład 2, część 3)
- „Negacyjna postać normalna” 1 i 2 (Wykład 3, część 1 i 2)
- „Funkcje boolowskie” (Wykład 4, część 1)
- „Zbiory zupełne spójników: Definicja” (Wykład 4, część 2)
- „Rezolucja” 1, 2 i 3 (Wykład 4, część 5, 6 i 7)
- „Zbiory” 1, 2, 3 i 4 (Wykład 6, część 4, 5, 6 i 7)
- „Zbiory nieskończone” 1, 2 i 3 (Wykład 7, część 1, 2 i 3)
- „Relacje” 3, 4 i 5 (Wykład 7, część 9, 10 i 11)
- „Funkcje” 1 i 2 (Wykład 8, część 4 i 5)

Rozdział 2.

Techniki dowodowe

2.1. Dowód

Na przedmiocie „Logika dla Informatyków" bardzo często będziemy się spotykać z pojęciem **dowodu**. Wiele zadań będzie polegało na udowodnieniu, że jakieś twierdzenie (zdanie) jest prawdziwe, bądź wykazaniu, że jest ono nieprawdziwe. Przez „dowód" rozumieć będziemy ciąg pewnych zdań, z których każde będzie albo pewną oczywistą prawdą (*aksjomatem*) albo będzie w pewien sposób **wynikać** z wcześniejszych zdań.

Żeby lepiej zrozumieć, czym dowód jest oraz jak wygląda, na przykładzie kilku twierdzeń przedstawimy kilka popularnych technik dowodowych.

2.2. Przykłady i kontrprzykłady

Przykład 1. Czy istnieje taka liczba naturalna n, że równość $n^2 = 2n$ jest prawdziwa?

Odpowiedzą na to pytanie jest oczywiście **tak**. To znaczy, że *istnieje taka liczba naturalna n, że równość $n^2 = 2n$ jest prawdziwa.* Jak jednak udowodnić, że to co napisaliśmy jest prawdą?

Zazwyczaj, by pokazać, że jakiś zdefiniowany przez nas obiekt matematyczny istnieje, najprościej jest go po prostu *wskazać*, czyli *podać przykład.* W naszym przypadku, obiektem który chcielibyśmy wskazać, jest taka liczba naturalna n, że równość $n^2 = 2n$ jest prawdziwa. Łatwo sprawdzić, że taką liczbą przykładowo może być 2. Możemy więc przeprowadzić dowód:

Dowód. Pokażemy, że istnieje taka liczba naturalna n, że równość $n^2 = 2n$ jest prawdziwa.

Weźmy $n = 2$.

Dla $n = 2$ mamy $n^2 = 2^2 = 4$ oraz $2n = 2 \cdot 2 = 4$. To znaczy, że dla $n = 2$, $n^2 = 4 = 2n$. Istnieje więc taka liczba naturalna $n = 2$, że równość $n^2 = 2n$ jest prawdziwa. □

Powyższy dowód składa się z dwóch głównych części. Po pierwsze, wskazaliśmy **przykład obiektu**, dla którego nasze zdanie byłoby prawdziwe (wskazaliśmy $n = 2$). Następnie, używając prostej arytmetyki, pokazaliśmy, że obiekt który wskazaliśmy rzeczywiście spełnia daną własność (pokazaliśmy, że dla $n = 2$ zachodzi $n^2 = 2n$).

Przykład 2. Czy równość $(n + m)^2 = n^2 + m^2$ jest prawdziwa dla wszystkich liczb naturalnych n, m?

Tym razem odpowiedzią na powyższe pytanie jest **nie**. To znaczy, że *nie dla wszystkich liczb naturalnych n, m równość $(n + m)^2 = n^2 + m^2$ jest prawdziwa.* Jak jednak udowodnić, że to co napisaliśmy jest prawdą?

W sytuacji takiej jak ta, w której mamy pokazać, że jakaś własność nie zachodzi dla **wszystkich** obiektów, zazwyczaj najłatwiej jest **wskazać kontrprzykład**, czyli przykład obiektu, który nie spełnia danej własności. Przeprowadźmy więc, jak w poprzednim przypadku, dowód:

Dowód. Pokażemy, że nie dla wszystkich liczb naturalnych n, m prawdziwa jest równość $(n + m)^2 = n^2 + m^2$. Innymi słowy pokażemy, że istnieją takie liczy naturalne n, m, że równość $(n + m)^2 = n^2 + m^2$ nie zachodzi.

Weźmy $n = 1$ i $m = 2$.

Dla $n = 1$ i $m = 2$ mamy:

- $(n + m)^2 = (1 + 2)^2 = 3^2 = 9$
- $n^2 + m^2 = 1^2 + 2^2 = 1 + 4 = 5$

Oczywiście, $5 \neq 9$, istnieją więc takie liczby naturalne $n = 1$ oraz $m = 2$, że równość $(n + m)^2 = n^2 + m^2$ nie zachodzi, czyli nie dla wszystkich liczb naturalnych jest ona prawdziwa. □

Powyższy dowód, podobnie jak poprzedni, składa się z dwóch głównych części. Po pierwsze, wskazaliśmy **kontrprzykład**, czyli przykład obiektu, dla którego nasze zdanie nie byłoby prawdziwe (wskazaliśmy $n = 1$ i $m = 2$). Następnie, używając prostej arytmetyki pokazaliśmy, że obiekt który wskazaliśmy rzeczywiście nie spełnia danej własności (pokazaliśmy, że dla $n = 1$ i $m = 2$ **nie** zachodzi $(n + m)^2 = n^2 + m^2$).

2.3. Rozpatrywanie przypadków

Przykład 3. Pokaż, że dla każdej liczby naturalnej a, takiej że $3 \nmid a$ (3 nie dzieli a), prawdą jest, że $3|(a^2-1)$ (3 dzieli a^2-1).

Zauważmy, że powyższe zdanie mówi, że mamy pokazać coś dla **każdej** liczby naturalnej. Nie możemy więc tego pokazać na przykładzie czy na konkretnej liczbie. Musimy wziąć **dowolną** liczbę naturalną a. Interesują nas jednak tylko takie liczby, dla których zachodzi $3 \nmid a$. Skoro inne liczby nas nie interesują, możemy wziąć dowolną liczbę a i założyć, że $3 \nmid a$. Następnie musimy udowodnić, że przy takim założeniu zachodzi również $3|a^2-1$.

Dowód. Pokażemy, że dla każdej liczby $a \in \mathbb{N}$ takiej, że $3 \nmid a$, zachodzi $3|a^2-1$.

Weźmy dowolną liczbę naturalną a i załóżmy, że $3 \nmid a$. Chcemy pokazać, że $3|a^2-1$.

Dość naturalnym sposobem, by rozwiązać takie zadanie, jest zastanowić się, jakie liczby naturalne **nie dzielą się** przez 3. Będą to liczby, których reszta z dzielenia przez 3, daje resztę 1 albo 2. Więc, innymi słowy, liczby w postaci $3k+1$ albo $3k+2$, dla pewnej liczby naturalnej k. Zamiast rozpatrywać oba przypadki razem, możemy każdy z nich rozpatrzeć z osobna.

Skoro a nie jest podzielne przez 3, to a jest w postaci $3k+1$ dla pewnej liczby naturalnej k, albo $3k+2$ dla pewnej liczby naturalnej k.

Rozpatrzmy przypadki:

- *Liczba a jest w postaci $3k+1$ dla pewnej liczby naturalnej k.*

  Chcemy powiedzieć coś o liczbie a^2-1. Spróbujmy więc rozpisać, czym jest ta liczba w naszym przypadku:

  Mamy więc, że $a^2-1=(3k+1)^2-1=9k^2+6k+1-1=9k^2+6k$.

  Naszym celem, jest wykazanie, że $3|a^2-1$, czyli, że a^2-1 jest podzielne przez 3.

  To oznacza, że $a^2-1=9k^2+6k=3\cdot(3k^2+2k)$, czyli, że a^2-1 jest podzielne przez 3.

  Pokazaliśmy więc, że jeśli $a=3k+1$, dla pewnej liczby naturalnej k, to a^2-1 jest podzielne przez 3.

- *Liczba jest w postaci $3k+2$ dla pewnej liczby naturalnej k.*

  Dowód przebiega analogicznie do poprzedniego przypadku. Najpierw, skoro chcemy powiedzieć coś o liczbie a^2-1, powinniśmy ją rozpisać:

  Mamy więc, że $a^2-1=(3k+2)^2-1=9k^2+12k+4-1=9k^2+12k+3$.

Znowu, naszym celem, jest wykazanie, że $3|a^2-1$, czyli, że a^2-1 jest podzielne przez 3.

To oznacza, że $a^2-1 = 9k^2+12k+3 = 3\cdot(3k^2+4k+1)$*, czyli, że* a^2-1 *jest podzielne przez* 3.

Pokazaliśmy więc, że jeśli $a = 3k+2$*, dla pewnej liczby naturalnej* k*, to* a^2-1 *jest podzielne przez* 3.

W obu przypadkach udowodniliśmy naszą tezę. Skoro to są jedyne przypadki przy naszych założeniach, to nasza teza jest prawdziwa dla każdej liczby naturalnej a*.*

□

Powyższy dowód mógłby ograniczyć się tylko do akapitów zapisanych kursywą, jednak w obecnej trochę rozciągniętej formie, nadal jest pełnoprawnym dowodem, przedstawiającym logiczny ciąg rozumowania, prowadzącym do udowodnienia zadanej przez nas tezy.

2.4. Dowody nie wprost

Przykład 4. Pokaż, że istnieje nieskończenie wiele liczb pierwszych.

Dowodzenie powyższej własności matematycznej (*„liczb pierwszych jest nieskończenie wiele"*) może okazać się dość trudne. Żeby pokazać wprost, że liczb pierwszych jest nieskończenie wiele, musielibyśmy bowiem w jakiś sposób przestawić nieskończony ciąg liczb pierwszych (na przykład za pomocą wzoru). W sytuacjach takich jak ta, czasem przydatne są **dowody nie wprost**. Dowody nie wprost podążają dość prostym schematem: jeśli chcemy udowodnić, że jakaś własność matematyczna zachodzi (w naszym przypadku własność to *„istnieje nieskończenie wiele liczb pierwszych"*), możemy najpierw założyć tezę do niej przeciwną (*„liczb pierwszych jest skończenie wiele"*) a potem przeprowadzić jakieś rozumowanie matematyczne, które doprowadzi nas do sprzeczności. Będzie to oznaczać, że nasze założenie nie było prawidłowe, a skoro tak, to nasza oryginalna teza była prawdziwa.

Dowód. Pokażemy, że liczb pierwszych jest nieskończenie wiele.

Korzystać będziemy z faktu:

Fakt 1. Dla każdej liczby $n > 1$, jeśli żadna liczba pierwsza mniejsza od n nie dzieli n, to n jest pierwsza.

Załóżmy nie wprost, że nasze twierdzenie nie jest prawdziwe i że liczb pierwszych jest skończenie wiele.

Niech $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$ będzie zbiorem **wszystkich** liczb pierwszych.

Rozważmy liczbę $m = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$.

Widzimy, że m jest większa od dowolnej liczby pierwszej $p_i \in \mathbb{P}$, więc $m \notin \mathbb{P}$.

Dodatkowo, dla każdej liczby pierwszej $p_i \in \mathbb{P}$, m nie jest podzielne przez p_i – reszta z dzielenia m przez p_i jest równa 1.

Oznacza to, że **żadna** liczba pierwsza nie dzieli m (bo w zbiorze $\mathbb{P}$ są wszystkie liczby pierwsze), więc w szczególności, żadna liczba pierwsza mniejsza od m nie dzieli m. Z faktu 1 mamy więc, że m jest liczbą pierwszą.

Dostaliśmy więc, że m jest liczbą pierwszą, która nie należy do zbioru $\mathbb{P}$, który był zbiorem **wszystkich** liczb pierwszych. To prowadzi nas do sprzeczności z założeniem, że liczb pierwszych jest skończenie wiele.

Skoro tak, to liczb pierwszych jest nieskończenie wiele, a to chcieliśmy pokazać. □

Powyższy dowód był typowym przykładem dowodu nie wprost. Żeby udowodnić naszą tezę, założyliśmy najpierw tezę przeciwną. Następnie przeprowadziliśmy rozumowanie, które doprowadziło nas do sprzeczności: *jeśli* zbiór liczb pierwszych byłby skończony, to moglibyśmy skonstruować zbiór $\mathbb{P}$ **wszystkich** liczb pierwszych, a następnie skonstruować liczbę pierwszą, która do tego zbioru nie należy. To oznacza, że nasz zbiór $\mathbb{P}$ nie był zbiorem **wszystkich** liczb pierwszych, więc nasze założenie, że liczb pierwszych jest skończenie wiele, było nieprawdziwe; liczb pierwszych musi być więc nieskończenie wiele.

Przykład 5. Pokaż, że dla dowolnej liczby naturalnej a, jeśli liczba a^2 jest parzysta, to liczba a także jest parzysta.

Ten dowód również można przeprowadzić nie wprost. Mamy pokazać, że dla dowolnej liczby naturalnej a, jeśli a^2 jest liczbą parzystą, to a także będzie liczbą parzystą. Na początku weźmiemy więc dowolną liczbę naturalną a i założymy, że a^2 jest liczbą parzystą, a potem założymy **nie wprost**, że a nie jest liczbą parzystą (lub, że jest liczbą *nieparzystą*). Następnie spróbujemy dojść do sprzeczności.

Dowód. Pokażemy, że dla dowolnej liczby naturalnej a, jeśli liczba a^2 jest parzysta, to liczba a także jest parzysta.

Weźmy dowolną liczbę naturalną a, taką, że a^2 jest parzyste.

Załóżmy nie wprost, że a nie jest liczbą parzystą. Skoro tak, to a jest w postaci $2k + 1$, dla pewnej liczby naturalnej k.

Skoro $a = 2k + 1$, to $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1$.

Ale to oznacza, że $a^2 = 2b + 1$ dla $b = 2k^2 + 2k$. b jest oczywiście liczbą naturalną, bo k jest liczbą naturalną.

Oznacza to, że a^2 nie jest liczbą parzystą, co jest sprzeczne z naszym założeniem.

Dowodzi to, że dla dowolnej liczby naturalnej a, jeśli liczba a^2 jest parzysta, to liczba a także jest parzysta. □

Dowód ten przebiega bardzo podobnie do poprzedniego. Założyliśmy, że liczba a nie jest parzysta mimo, że a^2 była parzysta. Prostymi rachunkami ustaliliśmy, że jeśli a nie byłaby parzysta, to a^2 także nie byłaby parzysta, a przecież naszym założeniem było, że a^2 jest liczbą parzystą.

Przykład 6. Pokaż, że $\sqrt{2}$ jest liczbą niewymierną.

Dowód. Pokażemy, że $\sqrt{2}$ jest liczbą niewymierną.

Załóżmy nie wprost, że $\sqrt{2}$ jest liczbą wymierną. To znaczy, że $\sqrt{2} = \frac{p}{q}$, dla pewnych $p, q \in \mathbb{N}$, które nie posiadają wspólnych dzielników (każdy ułamek mogę w ten sposób przedstawić, dzieląc licznik i mianownik przez ich wszystkie wspólne dzielniki).

Mamy więc, że $\sqrt{2} = \frac{p}{q}$, więc $2 = \frac{p^2}{q^2}$, czyli $p^2 = 2q^2$. To oznacza, że p^2 jest **liczbą parzystą** (bo jest równe iloczynowi dwójki przez jakąś liczbę). Korzystając z faktu, który udowodniliśmy w ćwiczeniu 5, wnioskujemy, że p także jest liczbą parzystą, tj. istnieje pewna liczba p', taka, że $p = 2p'$.

Mamy więc, że $p^2 = 2q^2$, oraz $p = 2p'$, czyli $2q^2 = p^2 = (2p')^2 = 4(p')^2$. To oznacza, że $4(p')^2 = 2q^2$, więc $2(p')^2 = q^2$. Oznacza to, że q^2 jest liczbą parzystą i znów, korzystając z faktu udowodnionego w ćwiczeniu 5 dochodzimy do wniosku, że q także musi być liczbą parzystą.

Oznacza to, że zarówno p jak i q są liczbami parzystymi, mają więc wspólny dzielnik: 2. Zakładaliśmy, że p i q nie mają wspólnych dzielników, dostajemy więc sprzeczność.

Oznacza to, że liczba $\sqrt{2}$ nie może być liczbą wymierną, czyli $\sqrt{2}$ jest liczbą niewymierną. □

Ten dowód przebiega w sposób bardzo podobny do poprzednich: żeby pokazać, że liczba $\sqrt{2}$ jest niewymierna, zakładamy najpierw, że jest wymierna, więc można ją zapisać jako (skrócony) ułamek. Następnie dochodzimy do sprzeczności z faktem, że ułamek był maksymalnie skrócony: skoro każdy ułamek możemy skrócić, to sprzeczność musiała wynikać z faktu, że zapisaliśmy $\sqrt{2}$ jako ułamek, czyli $\sqrt{2}$ nie może być wymierna; liczba $\sqrt{2}$ jest więc niewymierna.

2.5. Dowody niekonstruktywne

We wcześniejszych rozdziałach mówiliśmy, że zazwyczaj by udowodnić **istnienie** pewnego obiektu matematycznego, najłatwiej jest ten obiekt wskazać. Nie zawsze jest to jednak proste a czasem może okazać się niemożliwe. Metoda **dowodów**

niekonstruktywnych służy właśnie do tego, by pokazywać, że jakieś obiekty matematyczne istnieją, bez bezpośredniego wskazywania tych obiektów.

Przykład 7. Pokaż, że istnieją dwie niewymierne liczby x, y takie, że x^y jest wymierna.

Normalnie wystarczyłoby wskazać takie dwie niewymierne liczby spełniające warunki z zadania. Może się jednak okazać, że nie jest to takie proste. Dowód niekonstruktywny jest natomiast dość krótki i prosty:

Dowód. Istnieją dwie niewymierne liczby x, y takie, że x^y jest wymierna.

Skorzystamy z faktu, że liczba $\sqrt{2}$ jest niewymierna, który udowodniliśmy w ćwiczeniu 6.

Fakt 2. $\sqrt{2}^{\sqrt{2}}$ jest liczbą wymierną albo niewymierną.

Skoro tak, to możemy rozpatrzeć dwa przypadki:

- $\sqrt{2}^{\sqrt{2}}$ jest liczbą wymierną. Wtedy, dla $x = \sqrt{2}$ oraz $y = \sqrt{2}$ (liczb niewymiernych x, y), $x^y = \sqrt{2}^{\sqrt{2}}$ jest liczbą wymierną (z założenia).
- $\sqrt{2}^{\sqrt{2}}$ jest liczbą niewymierną. Wtedy, dla $x = \sqrt{2}^{\sqrt{2}}$ oraz $y = \sqrt{2}$ (liczb niewymiernych x, y), $x^y = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$ jest liczbą wymierną.

W obu przypadkach wskazaliśmy niewymierne liczby x, y takie, że x^y było liczbą wymierną. Skoro to jedyne przypadki, to nasze twierdzenie jest prawdziwe. □

Powyższy dowód nie wskazuje bezpośrednio liczb x, y spełniających warunki z zadania, nie jest więc dowodem konstruktywnym. Opiera się na spostrzeżeniu, że liczba $\sqrt{2}^{\sqrt{2}}$ jest albo wymierna albo niewymierna. Dowód ten dałoby się więc uprościć, pisząc zamiast niego dowód konstruktywny, jeśli udałoby się udowodnić, że liczba $\sqrt{2}^{\sqrt{2}}$ jest wymierna albo niewymierna, jednak wydaje się, że dowód tego faktu może okazać się dość trudny.

Rozdział 3.

Indukcja Matematyczna

3.1. Zbiór induktywny

Zanim zaczniemy mówić o indukcji oraz o tym, do czego można jej użyć, pomówmy o **liczbach naturalnych**. Nietrudno jest zauważyć, że zbiór $\mathbb{N}$ wszystkich liczb naturalnych jest zbiorem posiadającym poniższe własności:

- $0 \in \mathbb{N}$; czyli, że 0 jest liczbą naturalną
- dla dowolnej liczby m, jeśli $n \in \mathbb{N}$, to $n + 1 \in \mathbb{N}$; czyli, że jeśli n jest liczbą naturalną, to $n + 1$ także jest liczbą naturalną

Zbiór liczb naturalnych nie jest jednak jedynym zbiorem, który je posiada. Innym takim zbiorem może być na przykład zbiór liczb rzeczywistych $\mathbb{R}$, albo zbiór liczb wymiernych $\mathbb{Q}$. Dowolny zbiór liczb, który spełnia te własności, nazywać będziemy zbiorem **induktywnym**. Formalnie:

Definicja 1 (zbiór induktywny)**.** Zbiór X jest zbiorem **induktywnym**, jeśli spełnia warunki:

- $0 \in X$, oraz
- jeśli $n \in X$, to $n + 1 \in X$ dla dowolnego n.

Zbiór liczb naturalnych $\mathbb{N}$ jest więc zbiorem induktywnym. Jest też równocześnie dość szczególnym zbiorem induktywnym: wszystkie liczby, które uznajemy za naturalne, możemy uzyskać stosując powyższe reguły (to znaczy, każda liczba naturalna jest albo zerem, albo jest otrzymana poprzez dodanie jedynki do jakiejś liczby naturalnej). W zbiorze liczb naturalnych nie ma więc miejsca na liczby $\frac{1}{2}$, -1 czy $\sqrt{2}$.

Można więc powiedzieć, że zbiór liczb naturalnych $\mathbb{N}$ jest **najmniejszym** zbiorem induktywnym: nie posiada żadnych nadmiarowych elementów. Prawdą jest też stwierdzenie, że każdy zbiór induktywny **zawiera w sobie** zbiór liczb naturalnych (w dowolnym zbiorze induktywnym są wszystkie liczby naturalne).

3.2. Zasada indukcji

Spostrzeżenie, że zbiór $\mathbb{N}$ jest **najmniejszym** zbiorem induktywnym, to nic innego jak **zasada indukcji**. W innych słowach: jeśli zbiór X jest induktywnym podzbiorem zbioru liczb naturalnych (to znaczy, wszystkie elementy zbioru X są liczbami naturalnymi), to $X = \mathbb{N}$. Formalnie:

Twierdzenie 1 (zasada indukcji, wersja 1)**.** Niech X będzie takim podzbiorem liczb naturalnych $\mathbb{N}$, że:

- $0 \in X$, oraz
- dla dowolnego n, jeśli $n \in X$ to $n + 1 \in X$

Wtedy $X = \mathbb{N}$

Powyższe twierdzenie pozwala nam udowadniać, że wszystkie liczby naturalne posiadają jakąś (określoną przez nas) własność. Możemy na przykład pokazać, że dla dowolnej liczby naturalnej n, liczba $2n$ również jest naturalna, co więcej, jest parzysta. Możemy też pokazać coś bardziej skomplikowanego, na przykład, że suma n pierwszych liczb naturalnych jest równa $\frac{n(n+1)}{2}$.

Struktura takiego dowodu jest zazwyczaj taka sama:

1. Zdefiniowanie zbioru X, jako zbioru liczb naturalnych n dla których spełniona jest dana własność
2. Pokazanie, że zbiór X jest induktywny, to znaczy:
   - $0 \in X$, czyli, że x posiada daną własność; często ten etap nazywa się **podstawą indukcji**
   - pokazanie, że jeśli $n \in X$ to $n + 1 \in X$, czyli udowodnienie, że $n + 1$ posiada daną własność przy założeniu, że n ją posiada; ten etap często nazywa się **krokiem indukcyjnym**, a założenie, że $n \in X$ - **założeniem indukcyjnym**
3. powołanie się na zasadę indukcji by stwierdzić, że $X = \mathbb{N}$, czyli każda liczba naturalna należy do zbioru X, spełnia więc daną własność.

Taki dowód można rozumieć też jako algorytm, dzięki któremu moglibyśmy pokazać, że dowolne n posiada daną własność. Posiada ją bowiem 0 (z **podstawy indukcji**), a także $0 + 1 = 1$ (z **kroku indukcyjnego**: skoro 0 to i $0 + 1$), a także $1 + 1 = 2$, $2 + 1 = 3$, ..., $n - 1 + 1 = n$.

Przykład 1. Pokażemy, że dla dowolnej liczby naturalnej n, liczba $2n$ jest liczbą naturalną.

Dowód. Dla dowolnej $n \in \mathbb{N}$, $2n \in \mathbb{N}$.

1. Niech zbiór X będzie zbiorem liczb naturalnych n takich, że $2n$ jest liczbą naturalną. Formalnie:

   $$X = \{\ n \in \mathbb{N} \mid 2n \text{ jest liczbą naturalną } \}$$

   Zauważmy, że X jest podzbiorem zbioru liczb naturalnych.

2. Pokażemy, że zbiór X jest induktywny.

   - **Podstawa indukcji:**
     Zauważmy, że $2 \cdot 0 = 0$ jest liczbą naturalną, więc $0 \in X$ (to znaczy, że 0 spełnia własność).
   - **Krok indukcyjny:**
     Weźmy dowolne n i załóżmy, że $n \in X$ (**założenie indukcyjne**). Pokażemy, że $n + 1 \in X$ (to znaczy, że jeśli n posiada jakąś własność, to posiada ją też $n + 1$).
     Skoro $n \in X$, to $2n$ jest liczbą naturalną. Chcemy pokazać, że $n + 1 \in X$, czyli, że $2(n + 1)$ jest liczbą naturalną. Spróbujmy znaleźć powiązanie pomiędzy $2(n + 1)$ a $2n$:

     $$2(n + 1) = 2n + 2 = 2n + 1 + 1$$

     Z założenia indukcyjnego wiemy, że liczba $2n$ jest liczbą naturalną. Wiemy też, że $\mathbb{N}$ jest zbiorem induktywnym, więc dodając 1 do liczby naturalnej, otrzymamy liczbę naturalną. Skoro tak, to:

     - $2n + 1 \in \mathbb{N}$, bo $2n \in \mathbb{N}$ (z założenia indukcyjnego).
     - $2n + 2 \in \mathbb{N}$, bo $2n + 2 = (2n + 1) + 1$, a $2n + 1$ jest liczbą naturalną (z poprzedniego punktu).

     W takim razie $2(n + 1) \in \mathbb{N}$, czyli $n + 1 \in X$.

3. Zatem, na mocy twierdzenia 1, zbiór $X = \mathbb{N}$, czyli dla każdej liczby naturalnej n, $2n$ jest liczbą naturalną.

□

3.3. Zmiana podstawy indukcji

Twierdzenie 1 nie jest jedynym sposobem, na zapisanie zasady indukcji. W zależności od naszych potrzeb, możemy definiować własne zasady indukcji, upewniając się oczywiście, że są one poprawne. Dla przykładu, jeśli chcielibyśmy pokazać, że jakaś własność przysługuje wszystkim liczbom naturalnym większym od 0 (np. "dla każdej liczby naturalnej większej od 0, 2^n jest liczbą parzystą), możemy zmienić podstawę indukcji, by zaczynała się od 1 zamiast od 0:

Twierdzenie 2 (zasada indukcji, wersja 2)**.** Niech X będzie podzbiorem zbioru liczb naturalnych, takim, że

- $1 \in X$, oraz
- dla każdego n, jeśli $n \in X$ to $n + 1 \in X$

Wtedy dla każdej liczby $n \in \mathbb{N}_{\geq 1}$ (liczby naturalnej $n \geq 1$), $n \in X$

Intuicyjnie, powyższa zasada indukcji działa, ponieważ podaje nam algorytm pokazania, że każda liczba większa od 0 posiada daną własność: Posiada ją 1, a także $1 + 1 = 2$, $1 + 2 = 3$, ...

Nie jest to jednak dowód formalny; podaje nam tylko pewną intuicję. Formalny dowód można na przykład przeprowadzić **nie wprost**, biorąc dowolny zbiór X spełniający warunki z twierdzenia 2 i zakładając, że nie jest on zbiorem **wszystkich** liczb naturalnych większych bądź równych 1.

Dowód. Zasada indukcji z twierdzenia 2 jest poprawna.

Weźmy dowolny zbiór X spełniający warunki twierdzenia 2.

Załóżmy nie wprost, że X nie jest zbiorem liczb naturalnych większych bądź równych 1. Skoro X zawiera tylko liczby naturalne (bo z założenia jest podzbiorem $\mathbb{N}$), to musi istnieć $n \in \mathbb{N}_{\geq 1}$, takie, że $n \notin X$.

Weźmy więc **najmniejszą** liczbę n, taką, że $n \in \mathbb{N}_{\geq 1}$, ale $n \notin X$.

Rozpatrzmy przypadki:

- $n = 1$. Z konstrukcji zbioru X wiemy, że $1 \in X$ (pierwszy punkt z twierdzenia 2). Otrzymujemy więc sprzeczność z założeniem, że $n \notin X$.
- $n \geq 2$. Skoro n jest **najmniejszą** liczbą naturalną większą bądź równą 1 nie należącą do X, to oznacza, że $(n - 1) \in X$.

  Wiemy, że X spełnia warunek drugi z twierdzenia 2. Oznacza to, że dla dowolnej liczby naturalnej należącej do X, liczba o jeden większa również należy do X. Wiemy też, że $(n - 1) \in X$. Oznacza to, że $(n - 1 + 1) \in X$, czyli, że $n \in X$. Otrzymujemy więc sprzeczność z założeniem, że $n \in X$.

Oznacza to, że dla wszystkich liczb naturalnych $n \in \mathbb{N}_{\geq 1}$, $n \in X$, a to chcieliśmy pokazać. □

Zasadę indukcji z twierdzenia 2 można w dość naturalny sposób zastąpić taką, dzięki której można pokazać, że jakaś własność przysługuje liczbom naturalnym większym od pewnego a:

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

- $a \in X$, oraz
- dla każdego n, jeśli $n \in X$ to $n + 1 \in X$

Wtedy dla każdej liczby naturalnej $n \geq a$, $n \in X$

Ćwiczenie 1. Pokaż, że zasada indukcji z twierdzenia 3 jest poprawna.

3.4. Wzmacnianie założenia indukcyjnego

Zdarzają się sytuacje, kiedy założenie, że poprzednia liczba spełnia daną własność jest niewystarczające. Tworząc zasadę indukcji, która zakłada coś o kilku poprzednich elementach, należy uważać. Weźmy dla przykładu zbiór X posiadający następujące własności:

- $0 \in X$
- jeśli $n \in X$ oraz $n + 1 \in X$, to $n + 2 \in X$

Łatwo jest sprawdzić, że zbiór $\mathbb{N}$ spełnia powyższe własności. Czy jest jednak **najmniejszym** zbiorem który je spełnia? Spójrzmy, jak budowany jest ten zbiór. Oczywiście, 0 do niego należy. Czy z faktu, że 0 do niego należy wynika, że 1 też powinno? Odwróćmy pytanie: **kiedy** 1 **musi należeć do** X**?** Z punktu drugiego wynika, że $1 \in X$ jeśli $0 \in X$ oraz $-1 \in X$. Ale -1 nie musi należeć do X. Co z 2? Skoro 1 nie musi należeć do X, to przeprowadzając podobne rozumowanie, możemy dojść do wniosku, że 2 też nie musi być jego elementem.

Zbiory $X = \{\ 0\ \}$, $X = \{\ 0,\ 2\ \}$, czy zbiór liczb parzystych są tylko niektórymi przykładami zbiorów, które spełniają powyższe warunki. Zbiór liczb naturalnych nie jest więc **najmniejszym** takim zbiorem. Co ze zbiorem $X = \{\ 0,\ 1\ \}$? Skoro zarówno 0 jak i 1 należą do X, to 2 też musi do niego należeć. Zbiór X nie spełnia więc warunków. Co ze zbiorem $X = \{\ 0,\ 1,\ 2\ \}$? Skoro zarówno 1 jak i 2 należą do X, to 3 też powinno, więc zbiór X znów nie spełnia warunków. Podobnie zbiór $X = \{\ 0,\ 1,\ 2,\ 3\ \}$, $X = \{\ 0,\ 1,\ 2,\ 3,\ 4\ \}$ i tak dalej. Wygląda na to, że jeśli zbiór zawiera 0 i 1, to żeby spełniał warunki, musiałby zawierać już wszystkie liczby naturalne.

Twierdzenie 4 (zasada indukcji, wersja 4)**.** Niech X będzie podzbiorem zbioru liczb naturalnych, takim, że

- $0 \in X$ i $1 \in X$ oraz
- dla każdego n, jeśli $n \in X$ oraz $n+1 \in X$ to $n+2 \in X$

Wtedy $X = \mathbb{N}$

Dowód poprawności tej zasady indukcji można przeprowadzić podobnie do dowodu poprawności zasady indukcji z twierdzenia 2.

W tej zasadzie indukcji mamy dwie **podstawy indukcji**. Podobnie, pisząc zasadę indukcji, która w **kroku indukcyjnym** mówi coś o czterech poprzednich elementach, należy rozważyć cztery **podstawy indukcji**.

Ćwiczenie 2. Czy $\mathbb{N}$ jest najmniejszym zbiorem X, który spełnia poniższe własności?

- $0 \in X$
- jeśli $n \in X$ to $n+2 \in X$

Jeśli nie, to czy potrafisz „poprawić" własności, by tak było? Czy potrafisz napisać i uzasadnić zasadę indukcji, której podstawą będzie zbiór X?

Przykład 2. Dany jest ciąg, spełniający następujące własności: $a_0 = 0$, $a_1 = 1$, $a_n = a_{n-2} + 2$ dla $n \geq 2$. Pokażemy, że $a_n = n$ dla każdej liczby naturalnej n.

1. Niech X będzie takim podzbiorem zbioru liczb naturalnych, że

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

   Pokażemy, że $X = \mathbb{N}$

2. Użyjemy zasady indukcji z twierdzenia 4

3. Pokażmy, że:

   - **Podstawa indukcji:**
     - $0 \in X$, ponieważ $a_0 = 0$, z definicji ciągu
     - $1 \in X$, ponieważ $a_1 = 1$, z definicji ciągu
   - **Krok indukcyjny:**

     Weźmy dowolne n i załóżmy, że $n \in X$ oraz $n+1 \in X$ (założenie indukcyjne). Pokażemy, że $n+2 \in X$ to znaczy, że $a_{n+2} = n+2$.

Skoro $n \in X$ to, z definicji zbioru X, n jest liczbą naturalną, czyli także $n \geq 0$. Skoro tak, to $n + 2 \geq 2$, więc $a_{n+2} = a_n + 2$ (z definicji ciągu a_n). Z założenia indukcyjnego wiemy, że $a_n = n$. Stąd:

$$a_{n+2} = a_n + 2 = n + 2$$

Czyli, że $n + 2 \in X$.

Na mocy zasady indukcji z twierdzenia 4, $X = \mathbb{N}$, czyli dla każdej liczby naturalnej n, $a_n = n$.

Bazując na twierdzeniu 4 możemy skonstruować indukcję, która założy coś o a poprzednich elementach, dla dowolnego $a \geq 1$. Czasem jednak i to nie jest wystarczające. W pewnych sytuacjach chcielibyśmy założyć, że **wszystkie** elementy mniejsze bądź równe n są elementami zbioru X, żeby pokazać, że $n + 1$ też jest elementem X.

Twierdzenie 5 (zasada indukcji, wersja 5)**.** Niech $a \in \mathbb{N}$, a X będzie podzbiorem zbioru liczb naturalnych takim, że

- $a \in X$, oraz
- dla wszystkich liczb naturalnych $n \geq a$, jeśli $\forall a \leq i \leq n$ $(i \in X)$ (dla każdej liczby i, która jest większa bądź równa a ale mniejsza bądź równa n, $i \in X$), to $(n + 1) \in X$

Wtedy dla każdej liczby naturalnej $n \geq a$, $n \in X$

Dowód prawdziwości tej zasady indukcji można przeprowadzić podobnie do poprzednich.

Rzeczą na którą szczególnie trzeba zwrócić uwagę podczas korzystania z tego twierdzenia, jest założenie indukcyjne, a dokładniej przedział, w którym założenie to zachodzi. Spójrzmy na przykładowy dowód:

Przykład 3. Pokażę, że dla każdej liczby naturalnej n, n jest parzyste.

1. Niech X będzie takim podzbiorem zbioru liczb naturalnych, że

   $$X = \{\ n \in \mathbb{N} \mid n \text{ jest parzyste } \}$$

   Pokażemy, że dla każdego $n \in \mathbb{N}$, $n \in X$

2. Użyjemy zasady indukcji z twierdzenia 5

3. Pokażmy, że:

- **Podstawa indukcji:** Oczywiście, $0 \in X$, ponieważ 0 jest liczbą parzystą
- **Krok indukcyjny:** Weźmy dowolne n i załóżmy, że dla wszystkich liczb naturalnych i takich, że $i \geq 0$ oraz $i \leq n$, $i \in X$. Pokażemy, że $n+1 \in X$. Wiemy z założenia indukcyjnego, że $n-1 \in X$, więc $n-1$ jest liczbą parzystą. Skoro tak, to $n-1+2$ jest liczbą parzystą jako suma dwóch liczb parzystych. W takim razie $n+1 \in X$.

Na mocy zasady indukcji z twierdzenia 5, dla każdego $n \in \mathbb{N}$, $n \in X$, więc każde n jest parzyste.

Powyższe wnioskowanie jest oczywiście błędne. Mamy wiele przykładów liczb naturalnych, które nie są parzyste. Gdzie jest jednak błąd?

Żebyśmy mogli skorzystać z faktu, że $n-1 \in X$, musimy upewnić się, że nasze założenie indukcyjne mówiło coś o $n-1$, czyli, że $n-1 \geq 0$ i $n-1 \leq n$. Oczywiście, prawdą jest, że $n-1 \leq n$. Czy $n-1 \geq 0$? Jedyne co wiemy o n to fakt, że należy do zbioru X. To znaczy, że jest liczbą naturalną oraz liczbą parzystą. Skoro n jest parzystą liczbą naturalną, to w szczególności może być równe 0 – wtedy $n-1 = 0-1 = -1$. Oczywiście,$-1 \ngeq 0$. W takim razie nasze założenie indukcyjne nie mówiło nic o tym, że $n-1 \in X$, nie możemy więc z tego skorzystać.

Prawidłowy dowód wymagałby więc rozpatrzenia dwóch przypadków: gdy $n = 0$ oraz gdy $n \geq 0$. Jeśli $n \geq 0$, to całe rozumowanie jest poprawne. Jeśli jednak $n = 0$, to $n+1 = 1$ nie jest liczbą parzystą, więc nie należy do X. Z tego powodu dowód jest niepoprawny – należy zawsze sprawdzić, czy korzystając z założenia, nie wychodzimy poza zakres liczb, o których założyliśmy, że rzeczywiście są elementami X.

Poniższy przykład przedstawia poprawne rozumowanie z wykorzystaniem zasady indukcji w wersji 5

Przykład 4. Pokażemy, że dla każdej liczby naturalnej $n \geq 2$, n możemy zapisać jako iloczyn liczb pierwszych, to znaczy, $n = p_1 \cdot \ldots \cdot p_a$ dla jakichś liczb pierwszych $p_1, \ldots, p_a$.

1. Niech X będzie takim podzbiorem zbioru liczb naturalnych, że

$$X = \{\ n \in \mathbb{N} \mid n \text{ można zapisać jako iloczyn liczb pierwszych } \}$$

   Pokażemy, że dla każdego $n \geq 2$, $n \in X$

2. Użyjemy zasady indukcji z twierdzenia 5

3. Pokażmy, że:

   - **Podstawa indukcji:** Oczywiście, $2 \in X$, ponieważ 2 jest iloczynem jednej liczby pierwszej

- **Krok indukcyjny:** Weźmy dowolne n i załóżmy, że dla wszystkich liczb naturalnych i takich, że $i \geq 2$ oraz $i \leq n$, $i \in X$. Pokażemy, że $n+1 \in X$.

  Rozpatrzmy dwa przypadki:

  - $n+1$ jest liczbą pierwszą
    Wtedy $n+1$ jest iloczynem jednej liczy pierwszej, więc $n+1 \in X$
  - $n+1$ jest liczbą złożoną.
    To znaczy, że istnieje liczba pierwsza p, będąca dzielnikiem $n+1$, oraz jakaś liczba naturalna k taka, że $p \cdot k = n+1$.
    Chcemy skorzystać z faktu, że $k \in X$. Musimy pokazać, że $k \geq 2$ oraz $k \leq n$.

    * $k \geq 2$
      Przypomnijmy, że k jest taką liczbą naturalną, że istnieje liczba pierwsza p, taka, że $k \cdot p = n+1$.
      Skoro k jest liczbą naturalną, to $k \geq 0$.
      Zauważmy, że n jest liczbą naturalną, wiec $n+1 \geq 1$. Skoro tak, to $n+1 \neq 0$, więc $k \neq 0$. To oznacza, że $k \geq 1$.
      Wiemy też, że p jest liczbą pierwszą, a $n+1$ jest liczbą złożoną, więc $k \neq 1$, a skoro tak, to $k \geq 2$.
    * $k \leq n$
      Skoro p jest liczbą pierwszą, to $p \geq 2$. Skoro tak, to $k < n+1$, więc $k \leq n$.

    Wiemy więc, że $k \in X$. Skoro tak, to z definicji zbioru X, istnieją pewne liczby pierwsze $p_1, p_2, \ldots, p_i$, że $k = p_1 \cdot p_2 \cdot \cdots \cdot p_i$. Skoro tak, to $n+1$ możemy zapisać jako

    $$n+1 = p \cdot k = p \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_i$$

    Czyli $n+1$ możemy zapisać jako iloczyn liczb pierwszych.

Na mocy zasady indukcji z twierdzenia 5 dla każdej liczby naturalnej $n \geq 2$, $n \in X$, czyli każdą liczbę naturalną $n \geq 2$ można zapisać jako iloczyn liczb pierwszych.

3.5. Bardziej zaawansowane przykłady

Indukcja może również zostać użyta do pokazywania własności struktur bardziej skomplikowanych niż liczby naturalne. Dla przykładu, weźmy proste wyrażenia algebraiczne zbudowane jedynie z nawiasów, liczb naturalnych i działań: mnożenia, dzielenia, odejmowania i dodawania. Dla uproszczenia nie będziemy za wyrażenie uznawać wyrażenia pustego (to znaczy każde wyrażenie powinno zawierać przynajmniej jedną liczbę).

Przykładami wyrażeń algebraicznych mogą być: $1 + 2 - 10 \cdot 14$, $(1 + 2 - 10) \cdot 14$ czy 8, natomiast przykładami napisów, które wyrażeniem nie są, może być na przykład 3+ (+ powinien łączyć dwa wyrażenia algebraiczne) albo $4 + \cdot 2$ (+ i $\cdot$ nie mogą występować bezpośrednio obok siebie).

Długością takiego wyrażenia nazywać będziemy liczbę operacji, które ono zawiera. Tak więc $1 + 2 - 10 \cdot 14$ ma długość 3, tak samo jak $(1 + 2 - 10) \cdot 14$, z kolei 8 ma długość 0.

Spójrzmy teraz na poniższy dowód i zastanówmy się nad jego poprawnością:

Przykład 5 (Niepoprawny dowód indukcyjny)**.** Pokażmy, że dowolne wyrażenie długości n zawiera $n + 1$ liczb.

1. Niech X będzie takim podzbiorem $\mathbb{N}$, że

$$X = \{\ n \in \mathbb{N} \mid \text{dowolne wyrażenie długości } n \text{ zawiera } n + 1 \text{ liczb}\ \}$$

   Pokażemy, że $X = \mathbb{N}$

2. Użyjemy zasady indukcji w wersji 1

3. Pokażemy, że

   - **Podstawa indukcji:**

     Oczywiście, dowolne wyrażenie długości 0 składa się z jednej liczby, więc $0 \in X$.

   - **Krok indukcyjny:**

     Weźmy dowolne n i załóżmy, że $n \in X$. Pokażmy, że $n + 1 \in X$.

     Weźmy dowolne wyrażenie φ długości n, oraz dowolne działanie $\diamond$ i dowolną liczbę l.

     Skoro φ jest długości n, to z założenia indukcyjnego, φ zawiera $n + 1$ liczb. Skoro tak, to wyrażenie $\varphi \diamond l$ jest wyrażeniem długości $n + 1$ i zawiera $n + 1 + 1 = n + 2$ liczb, więc $n + 1 \in X$

   Na mocy zasady indukcji z twierdzenia 1, $X = \mathbb{N}$.

Czy powyższy dowód jest więc poprawny? Żeby się o tym przekonać zastanówmy się, czy rzeczywiście pokazaliśmy coś dla **dowolnego** wyrażenia. Oczywiście, dowolne wyrażenie długości 0 może być tylko w postaci pojedynczej liczby, z podstawą indukcji nie ma więc żadnego problemu. Spójrzmy jednak na krok indukcyjny. Czy rzeczywiście jest tak, że dowolne wyrażenie długości $n + 1$ mogę uzyskać „dopisując" coś do jakiegoś wyrażenia długości n? Co z wyrażeniem $(1 + 2) \cdot (1 + 2)$? Jest to wyrażenie długości 3, jednak czy istnieje jakieś wyrażenie długości 2 które, po „dopisaniu" jakiejś operacji, stanie się właśnie nim? Wygląda na to, że nie.

Ten problem często pojawia się podczas rozpatrywania struktur bardziej skomplikowanych niż liczby naturalne. Można by było oczywiście próbować w pewien sposób opisać wszystkie przypadki, jednak wydaje się, że byłoby to skomplikowane zadanie, oraz, że łatwo byłoby coś pominąć. Czy istnieje prostszy sposób na opisanie tego?

Rozpatrując struktury takie jak ta opisana wyżej, warto jest, zamiast **rozszerzać** problem mniejszy, zacząć od **większego** problemu, a potem **zredukować** go do problemu **mniejszego**. To znaczy, wziąć **dowolne** wyrażenie długości $n+1$ i spróbować znaleźć w nim wyrażenia mniejszej długości, dla których mamy założenie indukcyjne. Zastanówmy się więc, czy możemy znaleźć jakiś sposób, by w wyrażeniu długości $n+1$ znaleźć wyrażenia długości mniejszej.

Dowolne wyrażenie można oczywiście obliczyć, stosując znane nam reguły kolejności wykonywania działań. Można także mówić o działaniu, które wykonamy jako *ostatnie* podczas obliczania wyrażenia, tak więc w wyrażeniu $1+2-10\cdot 14$ ostatnim działaniem będzie „$-$”, z kolei w $(1+2-10)\cdot 14$ będzie nim „$\cdot$”. Dowolne wyrażenie można więc podzielić na dwa wyrażenia mniejszej długości i połączyć je tym działaniem, tak więc $1+2-10\cdot 14$ można rozpisać jako różnicę wyrażeń $1+2$ oraz $10\cdot 14$. Otrzymane w ten sposób wyrażenia są **mniejsze** niż wyrażenie, od którego zaczęliśmy. Uzbrojeni w tą wiedzę, możemy przeprowadzić już poprawny dowód indukcyjny. W tym celu wykorzystamy silniejszą zasadę indukcji.

Przykład 6. Pokażmy, że dowolne wyrażenie długości n zawiera $n+1$ liczb.

1. Niech X będzie takim podzbiorem $\mathbb{N}$, że

$$X = \{\ n \in \mathbb{N} \mid \text{dowolne wyrażenie długości } n \text{ zawiera } n+1 \text{ liczb}\ \}$$

   Pokażemy, że $X = \mathbb{N}$

2. Użyjemy zasady indukcji w wersji 5

3. Pokażemy, że

   - **Podstawa indukcji:**

     Dowolne wyrażenie długości 0 składa się z jednej liczby, więc $0 \in X$.

   - **Krok indukcyjny:**

     Weźmy dowolne n i załóżmy, że dla wszystkich liczb naturalnych i takich, że $i \geq 0$ oraz $i \leq n$, $i \in X$. Pokażmy, że $n+1 \in X$.

     W tym celu weźmy dowolne wyrażenie φ długości $n+1$, oraz wybierzmy działanie $\diamond$ które zostałoby wykonane jako ostatnie, podczas obliczana wartości wyrażenia, przy zastosowaniu standardowej kolejności wykonywania działań. Wyrażenie φ możemy zapisać jako $\varphi_1 \diamond \varphi_2$, gdzie φ_1 ma długość $n_1 \geq 0$ a φ_2 ma długość $n_2 \geq 0$.

Wiemy, że φ ma długość $n_1 + n_2 + 1$ ponieważ ma n_1 operacji w φ_1, n_2 operacji w φ_2 oraz dodatkową operację $\diamond$. Skoro $n_1 + n_2 + 1 = n + 1$, to $n_1 + n_2 = n$. Skoro zarówno n_1 jak i n_2 są większe bądź równe 0, to $n_1 \leq n$ oraz $n_2 \leq n$. Skoro tak, to z założenia indukcyjnego $n_1 \in X$ oraz $n_2 \in X$.
Wiemy więc, że φ_1 zawiera $n_1 + 1$ liczb, a φ_2 zawiera ich $n_2 + 1$.
Policzmy, ile liczb zawiera wyrażenie $\varphi_1 \diamond \varphi_2$:

$$n_1 + 1 + n_2 + 1 = n_1 + n_2 + 2 = n + 2$$

Zawiera więc $n + 2$ liczby.
Skoro dowolne wyrażenie długości $n + 1$ zawiera $n + 2$ liczby, to $n + 1 \in X$.

Na mocy zasady indukcji z twierdzenia 5, $X = \mathbb{N}$.

Umiejętność redukowania zadania większego do zadań mniejszych jest niezwykle istotna i pozwala nam uniknąć niepotrzebnego rozpatrywania wszystkich możliwych przypadków. Skoro chcemy pokazać coś dla **każdego** obiektu wielkości n, powinniśmy najpierw wziąć **dowolny** obiekt; tak jak w powyższym przykładzie, by pokazać coś dla każdego wyrażenia długości $n + 1$, na samym początku wzięliśmy **dowolne** wyrażenie danej długości, a następnie odnaleźliśmy w nim wyrażenia mniejsze, co umożliwiło nam wykorzystanie założenia indukcyjnego.

Rozdział 4.

Zbiory

4.1. Pojęcia pierwotne i aksjomaty

Język matematyki jest językiem sformalizowanym. Wszystkie nowe pojęcia budowane są na postawie pojęć już istniejących, które z kolei definiuje się za pomocą innych istniejących pojęć. W pewnym momencie trzeba jednak się zatrzymać, pewne pojęcia przyjmując za wiadome bez konieczności podawania definicji. Pojęcia takie nazywamy **pojęciami pierwotnymi**. Na podstawie tych właśnie pojęć definiuje się wszystkie inne.

Podstawowymi pojęciami pierwotnymi w **teorii mnogości** którą będziemy teraz omawiać, są pojęcia **zbioru** oraz relacja **należenia** (zapisujemy jako $\in$). Napis $x \in A$ czytać będziemy jako „x należy do A". Przykładem zbioru może być zbiór $\{pies, kot\}$, do którego należą elementy $pies$ oraz kot (czyli $pies \in \{pies, kot\}$ oraz $kot \in \{pies, kot\}$). W zbiorze elementy nie mogą się powtarzać, nie ważna jest też kolejność wypisywania elementów.

Rozważać będziemy zarówno zbiory skończone (zawierające n elementów, dla pewnej liczby naturalnej n) jak i zbiory nieskończone (których liczby elementów nie możemy ograniczyć przez żadne n, na przykład zbiór liczb naturalnych $\mathbb{N}$).

Warto zwrócić uwagę na to, że elementami zbioru mogą być dowolne obiekty. Możemy sobie na przykład wyobrazić zbiór $\{1, kot, \mathbb{N}\}$, którego posiada trzy elementy: 1, kot oraz $\mathbb{N}$.

Zbiorem, który nie zawiera żadnych elementów, nazywać będziemy **zbiorem pustym** i zapisywać będziemy jako $\emptyset$. Prawdziwe jest więc stwierdzenie

$$\forall x \; x \notin \emptyset$$

„Dla każdego elementu x, x nie należy do zbioru pustego"

Zbiory $A = \{1, 2\}$ oraz $B = \{2, 1\}$ są **równe**, ponieważ zawierają dokładnie te same elementy. Ściślej mówiąc, każdy element należący do A należy też do B, a każdy element który należy do B należy także do A. Zbiory są równe **tylko wtedy** gdy spełniają powyższą zależność. Zasadę tą nazywamy **zasadą ekstensjonalności**

Aksjomat 1 (Zasada ekstensjonalności)**.** Dla dowolnych zbiorów A oraz B, mówimy, że $A = B$ wtedy i tylko wtedy, gdy prawdziwa jest formuła

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

„Dla każdego elementu x, x należy do A wtedy i tylko wtedy, gdy x należy do B"

Powyższe zdanie jest przykładem **aksjomatu**, czyli zdania które przyjmujemy za prawdziwe bez potrzeby podawania jego dowodu. Podobnie jak w przypadku pojęć pierwotnych, które służyły jako podstawa do definiowania nowych pojęć, aksjomaty stanowią podstawę do przeprowadzania dowodów.

W omawianej przez nas teorii mnogości aksjomatów jest więcej. Jednym z przykładów może być **aksjomat zbioru pustego** który gwarantuje nam, że istnieje zbiór który nie zawiera żadnych elementów:

Aksjomat 2 (Aksjomat zbioru pustego)**.** Zbiór pusty istnieje

Nie będziemy tutaj definiować wszystkich aksjomatów ani szczegółowo ich omawiać, warto jednak zdawać sobie sprawę z tego, że pewne aksjomaty istnieją i są potrzebne, nawet jeśli w większości przypadków nie będziemy z nich jawnie korzystać. Zainteresowanych czytelników odsyłamy więc do podręczników do teorii mnogości.

Aksjomat zbioru pustego gwarantuje nam więc, że istnieje przynajmniej jeden zbiór pusty. Używając **zasady ekstensjonalności** możemy wzmocnić to twierdzenie, pokazując, że zbiór pusty jest dokładnie jeden.

Dowód. Załóżmy nie wprost, że istnieją przynajmniej dwa zbiory puste. Weźmy więc dwa dowolne, różne zbiory puste $\emptyset_1$ oraz $\emptyset_2$. Wiemy, że zbiory są różne, to znaczy, że $\emptyset_1 \neq \emptyset_2$.

Zauważmy, że z definicji zbioru pustego, dla każdego x, formuły $x \in \emptyset_1$ oraz $x \in \emptyset_2$ są fałszywe. Skoro tak, to formuła $x \in \emptyset_1 \Leftrightarrow x \in \emptyset_2$ jest prawdziwa dla dowolnego x. Prawdziwa jest więc formuła:

$$\forall x \ (x \in \emptyset_1 \Leftrightarrow x \in \emptyset_2)$$

Powyższa formuła to nic innego jak **zasada ekstensjonalności**. Na jej mocy możemy więc stwierdzić, że zbiory $\emptyset_1$ i $\emptyset_2$ są równe.

Otrzymujemy sprzeczność z założeniem, że istnieją przynajmniej dwa zbiory puste. Oznacza to, że istnieje co najwyżej jeden zbiór pusty, a z **aksjomatu zbioru**

pustego wiemy, że istnieje przynajmniej jeden zbiór pusty. Skoro tak, to istnieje dokładnie jeden zbiór pusty.

□

4.2. Podzbiory

Używając zdefiniowanych wyżej pojęć pierwotnych (**zbiór** oraz **należenie**) zdefiniować możemy relację **zawierania** (co oznaczać będziemy jako $\subseteq$).

Definicja 1 (Podzbiór)**.** Zbiór A będzie **podzbiorem** zbioru B (co będziemy zapisywać jako $A \subseteq B$), jeśli każdy element należący do zbioru A, będzie należeć także do zbioru B.

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

„Dla każdego elementu x, jeśli x należy do A, to x należy także to B"

Zbiór $\{kot\}$ jest więc podzbiorem zbioru $\{kot, pies\}$ (czyli $\{kot\} \subseteq \{kot, pies\}$), ponieważ każdy element zbioru $\{kot\}$ (jest dokładnie jeden element, kot) jest elementem zbioru $\{kot, pies\}$.

W przypadku podzbiorów bardzo ważnym jest, by pamiętać o różnicy pomiędzy **zawieraniem** a **należeniem**. Dla przykładu, dla zbioru $A = \{1, kot, \mathbb{N}\}$, $\mathbb{N}$ jest **elementem** zbioru A, więc $\mathbb{N} \in A$. Nie jest jednak prawdą, że $\mathbb{N} \subseteq A$, ponieważ w zbiorze $\mathbb{N}$ istnieją elementy (na przykład $2 \in \mathbb{N}$) które do zbioru A nie należą. Prawdą jest jednak, że $\{\mathbb{N}\} \subseteq A$ (ale w tym przypadku nieprawdą jest, że $\{\mathbb{N}\} \in A$).

Zgodnie z definicją, zbiór $\{1, 2\}$ jest podzbiorem zbioru $\{1, 2\}$. Dowolny zbiór A jest swoim własnym podzbiorem, ponieważ wszystkie elementy należące do zbioru A w oczywisty sposób należą też do zbioru A.

Podobnie zbiór pusty $\emptyset$ jest podzbiorem dowolnego zbioru A, ponieważ wszystkie elementy należące do zbioru pustego (a nie ma takich elementów), należą do zbioru A. Można też o tym myśleć w drugą stronę: czy istnieje jakiś element, który należy do zbioru $\emptyset$ a nie należy do zbioru A? Zbiór pusty nie zawiera żadnych elementów, nie znajdziemy więc w nim kontrprzykładu.

Podzbiory posiadają jeszcze jedną ciekawą własność. Jeśli zbiór A jest podzbiorem zbioru B, oraz zbiór B jest podzbiorem zbioru A (czyli $A \subseteq B$ i $B \subseteq A$), to $A = B$. Własność tą można udowodnić korzystając z **zasady ekstensjonalności**:

Dowód. Pokażemy, że dla dowolnych zbiorów A i B, jeśli $A \subseteq B$ oraz $B \subseteq A$, to $A = B$.

Weźmy więc dowolne zbiory A i B i załóżmy, że $A \subseteq B$ oraz $B \subseteq A$. Skoro tak, to prawdziwa jest formuła

$$\underbrace{\forall x\ (x \in A \Rightarrow x \in B)}_{\text{Bo } A \subseteq B} \wedge \underbrace{\forall x\ (x \in B \Rightarrow x \in A)}_{\text{Bo } B \subseteq A}$$

Korzystając z znanych nam praw rachunku kwantyfikatorów, możemy przeprowadzić ciąg równoważnych przejść:

$$\begin{aligned} A \subseteq B \wedge B \subseteq A &\equiv \forall x\ (x \in A \Rightarrow x \in B) \wedge \forall x\ (x \in B \Rightarrow x \in A) \\ &\equiv \forall x\ (x \in A \Rightarrow x \in B \wedge x \in B \Rightarrow x \in A) \\ &\equiv \forall x\ (x \in A \Leftrightarrow x \in B) \end{aligned}$$

Prawdziwa jest więc formuła $\forall x\ (x \in A \Leftrightarrow x \in B)$. Korzystając z *zasady ekstensjonalności* możemy więc stwierdzić, że $A = B$ □

Dowód ten łatwo jest przeprowadzić także w drugą stronę. Możemy więc stwierdzić, że $A = B$ *wtedy i tylko wtedy*, gdy $A \subseteq B$ oraz $B \subseteq A$.

Przy okazji powyższego dowodu, warto zwrócić uwagę na użycie „$\equiv$“ zamiast „$\Leftrightarrow$“. Ma to na celu zaznaczyć, że napis „$L \equiv P$” nie jest formułą, w przeciwieństwie do napisu „$L \Leftrightarrow P$”. Napis „$L \equiv P$” jest napisem **metajęzyka** (czyli języka, w którym rozmawiamy o matematyce, w przeciwieństwie do samego języka matematyki) oznaczającym, że napisy L oraz P są równoważne, lub, że formuła $L \Leftrightarrow P$ jest prawdziwa.

Ćwiczenie 1. Czy istnieją zbiory A i B takie, że:

- $A \in B$ i $A \subseteq B$?
- $A \in A$?
- $A \in B$ i $B \in A$
- $A \subseteq A$?

4.3. Rodziny zbiorów

Elementami zbiorów mogą być różne obiekty, w szczególności same zbiory. Łatwo jest sobie wyobrazić zbiór złożony tylko i wyłącznie ze zbiorów. Przykładem takiego zbioru może być zbiór złożony ze zbioru $\{1\}$ oraz zbioru $\{1, 2\}$, to znaczy zbiór $\{\{1\}, \{1, 2\}\}$.

Zbiór, którego elementami są inne zbiory, nazywany jest **rodziną zbiorów**. Innym przykładem rodziny zbiorów może być zbiór złożony ze zbioru liczb naturalnych i zbioru liczb rzeczywistych $\{\mathbb{N}, \mathbb{R}\}$.

Dla dowolnego zbioru A możemy zdefiniować zbiór, którego elementami są wszystkie podzbiory zbioru A. Na przykład podzbiorami zbioru $\{1, 2\}$ są zbiory $\{1\}$, $\{2\}$, $\{1, 2\}$ oraz oczywiście zbiór pusty $\emptyset$. Zbiór $\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ nazywamy **zbiorem potęgowym** zbioru $\{1, 2\}$. Podobnie, zbiorem potęgowym zbioru $\{\mathbb{N}, \mathbb{R}\}$ jest zbiór $\{\emptyset, \{\mathbb{N}\}, \{\mathbb{R}\}, \{\mathbb{N}, \mathbb{R}\}\}$.

Definicja 2 (Zbiór potęgowy)**.** Zbiorem potęgowym zbioru A, oznaczane $P(A)$, nazywamy zbiór złożony ze wszystkich podzbiorów A.

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

„Zbiór wszystkich elementów B takich, że B jest podzbiorem A"

Dowolny zbiór potęgowy jest również **rodziną zbiorów**, ponieważ jego elementami są inne zbiory.

4.4. Operacje na zbiorach

Podstawowymi operacjami, które będziemy wykonywać na zbiorach, będą operacje **sumy**, **przekroju** oraz **różnicy**. Zacznijmy od ich zdefiniowania.

Definicja 3 (Suma zbiorów)**. Sumą** zbiorów A i B nazywamy zbiór zawierający wszystkie elementy należące do zbioru A lub do zbioru B i niezawierający innych elementów. Sumę zapisywać będziemy jako $A \cup B$. Formalnie:

$$x \in A \cup B \overset{\text{def}}{\iff} x \in A \vee x \in B$$

x należy do sumy zbiorów A i B z definicji wtedy i tylko wtedy, gdy x należy do A lub x należy do B

Definicja 4 (Przekrój zbiorów)**. Przekrojem** zbiorów A i B nazywamy zbiór zawierający wszystkie elementy które należą zarówno do zbioru A jak i do zbioru B i niezawierający innych elementów. Przekrój zapisywać będziemy jako $A \cap B$. Formalnie:

$$x \in A \cap B \overset{\text{def}}{\iff} x \in A \wedge x \in B$$

x należy do przekroju zbiorów A i B z definicji wtedy i tylko wtedy, gdy x należy do A oraz x należy do B

Definicja 5 (Różnica zbiorów)**. Różnicą** zbiorów A i B nazywamy zbiór zawierający wszystkie elementy należące do zbioru A, ale nie należące do zbioru B i niezawierający innych elementów. Różnicę zapisywać będziemy jako $A \setminus B$. Formalnie:

$$x \in A \setminus B \overset{\text{def}}{\iff} x \in A \wedge x \notin B$$

x należy do różnicy zbiorów A i B z definicji wtedy i tylko wtedy, gdy x należy do A oraz x nie należy do B

Dla przykładu, dla zbiorów $A = \{1, 2, 3\}$ i $B = \{3, 4\}$, suma $A \cup B$ wynosi $\{1, 2, 3\} \cup \{3, 4\} = \{1, 2, 3, 4\}$ (ponieważ $1, 2, 3$ należą do A, a 4 należy do B), przekrój $A \cap B$ wynosi $\{1, 2, 3\} \cap \{3, 4\} = \{3\}$ (ponieważ tylko 3 należy zarówno do A jak i do B), a różnica $A \setminus B$ wynosi $\{1, 2, 3\} \setminus \{3, 4\} = \{1, 2\}$ (ponieważ $1, 2$ należą do A ale nie należą do B, z kolei 3 należy zarówno do A jak i do B).

Ćwiczenie 2. Dla poniższych zbiorów A i B, oblicz $A \cup B$, $A \cap B$ oraz $A \setminus B$.

- $A = \{1, 2\}$, $B = \{3\}$
- $A = \{3\}$, $B = \{1, 2\}$
- $A = \{1, 2\}$, $B = \emptyset$
- $A = \{1, 2\}$, $B = \{\emptyset\}$
- $A = \{\{1, 2\}, \{3, 4\}\}$, $B = \{\{1, 2\}, 3, 4\}$

Powyższe operacje posiadają wiele ciekawych własności. Dla przykładu, można pokazać, że $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Dowód. Pokażemy, że $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. W tym celu skorzystamy z faktu, że dla dowolnych zbiorów X oraz Y, jeśli $X \subseteq Y$ oraz $Y \subseteq X$ to $X = Y$. Pokażemy więc dwie inkluzje (zawierania).

1. $\underbrace{A \cup (B \cap C)}_{L} \subseteq \underbrace{(A \cup B) \cap (A \cup C)}_{P}$

   Musimy pokazać coś dla dowolnych zbiorów. Weźmy więc dowolne zbiory A, B oraz C. Z definicji zawierania musimy pokazać, że dla dowolnego x, jeśli $x \in L$ to $x \in P$. Weźmy więc dowolnego x i załóżmy, że $x \in A \cup (B \cap C)$. Z definicji oznacza to, że $x \in A$ lub $x \in B \cap C$.

   Musimy pokazać, że $x \in (A \cup B) \cap (A \cup C)$, to znaczy, z definicji przekroju zbiorów, że $x \in A \cup B$ **oraz** $x \in A \cup C$.

   Wiemy, że $x \in A$ lub $x \in B \cap C$, rozpatrzmy więc dwa przypadki:

- $x \in A$. W takim razie wiemy, z definicji sumy zbiorów, że zachodzi również $x \in A \cup B$ oraz $x \in A \cup C$ (ponieważ x należy do A, należy też do sumy A i dowolnego zbioru), a to chcieliśmy pokazać.

- $x \in B \cap C$. Z definicji przekroju oznacza to, że $x \in B$ oraz $x \in C$. Skoro $x \in B$, to z definicji sumy zbiorów, $x \in A \cup B$. Podobnie, skoro $x \in C$, to z definicji sumy zbiorów, $x \in A \cup C$. Mamy więc, że $x \in A \cup B$ oraz $x \in A \cup C$, a to chcieliśmy pokazać.

Pokazaliśmy, że jeśli $x \in A \cup (B \cap C)$ to $x \in (A \cup B) \cap (A \cup C)$, więc inkluzja zachodzi.

2. $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

   Weźmy dowolne zbiory A, B oraz C. Weźmy również dowolny element x i załóżmy, że $x \in (A \cup B) \cap (A \cup C)$. Korzystając z definicji przekroju możemy więc wywnioskować, że $x \in A \cup B$ oraz $x \in A \cup C$.

   Musimy pokazać, że $x \in A \cup (B \cap C)$, to znaczy, z definicji sumy zbiorów, że $x \in A$ **lub** $x \in B \cap C$. Rozpatrzmy dwa przypadki:

   - $x \in A$. W tym przypadku nie musimy nic pokazywać, ponieważ $x \in A$.

   - $x \notin A$. Skoro $x \in A \cup B$ oraz $x \notin A$, to z definicji sumy wiemy, że $x \in B$. Podobnie, skoro $x \in A \cup C$ oraz $x \notin A$, to z definicji sumy $x \in C$. Z definicji przekroju mamy więc, że $x \in B \cap C$, a to chcieliśmy pokazać.

   Pokazaliśmy dwie inkluzje, mamy więc, że $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ □

Powyższy dowód można przeprowadzić rozpisując definicje i korzystając z praw rachunku zdań oraz praw rachunku kwantyfikatorów.

Dowód. Pokażemy, że $\underbrace{A \cup (B \cap C)}_{L} = \underbrace{(A \cup B) \cap (A \cup C)}_{P}$.

Korzystając z definicji oraz praw rachunku zdań oraz praw rachunku kwantyfikatorów pokażemy, że napis $x \in L$ jest równoważny napisowi $x \in P$. Oznaczać to będzie, że formuła $\forall x\ (x \in L \Leftrightarrow x \in P)$ jest prawdziwa, więc, z **zasady ekstensjonalności**, $L = P$.

$$\begin{aligned} x \in L \equiv\ & x \in A \cup (B \cap C) \\ \overset{(1)}{\equiv}\ & x \in A \vee x \in (B \cap C) \\ \overset{(2)}{\equiv}\ & x \in A \vee (x \in B \wedge x \in C) \\ \overset{(3)}{\equiv}\ & (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ \overset{(4)}{\equiv}\ & x \in (A \cup B) \wedge x \in (A \cup C) \\ \overset{(5)}{\equiv}\ & x \in ((A \cup B) \cap (A \cup C)) \\ \equiv\ & x \in P \end{aligned}$$

Przejście (1) wynika z definicji sumy zbiorów. Przejście (2) wynika z definicji przekroju zbiorów. Przejście (3) wynika z *prawa rozdzielności alternatywy względem koniunkcji*. Przejście (4) również wynika z definicji sumy zbiorów, a przejście (5) z definicji przekroju zbiorów. □

Korzystając z powyższego sposobu, czasem warto jest najpierw maksymalnie rozpisać lewą i prawą stronę, a potem zauważyć związek pomiędzy nimi.

4.5. Operacje nieskończone na zbiorach

Operacje sumy i przekroju można uogólnić na dowolne rodziny zbiorów. Przypomnijmy, że rodzina zbiorów, to zbiór, którego elementami są inne zbiory.

Do tej pory mówiliśmy, że sumą $A \cup B$ nazywamy zbiór, którego każdy element należy albo do A albo do B. Gdybyśmy dodali do tej sumy kolejny zbiór i próbowali zdefiniować, co znaczy suma $A \cup B \cup C$, naturalną wydaje się być definicja mówiąca, że wynikiem będzie zbiór którego każdy element należy albo do A albo do B albo do C. Innymi słowy, należy do **któregokolwiek** ze zbiorów A, B lub C.

Podobnie sprawa ma się z przekrojem. Przekrojem $A \cap B$ nazywamy zbiór, którego każdy element należy zarówno do A jak i do B. $A \cap B \cap C$ to zbiór, którego każdy element należy do A, do B oraz do C. Innymi słowy, należy do **każdego** ze zbiorów A, B i C.

Definicja 6 (Suma rodziny zbiorów)**.** Sumą rodziny zbiorów $\mathcal{A}$ nazywać będziemy zbiór zawierający tylko elementy, które występują w **którymkolwiek** ze zbiorów należących do $\mathcal{A}$. Formalnie:

$$\bigcup \mathcal{A} = \{\ x \mid \exists X \in \mathcal{A}\ (x \in X)\ \}$$

Zbiór takich elementów x, że istnieje zbiór X należący do rodziny zbiorów A taki, że $x \in X$

Definicja 7 (Przekrój rodziny zbiorów)**.** Przekrojem rodziny zbiorów $\mathcal{A}$ nazywać będziemy zbiór zawierający tylko elementy, które występują w **każdym** ze zbiorów należących do $\mathcal{A}$. Formalnie:

$$\bigcap \mathcal{A} = \{\ x \mid \forall X \in \mathcal{A}\ (x \in X)\ \}$$

Zbiór takich elementów x, że dla każdego zbioru X należącego do rodziny zbiorów A zachodzi $x \in X$

Weźmy przykładową rodzinę zbiorów $\mathcal{A} = \{\{1,2\},\{2,3\},\{2,3,4\}\}$. Policzmy sumę rodziny zbiorów $\mathcal{A}$:

$$\begin{aligned}\bigcup \mathcal{A} &= \bigcup \{\{1,2\},\{2,3\},\{2,3,4\}\} \\ &= \{1,2\} \cup \{2,3\} \cup \{2,3,4\} \\ &= \{1,2,3\} \cup \{2,3,4\} \\ &= \{1,2,3,4\}\end{aligned}$$

Wynikiem jest więc zbiór $\{1,2,3,4\}$. Każdy z elementów tego zbioru należy bowiem do jakiegoś (przynajmniej jednego) zbioru z rodziny zbiorów $\mathcal{A}$, co więcej nie ma elementu, który należałby do jakiegoś zbioru z rodziny zbiorów $\mathcal{A}$, a nie należy do naszego wyniku. Co z przekrojem rodziny zbiorów $\mathcal{A}$?

$$\begin{aligned}\bigcap \mathcal{A} &= \bigcap \{\{1,2\},\{2,3\},\{2,3,4\}\} \\ &= \{1,2\} \cap \{2,3\} \cap \{2,3,4\} \\ &= \{2\} \cap \{2,3,4\} \\ &= \{2\}\end{aligned}$$

Wynikiem jest więc zbiór $\{2\}$. 2 jest bowiem jedynym elementem, który należy do każdego ze zbiorów z rodziny $\mathcal{A}$ (to znaczy należy do każdego ze zbiorów z rodziny $\mathcal{A}$, a także nie ma elementu, który należałby do każdego ze zbiorów z rodziny $\mathcal{A}$ a nie należałby do naszego wyniku).

Czasem będzie nam wygodnie nazywać w jakiś sposób elementy rodziny zbiorów. Dla powyższego przykładu, możemy nazwać zbiór $\{1,2\}$ jako A_1, zbiór $\{2,3\}$ jako A_2 a zbiór $\{2,3,4\}$ jako A_3. Rodzina zbiorów $\mathcal{A}$ składa się więc ze zbiorów A_1, A_2 i A_3. Taką rodzinę zbiorów $\mathcal{A}$ nazywać będziemy **rodziną zbiorów indeksowaną elementami zbioru** $\{1,2,3\}$. Oznacza to tyle, że elementami rodziny zbiorów $\mathcal{A}$ są zbiory A_1, A_2 i A_3 czyli zbiory A z indeksami będącymi liczbami 1, 2 i 3. Taką rodzinę oznaczyć możemy na przykład $\{A_i\}_{i\in\{1,2,3\}}$ lub $\{\ A_i \mid i \in \{1,2,3\}\ \}$

Zbiór indeksów może być większy. Dla przykładu, zdefiniujmy sobie najpierw zbiór $A_i = \{\ x \in \mathbb{N} \mid x \leq i\ \}$ (zbiór wszystkich liczb naturalnych mniejszych bądź

równych i). Niech teraz zbiór indeksów będzie zbiorem liczb naturalnych $\mathbb{N}$. Wtedy rodzina zbiorów $\{A_i\}_{i\in\mathbb{N}}$ wygląda następująco:

$$\begin{aligned}\{A_i\}_{i\in\mathbb{N}} &= \{A_0, A_1, A_2, A_3, \dots\} \\ &= \{\{0\}, \{0,1\}, \{0,1,2\}, \{0,1,2,3\}, \dots\}\end{aligned}$$

Zauważmy, że w powyższym przypadku kluczowe znaczenie ma poprawne zdefiniowanie zbioru indeksów. Rodzina zbiorów $\{A_i\}_{i\in\mathbb{N}}$ indeksowana liczbami naturalnymi jest bowiem inna niż rodzina $\{A_i\}_{i\in\mathbb{Z}}$ indeksowana liczbami całkowitymi, która wyglądałaby tak:

$$\begin{aligned}\{A_i\}_{i\in\mathbb{Z}} &= \{\dots, A_{-2}, A_{-1}, A_0, A_1, A_2 \dots\} \\ &= \{\dots, \emptyset, \emptyset, \{0\}, \{0,1\}, \{0,1,2\}, \dots\} \\ &= \{\emptyset, \{0\}, \{0,1\}, \{0,1,2\}, \{0,1,2,3\}, \dots\}\end{aligned}$$

Bo zbiór A_i, dla każdego $i < 0$, jest zbiorem pustym.

Oczywiście rozpatrywać możemy też pary, trójki, czwórki czy większe liczby indeksów. Zdefiniujmy sobie dla przykładu zbiór $A_{i,j} = \{\ x \in \mathbb{N} \mid i \le x \le j\ \}$ (zbiór wszystkich liczb naturalnych z przedziału $[i, j]$) dla i, j - dowolnych liczb naturalnych. Wtedy rodzina zbiorów $\{A_{i,j}\}_{\substack{i\in\mathbb{N},\\ j\in\mathbb{N}}}$ wygląda następująco:

$$\begin{aligned}\{A_{i,j}\}_{\substack{i\in\mathbb{N},\\ j\in\mathbb{N}}} &= \{\ A_{0,0},\ A_{0,1},\quad A_{0,2},\quad \dots, A_{1,0}, A_{1,1},\ A_{1,2},\ \dots, A_{2,0}, A_{2,1}, A_{2,2}, \dots\} \\ &= \{\ \{0\},\ \{0,1\}, \{0,1,2\}, \dots,\quad \emptyset,\quad \{1\},\ \{1,2\}, \dots,\quad \emptyset,\quad \emptyset,\quad \{2\},\ \dots\}\end{aligned}$$

Definicje sumy i przekroju indeksowanych rodzin zbiorów są takie same jak w przypadku zwykłych rodzin zbiorów. Dla rodziny zbiorów $\{A_i\}_{i\in I}$, sumę $\bigcup\{A_i\}_{i\in I}$ dla uproszczenia oznaczać będziemy $\bigcup\limits_{i\in I} A_i$, podobnie przekrój $\bigcap\{A_i\}_{i\in I}$ oznaczać będziemy $\bigcap\limits_{i\in I} A_i$.

Spójrzmy na wyrażenie $x \in \bigcup\limits_{i\in I} A_i$. Z definicji sumy rodziny zbiorów, oznacza to, że istnieje jakiś zbiór X w rodzinie zbiorów $\{A_i\}_{i\in I}$, taki, że $x \in X$. W przypadku indeksowanej rodziny zbiorów, oznacza to, że **istnieje** pewien **indeks** $i' \in I$, taki, że $x \in A_{i'}$.

Podobnie, w przypadku przekroju indeksowanej rodziny zbiorów, wyrażenie $x \in \bigcap\limits_{i\in I} A_i$ oznacza, że **dla każdego indeksu** $i' \in I$, $x \in A_{i'}$.

Przykład 1. Rozpatrzmy zbiory $A_{i,j} = \{i, i+1, \ldots, i+j-1\}$ gdzie $i \in \mathbb{Z}$ jest dowolną liczbą całkowitą, a $j \in \mathbb{N}$ jest dowolną liczbą naturalną. Jak nietrudno zauważyć, jest to zbiór j kolejnych liczb całkowitych, poczynając od i. Przykładowo, $A_{-1,10}$ jest zbiorem $\{-1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$, z kolei zbiór $A_{1,0}$ jest zbiorem pustym. Policzmy następujące zbiory:

1. $\bigcup_{j\geq 0} A_{0,j}$

   Mamy więc sumę rodziny zbiorów $\{A_{0,j}\}_{j\geq 0} = \{A_{0,0}, A_{0,1}, A_{0,2}, \ldots\}$. Zgodnie z definicją, każdy element tej sumy należy do zbioru $A_{0,j'}$ dla **jakiegoś** indeksu $j' \geq 0$. Wynik możemy policzyć, wykonując operację sumy na kolejnych elementach indeksowanej rodziny zbiorów:

   $$\begin{aligned}\bigcup_{j\geq 0} A_{0,j} &= A_{0,0} \cup A_{0,1} \cup A_{0,2} \cup A_{0,3} \cup \ldots \\ &= \emptyset \cup \{0\} \cup \{0,1\} \cup \{0,1,2\} \cup \ldots \\ &= \{0, 1, 2, 3, \ldots\} \\ &= \mathbb{N}\end{aligned}$$

   Mamy więc $\bigcup_{j\geq 0} A_{0,j} = \mathbb{N}$. Powyższe obliczenia nie są jednak jeszcze dowodem, a jedynie pewnym sposobem dotarcia do wyniku. Równość jeszcze należy udowodnić.

   Dowód. Pokażemy, że $\bigcup_{j\geq 0} A_{0,j} = \mathbb{N}$. W tym celu pokażemy dwa zawierania.

   - $\bigcup_{j\geq 0} A_{0,j} \subseteq \mathbb{N}$

     Weźmy dowolny element $x \in \bigcup_{j\geq 0} A_{0,j}$. Z definicji zawierania musimy pokazać, że $x \in \mathbb{N}$.

     Wiemy, że $x \in \bigcup_{j\geq 0} A_{0,j}$, co z definicji sumy rodziny zbiorów oznacza, że istnieje taki indeks $j' \geq 0$, że $x \in A_{0,j'}$.

     Weźmy więc taki indeks $j' \geq 0$, że $x \in A_{0,j'}$. Ponownie skorzystajmy z definicji, tym razem definicji zbioru $A_{0,j'}$.

     Zbiór $A_{0,j'}$ jest zbiorem j' kolejnych liczb całkowitych, począwszy od zera, więc każdy jego element jest liczbą naturalną. W takim razie x, będący pewnym elementem zbioru $A_{0,j'}$ także jest liczbą naturalną, więc $x \in \mathbb{N}$, a to chcieliśmy pokazać.

   - $\mathbb{N} \subseteq \bigcup_{j\geq 0} A_{0,j}$

     Weźmy dowolny element $x \in \mathbb{N}$. Z definicji zawierania musimy pokazać, że $x \in \bigcup_{j\geq 0} A_{0,j}$. Musimy więc pokazać, że istnieje taki indeks $j' \geq 0$, że $x \in A_{0,j'}$.

     Niech więc $j' = x + 1$. Musimy pokazać, że $j' \geq 0$ oraz $x \in A_{0,j'}$

– Wiemy, że x jest liczbą naturalną, więc $x + 1 = j' \geq 0$.

– Z definicji zbioru $A_{0,j'}$:

$$A_{0,j'} = A_{0,x+1} = \{0, 1, 2, \ldots, x + 1 - 1\} = \{0, 1, 2, \ldots, x\}$$

Więc rzeczywiście $x \in A_{0,j'}$.

□

2. $\bigcup_{j\geq 0} A_{i,j}$

$$\begin{aligned}\bigcup_{j\geq 0} A_{i,j} &= A_{i,0} \cup A_{i,1} \cup A_{i,2} \cup A_{i,3} \cup \ldots \\ &= \emptyset \cup \{i\} \cup \{i, i+1\} \cup \{i, i+1, i+2\} \cup \ldots \\ &= \{i, i+1, i+2, \ldots\} \\ &= \{\ x \in \mathbb{Z} \mid x \geq i\ \}\end{aligned}$$

Mamy więc $\bigcup_{j\geq 0} A_{i,j} = \{\ x \in \mathbb{Z} \mid x \geq i\ \}$. Powyższe obliczenia nie są jednak jeszcze dowodem, a jedynie pewnym sposobem dotarcia do wyniku. Równość jeszcze należy udowodnić.

Dowód. Pokażemy, że $\bigcup_{j\geq 0} A_{i,j} = \{\ x \in \mathbb{Z} \mid x \geq i\ \}$. W tym celu pokażemy dwa zawierania.

- $\bigcup_{j\geq 0} A_{i,j} \subseteq \{\ x \in \mathbb{Z} \mid x \geq i\ \}$

  Weźmy dowolny element $x \in \bigcup_{j\geq 0} A_{i,j}$. Z definicji zawierania musimy pokazać, że $x \in \{\ x \in \mathbb{Z} \mid x \geq i\ \}$ to znaczy, że $x \in \mathbb{Z}$ oraz $x \geq i$.

  Wiemy, że $x \in \bigcup_{j\geq 0} A_{i,j}$, co z definicji sumy rodziny zbiorów oznacza, że istnieje indeks $j' \geq 0$ taki, że $x \in A_{i,j'}$.

  Weźmy więc taki indeks $j' \geq 0$, że $x \in A_{i,j'}$ i skorzystajmy z definicji zbioru $A_{i,j'}$. Zbiór $A_{i,j'}$ jest zbiorem j' kolejnych liczb całkowitych, począwszy od i. Element x pochodzący ze zbioru $A_{i,j'}$ jest więc liczbą całkowitą większą od i, więc $x \in \{\ x \in \mathbb{Z} \mid x \geq i\ \}$.

- $\{\ x \in \mathbb{Z} \mid x \geq i\ \} \subseteq \bigcup_{j\geq 0} A_{i,j}$

  Weźmy dowolny element $x \in \mathbb{Z}$, $x \geq i$. Z definicji zawierania musimy pokazać, że $x \in \bigcup_{j\geq 0} A_{i,j}$, to znaczy, że istnieje taki indeks $j' \geq 0$, że $x \in A_{i,j'}$.

  Niech więc $j' = x - i + 1$. Musimy pokazać, że $j' \geq 0$ oraz, że $x \in A_{i,j'}$.

  – Wiemy, że $x \geq i$, więc $x - i + 1 = j' \geq 0$.

– Z definicji zbioru $A_{i,j'}$:

$$A_{i,j'} = A_{i,x-i+1} = \{i, i+1, \ldots, i+x-i+1-1\} = \{i, i+1, \ldots, x\}$$

Co oznacza, że $x \in A_{i,j'}$.

□

3. $\bigcap\limits_{j\geq 1} A_{0,j}$

Mamy więc przekrój rodziny zbiorów $\{A_{0,j}\}_{j\geq 1} = \{A_{0,1}, A_{0,2}, A_{0,3}, \ldots\}$. Zgodnie z definicją, każdy element tego przekroju należy do zbioru $A_{0,j'}$ dla **dowolnego** indeksu $j' \geq 1$. Wynik możemy policzyć, wykonując operację przekroju na kolejnych elementach indeksowanej rodziny zbiorów:

$$\begin{aligned}\bigcap_{j\geq 1} A_{0,j} &= A_{0,1} \cap A_{0,2} \cap A_{0,3} \cap \ldots \\ &= \{0\} \cap \{0,1\} \cap \{0,1,2\} \cap \ldots \\ &= \{0\}\end{aligned}$$

Mamy więc $\bigcap\limits_{j\geq 1} A_{0,j} = \{0\}$.

Dowód. Pokażemy, ze $\bigcap\limits_{j\geq 1} A_{0,j} = \{0\}$. W tym celu pokażmy dwa zawierania

- $\bigcap\limits_{j\geq 1} A_{0,j} \subseteq \{0\}$

  Weźmy dowolny element $x \in \bigcap\limits_{j\geq 1} A_{0,j}$. Z definicji zawierania musimy pokazać, że $x \in \{0\}$.

  Wiemy, że $x \in \bigcap\limits_{j\geq 1} A_{0,j}$ co z definicji przekroju rodziny zbiorów oznacza, że dla każdego indeksu $j' \geq 1$, $x \in A_{0,j'}$.

  Skoro dla każdego indeksu $j' \geq 1$ zachodzi $x \in A_{0,j'}$, to w szczególności dla indeksu $j' = 1$ zachodzi $x \in A_{0,1}$, a z definicji $A_{0,1} = \{0\}$, więc $x \in \{0\}$, a to chcieliśmy pokazać.

- $\{0\} \subseteq \bigcap\limits_{j\geq 1} A_{0,j}$

  Weźmy dowolny element $x \in \{0\}$. Z definicji zawierania musimy pokazać, że $x \in \bigcap\limits_{j\geq 1} A_{0,j}$, to znaczy, że dla każdego indeksu $j' \geq 1$, $x \in A_{0,j'}$.

  Zauważmy, że $x = 0$, ponieważ zbiór $\{0\}$ ma jeden element. Musimy więc pokazać, że dla dowolnego indeksu $j' \geq 1$, $0 \in A_{0,j'}$.

  Weźmy więc dowolny indeks $j' \geq 1$. $A_{0,j'}$ jest zbiorem j' kolejnych elementów, począwszy od 0. To znaczy, $A_{0,j'} = \{0, 1, \ldots, j'-1\}$. Skoro $j' \geq 1$, to $0 \in A_{0,j'}$, a to chcieliśmy pokazać.

□

4. $\bigcap\limits_{j\geq 1} A_{i,j}$

$$\begin{aligned}\bigcap_{j\geq 1} A_{i,j} &= A_{i,1} \cap A_{i,2} \cap A_{i,3} \cap \dots \\ &= \{i\} \cap \{i, i+1\} \cap \{i, i+1, i+2\} \cap \dots \\ &= \{i\}\end{aligned}$$

Mamy więc $\bigcap\limits_{j\geq 1} A_{i,j} = \{i\}$.

Dowód. Pokażemy, ze $\bigcap\limits_{j\geq 1} A_{i,j} = \{i\}$. W tym celu pokażmy dwa zawierania

- $\bigcap\limits_{j\geq 1} A_{i,j} \subseteq \{i\}$
  Weźmy dowolny element $x \in \bigcap\limits_{j\geq 1} A_{i,j}$. Z definicji zawierania musimy pokazać, że $x \in \{i\}$.
  Wiemy, że $x \in \bigcap\limits_{j\geq 1} A_{i,j}$ co z definicji przekroju rodziny zbiorów oznacza, że dla każdego indeksu $j' \geq 1$, $x \in A_{i,j'}$.
  Skoro dla każdego indeksu $j' \geq 1$ zachodzi $x \in A_{0,j'}$, to w szczególności dla indeksu $j' = 1$, $x \in A_{i,1}$. Z definicji zbioru $A_{i,1} = \{i\}$, więc $x \in \{i\}$, a to właśnie chcieliśmy pokazać.
- $\{i\} \subseteq \bigcap\limits_{j\geq 1} A_{i,j}$
  Weźmy dowolny element $x \in \{i\}$. Z definicji zawierania musimy pokazać, że $x \in \bigcap\limits_{j\geq 1} A_{i,j}$, to znaczy, że dla każdego indeksu $j' \geq 1$, $x \in A_{i,j'}$.
  Zauważmy, że $x = i$, ponieważ zbiór $\{i\}$ ma jeden element. Musimy więc pokazać, że dla dowolnego indeksu $j' \geq 1$, $i \in A_{0,j'}$.
  Weźmy więc dowolny indeks $j' \geq 1$. $A_{i,j'}$ jest zbiorem j' kolejnych elementów, począwszy od i. To znaczy $A_{i,j'} = \{i, i+1, \dots, i+j'-1\}$. Skoro $j' \geq 1$, to $i \in A_{i,j'}$.

□

5. $\bigcap\limits_{i\leq 3} \bigcup\limits_{j\geq 0} A_{i,j}$
   W tym przypadku zacznijmy od środka. Zdefiniujmy najpierw zbiór $B_i = \bigcup\limits_{j\geq 0} A_{i,j}$. Z jednego z poprzednich punktów wiemy, że $B_i = \{\ x \in \mathbb{Z} \mid x \geq i\ \}$. Wystarczy więc policzyć $\bigcap\limits_{i\leq 3} B_i$.

$$\begin{aligned}\bigcap_{i\leq 3} B_i &= B_3 \cap B_2 \cap B_1 \cap B_0 \cap B_{-1} \cap \dots \\ &= \{3, 4, 5, \dots\} \cap \{2, 3, 4, \dots\} \cap \dots \\ &= \{3, 4, 5, \dots\} \\ &= \{\ x \in \mathbb{Z} \mid x \geq 3\ \}\end{aligned}$$

Dowód. Pokażemy, że $\bigcap_{i\leq 3} B_i = \{\ x \in \mathbb{Z} \mid x \geq 3\ \}$

- $\bigcap_{i\leq 3} B_i \subseteq \{\ x \in \mathbb{Z} \mid x \geq 3\ \}$
  Weźmy dowolny $x \in \bigcap_{i\leq 3} B_i$. Z definicji zawierania musimy pokazać, że $x \in \{\ x \in \mathbb{Z} \mid x \geq 3\ \}$.
  Wiemy, że $x \in \bigcap_{i\leq 3} B_i$ co z definicji przekroju rodziny zbiorów oznacza, że dla każdego indeksu $i' \leq 3$, $x \in B_{i'}$.
  Skoro dla każdego indeksu $i' \leq 3$, $x \in B_{i'}$, to w szczególności dla indeksu $i' = 3$ zachodzi $x \in B_3$. Z definicji $B_3 = \{\ \mathbb{Z} \mid x \geq 3\ \}$, więc $x \in \{\ \mathbb{Z} \mid x \geq 3\ \}$, a to chcieliśmy pokazać.
- $\{\ x \in \mathbb{Z} \mid x \geq 3\ \} \subseteq \bigcap_{i\leq 3} B_i$
  Weźmy dowolny $x \in \{\ x \in \mathbb{Z} \mid x \geq 3\ \}$. Z definicji zawierania musimy pokazać, że $x \in \bigcap_{i\leq 3} B_i$, to znaczy, że dla każdego indeksu $i' \leq 3$, $x \in B_{i'}$.
  Weźmy więc dowolny indeks $i' \leq 3$. Wiemy, że $x \in \{\ x \in \mathbb{Z} \mid x \geq 3\ \}$, co znaczy, że $x \in \mathbb{Z}$ oraz $x \geq 3$. Skoro $x \geq 3$ i $3 \geq i'$, to $x \geq i'$.
  Skoro $x \geq i'$ oraz $x \in \mathbb{Z}$, to $x \in \{\ x \in \mathbb{Z} \mid x \geq i'\ \}$ więc $x \in B_{i'}$.

□

6. $\bigcup_{i\leq -3} \bigcap_{j\geq 1} A_{i,j}$
   Podobnie jak poprzednio, zacznijmy od środka. Niech $B_i = \bigcap_{j\geq 1} A_{i,j}$. Z jednego z poprzednich punktów wiemy, że $B_i = \{i\}$. Wystarczy więc policzyć $\bigcup_{i\leq -3} B_i$

$$\begin{aligned}\bigcup_{i\leq -3} B_i &= B_{-3} \cup B_{-4} \cup B_{-5} \cup \dots \\ &= \{-3\} \cup \{-4\} \cup \{-5\} \cup \dots \\ &= \{-3, -4, -5, \dots\} \\ &= \{\ x \in \mathbb{Z} \mid x \leq -3\ \}\end{aligned}$$

Dowód. Pokażemy, że $\bigcup_{i\leq -3} B_i = \{\ x \in \mathbb{Z} \mid x \leq -3\ \}$

- $\bigcup_{i\leq -3} B_i \subseteq \{\ x \in \mathbb{Z} \mid x \leq -3\ \}$
  Weźmy dowolny $x \in \bigcup_{i\leq -3} B_i$. Z definicji zawierania musimy pokazać, że $x \in \mathbb{Z}$ oraz $x \leq -3$.
  Wiemy, że $x \in \bigcup_{i\leq -3} B_i$ co z definicji sumy rodziny zbiorów oznacza, że istnieje indeks $i' \in \mathbb{Z}$, $i' \leq -3$ taki, że $x \in B_{i'}$.
  Weźmy więc taki indeks $i' \in \mathbb{Z}$, $i' \leq -3$, że $x \in B_{i'}$.

Z definicji zbioru $B_{i'} = \{i'\}$. Skoro $x \in \{i'\}$, to $x = i'$ (bo $\{i'\}$ ma jeden element), a skoro $i' \leq -3$ oraz $i' \in \mathbb{Z}$, to $x \leq -3$ oraz $x \in \mathbb{Z}$. Oznacza to, że $x \in \{\ x \in \mathbb{Z} \mid x \leq -3\ \}$, a to chcieliśmy pokazać.

- $\{\ x \in \mathbb{Z} \mid x \leq -3\ \} \subseteq \bigcup_{i \leq -3} B_i$

  Weźmy dowolny $x \in \{\ x \in \mathbb{Z} \mid x \leq -3\ \}$. Z definicji zawierania musimy pokazać, że $x \in \bigcup_{i \leq -3} B_i$, to znaczy, że istnieje indeks $i' \leq -3$ taki, że $x \in B_{i'}$.

  Niech więc $i' = x$. Musimy pokazać, że $i' \leq -3$ oraz, że $x \in B_{i'}$

  – Skoro $x \in \{\ x \in \mathbb{Z} \mid x \leq -3\ \}$, to $x \leq -3$, więc $x = i' \leq -3$.
  – Wiemy, że $x \in \{x\}$, oraz $\{x\} = B_x = B_{i'}$, więc $x \in B_{i'}$.

□

Powyższe ćwiczenie powinno przede wszystkim pokazać, że o ile być może łatwiej jest sobie na początku wyobrazić sumę i przekrój rodziny zbiorów jako wykonanie operacji sumy/przekroju na kolejnych elementach rodziny zbioru, to jest to tylko intuicja, dzięki której możemy dojść do jakiegoś wyniku. Otrzymany wynik należy jeszcze udowodnić zgodnie z podanymi definicjami, co zazwyczaj sprowadza się do pokazania równości zbiorów (początkowego i wynikowego). Dowody równości zbiorów mogą, jak w ćwiczeniu powyżej, zostać przeprowadzone opisowo, ale mogą być także przeprowadzone za pomocą rozpisania definicji i korzystania z praw rachunku zdań oraz praw rachunku kwantyfikatorów.

Rozdział 5.

Relacje

5.1. Pary

Parę uporządkowaną (lub po prostu **parę**) zapisywać będziemy w postaci $\langle a, b\rangle$. Para jest jednym z **pojęć pierwotnych**. Przyjmiemy, że para spełnia następujący aksjomat:

Aksjomat 1. $\langle a, b\rangle = \langle c, d\rangle$ wtedy i tylko wtedy, gdy $a = c$ oraz $b = d$.

Aksjomat ten mówi, że dwie pary są równe, jeśli są równe zarówno na pierwszym jak i na drugim elemencie. To znaczy, że pary $\langle 1, 2\rangle$ i $\langle 1, 3\rangle$ nie są równe (bo są różne na drugim elemencie), natomiast pary $\langle 1, 2\rangle$ oraz $\langle 1, 2\rangle$ są.

Zbiór wszystkich par, których pierwszy element pochodzi z jakiegoś zbioru A a drugi z jakiegoś zbioru B nazywać będziemy **iloczynem kartezjańskim** i zapisywać jako $A \times B$. Formalnie:

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

Dla przykładu, dla zbiorów $A = \{1, 2\}$ oraz $B = \{3, 4\}$, iloczyn kartezjański $A \times B$ to zbiór $\{1, 2\} \times \{3, 4\} = \{\langle 1, 3\rangle, \langle 1, 4\rangle, \langle 2, 3\rangle, \langle 2, 4\rangle\}$.

Ćwiczenie 1. Zapisz iloczyny kartezjańskie poniższych zbiorów:

- $A = \{1\}$, $B = \{1, 2\}$
- $A = \{1, 2\}$, $B = \{1, 2\}$
- $A = \emptyset$, $B = \{1, 2\}$
- $A = \{1, 2\}$, $B = \emptyset$
- $A = \emptyset$, $B = \emptyset$

Czasem, zamiast pisać $A \times A$ (zbiór wszystkich par w których zarówno pierwszy jak i drugi element pochodzą ze zbioru A) będziemy pisać A^2.

Przyjrzyjmy się teraz poniższej równości:

$$\underbrace{(A \cap B) \times C}_{L} = \underbrace{(A \times C) \cap (B \times C)}_{P}$$

Jak stwierdzić, czy jest ona prawdziwa?

Zarówno L jak i P są **zbiorami**. Wiemy, że są one równe, jeśli dla dowolnego elementu $z \in L$, $z \in P$ oraz dla dowolnego elementu $z \in P$, $z \in L$. Elementami zarówno zbioru L jak i zbioru P są **pary**. Weźmy więc dowolną parę $\langle x, y \rangle \in L$

$$\begin{aligned} \langle x, y \rangle \in L &\equiv \langle x, y \rangle \in (A \cap B) \times C \\ &\overset{(1)}{\equiv} x \in (A \cap B) \wedge y \in C \\ &\overset{(2)}{\equiv} x \in A \wedge x \in B \wedge y \in C \end{aligned}$$

Przejście (1) wynika wprost z definicji **iloczynu kartezjańskiego** który poznaliśmy w tym rozdziale: para $\langle x, y \rangle$ należy do iloczynu kartezjańskiego $(A \cap B) \times C$, z definicji wtedy i tylko wtedy gdy x należy do $A \cap B$, a y należy do C. Przejście (2) wynika z definicji przekroju zbiorów, którą już znamy.

Weźmy teraz dowolną parę $\langle x, y \rangle \in P$

$$\begin{aligned} \langle x, y \rangle \in P &\equiv \langle x, y \rangle \in (A \times C) \cap (B \times C) \\ &\overset{(1)}{\equiv} \langle x, y \rangle \in (A \times C) \wedge \langle x, y \rangle \in (B \times C) \\ &\overset{(2)}{\equiv} x \in A \wedge y \in C \wedge x \in B \wedge y \in C \\ &\overset{(3)}{\equiv} x \in A \wedge y \in C \wedge x \in B \\ &\overset{(4)}{\equiv} x \in A \wedge y \in B \wedge x \in C \\ &\overset{(5)}{\equiv} x \in (A \cap B) \wedge y \in C \\ &\overset{(6)}{\equiv} \langle x, y \rangle \in (A \cap B) \times C \equiv \langle x, y \rangle \in L \end{aligned}$$

Przejście (1) wynika z definicji przekroju zbiorów, przejście (2) wynika z definicji iloczynu kartezjańskiego, przejścia (3) oraz (4) wynikają z własności formuł rachunku zdań ($\varphi \wedge \varphi \equiv \varphi$ oraz przemienność koniunkcji) natomiast przejścia (5) i (6) rozpisaliśmy wyżej.

Możemy z tego wywnioskować, że $pairxy \in L \equiv \langle x, y \rangle \in P$. Skoro napisy te są równoważne, to dowolny element należący do L należy też do P, a dowolny element

należący do P należy też do L. To oznacza, że zbiory L oraz P są równe, więc równość

$$\underbrace{(A \cap B) \times C}_{L} = \underbrace{(A \times C) \cap (B \times C)}_{P}$$

Jest prawdziwa.

5.2. Relacje

Relacją binarną (lub dwuargumentową) nazywać będziemy dowolny zbiór **par**, których pierwszy element należy do zbioru A, a drugi element do zbioru B. Bardziej formalnie:

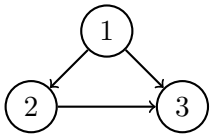
Definicja 1 (Relacja binarna)**.** Relacją binarną (dwuargumentową) nazywamy dowolny podzbiór $R \subseteq A \times B$.

Elementy a i b są **w relacji** R, jeśli para $\langle a, b\rangle$ jest elementem zbioru R. Podzbiory $A \times A$ (czyli zbiory par z których zarówno pierwszy jak i drugi element pochodzą ze zbioru A), nazywamy **relacjami binarnymi na zbiorze** A.

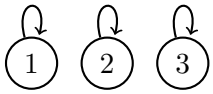
Przykładem relacji może być znana nam relacja **mniejszości** na zbiorze liczb naturalnych ($\{\ \langle x, y\rangle \in \mathbb{N}^2 \mid x < y\ \}$): liczby naturalne x i y są w relacji (xRy)), jeśli x jest **mniejsze** niż y. Relacją jest także relacja **identyczności** na zbiorze liczb naturalnych ($I_{\mathbb{N}} = \{\ \langle x, x\rangle \in \mathbb{N}^2 \mid x \in \mathbb{N}\ \}$): każda liczba naturalna jest w relacji jedynie z samą sobą (xRx dla każdej liczby naturalnej). Inną relacją jest relacja **bycia kwadratem** ($\{\ \langle x, y\rangle \in \mathbb{Z} \times \mathbb{N} \mid y = x^2\ \}$): dowolna liczba całkowita x jest w relacji z liczbą naturalną, będącą kwadratem liczby x.

Relację binarną na zbiorze A (to znaczy relację $R \subseteq A \times A$) wyobrażać sobie można jako **graf skierowany**: zbiór **wierzchołków** (reprezentujących elementy zbioru A), które mogą być połączone **krawędziami** (reprezentującymi relację) tak, że każda krawędź zaczyna się i kończy w jakimś wierzchołku.

Przykładowo, rozpatrzmy relację mniejszości na zbiorze $\{1, 2, 3\}$, to znaczy $R = \{\ \langle x, y\rangle \in \{1, 2, 3\}^2 \mid x < y\ \}$, czyli zbiór par $\{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle\}$. Relację tą możemy sobie wyobrażać jako następujący graf:



Podobnie możemy przedstawić relację identyczności na tym samym zbiorze: $I_{\{1,2,3\}} = \{\ \langle x, x\rangle \in \{1, 2, 3\}^2 \mid x \in \{1, 2, 3\}\ \}$, czyli zbiór par $\{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$. Tą relację możemy sobie wyobrażać jako następujący graf:



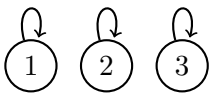
Relacje na dowolnym zbiorze A (czyli relacje $R \subseteq A \times A$) mogą posiadać różne własności:

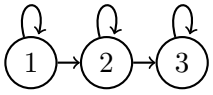
Definicja 2. Relacja $R \subseteq A \times A$ jest:

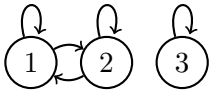
- **zwrotna**, jeśli dla wszystkich $a \in A$ zachodzi aRa (czyli dla każdego a, a jest w relacji z samym sobą).
- **symetryczna**, jeśli dla wszystkich $a, b \in A$, jeśli aRb, to bRa (czyli dla każdych a, b jeśli a jest w relacji z b, to b jest w relacji z a).
- **przechodnia**, jeśli dla wszystkich $a, b, c \in A$, jeśli aRb oraz bRc, to aRc (czyli dla każdych a, b, c jeśli a jest w relacji z b i b jest w relacji z c, to a jest w relacji z c).
- **antyzwrotna**, jeśli dla każdego a, **nie** zachodzi aRa (czyli dla każdego a, a nie jest w relacji z a).
- **antysymetryczna**, jeśli dla wszystkich a, b, jeśli aRb, to nie zachodzi bRa (czyli, dla dowolnych a, b, jeśli a jest w relacji z b, to b nie jest w relacji z a).
- **słabo antysymetryczna**, jeśli dla wszystkich a, b, jeśli aRb oraz bRa, to $a = b$ (czyli, dla dowolnych a, b, jeśli a jest w relacji z b, oraz b jest w relacji z a, to a jest równie b).

Poniżej przedstawiamy graficzne (grafowe) zobrazowanie podanych wyżej definicji:

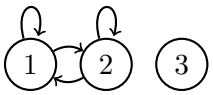
- Relacja jest zwrotna, jeśli dla każdego $a \in A$ zachodzi aRa. W przypadku grafu oznacza to, że każdy element ma krawędź do samego siebie. Poniższe relacje są przykładami relacji zwrotnych:





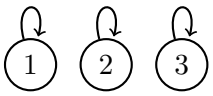


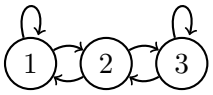
z kolei



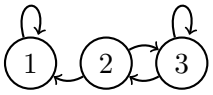
relacją zwrotną nie jest (ponieważ 3 nie jest w relacji z 3).

- Relacja jest symetryczna, jeśli dla każdego $a, b \in A$, jeśli aRb to bRa. W przypadku grafu oznacza to, że dla dowolnych elementów, jeśli istnieje krawędź z jednego do drugiego, to istnieje także krawędź w drugą stronę. Przykładowo, poniższe relacje są symetryczne:

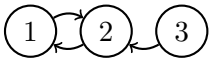




z kolei

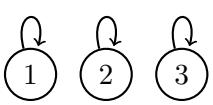


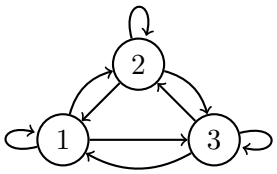
nie jest relacją symetryczną – elementy 1 i 2 są w relacji, natomiast 2 i 1 nie są. Podobnie



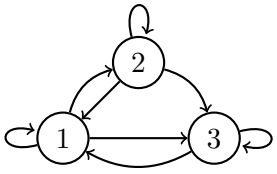
nie jest relacją symetryczną, bo elementy 3 i 2 są w relacji, a 2 i 3 nie są.

- Relacja jest przechodnia, jeśli dla wszystkich $a, b, c \in A$, jeśli aRb i bRc to aRc. W przypadku grafów oznacza to, że jeśli z jakiegoś wierzchołka do innego potrafię dotrzeć w dwóch krokach, to powinienem też móc tam dotrzeć w jednym kroku. Poniższe relacje są przykładami relacji przechodnich:

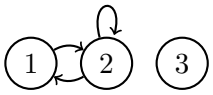




z kolei

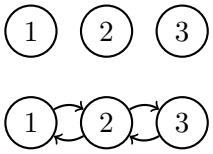


relacją przechodnią nie jest – 3 jest w relacji z 1 (pierwszy krok), 1 jest w relacji z 2 (drugi krok), ale 3 nie jest w relacji z 2 (czyli z 3 do 2 możemy dotrzeć w dwóch krokach, ale nie możemy dotrzeć w jednym). Relacja

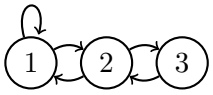


również **nie jest** przechodnia – 1 jest w relacji z 2 (pierwszy krok) a 2 jest w relacji z 1, ale 1 nie jest w relacji z 1 (z 1 do 1 mogę dotrzeć w dwóch krokach, ale nie mogę dotrzeć w jednym).

- Relacja jest antyzwrotna, jeśli dla każdego $a \in A$ nie zachodzi aRa. W przypadku grafu oznacza to, że nie ma elementu który ma krawędź sam do siebie. Poniższe relacje są przykładami relacji antyzwrotnych:

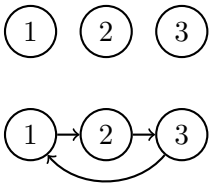


z kolei relacja

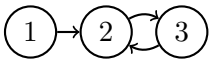


antyzwrotna nie jest, ponieważ 1 jest w relacji z samą sobą (1 ma strzałkę do samego siebie).

- Relacja jest antysymetryczna, jeśli dla wszystkich $a, b \in A$, jeśli aRb to nie zachodzi bRa. W przypadku grafów oznacza to, że jeśli istnieje krawędź w jedną stronę, to nie istnieje krawędź w drugą. Ponosze relacje są przykładami relacji antysymetrycznych:



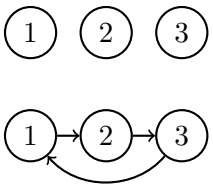
z kolei relacja



antysymetryczna nie jest – 2 jest w relacji z 3 oraz 3 jest w relacji z 2. Relacja

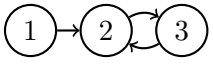
także nie jest antysymetryczna – 3 jest w relacji z 3 oraz 3 jest w relacji z 3 (dla **każdych** a, b jeśli aRb, to nie może zachodzić bRa – skoro dla każdych, to w szczególności dla $a = b = 3$).

- Relacja jest słabo antysymetryczna, jeśli dla wszystkich $a, b \in A$, jeśli aRb i bRa, to $a = b$. Zauważmy, że dowolna relacja antysymetryczna jest też słabo antysymetryczna. W przypadku grafu oznacza to więc, że jeśli istnieje krawędź w jedną stronę, to nie istnieje krawędź w drugą, **chyba, że** jest to „pętla" (krawędź z wierzchołka do jego samego, czyli aRa). Relacje



są słabo antysymetryczne (ponieważ są też antysymetryczne). Dodatkowo, relacja

która, jak ustaliliśmy wcześniej, antysymetryczna nie jest, jest słabo antysymetryczna. Relacja



nie jest jednak słabo antysymetryczna – 2 jest w relacji z 3 i 3 jest w relacji z 2, jednak $2 \neq 3$ (istnieje krawędź w jedną i w drugą stronę, ale nie jest to krawędź z wierzchołka do samego siebie).

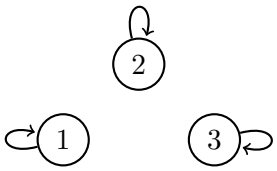
Czy istnieje relacja, która jest zarazem antysymetryczna jak i zwrotna? Wydaje się, że odpowiedź to **nie** – skoro każdy element musi mieć krawędź do samego siebie (być w relacji z samym sobą), wyklucza to antysymetryczność. Zaskakująco jednak, odpowiedź brzmi **tak**. Przykładem takiej relacji jest relacja **pusta** na zbiorze **pustym**: relacja, w której nie ma żadnych elementów, nad zbiorem w którym także nie ma żadnych elementów. Taka relacja spełnia wszystkie kryteria bycia relacją (jest zbiorem par), relacji zwrotnej (**dla każdego** elementu $a \in \emptyset$, a wiemy, że taki element nie istnieje) oraz relacji słabo antysymetrycznej (nie ma żadnej krawędzi, więc w szczególności nie zachodzi sytuacja, że jest krawędź w jedną stronę i krawędź w drugą stronę). Analogicznie można myśleć o tym, że nie znajdziemy **kontrprzykładu** na fakt, że relacja **jest zwrotna**: żeby relacja nie była zwrotna, musi istnieć wierzchołek, który nie ma krawędzi sam do siebie (czyli istnieć element, który nie jest ze sobą w relacji), jednak takiego elementu nie znajdziemy, ponieważ zbiór, na którym określamy relację, jest pusty.

Relacja pusta na zbiorze pustym jest szczególnym przypadkiem relacji, która spełnia wszystkie powyższe definicje: jest **przechodnia**, **zwrotna** i **antyzwrotna**, **symetryczna** i **antysymetryczna** a także **słabo antysymetryczna**. Zauważmy, że jeśli zbiór, na którym określamy relację, ma przynajmniej jeden element, to spełnienie wszystkich definicji jednocześnie jest niemożliwe: w szczególności, relacja na zbiorze który posiada przynajmniej jeden element nie może być jednocześnie zwrotna i antysymetryczna (ponieważ istnieje element $a \in A$ taki, że aRa, ale skoro istnieje takie a, że aRa, to z definicji relacja nie jest antysymetryczna).

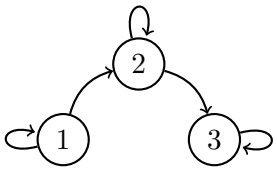
Przykład 1. Czy istnieje relacja, która jest zwrotna i symetryczna, ale nie jest przechodnia?

Spróbujmy zbudować taką relację. Zacznijmy więc od zdefiniowania zbioru A, na którym będziemy relację określać. Wiemy, z wcześniejszych obserwacji, że dla $A = \emptyset$ (dla której istnieje tylko jedna relacja – relacja pusta), relacja będzie symetryczna. Dla zbioru $A = \{1\}$, istnieje tylko jedna relacja zwrotna:

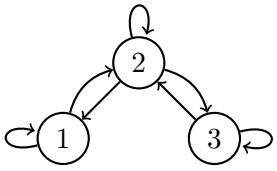
Powyższa relacja jest jednak przechodnia. W zbiorze $\{1, 2\}$ są tylko cztery relacje zwrotne, jednak wszystkie z nich są przechodnie (łatwo jest rozrysować wszystkie cztery i sprawdzić). Spróbujmy więc rozpatrzeć zbiór $\{1, 2, 3\}$. Wszystkie relacje, które powstaną przez dorysowanie krawędzi do relacji



będą zwrotne. Przykładem relacji zwrotnej, która nie jest przechodnia, może być następująca relacja:



W powyższej relacji mamy 1 w relacji z 2 i 2 w relacji z 3, ale 1 nie jest w relacji z 3. Relacja ta nie jest jednak symetryczna. Spróbujmy więc sprawić, żeby była:



Relacja ta jest zwrotna, jest symetryczna ale nie jest przechodnia. Powyższa relacja jest więc odpowiedzią. Zapiszmy tą relację jako zbiór par:

$$R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,2\rangle, \langle 3,3\rangle\}$$

Żeby sprawdzić, czy relacja jest rzeczywiście zwrotna, symetryczna i nie jest przechodnia, należy sprawdzić, czy dla każdego $a \in A$ para $\langle a,a\rangle$ należy do zbioru R (zwrotność), czy dla każdej pary $\langle a,b\rangle$ należącej do R, para $\langle b,a\rangle$ też należy do R (symetryczność), oraz pokazać, że istnieją takie $a,b,c \in A$, że $\langle a,b\rangle \in R$ oraz $\langle b,c\rangle \in R$, ale $\langle a,c\rangle \notin R$ (przykładem takich a,b,c są kolejno $1,2,3$).

Przykład 2. Pokaż, że relacja $R \subseteq \mathbb{Q} \times \mathbb{Q}$ jest zwrotna, symetryczna i przechodnia.

$$xRy \overset{def}{\iff} \frac{x-y}{2} \in \mathbb{Z}$$

Zacznijmy od pokazania, że relacja R jest **zwrotna**:

Dowód. Relacja R jest zwrotna.

Żeby to pokazać, skorzystamy z definicji zwrotności. Przypomnijmy, że relacja jest zwrotna, jeśli dla każdego $a \in \mathbb{Q}$, zachodzi aRa, czyli, że a jest w relacji z a.

Weźmy więc dowolną liczbę wymierną a. Z definicji, aRa jeśli $\frac{a-a}{2} \in \mathbb{Z}$. Ale $\frac{a-a}{2} = \frac{0}{2} = 0$, i $0 \in \mathbb{Z}$, a to chcieliśmy pokazać. □

Wiemy już, że relacja jest zwrotna, pokażmy więc, że jest także symetryczna:

Dowód. Relacja R jest symetryczna.

Żeby to pokazać, skorzystamy z definicji symetryczności. Przypomnijmy, że relacja jest symetryczna, jeśli dla dowolnych $a, b \in \mathbb{Q}$, zachodzi $aRb \Rightarrow bRa$, czyli jeśli a jest w relacji z b, to b jest w relacji z a.

Weźmy więc dowolne liczby wymierne a, b i załóżmy, że aRb, czyli, że $\frac{a-b}{2} = x$ dla pewnej liczby całkowitej x.

Pokażemy, że bRa, czyli, z definicji, że $\frac{b-a}{2} \in \mathbb{Z}$. Ale $\frac{b-a}{2} = -\frac{a-b}{2} = -x$. Skoro x było liczbą całkowitą, to $-x$ także jest liczbą całkowitą, a to chcieliśmy pokazać. □

Do pokazania zostało nam że R jest przechodnia:

Dowód. Relacja R jest przechodnia.

Żeby to pokazać, skorzystamy z definicji przechodniości. Przypomnijmy, że relacja jest przechodnia, jeśli dla dowolnych $a, b, c \in \mathbb{Q}$ zachodzi $aRb \wedge bRc \Rightarrow aRc$, czyli jeśli a jest w relacji z b i b jest w relacji z c, to a jest w relacji z c.

Weźmy więc dowolne liczby wymierne a, b, c i załóżmy, że aRb i bRc, czyli, że $\frac{a-b}{2} = x$ i $\frac{b-c}{2} = y$ dla pewnych liczb całkowitych x oraz y.

Pokażemy, że aRc, czyli, z definicji, że $\frac{a-c}{2} \in \mathbb{Z}$.

$$\frac{a-c}{2} = \frac{a-(b-b)-c}{2} = \frac{a-b+b-c}{2} = \frac{a-b}{2} + \frac{b-c}{2} = x + y$$

Skoro x oraz y były liczbami całkowitymi, to $x + y$ także jest liczbą całkowitą, a to chcieliśmy pokazać. □

5.3. Złożenie relacji, relacja odwrotna

Definicja 3 (Złożenie relacji)**.** Złożeniem relacji $P \subseteq A \times B$ i $Q \subseteq B \times C$ nazywamy relację

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

Innymi słowy, $a \in A$ i $c \in C$ są w relacji $P;Q$, jeśli istnieje pewne „pośrednie” $b \in B$, takie, że a jest w relacji P z b i b jest w relacji Q z c.

Przykład 3. Niech $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ i $C = \{7, 8\}$. Dla relacji $P \subseteq A \times B$ i $Q \subseteq B \times C$, zapisz relację $P;Q$.

$P = \{\langle 1,4\rangle, \langle 1,6\rangle, \langle 3,6\rangle, \langle 2,5\rangle\}$

$Q = \{\langle 4,8\rangle, \langle 6,7\rangle, \langle 5,8\rangle\}$

$$P;Q = \{\langle 1,8\rangle, \langle 1,7\rangle, \langle 3,7\rangle, \langle 2,8\rangle\}$$

- Para $\langle 1,8\rangle \in P;Q$, bo $\langle 1,4\rangle \in P$ i $\langle 4,8\rangle \in Q$.
- Para $\langle 1,7\rangle \in P;Q$, bo $\langle 1,6\rangle \in P$ i $\langle 6,7\rangle \in Q$.
- Para $\langle 3,7\rangle \in P;Q$, bo $\langle 3,6\rangle \in P$ i $\langle 6,7\rangle \in Q$.
- Para $\langle 2,8\rangle \in P;Q$, bo $\langle 2,5\rangle \in P$ i $\langle 5,8\rangle \in Q$.

Definicja 4 (Relacja odwrotna)**.** Relacją odwrotną do relacji $P \subseteq A \times B$ nazywamy relację

$$P^{-1} = \{\ \langle b,a\rangle \mid \langle a,b\rangle \in P\ \} \subseteq B \times A$$

Innymi słowy, $b \in B$ i $a \in A$ są w relacji P^{-1}, jeśli a i b są w relacji P.

Przykład 4. Niech $A = \{1,2,3\}$ i $B = \{4,5,6\}$. Dla relacji $P \subseteq A \times B$, zapisz relację P^{-1}.

$P = \{\langle 1,4\rangle, \langle 1,6\rangle, \langle 3,6\rangle, \langle 2,5\rangle\}$

$$P^{-1} = \{\langle 4,1\rangle, \langle 6,1\rangle, \langle 6,3\rangle, \langle 5,2\rangle\}$$

- Para $\langle 4,1\rangle \in P^{-1}$, bo $\langle 1,4\rangle \in P$.
- Para $\langle 6,1\rangle \in P^{-1}$, bo $\langle 1,6\rangle \in P$.
- Para $\langle 6,3\rangle \in P^{-1}$, bo $\langle 3,6\rangle \in P$.
- Para $\langle 5,2\rangle \in P^{-1}$, bo $\langle 2,5\rangle \in P$.

5.4. Relacyjny rachunek dziedzin

Relacyjny rachunek dziedzin jest jednym z języków zapytań, używanych w teorii **relacyjnych baz danych**, czyli baz danych, który opiera się na pojęciu **relacji**. Dane w takich bazach przedstawiane są za pomocą tabel (**relacji**) a ich zawartość wydobywa się za pomocą różnych języków zapytań, których przykładem może być omawiany w tym rozdziale **relacyjny rachunek dziedzin**.

Relacyjny rachunek dziedzin używa pojęć, które poznaliśmy podczas omawiania zbiorów i relacji, a także z formuł rachunku kwantyfikatorów i jest używany w praktyce, do zapewnienia teoretycznych podstaw do relacyjnych baz danych.

Zapytania w tym języku są wyrażeniami w postaci

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

Gdzie φ jest formułą rachunku kwantyfikatorów zawierająca zmienne wolne $x_1, \ldots, x_n$. Jest to więc zbiór obiektów $x_1, x_2, \ldots, x_n$, spełniających formułę φ. Zbiór takich obiektów czasem będziemy nazywać *wykazem*.

Dla przykładu *„wykaz studentów informatyki"*, dla zbioru wszystkich studentów S, kierunków K oraz relacji $Studiuje \subseteq S \times K$, można wyrazić zapytaniem $\{ x \mid x \in S \wedge Studiuje(x, "Informatyka") \}$.

W powyższym przykładzie warto zwrócić uwagę na $x \in S$ – musimy zapewnić, że obiekty są w rzeczywistości studentami, oraz na relację $Studiuje$ – ważna jest tu kolejność argumentów.

Przykład 5. Rozważmy zbiory osób O, barów B oraz soków S a także relacje $Bywa \subseteq O \times B$, $Lubi \subseteq O \times S$ i $Podawany \subseteq S \times B$, informujące odpowiednio o tym, jakie osoby bywają w jakich barach, jakie osoby lubią jakie soki i jakie soki podawane są w jakich barach. W relacyjnym rachunku dziedzin wyraź poniższe zapytania:

- Wykaz osób które nie bywają w żadnym barze, w którym podają sok „Malinowy".

  Przypomnijmy, że zapytanie musi być w postaci $\{ x \mid \varphi \}$, gdzie φ jest formułą rachunku kwantyfikatorów zawierającą zmienną wolną x.

  Formuła φ powinna opisywać zdanie *„x jest osobą, która nie bywa w żadnym barze, w którym podają sok malinowy"*.

  Przede wszystkim więc musimy zapisać, że $x \in O$, to znaczy, że interesują nas tylko obiekty, które są osobami. Po drugie, x nie bywa w żadnym barze, w którym podają sok „Malinowy", lub inaczej, w każdym barze, w którym x bywa, sok „Malinowy" nie jest podawany, co możemy zapisać jako $\forall b \in B(Bywa(x, b) \Rightarrow \neg Podawany(''Malinowy'', b))$.

  Zauważmy, że w tej części zapytania jest *implikacja*. Zazwyczaj po kwantyfikatorze ogólnym występuje właśnie implikacja. Gdybyśmy zamiast tego użyli koniunkcji, jeśli istniałby bar w którym x nie bywa, formuła byłaby fałszywa, zbiór byłby więc pusty.

  Ostatecznie, nasze zapytanie w relacyjnym rachunku dziedzin przyjmuje postać:

  $$\{ x \mid x \in O \wedge \forall b \in B(Bywa(x, b) \Rightarrow \neg Podawany(''Malinowy'', b)) \}$$

- Wykaz osób, które nie lubią żadnego soku, podawanego w barze „Jagoda"

  Ponownie, zapytanie musi być w postaci $\{ x \mid \varphi \}$.

Formuła φ powinna więc opisywać zdanie *„x jest osobą, która nie lubi żadnego soku, podawanego w barze „Jagoda”.*

Ponownie, pamiętać musimy o zapisaniu, że interesują nas tylko osoby: $x \in O$. Po drugie, zapisać musimy, że x nie lubi żadnego soku podawanego w barze „Jagoda”, lub inaczej, dla każdego soku podawanego w barze „Jagoda”, x go nie lubi: $\forall s \in S(Podawany(s,'' Jagoda'') \Rightarrow \neg Lubi(x, s))$.

Ostatecznie, nasze zapytanie w relacyjnym rachunku dziedzin przyjmuje postać:

$$\{ \; x \mid x \in O \wedge \forall s \in S(Podawany(s,'' Jagoda'') \Rightarrow \neg Lubi(x, s)) \; \}$$

- Wykaz osób bywających w barze „Jagoda”, które lubią pewien podawany tam sok, którego nie lubi „Bartek”.

  Ponownie, zapytanie musi być w postaci $\{ \; x \mid \varphi \; \}$.

  Formuła φ powinna więc opisywać zdanie *„x jest osobą bywającą w barze „Jagoda”, która lubi pewien podawany tam sok, którego nie lubi „Bartek”.*

  Ponownie, pamiętać musimy o zapisaniu, że interesują nas tylko osoby: $x \in O$. Osoba x musi także bywać w barze „Jagoda”: $Bywa(x,'' Jagoda'')$. Na koniec zapisać musimy, że w barze „Jagoda” podają jakiś sok, lubiany przez x, którego nie lubi „Bartek”, lub inaczej, że istnieje sok, podawany w barze „Jagoda”, lubiany przez x, którego nie lubi „Bartek”:

  $\exists s \in S(Podawany(s,'' Jagoda'') \wedge Lubi(x, s) \wedge \neg Lubi(''Bartek'', s))$

  Warto zwrócić uwagę, że w tej części zapytania pojawiła się *koniunkcja.* Zazwyczaj po kwantyfikatorze egzystencjalnym występuje właśnie koniunkcja.

  Ostatecznie, nasze zapytanie w relacyjnym rachunku dziedzin przyjmuje postać:

$$\begin{aligned} \{ \; x \mid \; & x \in O \wedge \\ & Bywa(x,'' Jagoda'') \wedge \\ & \exists s \in S \; (Podawany(s,'' Jagoda'') \wedge Lubi(x, s) \wedge \neg Lubi(''Bartek'', s) \; \} \end{aligned}$$

Relacyjny rachunek dziedzin w dużej mierze opiera się na odpowiedniej interpretacji zdań w języku polskim, oraz umiejętnym zapisaniu ich w języku matematyki. Dla lepszego zrozumienia dobrze jest zadawać sobie pytania o przypadki brzegowe. Dla przykładu, *„co jeśli żadna osoba nie lubi żadnego soku”* lub, *„Co jeśli w barze ,, Jagoda'' nie podają żadnego soku.*

Rozdział 6.

Zakończenie

6.1. Cel pracy

Mimo, że przedmiot „Logika dla Informatyków" nie jest przedmiotem trudnym, sprawia on dużo problemów części nowych studentów, którzy po raz pierwszy spotykają się z takimi typami zadań. Tacy studenci często potrzebują jakiegoś wsparcia, materiałów poza wykładem. Choć dostępna jest literatura która wyjaśnia poszczególne zagadnienia, studenci pierwszego roku często nie potrafią z niej korzystać, a forma przedmiotu sprawia, że nie zrozumienie pierwszych kilku tematów, utrudnia znacznie zrozumienie dalszego materiału. Zbierając cały materiał w przystępnej formie można umożliwić studentom lepszy start, dając im szanse dogonić lepiej przygotowanych kolegów.

Powyższa praca stanowi szkic podręcznika, który każdy student pierwszego roku, bez znajomości materiału, mógłby przeczytać, w celu lepszego zrozumienia poszczególnych działów przedmiotu „Logika dla Informatyków". Poza zaprezentowaną wyżej częścią pisemną, w skład pracy wchodzą także materiały audiowizualne, w których autor pracy przedstawia niektóre zagadnienia.

Część audiowizualna udostępniana była studentom pierwszego roku w roku akademickim 2020/2021. Materiały te, uzupełnione o materiały autorstwa Bartosza Bednarczyka i Anny Karykowskiej, spotkały się z pozytywnym odbiorem. Każdy z udostępnionych filmów zbierał kilkaset wyświetleń (150-350). Filmy były więc regularnie oglądane, co świadczy o tym, że przynajmniej część studentów odbierała je pozytywnie i uznawała za pomocne.

Część pisemna w pewnej mierze pokrywa się z materiałami audiowizualnymi, pokazując podobne przykłady i podobne sposoby rozumowania. Dodatkowo, niektóre przykłady prezentowane w części pisemnej wzorowane były na materiałach autorstwa Bartosza Bednarczyka i Anny Karykowskiej, udostępnionych studentom w ramach tej samej inicjatywy co część audiowizualna tej pracy.
Przykłady 2 oraz 5 z rozdziału 2., a także przykłady 3 oraz 5 z rozdziału 5. wzo-

rowane były na przykładach zaprezentowanych w materiałach Anny Karykowskiej. Przykłady 4 oraz 6 z rozdziału 2. a także przykład 1 z rozdziału 4. wzorowane były na przykładach zaprezentowanych w materiałach Bartosza Bednarczyka.

Celem pracy jest pomoc studentom w zrozumieniu materiału. Przykładowe rozwiązania nie są przedstawiane w celu umożliwiania studentom bezmyślnego kopiowania rozwiązań, a raczej stanowią pomoc dydaktyczną, by na prostych przykładach zrozumieć poszczególne pojęcia, a także oswoić się z popularnymi typami zadań: nauczyć się czytać ich treść i dowiedzieć się, jak powinno się za takie zadania zabierać.

6.2. Cel przedmiotu

Choć „Logika dla Informatyków" jest przedmiotem obowiązkowym, nie jest to jedyny powód by dobrze zrozumieć przedstawiony materiał.

Materiał przestawiony na przedmiocie pomaga studentom zapoznać się ze światem matematyki, z którym studenci muszą być zaznajomieni przez cały okres studiów. Umiejętność czytania treści i definicji czy przeprowadzania i przedstawiania prostych rozumowań to umiejętności niezbędne by w przyszłości poradzić sobie na trudniejszych przedmiotach, a także w dalszej karierze zawodowej.

Język logiki jest także nieodłączną częścią informatyki, zarówno teoretycznej jak i praktycznej. Wiele pojęć i koncepcji przedstawianych jest w języku, którego część studenci poznają właśnie na przedmiocie „Logika dla Informatyków". Przeprowadzając dowody na temat struktur danych z których korzystają programiści, posługujemy się właśnie językiem logiki.

6.2.1. Dowody poprawności algorytmów

Jednym z zastosowań logiki w praktyce jest dowodzenie, że dany algorytm jest poprawny.

Algorytm będziemy uznawać za **poprawny**, jeśli:

- Przy poprawnym wejściu, algorytm zawsze zwraca poprawne (spełniające specyfikację) wyjście
- Przy poprawnym wejściu algorytm zawsze się zatrzymuje

Żeby pokazać, jak logika może zostać użyta do dowodzenia poprawności algorytmów, użyjemy dość prostego i intuicyjnego algorytmu sortowania bąbelkowego i udowodnimy jego poprawność używając technik poznanych w tej pracy.

Przykład 1. Dany jest algorytm:

Algorytm 1: Sortowanie bąbelkowe

Wejście: Ciąg liczb naturalnych $A = (a_1, a_2, \ldots, a_n)$
Liczba naturalna n
Wyjście: Posortowany rosnąco ciąg A

```
for i = n to 1 do
    for j = 1 to i − 1 do
        if a_j > a_{j+1} then
            zamień(a_j, a_{j+1})
        end
    end
end
```

Chcemy pokazać, że *Algorytm* jest poprawny, to znaczy, że jeśli podamy mu poprawne wejście (skończony ciąg A liczb naturalnych oraz jego długość), *Algorytm* zawsze się zatrzyma i zawsze zwróci poprawne wyjście (posortowany rosnąco ciąg A).

Zacznijmy od rozbicia naszego programu na dwie części: **pętlę zewnętrzną** i **pętlę wewnętrzną**. Pokażemy następnie pewne twierdzenie o pętli wewnętrznej i pewne twierdzenie o pętli zewnętrznej, których użyjemy by pokazać prawdziwość algorytmu sortowania bąbelkowego.

Definicja 1 (Pętla wewnętrzna)**. Pętlą wewnętrzną** nazywamy następującą część algorytmu sortowania bąbelkowego:

```
for j = 1 to i − 1 do
    if a_j > a_{j+1} then
        zamień(a_j, a_{j+1})
    end
end
```

Definicja 2 (Pętla zewnętrzna)**. Pętlą zewnętrzną** nazywamy następującą część algorytmu sortowania bąbelkowego:

```
for i = n to 1 do
    pętla wewnętrzna
end
```

Twierdzenie 1 (Problem stopu algorytmu sortowania bąbelkowego)**.** Dla każdych poprawnych danych wejściowych, algorytm sortowania bąbelkowego zawsze się zatrzymuje.

Dowód. Dowód tego twierdzenia jest dość prosty. Zauważmy, że dla poprawnych danych wejściowych, pętla wewnętrzna wykona się $i-1$ razy, dla i idącego od n do 1. To znaczy, sumarycznie, wykona się $n-1+n-2+\cdots+1=\frac{n(n-1)}{2}$ razy. Wykonanie pętli czasem może skutkować wywołaniem procedury *zamień*, ale niezależnie od tego, ile razy zostanie ona wykonana, pętla zawsze się zakończy. To znaczy, że algorytm sortowania bąbelkowego zawsze zatrzyma się dla poprawnych danych. □

Twierdzenie 2 (Niezmiennik pętli wewnętrznej)**.** Dla dowolnej liczby naturalnej m i dowolnego ciągu liczb naturalnych A, po m-tym przejściu pętli wewnętrznej, maksymalny element ciągu $(a_1, a_2, \ldots, a_{m+1})$ znajdzie się na pozycji $m+1$.

Dowód. Udowodnimy to używając **indukcji**, poznanej w rozdziale 3.

Niech własność $\varphi(m)$ mówi, że dla dowolnego ciągu liczb naturalnych A, po m-tym przejściu pętli wewnętrznej, maksymalny element ciągu $(a_1, a_2, \ldots, a_{m+1})$ znajduje się na pozycji $m+1$.

Zdefiniujmy X jako

$$X = \{\ m \in \mathbb{N} \mid \varphi(m)\ \}$$

Pokażemy, że $X = \mathbb{N}$. Użyjemy do tego indukcji w wersji 1.

- **Podstawa indukcji:**

  Weźmy dowolny ciąg liczb naturalnych A. Musimy pokazać, że w zerowym przejściu pętli (tzn. przed pierwszym przejściem), element maksymalny ciągu (a_1) znajduje się na pozycji 1. Maksymalnym elementem tego ciągu jest oczywiście a_1, który znajduje się na pozycji 1, więc $0 \in X$.

- **Krok indukcyjny:**

  Weźmy dowolną liczbę naturalną m i załóżmy, że $m \in X$, czyli, że dla dowolnego ciągu liczb naturalnych A, po m-tym przejściu pętli wewnętrznej, maksymalny element ciągu $(a_1, a_2, \ldots, a_{m+1})$ znajdzie się na pozycji $m+1$.

  Musimy pokazać, że $m+1 \in X$. Trzeba pokazać, że dla dowolnego ciągu liczb naturalnych A, po $(m+1)$-wszym przejściu pętli wewnętrznej, maksymalny element ciągu $(a_1, a_2, \ldots, a_{m+2})$ znajdzie się na pozycji $m+2$.

  Weźmy dowolny ciąg liczb naturalnych A. Wiemy, z założenia indukcyjnego, że dla tego ciągu, po m-tym przejściu pętli wewnętrznej, maksymalny element $(a_1, a_2, \ldots, a_{m+1})$ znajduje się na pozycji $m+1$. W przejściu $(m+1)$-wszym maksymalnym elementem ciągu $(a_1, a_2, \ldots, a_{m+2})$ jest więc albo element a_{m+1}, albo element a_{m+2}. Rozpatrzmy więc dwa przypadki:

  – W przejściu $(m+1)$-wszym, maksymalny element znajduje się na pozycji $m+1$. Wtedy, warunek „**if** $a_{m+1} > a_{m+2}$" zwróci **True**, wykona się więc

procedura *zamień*. Po $(m+1)$-wszym przejściu pętli, element ten znajdzie się więc na pozycji $m+2$, a to chcieliśmy udowodnić.

– W przejściu $(m+1)$-wszym, maksymalny element znajduje się na pozycji $m+2$. Wtedy, warunek „**if** $a_{m+1} > a_{m+2}$" zwróci **False**, nie wykona się więc procedura *zamień*. Po $(m+1)$-wszym przejściu pętli element pozostanie więc na swoim miejscu (pozycji $m+2$), a to chcieliśmy udowodnić.

W obu przypadkach, po $(m+1)$-wszym przejściu pętli, maksymalny element ciągu $(a_1, a_2, \ldots, a_{m+2})$ będzie na pozycji $m+2$, więc $m+1 \in X$.

Na mocy zasady indukcji, $X = \mathbb{N}$, co kończy dowód twierdzenia. □

Definicja 3. k-tym maksymalnym elementem ciągu A nazywać będziemy k-ty element od końca w posortowanym rosnąco ciągu A.

Przykładowo, 3-cim maksymalnym elementem ciągu $(1, 6, 2, 9, 8, 1, 4, 8)$ jest element 8 bo 8 jest 3-cim od końca elementem ciągu $(1, 1, 2, 4, 6, 8, 8, 9)$.

Twierdzenie 3 (Niezmiennik pętli zewnętrznej)**.** Dla dowolnej liczby naturalnej m i dowolnego ciągu liczb naturalnych A długości n, po m-tym przejściu pętli zewnętrznej, dla **każdego** $k < m$, a_{n-k} jest $(k+1)$-wszym maksymalnym elementem ciągu $(a_1, a_2, \ldots, a_n)$.

Lub, opisując to innymi słowami, po m-tym przejściu pętli zewnętrznej, ciąg $(a_{n-m+1}, a_{n-m+2}, \ldots, a_n)$ jest posortowany rosnąco i zawiera m kolejnych maksymalnych elementów ciągu $(a_1, a_2, \ldots, a_n)$.

Dowód. Udowodnimy to ponownie używając **indukcji**.

Niech własność $\psi(m)$ mówi, że dla dowolnego ciągu liczb naturalnych A długości n, po m-tym przejściu pętli zewnętrznej, dla każdego $k < m$, a_{n-k} jest $(k+1)$-wszym maksymalnym elementem ciągu $(a_1, a_2, \ldots, a_n)$.

Zdefiniujmy X jako

$$X = \{\ m \in \mathbb{N} \mid \psi(m)\ \}$$

Pokażemy, że $X = \mathbb{N}$. Użyjemy do tego indukcji z wersji 1.

- **Podstawa indukcji:**

  Weźmy dowolną liczbę n i dowolny ciąg liczb naturalnych A długości n. W zerowym przejściu pętli zewnętrznej (tzn. przed pierwszym przejściem) nie mamy żadnych $k < m$, więc $0 \in X$.

- **Krok indukcyjny:**

Weźmy dowolną liczbę naturalną m i załóżmy, że $m \in X$, czyli, że dla dowolnej liczby naturalnej n i dowolnego ciągu liczb naturalnych A długości n, po m-tym przejściu pętli zewnętrznej, dla każdego $k < m$, a_{n-k} jest $(k+1)$-wszym maksymalnym elementem ciągu $(a_1, a_2, \ldots, a_n)$.

Musimy pokazać, że $m+1 \in X$, czyli, że dla dowolnej liczby n i dowolnego ciągu liczb naturalnych A długości n, po $m+1$-wszym przejściu pętli zewnętrznej, dla każdego $k < m+1$, a_{n-k} jest $(k+1)$-wszym maksymalnym elementem ciągu $(a_1, a_2, \ldots, a_n)$.

Weźmy więc dowolną liczbę naturalną n i dowolny ciąg liczb naturalnych A długości n.

Na mocy założenia indukcyjnego, dla tej liczby n i tego ciągu A, po m-tym przejściu pętli zewnętrznej, dla każdego $k < m$, a_{n-k} jest $(k+1)$-wszym maksymalnym elementem ciągu $(a_1, a_2, \ldots, a_n)$.

Zostało więc pokazać, że po $m+1$-wszym przejściu pętli zewnętrznej, pozycje elementów $a_{n-m+1}, a_{n-m+2}, \ldots, a_n$ nie zmienią się, a element a_{n-m} stanie się $m+1$-wszym maksymalnym elementem ciągu A (twierdzenie dla $k = m$).

Wiemy, że w $m+1$-wszym przejściu pętli zewnętrznej, parametr i będzie wynosić $n-m$. Skoro tak, to parametr j może maksymalnie wynieść $n-m-1$. Oznacza to, że pętla wewnętrzna nie będzie w stanie zmienić pozycji elementów $a_{n-m+1}, a_{n-m+2}, \ldots, a_n$.

Zauważmy, że $m+1$-wszy największy element ciągu A znajduje się gdzieś na pozycjach $1, 2, \ldots, n-m$. Dodatkowo, ten element jest elementem maksymalnym ciągu $(a_1, a_2, \ldots, a_{n-m})$.

Możemy teraz użyć twierdzenia 2 żeby stwierdzić, że po $(n-m-1)$-wszym przejściu pętli wewnętrznej, na miejscu $(n-m)$-tym znajdzie się maksymalny element ciągu $(a_1, a_2, \ldots, a_{n-m})$.

Oznacza to, że po $(m+1)$-wszym przejściu pętli zewnętrznej, element a_{n-m} jest $(m+1)$-wszym maksymalnym elementem ciągu A.

W takim razie $m+1 \in X$.

Na mocy zasady indukcji, $X = \mathbb{N}$, co kończy dowód twierdzenia. □

Mając te twierdzenia, możemy w końcu udowodnić prawdziwość sortowania bąbelkowego.

Twierdzenie 4 (Poprawność sortowania bąbelkowego)**.** Przedstawiony algorytm sortowania bąbelkowego jest poprawny.

Dowód. Z twierdzenia 1 wiemy, że dla poprawnych danych algorytm sortowania bąbelkowego się zatrzymuje. Musimy tylko pokazać, że dla dowolnych poprawnych danych, zwróci poprawny wynik.

Weźmy dowolną liczbę naturalną n i dowolny ciąg liczb naturalnych A długości n. Pokażemy, że po wykonaniu algorytmu sortowania bąbelkowego, ciąg A będzie posortowany.

Z twierdzenia 3 wiemy, że dla dowolnych liczb naturalnych n, m i dla dowolnego ciągu A długości n, po m-tym przejściu pętli zewnętrznej, element a_{n-k}, dla $k \in \{0, 1, \ldots, (m-1)\}$ jest $(k+1)$-wszym maksymalnym elementem ciągu A.

Wiemy też, że dla danego n i danego ciągu A długości n, pętla zewnętrzna wykona się n razy.

Na mocy twierdzenia 3, po n-tym przejściu pętli zewnętrznej, element a_{n-k}, dla $k \in \{0, 1, \ldots, (n-1)\}$ jest $(k+1)$-wszym maksymalnym elementem ciągu A.

To oznacza, że ciąg jest posortowany rosnąco (maksymalny element znajduje się na pozycji n, drugi maksymalny na pozycji $n-1$, i tak dalej, aż w końcu n-ty maksymalny znajdzie się na pozycji $n-(n-1)=1$). □

6.2.2. Relacyjny rachunek dziedzin a język zapytań SQL

W tym rozdziale zaprezentujemy jak poznane w rozdziale 5. zapytania w relacyjnym rachunku dziedzin mogą zostać przepisane na równoważne im zapytania w *SQL*. Użyjemy do tego pierwszego punktu z przykładu 5 znajdującego się w rozdziale 5.

Założenia wstępne

Zamieszczony poniżej przykład ma jedynie zilustrować jak zapytania w relacyjnym rachunku dziedzin mogą przełożyć się na zapytania w języku **SQL**. Nie będziemy więc zwracać uwagi na efektywność zapytań, nie będziemy też używać kluczy czy operatorów typu *union*.

Baza danych

Dla zilustrowania przykładu, stworzymy nową bazę **mysql**[3], zawierającą trzy główne tabele: **„osoba”**, **„sok”** i **„bar”**, każda z nich zawierająca dwie kolumny *(id, nazwa)*. W celu zaprezentowania relacji pomiędzy zbiorami osób, soków i barów stworzymy trzy kolejne tabele: **„bywa”** z kolumnami *(osobaId, barId)*, **„lubi”** z kolumnami *(osobaId, sokId)* i **„podawany”** z kolumnami *(sokId, barId)*.

Osoba	
id	nazwa
1	Balbina
2	Oskar
3	Danuta
4	Eryk
5	Ernest
6	Allan
7	Klara
8	Anatolia
9	Bartek
10	Katarzyna

Sok	
id	nazwa
1	Malinowy
2	Gruszkowy
3	Bananowy
4	Porzeczkowy
5	Truskawkowy

Bar	
id	nazwa
1	Jagoda
2	Alibi
3	Saloon

Tablica 6.1: Zbiory

Bywa	
osobaId	barId
1	1
1	2
2	1
3	2
3	3
4	1
5	1
6	1
6	3
7	3
9	1
9	2
10	2

Lubi	
osobaId	sokId
1	2
2	1
2	5
3	3
3	4
4	4
5	1
5	5
6	3
7	2
7	5
8	1
9	3
10	1
10	3

Podawany	
sokId	barId
1	1
3	1
4	1
1	2

Tablica 6.2: Relacje

6.2.3. Przykład

Przykład 2. Zapisz w języku **SQL** poniższe zapytanie:

Wykaz osób które nie bywają w żadnym barze, w którym podają sok „Malinowy".

Przypomnijmy, że nasze zapytanie w relacyjnym rachunku dziedzin wyglądało następująco:

$$\{ x \mid x \in O \wedge \forall b \in B(Bywa(x, b) \Rightarrow \neg Podawany(''Malinowy'', b)) \}$$

W języku **SQL** nie ma implikacji, nie ma też kwantyfikatora ogólnego. Mamy za to operator *exists*, więc na początek przeróbmy lekko nasze zapytanie:

$$\{ x \mid x \in O \wedge \neg(\exists b \in B(Bywa(x, b) \wedge Podawany(''Malinowy'', b))) \}$$

Zacznijmy zapisywać zapytanie od środka. Język **SQL** nie posiada symboli relacyjnych, musimy więc znaleźć inny sposób na zapisanie, że x bywa w barze b. Możemy to zrobić mówiąc, że w tabeli *Bywa* istnieje para *(osobaId,barId)*, gdzie *osobaId* to *id* osoby x, a *barId* to *id* baru b.

Innymi słowy, chcielibyśmy wybrać z bazy wszystkie rekordy, które spełniają nasze zapytanie, a potem poprzedzić to słowem kluczowym *exists*, żeby sprawdzić, czy takie rekordy istnieją:

```
exists (
    select * from bywa where
    bywa.barId = b.id and
    bywa.osobaId = x.id
)
```

Podobnie, fakt, że w barze b podawany jest sok *Malinowy* możemy zapisać jako:

```
exists (
    select * from podawany, sok where
    podawany.barId = b.id and
    podawany.sokId = sok.id and
    sok.nazwa = 'Malinowy'
)
```

Żeby sprawdzić, czy istnieje bar, w którym x bywa i w którym podawany jest sok *Malinowy*, możemy, podobnie jak powyżej, napisać zapytanie które wybiera wszystkie takie bary, a następnie poprzedzić je operatorem *exists*:

```
exists (
    select * from bar b where
    exists (
        select * from bywa where
        bywa.barId = b.id and
        bywa.osobaId = x.id
    ) and exists (
        select * from podawany, sok where
        podawany.barId = b.id and
        podawany.sokId = sok.id and
        sok.nazwa = 'Malinowy'
    )
)
```

Oczywiście, w zapytaniu mamy negację, jednak łatwo ją zapisać używając słowa kluczowego *not*:

```
not (exists (
    select * from bar b where
        exists (
            select * from bywa where
                bywa.barId = b.id and
                bywa.osobaId = x.id
        ) and exists (
            select * from podawany, sok where
                podawany.barId = b.id and
                podawany.sokId = sok.id and
                sok.nazwa = 'Malinowy'
        )
))
```

A ostatecznie interesować nas będą osoby x, dla których powyższe zapytanie będzie prawdziwe, dostajemy więc:

```
select * from osoba x where
     not (exists (
          select * from bar b where
               exists (
                    select * from bywa where
                         bywa.barId = b.id and
                         bywa.osobaId = x.id
               ) and exists (
                    select * from podawany, sok where
                         podawany.barId = b.id and
                         podawany.sokId = sok.id and
                         sok.nazwa = 'Malinowy'
               )
     ))
```

Wynikiem naszego zapytania jest

id	nazwa
7	Klara
8	Anatolia

Łatwo sprawdzić, że *Klara* i *Antonina* są rzeczywiście jedynymi osobami spełniającymi zapytanie. *Saloon* jest jedynym barem w którym nie podają soku *Malinowy*, a wszystkie inne osoby chodzą do przynajmniej jednego z dwóch pozostałych barów.

Pozostałe przykłady opisane w rozdziale 5. mogą zostać przepisane analogicznie do powyższego.

6.2.4. Wnioski

Powyższy przykład ilustruje, że relacyjny rachunek dziedzin jest (nieprzypadkowo) dość mocno związany z językiem **SQL**, stosowanym w wielu popularnych rodzajach baz danych. Choć dokładne opisanie zależności pomiędzy nimi wykracza poza zakres tej pracy, to warto zaznaczyć, że dobre zrozumienie relacyjnego rachunku dziedzin może znacznie ułatwić prowadzenie rozumowań na temat zapytań w języku **SQL**, na przykład analizę statyczną zapytań czy tworzenie systemów integracji informacji i wymiany danych.

Bibliografia

[1] W. Charatonik, L. Pacholski, T. Wierzbicki, A. Kościelski *Logika dla informatyków materiały do zajęć*

[2] J. Tiuryn *Wstęp do teorii mnogości i logiki*

[3] https://www.mysql.com/

[4] Wojciech Guzicki, Piotr Zakrzewski *Wykłady ze wstępu do matematyki, Wprowadzenie do teorii mnogości* oraz *Wstęp do matematyki. Zbiór zadań*

[5] Kazimierz Kuratowski *Wstęp do teorii mnogości i topologii*

[6] Kazimierz Kuratowski *Teoria mnogości*

[7] Marek Wiktor, Janusz Onyszkiewicz *Elementy logiki i teorii mnogości w zadaniach*

[8] Helena Rasiowa *Wstęp do matematyki współczesnej*

[9] Kenneth A. Ross, Charles R. B. Wright *Matematyka dyskretna*

[10] Jerzy Słupecki, Ludwik Borkowski *Elementy logiki matematycznej i teorii mnogości*

[11] Michael Huth, Mark Ryan *Logic in computer science*

[12] Susanna S. Epp *Discrete mathematics with applications*

[13] Keith Devlin *Myślenie matematyczne. Twój nowy sposób pojmowania świata*