Indukcja

Materiały pomocnicze do wykładu

wykładowca: **dr Magdalena Kacprzak**

Charakteryzacja zbioru liczb naturalnych

Arytmetyka liczb naturalnych

Jedną z najważniejszych teorii matematycznych jest arytmetyka liczb naturalnych. Elementarna arytmetyka liczb naturalnych używa języka, w którym oprócz stałej 0 występuje jednoargumentowa funkcja

suc

nazywana następnikiem, i relacja równości.

Aksjomaty Peano

Aksjomaty tej teorii, a więc podstawowe prawa rządzące liczbami naturalnymi, sformułował Peano.

Aksjomaty Peano

<u>Aksjomaty Peano liczb naturalnych</u>

Ax1. Zero jest liczbą naturalną.

Ax2. Dla każdej liczby naturalnej n istnieje dokładnie jedna liczba naturalna suc(n), która jest następnikiem n.

Ax3. Zero nie jest następnikiem żadnej liczby naturalnej.

Ax4. Jeżeli k jest następnikiem liczby n, k=suc(n), i k jest następnikiem liczby m, k=suc(m), to n = m.

Aksjomaty Peano c.d.

Ax5. Zasada indukcji matematycznej:

Jeżeli A jest podzbiorem zbioru liczb naturalnych N takim, że spełnione są warunki (1), (2):

(1) $0 \in A$,

(2) dla każdej liczby naturalnej n,
jeżeli $n \in A$ i m jest następnikiem n, to $m \in A$,

to $A = N$.

Intuicje

Aksjomat piąty mówi jak można zbudować zbiór liczb naturalnych z zera przez sukcesywne zastosowanie funkcji następnika: każda liczba naturalna n jest otrzymana z zera przez n-krotne wykonanie operacji następnika,

$$1 =^{df} suc(0)$$

$$2 =^{df} suc(suc(0))$$

$$3 =^{df} suc(suc(suc(0)))$$

…………

Intuicje

Fakt ten wielokrotnie, i często nieświadomie, wykorzystuje się w programowaniu z użyciem pętli "while" stwierdzając, że program

{x:= 0; while x < y do x := x+1 od }

nie zapętla się dla wszystkich wartości naturalnych zmiennej y.

Przykład

Twierdzenie:

Każda liczba postaci n^5-n dla $n \in N$ jest podzielna przez 5.

Dowód. Niech

$$A=\{n \in N: (n^5 - n) \bmod 5 = 0\}.$$

Udowodnimy, że N=A.

1. $0 \in A$, ponieważ $0^5 - 0 = 0$.

Przykład

2. Weźmy jakąś ustaloną liczbę n należącą do A. Wynika stąd oczywiście, że dla pewnego naturalnego k, mamy

$$n^5 - n = 5k.$$

Wtedy jednak $(n+1)^5 - (n+1)$ jest też podzielne przez 5, bo

$$(n+1)^5-(n+1) =$$
$$n^5+5n^4+10n^3+10n^2+5n+1-n-1 =$$
$$n^5 - n + 5(n^4+2n^3+2n^2+n) =$$
$$5(k+n^4+2n^3+2n^2+n) .$$

Stąd $n+1 \in A$.

Przykład

Ponieważ oba założenia zasady indukcji matematycznej zostały spełnione, zatem możemy wywnioskować, że A=N. Oznacza to, że dla dowolnej liczby naturalnej n, liczba n^5-n jest podzielna przez 5.

Zasada minimum

Zasada minimum

Z zasady indukcji matematycznej wynika natychmiast następujące twierdzenie zwane "zasadą minimum".

Twierdzenie

W każdym niepustym zbiorze liczb naturalnych istnieje liczba najmniejsza.

Dowód zasady minimum

Niech $A \neq \emptyset$, $A \subseteq N$ i przypuśćmy, że w A nie ma liczby najmniejszej (tzn. A nie ma elementu pierwszego). Oznacza to w szczególności, że $0 \notin A$. Rozważmy zbiór B takich liczb naturalnych n, że ani n ani żadna liczba mniejsza od n nie należy do A,

$$B = \{n : (\forall\ m \leq n)\ m \notin A\}.$$

Udowodnimy, że wobec przyjętych założeń, musi być B=N. Dowód tego faktu przeprowadzimy wykorzystując zasadę indukcji matematycznej.

Dowód zasady minimum

(1) Ponieważ 0 nie należy do A, to z definicji zbioru B wynika, że $0 \in B$.

(2) Załóżmy, że dla pewnego n, $n \in B$. Udowodnimy, że liczba n+1 należy do B.

Dowód zasady minimum

Z założenia indukcyjnego wynika, że wszystkie liczby mniejsze od n oraz samo n nie należą do zbioru A. Gdyby więc $(n+1) \in A$, to byłby to element najmniejszy w A, co nie jest możliwe wobec przyjętego w A założenia. Zatem $(n+1) \notin A$, a stąd $(n+1) \in B$.

Ponieważ wykazaliśmy, że oba założenia zasady indukcji są spełnione, to na mocy tejże zasady indukcji wszystkie liczby naturalne należą do B.

Dowód zasady minimum

Skoro jednak udowodniliśmy, że N=B, to zbiór A musi być pusty, wbrew założeniu. Sprzeczność ta dowodzi, że nie można znaleźć takiego niepustego podzbioru A zbioru liczb naturalnych, który nie miałby elementu pierwszego, a to oznacza, że każdy niepusty podzbiór N ma element pierwszy.

Przykład

Udowodnimy, że

$$\{n \in N : 3|(n^3-n)\} = N.$$

W przedstawionym dowodzie "nie wprost" wykorzystamy zasadę minimum. Niech

$$A = \{n \in N : 3|(n^3-n)\}.$$

Przypuśćmy, że $A \neq N$. Wtedy na mocy zasady minimum, w zbiorze $N \setminus A$ istnieje element najmniejszy. Ponieważ $3|0$, więc $0 \in A$, a tym samym 0 nie jest elementem najmniejszym w $N \setminus A$. Niech więc elementem najmniejszym w $N \setminus A$ będzie jakaś liczba $k>0$. Jako element zbioru $N \setminus A$, k nie jest dzielnikiem (k^3-k).

Przykład

Rozważmy liczbę k-1. Mamy $(k-1) \in N$ oraz

$$(k-1)^3 - (k-1) =$$
$$k^3 - 3k^2 + 3k - 1 - k + 1 =$$
$$(k^3 - k) - 3k(k-1).$$

Ponieważ (k^3-k) nie dzieli się całkowicie przez 3, a $3k(k-1)$ jest wielokrotnością 3, zatem liczba $(k-1)^3 - (k-1)$ nie dzieli się przez 3.
Wynika stąd, że $(k-1) \in N \setminus A$, co przeczy założeniu, że k było liczbą najmniejszą w zbiorze $N \setminus A$. W konsekwencji musi być $A=N$.

Zasada indukcji – różne sformułowania

Zasada indukcji matematycznej 1

Jeżeli

(1) W(0), tzn. 0 ma własność W, oraz

(2) dla dowolnej liczby naturalnej k,

jeśli W(k), to W(k+1),

to dla każdej liczby naturalnej n, W(n)

(tzn. każda liczba naturalna ma własność W).

Przykład

Lemat:

Liczba wszystkich podzbiorów zbioru n elementowego wynosi 2^n, czyli dla dowolnego zbioru X, jeśli $|X| = n$, to $|P(X)| = 2^n$.

Dowód lematu

Oznaczmy przez W zdanie wyrażające własność liczb naturalnych taką, że

W(n) wttw liczba podzbiorów zbioru n elementowego wynosi 2^n.

Dowód lematu

Baza indukcji.

Ponieważ zbiór pusty ma dokładnie jeden podzbiór, zatem jeśli $|X| = 0$, to $|P(X)|= 1=2^0$.

Wynika stąd, że liczba 0 ma własność W.

Dowód lematu

Założenie indukcyjne.

Załóżmy, że wszystkie zbiory
k elementowe mają własność W(k), tzn.
liczba wszystkich podzbiorów zbioru
k-elementowego wynosi 2^k.

Dowód lematu

<u>Teza indukcyjna.</u>

Będziemy dowodzili, że zbiór
(k+1)-elementowy ma też własność W.

Dowód lematu

Dowód tezy indukcyjnej.

Rozważmy zbiór (k+1)-elementowy X,

$$X=\{x_1,x_2,\ldots, x_k,x_{k+1}\}.$$

Podzielmy wszystkie podzbiory zbioru X na dwie kategorie:

- Podzbiory zbioru X, w których nie występuje element x_{k+1},
- Podzbiory zbioru X, w których występuje element x_{k+1}.

Dowód lematu

Podzbiory pierwszej kategorii są to wszystkie podzbiory zbioru k-elementowego, więc na mocy założenia indukcyjnego jest ich 2^k.

Dowód lematu

Podzbiory drugiej kategorii otrzymujemy biorąc jakikolwiek podzbiór A zbioru k-elementowego $X \setminus \{x_{k+1}\}$, a następnie dołączając element x_{k+1}.
Takich podzbiorów, znów na mocy założenia indukcyjnego jest 2^k.

Razem $2^k + 2^k = 2^{k+1}$ podzbiorów. Czyli własność W jest prawdziwa dla k+1.

Dowód lematu

Na mocy zasady indukcji możemy teraz wyciągnąć wniosek, że zdanie $W(n)$ jest prawdziwe dla wszystkich liczb naturalnych.

Zasada indukcji matematycznej 2

Jeżeli A jest podzbiorem zbioru N takim, że

1. $0 \in A$, oraz
2. dla każdej liczby n, jeśli $k \in A$ dla wszystkich $k < n+1$, to $n+1 \in A$,

to $A = N$.

Przykład

Lemat:

Udowodnić, wykorzystując jedną z postaci zasady indukcji matematycznej, że dla dowolnego $a>-1$ i dla dowolnej liczby naturalnej n,

$$(1+a)^n \geq 1 + na.$$

Dowód lematu

Niech W(n) oznacza zdanie

$$(1+a)^n \geq 1+ na.$$

<u>Baza indukcji:</u>

Ponieważ $(1+a)^0 \geq 1$, zatem zachodzi W(0).

Dowód lematu

Założenie indukcyjne:

Załóżmy, W(k) dla pewnego k,
tzn. mamy $(1+a)^k \geq 1+ka$.

Teza: W(k+1) jest zdaniem prawdziwym, tzn.

$$(1+a)^{k+1} \geq 1+(k+1)a.$$

Dowód lematu

<u>Dowód tezy:</u>

$(1+a)^{k+1}=(1+a)^k(1+a).$

Wykorzystamy teraz założenie indukcyjne i otrzymamy

$$(1+a)^{k+1} \geq (1+ ka)(1+a)$$
$$\geq 1+ka+a+kaa$$
$$\geq 1+ (k+1)a + ka^2.$$

Dowód lematu

Ponieważ $ka^2 \geq 0$, zatem ostatecznie

$$(1+a)^{k+1} \geq 1+(k+1)a.$$

Czyli prawdziwe jest zdanie $W(k+1)$.

Ponieważ oba założenia zasady indukcji matematycznej są spełnione, zatem wnioskujemy, że $W(n)$ jest prawdziwe dla wszystkich liczb naturalnych n.

Zasada indukcji dla liczb całkowitych

Niech m będzie liczbą całkowitą oraz niech $\alpha(n)$ będzie zdaniem określonym na zbiorze

$$\{n \in Z : n \geq m\}.$$

Jeśli

1. zdanie α (m) jest prawdziwe, oraz
2. jeśli wszystkie zdania $\alpha(m)$, $\alpha(m+1),\ldots,$ $\alpha(k-1)$ dla pewnego $k>m$ są prawdziwe, to $\alpha(k)$ też jest zdaniem prawdziwym,

to $\alpha(n)$ jest zdaniem prawdziwym dla dowolnych liczb całkowitych $n \geq m$.

Zasada skończonej indukcji

Niech m i k będą liczbami naturalnymi oraz niech $\alpha(n)$ będzie zdaniem wyrażającym pewne własności liczb naturalnych $m \leq n \leq k$. Jeśli

1. zdanie $\alpha(m)$ jest prawdziwe, oraz
2. jeśli z prawdziwości zdania $\alpha(i)$ dla pewnego $m \leq i < k$ wynika, że zdanie $\alpha(i+1)$ też jest prawdzie,

to $\alpha(n)$ jest zdaniem prawdziwym dla dowolnych $n \geq m$ i $n \leq k$.

Definicje indukcyjne

Ciąg nieskończony

Ciąg nieskończony jest to, jak wiadomo funkcja całkowita określona na zbiorze liczb naturalnych N.
Jednym z wygodnych sposobów określania wyrazów ciągu jest **definicja indukcyjna.**
Ten sposób definiowania polega na określeniu pierwszego wyrazu ciągu (lub kilku pierwszych wyrazów) np. a_0, i podaniu metody konstrukcji wyrazu (n+1)-go w zależności od wyrazu n-tego lub innych wyrazów już zdefiniowanych.

Ciąg nieskończony

Przyjmijmy następującą definicję ciągu $(a_i)_{i \in N}$:

$$a_0 = 1,\ a_{n+1} = a_n + 2$$

dla wszystkich $n \geq 0$.

Łatwo wyliczyć, że

$a_1 = a_0 + 2 = 1+2 = 3$, $a_2 = a_1 +2 = 5$ itd.

Przyglądając się bliżej tym definicjom zauważymy, że

$a_1 = a_0 + 2 = 1+ 1\cdot2$,

$a_2 = 1 +2\cdot2 = 5$,

$a_3 = 1 +2\cdot2 +2 = 1 +3\cdot2$.

Ciąg nieskończony

Domyślamy się, że

$$a_k = 1 + k\cdot 2$$

dla wszystkich $k>0$.

Stosując zasadę indukcji matematycznej możemy pokazać, że $a_k = 1 + 2k$ dla wszystkich k. Rzeczywiście, dla $k=0$ otrzymujemy $a_0 = 1$. Natomiast krok indukcyjny wynika z indukcyjnej definicji ciągu, założenia indukcyjnego dla k i prostego przekształcenia wzoru:

$$a_{k+1} = a_k + 2 = (1 + 2k) + 2 = 1 + 2(k+1).$$

Niezmienniki

Definicja

Powiemy, że zdanie α jest niezmiennikiem pętli postaci **while** γ **do** I **od**, gdzie γ jest warunkiem, a I treścią pętli, jeśli dla każdej iteracji tej pętli z tego, że warunki γ i α są spełnione przed wykonaniem treści pętli I, wynika że α jest prawdziwe po jej wykonaniu.

Przykład – algorytm Euklidesa

NWD(n,m) (n,m $\neq 0$)

```
{x:=n; y := m;
    while x ≠ y
    do
       if x>y then
              x := x-y
       else
              y:=y-x
       fi
    od;
    return y;}
```

Przykład – algorytm Euklidesa

Niezmiennikiem pętli w tym algorytmie jest formuła

$$nwd(x,y)=nwd(n,m).$$

Rzeczywiście, załóżmy że $x \neq y$ i formuła $nwd(x,y)= nwd(n,m)$ jest prawdziwa w chwili wejścia do pętli while.

Przykład – algorytm Euklidesa

Lemat: Jeśli x>y, to nwd(x-y,y)=nwd(x,y).

Wykonując jedyną przewidzianą w tym przypadku instrukcję

$$x := x-y,$$

spowodujemy (nową wartością x jest stara wartość x-y), że na nowo spełniona jest równość nwd(x,y)=nwd(n,m).

Przykład – algorytm Euklidesa

Analogicznie w drugim przypadku. Zatem, po wykonaniu instrukcji "if" nadal jest spełniona formuła

$$nwd(x,y)=nwd(n,m).$$

Przykład – algorytm Euklidesa

Zakończenie całego procesu nastąpi wówczas, gdy $x=y$. Stosując skończoną zasadę indukcji matematycznej, skoro

$$nwd(x,y)=nwd(n,m)$$

jest prawdziwa tuż przed wykonaniem pętli "while" i dla każdej iteracji z prawdziwości tej formuły przed wykonaniem instrukcji "if" wynika jej prawdziwość po wykonaniu instrukcji "if", to

$$nwd(x,y)=nwd(n,m)$$

jest też prawdziwa po wyjściu z pętli "while". Ale wtedy $nwd(n,m)=nwd(x,y)= nwd(y,y)=y$.

Przykład – algorytm Euklidesa

Wynika stąd, że wyliczona przez procedurę wartość jest rzeczywiście największym wspólnym dzielnikiem liczb n i m.

Przykład – algorytm Euklidesa

Pozostał jeszcze jeden problem, czy ten algorytm kiedykolwiek doprowadzi do sytuacji, w której

$$x=y.$$

Czy pętla "while" zatrzyma się kiedykolwiek?

Przykład – algorytm Euklidesa

Tutaj znów przychodzi nam z pomocą indukcja matematyczna. Zauważmy, że jeśli wartości x i y kolejno uzyskiwane w czasie działania algorytmu zapiszemy jako kolejne pozycje ciągu $(x_1,y_1), (x_2,y_2),\ldots$, to iloczyn

$$(x_i y_i)$$

tworzy ciąg malejący.

Przykład – algorytm Euklidesa

Ponieważ jest to ciąg liczb naturalnych, zatem na mocy zasady minimum nie może być ciągiem nieskończonym.

Istnieje więc taka iteracja, w której

$$x_i = y_i,$$

czyli algorytm zatrzyma się.

Lemat

Jeśli zdanie α jest prawdziwe przed wykonaniem instrukcji "while" i jest niezmiennikiem tej pętli, to po wykonaniu instrukcji "while" jest prawdziwe zdanie

$$(\alpha \wedge \neg \gamma).$$