

Stefan Sokołowski

MATEMATYKA DYSKRETNA

wykład 1

Inst. Informatyki Stosowanej, ANS
Elbląg, 2024/2025

Wykład 1, str. 1

Sumy wielu podobnych składników

$$\sum_{i=p}^q a_i \stackrel{\text{def}}{=} a_p + a_{p+1} + a_{p+2} + \dots + a_{q-1} + a_q$$

W tym zapisie i **nie jest zmienną**, jest „okienkiem”, w które należy wpisywać kolejne liczby od p do q .

Przykład:

$$\sum_{\square=1}^7 \square = 1 + 2 + 3 + 4 + 5 + 6 + 7$$

Przykład:

$$\sum_{\square=7}^{14} \frac{1}{\square} = \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14}$$

Jak dojść do prawdy?



Jak dojść do prawdy?

Przykład statystyczny

Luźna obserwacja:

blondyni programują lepiej niż bruneci.

Hipoteza:

liczba blondynów w grupie, którzy zaliczyli „Podstawy programowania I”, przekracza liczbę brunetów, którzy tego dokonali.

Na pewno da się tą hipotezę

- albo wprost sfalsyfikować, więc **śmietnik**,
- albo pozytywnie zweryfikować, więc **twierdzenie** (jednak słabo powiązane z luźną obserwacją).

Jak dojść do prawdy?

Przykład arytmetyczny

Luźna obserwacja:

$1 + 3 + 5 = 9 = 3^2$; to się pewnie uogólnia na dłuższe sumy liczb.

Hipoteza:

Dla dowolnej liczby naturalnej $n \geq 1$ zachodzi równość

$$\sum_{i=1}^n (2i - 1) = n^2$$

Czyli:

$$\underbrace{1 + 3 + 5 + \dots + (2n - 1)}_{\text{suma kolejnych } n \text{ liczb nieparzystych}} = n^2$$

$$\begin{array}{rclcl} 1 & = & 1 & = & 1^2 \\ 1 + 3 & = & 4 & = & 2^2 \\ 1 + 3 + 5 & = & 9 & = & 3^2 \\ 1 + 3 + 5 + 7 & = & 16 & = & 4^2 \\ \dots & & & & \dots \end{array}$$

Czy to się da udowodnić?

Sięganie do nieskończoności

Hipotezę $\sum_{i=1}^n (2i - 1) = n^2$ sprawdziliśmy dla kilku liczb n — ale to za mało, żeby wiedzieć, że jest prawdziwa **zawsze**. Ogólniej:

Jak udowadniać twierdzenia postaci

$$\forall_{n \in \mathbb{N}} P(n)$$

gdzie

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ — zbiór liczb naturalnych
- $P(\dots)$ jest jakąś własnością liczb naturalnych to może być jakaś równość, albo nierówność, albo jeszcze coś innego...

w poprzednim przykładzie chodziło o **równość**

$$P(n) \iff \sum_{i=1}^n (2i - 1) = n^2$$

Możemy sprawdzać po kolei

$$P(0), P(1), P(2), \dots$$

ale w ten sposób **nigdy** nie sprawdzimy dla wszystkich liczb naturalnych.

Sięganie do nieskończoności — indukcja matematyczna

Zasada indukcji jest zwykle podawana w takiej postaci:

$P(0)$	←przypadek bazowy— to musimy udowodnić;
$P(n) \Rightarrow P(n+1)$	←krok indukcyjny— to musimy udowodnić;
$P(n)$	←teza— to z powyższych faktów wynika

W rozważanym przykładzie:

suma bez składników jest zerowa

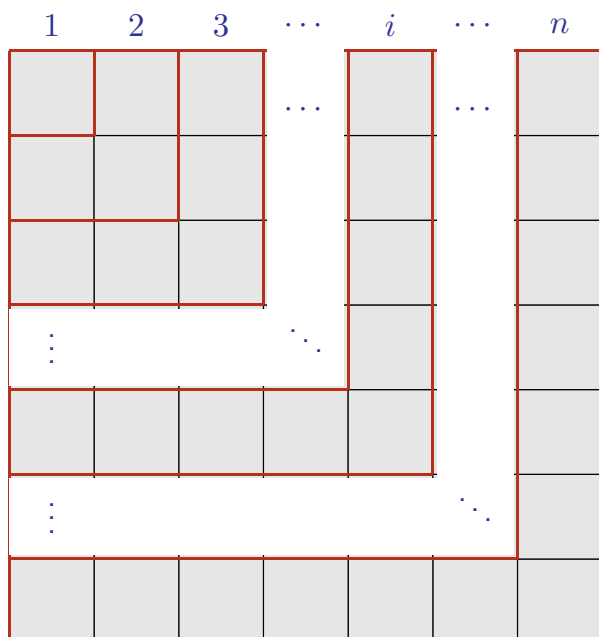
Przyp. bazowy: $\sum_{i=1}^0 (2i-1) \stackrel{?}{=} 0^2$

Krok indukcyjny: $\sum_{i=1}^n (2i-1) = n^2 \stackrel{?}{\Rightarrow} \sum_{i=1}^{n+1} (2i-1) = (n+1)^2$

$$\begin{aligned}
 & \sum_{i=1}^{n+1} (2i-1) \\
 &= (2 \cdot 1 - 1) + (2 \cdot 2 - 1) + \dots + (2 \cdot n - 1) + (2 \cdot (n+1) - 1) \\
 &= \sum_{i=1}^n (2i-1) + (2 \cdot (n+1) - 1) \\
 &= n^2 + (2 \cdot (n+1) - 1) \\
 &= n^2 + 2 \cdot n + 1 \\
 &= (n+1)^2
 \end{aligned}$$

Sięganie do nieskończoności

$$1 + 3 + 5 + \dots + (2i-1) + \dots + (2n-1) = n^2$$



Błędne koło w dowodzie?

$$\frac{P(0) \quad P(n) \Rightarrow P(n+1)}{P(n)}$$

Żeby udowodnić $P(n)$ musimy udowodnić

- przyp. bazowy $P(0)$ (zwykle łatwe), oraz
- krok indukcyjny: implikację o poprzedniku $P(n)$, więc musimy założyć $P(n)$, żeby w końcu wywnioskować $P(n)$.

To jest **pozorne** błędne koło. Starannie napisana zasada indukcji:

$$\frac{P(0) \quad \forall_{n \geq 0} (P(n) \Rightarrow P(n+1))}{\forall_{n \geq 0} P(n)}$$

Nie zakładamy tezy $\forall_{n \geq 0} P(n)$, a tylko $P(n)$ dla każdego n z osobna.

Do czego służy indukcja?

Indukcja służy do **udowodniania hipotez o liczbach naturalnych.**

Indukcja

- **nie pomaga** we wpadaniu na pomysł;
- **nie pomaga** w formułowaniu hipotezy;
- **nie zawsze rozstrzyga**, czy hipoteza jest prawdziwa;
 - jeśli dowód wyjdzie, to hipoteza **jest prawdziwa**
 - jeśli nie wyjdzie, to **nic nie wiadomo**: może być prawdziwa, może być fałszywa



Do czego służy indukcja?

Indukcja **tylko** dla liczb naturalnych!

Pseudotwierdzenie:

Każda liczba rzeczywista jest naturalna.

Pseudodowód:

przyp. bazowy: 0 jest liczbą naturalną,
krok. induk.: założmy, że jakieś n jest
 liczbą naturalną; wtedy $n + 1$ jest
 liczbą naturalną — to oczywiste.
 Wobec tego każda liczba rzeczywista
 jest naturalna.

□

Pseudotwierdzenie:

Dla dowolnego rzeczywistego x :

$$\sin(x \cdot 180^\circ) = 0$$

Pseudodowód:

przyp. bazowy dla $x = 0$:

$$\sin(0 \cdot 180^\circ) = \sin(0) = 0$$

krok. induk.: założmy, że

$$\sin(x \cdot 180^\circ) = 0; \text{ wtedy}$$

$$\sin((x + 1) \cdot 180^\circ)$$

$$= \sin(x \cdot 180^\circ + 180^\circ)$$

$$= \sin(x \cdot 180^\circ) \cdot \cos(180^\circ)$$

$$+ \cos(x \cdot 180^\circ) \cdot \sin(180^\circ)$$

$$= \sin(x \cdot 180^\circ) \cdot \cos(180^\circ)$$

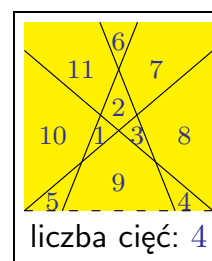
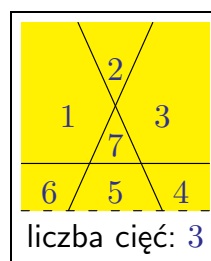
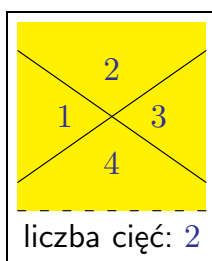
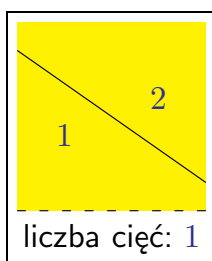
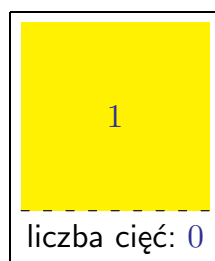
$$= 0$$

□

Twierdzenie dowodzone przez indukcję może dotyczyć liczb innych niż naturalne (albo dowolnej innej rzeczywistości); ale indukcja musi biec po liczbach naturalnych i teza będzie stosować się tylko do liczb naturalnych (np. $\forall_{n \in \mathbb{N}} \sin(n \cdot 180^\circ) = 0$ jest OK).

O krajaniu tortu

Na ile kawałków da się podzielić
 płaszczyznę przy pomocy n prostoli-
 niowych cięć?



Hipoteza:

$$\text{obszary} = 1 + \frac{\text{cięcia} \cdot (\text{cięcia} + 1)}{2}$$

...wzięta całkiem z sufitu...

O krajaniu tortu

Twierdzenie: Dla dowolnej liczby naturalnej $n \geq 0$ zachodzi

$$a_n = 1 + \frac{n \cdot (n + 1)}{2}$$

n — liczba cięć

a_n — liczba obszarów

tę równość możemy zakładać

a tę mamy udowodnić

Dowód:

Przyp. bazowy: $a_0 \stackrel{?}{=} 1 + \frac{0 \cdot (0+1)}{2}$

lewa str.: $a_0 = 1$

prawa str.: $1 + \frac{0 \cdot (0+1)}{2} = 1$

OK

Krok indukcyjny: $a_n = 1 + \frac{n \cdot (n+1)}{2} \Rightarrow \underbrace{a_{n+1}}_L = 1 + \underbrace{\frac{(n+1) \cdot ((n+1)+1)}{2}}_R$

Nowa $(n+1)$ -wsza linia przecina n „starych” linii, rozdzielających $n+1$ obszarów, więc dodaje $n+1$ obszarów do istniejących:

$$L = a_{n+1} = a_n + (n+1) = \quad \quad \quad (\text{z zał. ind.})$$

$$= 1 + \frac{n \cdot (n+1)}{2} + (n+1) = 1 + \frac{n \cdot (n+1) + 2(n+1)}{2}$$

$$= 1 + \frac{(n+1) \cdot (n+2)}{2} = R$$

□

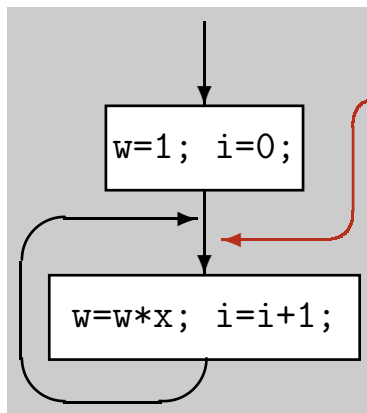
Wniosku z krajania tortu

Hipoteza może być podana bez uzasadnienia (zgadnięta);

ale jeśli zostanie potwierdzona dowodem indukcyjnym,

to staje się **pełnoprawnym twierdzeniem**.

Analiza pętli w programie



Niech w_n i i_n — wartości zmiennych w i i po wykonaniu n obrotów pętli, w tym miejscu programu. Wtedy

$$w_0 = 1 \\ w_{n+1} = w_n \cdot x$$

$$i_0 = 0 \\ i_{n+1} = i_n + 1$$

Twierdzenie:

Dla dowolnego $n \in \mathbb{N}$ (czyli po wykonaniu n obrotów pętli) zachodzi

$$i_n = n \wedge w_n = x^n$$

Dowód:

Przyp. bazowy: $i_0 = 0 \wedge w_0 = 1$ wynika z komendy w pierwszym pudełku.

Krok ind.: Zakładamy

$$i_n = n \wedge w_n = x^n \quad (\text{założenie indukcyjne})$$

Stąd

$$i_{n+1} = i_n + 1 = n + 1 \quad \text{oraz} \quad w_{n+1} = w_n \cdot x = x^n \cdot x = x^{n+1}$$

więc zostało wyprowadzone

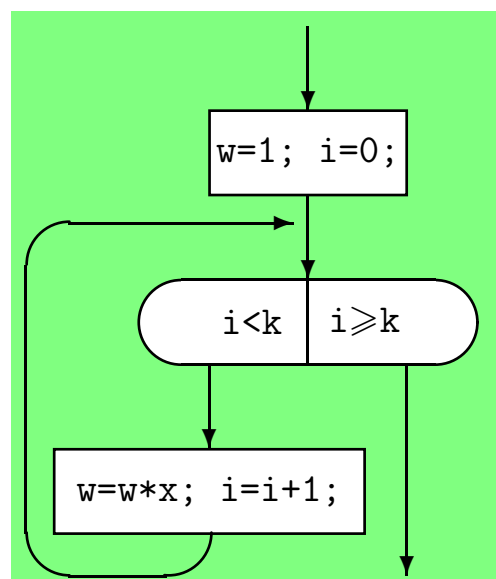
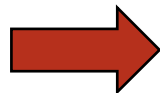
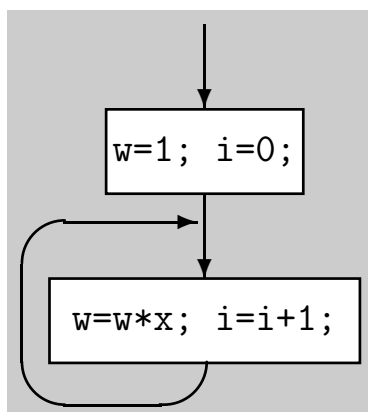
$$i_{n+1} = n + 1 \wedge w_{n+1} = x^{n+1} \quad (\text{teza indukcyjna})$$

□

Analiza pętli w programie

Udowodniona własność programu: $i_n = n \wedge w_n = x^n$.

Więc program liczy bez końca kolejne potęgi x . Żeby móc znaleźć k -tą potęgę, należy go zatrzymać, kiedy wartość zmiennej i dojdzie do k :

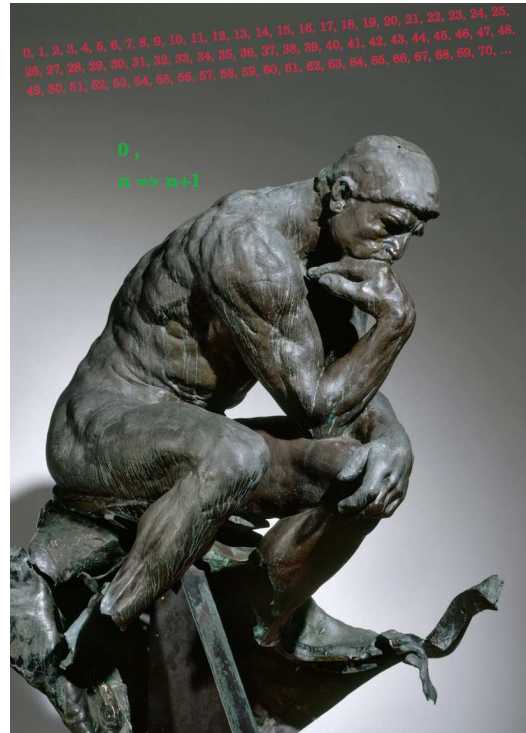


Indukcja matematyczna a programy

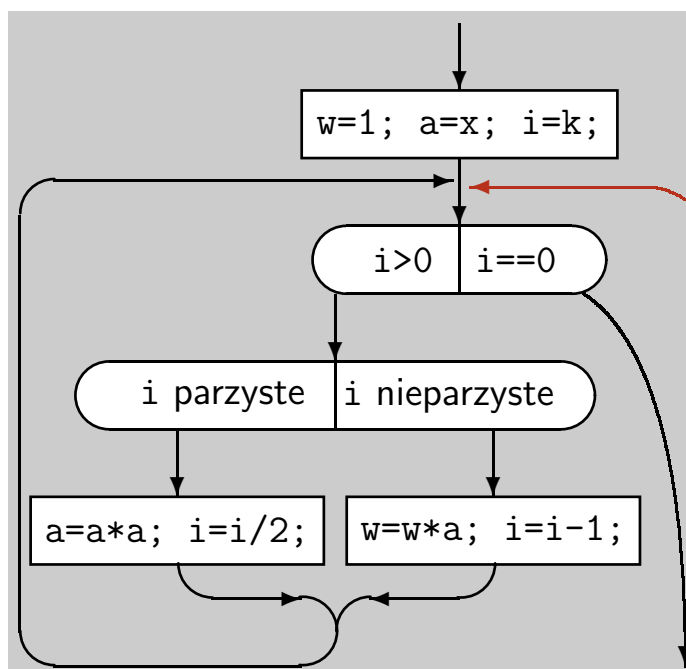
Wniosek:

O działaniu programów **można** rozumować matematycznie.

Głównym narzędziem intelektualnym jest w tym **indukcja matematyczna**.



Analiza trudniejszej pętli



$$w_0 = 1$$

$$a_0 = x$$

$$i_0 = k$$

jeśli i_n parzyste:

$$w_{n+1} = w_n$$

$$a_{n+1} = a_n \cdot a_n$$

$$i_{n+1} = i_n / 2$$

jeśli i_n nieparzyste:

$$w_{n+1} = w_n \cdot a_n$$

$$a_{n+1} = a_n$$

$$i_{n+1} = i_n - 1$$

Twierdzenie: W tym miejscu programu $w_n \cdot a_n^{i_n} = x^k$.

Wniosek: Więc, jeśli $i_n = 0$, to $w_n = x^k$ — program liczy potęgę.

Analiza trudniejszej pętli

Twierdzenie:

Założmy, że

$$\begin{array}{l} w_0 = 1 \\ a_0 = x \\ i_0 = k \end{array} \quad \text{oraz} \quad \left\{ \begin{array}{l} \text{jeśli } i_n \text{ jest parzyste, to} \\ \quad w_{n+1} = w_n, a_{n+1} = a_n \cdot a_n, i_{n+1} = i_n / 2 \\ \\ \text{jeśli } i_n \text{ jest nieparzyste, to} \\ \quad w_{n+1} = w_n \cdot a_n, a_{n+1} = a_n, i_{n+1} = i_n - 1 \end{array} \right.$$

Wtedy dla każdego $n \in \mathbb{N}$ zachodzi $w_n \cdot a_n^{i_n} = x^k$.

Dowód:

Przyp. bazowy: $w_0 \cdot a_0^{i_0} \stackrel{?}{=} x^k$

sprowadza się do $1 \cdot x^k \stackrel{?}{=} x^k$, które jest oczywiste.

Krok indukcyjny: zał.: $w_n \cdot a_n^{i_n} = x^k$, trzeba dowieść: $w_{n+1} \cdot a_{n+1}^{i_{n+1}} \stackrel{?}{=} x^k$

Przyp. i_n parzyste: $w_{n+1} \cdot a_{n+1}^{i_{n+1}} = w_n \cdot (a_n \cdot a_n)^{i_n/2} = w_n \cdot a_n^{i_n} = x^k$

Przyp. i_n nieparzyste:

$$w_{n+1} \cdot a_{n+1}^{i_{n+1}} = (w_n \cdot a_n) \cdot a_n^{i_n-1} = w_n \cdot (a_n \cdot a_n^{i_n-1}) = w_n \cdot a_n^{i_n} = x^k$$

□

Porównanie działania programów potęgujących

Potęgowanie proste (przykład):

$$\begin{aligned} 2^{12} &= 2 \cdot 2^{11} = 4 \cdot 2^{10} = 8 \cdot 2^9 \\ &= 16 \cdot 2^8 = 32 \cdot 2^7 = 64 \cdot 2^6 \\ &= 128 \cdot 2^5 = 256 \cdot 2^4 = 512 \cdot 2^3 \\ &= 1024 \cdot 2^2 = 2048 \cdot 2^1 = 4196 \cdot 2^0 \\ &= 4196 \end{aligned} \quad (11 \text{ mnożeń...})$$

Potęgowanie binarne (przykład):

$$\begin{aligned} 2^{12} &= 1 \cdot 2^{12} = 1 \cdot 4^6 = 1 \cdot 16^3 \\ &= 16 \cdot 16^2 = 16 \cdot 256^1 = 4196 \cdot 256^0 \\ &= 4196 \end{aligned} \quad (5 \text{ mnożeń...})$$