# Teorioinformacyjne twierdzenie Gödla,

*czyli co ma logika do statystyki?*

Łukasz Dębowski
ldebowsk@ipipan.waw.pl

Instytut Podstaw Informatyki PAN

# Temat referatu

Twierdzenie, o którym opowiem, jest pomysłem Gregory Chaitina – jednego z twórców algorytmicznej teorii informacji.

## Twierdzenie (Gödla)-Chaitina

Dysponując systemem aksjomatów, zapisanym na papierze za pomocą **N** znaków, nie można udowodnić niekompresowalności dowolnego konkretnego napisu długości większej niż $\mathbf{N} + \mathbf{C} \log \mathbf{N}$, gdzie **C** jest pewną stałą.

# Aksjomaty, twierdzenia, dowody

Formalny system wnioskowania:

- aksjomaty – zdania w pewnym języku formalnym;
- reguły wnioskowania – reguły przekształcania zdań w zdania.

**Twierdzenie**: zdanie, które można skonstruować z aksjomatów stosując reguły wnioskowania skończoną liczbę razy.

**Dowód twierdzenia**: ciąg ww. zastosowań reguł wnioskowania.

System wnioskowania jest niesprzeczny, jeżeli nie można udowodnić jednocześnie pewnego zdania i jego zaprzeczenia.

# Gödla idea dowodu niedowodliwości

Skonstruować formalne zdanie następującej postaci:

> Niniejsze zdanie nie ma dowodu.

Konstrukcja odwołuje się do argumentu przekątniowego.

# Gödla dowód niedowodliwości

Zdania, predykaty, i dowody można ponumerować liczbami.

Istnieją następujące predykaty:

1. **Prov(m, n)** $\overset{\text{def}}{\iff}$ **m**-ty dowód dowodzi **n**-tego zdania;
2. **Diag(n)** $\overset{\text{def}}{\iff}$ nie istnieje dowód zdania $\phi$**(n)**, gdzie $\phi$ jest **n**-tym predykatem jednoargumentowym.

Załóżmy, że system wnioskowania jest niesprzeczny.

Jeżeli **Diag** jest **d**-tym predykatem, to zdanie **Diag(d)**:

- nie może być fałszywe
  *(istniałyby wówczas dowody zdań* **Diag(d)** *i* $\neg$ **Diag(d)***)*,
- nie ma dowodu, skoro jest prawdziwe.

# Paradoksy samoodniesienia

*To stwierdzenie jest fałszywe.*

*Epimenides, Kreteńczyk, twierdzi:*
*Kreteńczycy zawsze kłamią.*

*Fryzjer w naszym miasteczku goli tylko*
*tych mieszkańców, którzy nie golą się sami.*

# Nierozstrzygalność problemu stopu

**Twierdzenie Turinga**

Nie istnieje program dla komputera, który wyliczałby w skończonym czasie dla każdego programu-argumentu, czy ma on własność stopu (tzn. czy komputer wykonując program-argument zatrzyma się w skończonym czasie).

**ERGO:**

Za pomocą niesprzecznego systemu wnioskowania nie możemy dowieść własności stopu bądź jej zaprzeczenia dla wszystkich możliwych programów.

- W przeciwnym razie istniałby program mający własność stopu dla każdego programu-argumentu i sprawdzający własność stopu dla niego **przez przeszukanie wszystkich dowodów**.

# Paradoks losowości (Laplace, Kołmogorow)

Prosimy dwie osoby o podanie ciągu 20 rzutów uczciwą monetą.

- Pierwsza osoba:
  ORORORRRORRORROORROO
- Druga osoba:
  RRRRRRRRRRRRRRRRRRRR

Osobie pierwszej wierzymy, osobie drugiej nie.

Dlaczego, skoro oba ciągi mają to samo prawdopodobieństwo?

# Ku losowości algorytmicznej

W pewnym intuicyjnym sensie "losowy ciąg znaków"
nie powinien wykazywać żadnych regularności.

Chyba się zgodzimy, że następujące napisy nie są losowe:

- 01010101010101010101010101010
- 01001000100001000001000000001

# Definiowanie napisów przez programy

Dowolny skończony napis można wygenerować
za pomocą pewnego programu komputerowego.

- **Przykład 1:**
  program `print "R" x 20;`
  generuje napis RRRRRRRRRRRRRRRRRRRR;
- **Przykład 2:**
  program `print "ORORORRRORRORRROORROO";`
  generuje napis ORORORRRORRORRROORROO.

Napisy, które wykazują "więcej regularności" można definiować za pomocą krótszych programów.

# Losowość algorytmiczna

*Dla uproszczenia załóżmy, że komputer akceptuje tylko programy zapisane kodem binarnym i generuje napisy w kodzie binarnym.*

Liczba napisów długości $\leq \mathbf{n}$:

$$\mathbf{2^0 + 2^1 + 2^2 + 2^3 + ... + 2^n = 2^{n+1} - 1}$$

Programów długości $\leq \mathbf{n}$ jest co najwyżej tyle samo.

**Definicja**

Napis nazywamy niekompresowalnym, jeżeli każdy program, który go generuje, ma długość nie mniejszą od długości tego napisu.

# Losowość algorytmiczna (II)

**Twierdzenie**

Napisów niekompresowalnych jest nieskończenie wiele.

**Dowód:**

Niech $\mathbf{P}$ będzie liczbą napisów niekompresowalnych.

Liczba kompresowalnych napisów długości $\leq \mathbf{n}$ jest $\leq \sum_{\mathbf{i=0}}^{\mathbf{n-1}} \mathbf{2^i}$.

Zatem liczba wszystkich napisów długości $\leq \mathbf{n}$ spełnia nierówność

$$\sum_{\mathbf{i=0}}^{\mathbf{n}} \mathbf{2^i} \leq \mathbf{P} + \sum_{\mathbf{i=0}}^{\mathbf{n-1}} \mathbf{2^i}.$$

Stąd $\mathbf{P} \geq \mathbf{2^n}$.

# Paradoks Berry'ego

$$\underbrace{\text{Najmniejsza liczba, której najkrótsza definicja ma więcej niż 11 słów.}}_{\text{10 słów}}$$

# Analogia

$$\frac{\text{paradoks Berry'ego}}{\text{twierdzenie (Gödla)-Chaitina}} \approx \frac{\text{paradoksy samoodniesienia}}{\text{oryginalne twierdzenie Gödla}}$$

# Twierdzenie (Gödla)-Chaitina

**Twierdzenie**

Dysponując systemem aksjomatów, zapisanym na papierze za pomocą **N** znaków, nie można udowodnić niekompresowalności dowolnego konkretnego napisu długości większej niż $\mathbf{N} + \mathbf{C} \log \mathbf{N}$, gdzie **C** jest pewną stałą.

# Dowód

**Dowód:**

1. Skonstruujmy program, który po otrzymaniu liczby **P**, **przeszukuje wszystkie dowody**, aż odnajdzie pierwszy dowód **niekompresowalności** pewnego napisu długości **P**.
2. Jeżeli taki napis istnieje, to program ten można przekształcić w program wypisujący ów napis, o długości $\leq \mathbf{N} + \mathbf{C'} \log \mathbf{P}$, gdzie $\mathbf{C'} \log \mathbf{P}$ jest (mniej więcej) długością przedstawienia binarnego liczby **P**.

Z niekompresowalności wynika ograniczenie

$$\mathbf{P} \leq \mathbf{N} + \mathbf{C'} \log \mathbf{P}.$$

Stąd z kolei mamy $\mathbf{P} \leq \mathbf{N} + \mathbf{C} \log \mathbf{N}$, gdzie **C** zależy od $\mathbf{C'}$.

# Ważenie twierdzeń i aksjomatów

*I would like to measure the power of a set of axioms and rules of inference. I would like to be able to say that if one has ten pounds of axioms and a twenty-pound theorem, then that theorem cannot be derived from those axioms.*

*Gregory J. Chaitin.*
*Gödel's Theorem and Information.*
*International Journal of Theoretical Physics,*
*22:941–954, 1982.*

# Uogólnienie twierdzenia Chaitina

**Złożoność Kołmogorowa** (złożoność algorytmiczna) napisu — to długość najkrótszego programu generującego ten napis.

**Twierdzenie**

Dysponując systemem aksjomatów, zapisanym na papierze za pomocą **N** znaków, nie można udowodnić że złożoność Kołmogorowa dowolnego konkretnego napisu jest większa niż $\mathbf{N} + \mathbf{C} \log \mathbf{N}$, gdzie **C** jest pewną stałą.

**Dowód:**

Analogiczny. Tym razem program poszukuje pierwszego napisu o dowodliwej złożoności Kołmogorowa nie mniejszej niż **P**.

# Pozorny paradoks

- Istnieje dziedzina matematyki, która de facto zajmuje się badaniem własności ciągów niekompresowalnych.
- Jest to nowoczesny rachunek prawdopodobieństwa i statystyka — oparte na teorii miary ( $\Longrightarrow$ mocne prawa wielkich liczb).

Można udowodnić, że wynik rzutów uczciwą monetą jest prawie na pewno (prawie) niekompresowalny.

# Prawo wielkich liczb dla złożoności Kołmogorowa

- Niech zmienne losowe $\mathbf{X_i}$ modelują kolejne rzuty monetą:

$$\mathbf{X_{1:n}} = (\mathbf{X_1}, \mathbf{X_2}, ..., \mathbf{X_n}) \text{ — zmienne losowe (napisy),}$$
$$\mathbf{x_{1:n}} = (\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}) \text{ — napisy (konkretne).}$$

- Wówczas $\mathbf{P(X_{1:n} = x_{1:n}) = 1/2^n}$ dla każdego napisu $\mathbf{x_{1:n}}$.

Niech $\mathbf{K(x_{1:n})}$ będzie złożonością Kołmogorowa napisu $\mathbf{x_{1:n}}$.

**Twierdzenie**

$$\mathbf{P}\left(\lim_{n\to\infty} \frac{K(X_{1:n})}{n} \neq 1\right) = 0$$

# Podsumowanie

*[I]t is possible to argue that if a theorem contains more information than a given set of axioms, then it is impossible for the theorem to be derived from the axioms.*

*In contrast with the traditional proof based on the paradox of the liar, this new viewpoint suggests that the incompleteness phenomenon discovered by Gödel is natural and widespread rather than pathological and unusual.*

*Gregory J. Chaitin.*
*Gödel's Theorem and Information.*
*International Journal of Theoretical Physics,*
*22:941–954, 1982.*

# Do poczytania


- Gregory J. Chaitin (1982), *Gödel's Theorem and Information*, International Journal of Theoretical Physics, 22:941–954.
- Ming Li, Paul Vitanyi (1993, 1997), *An Introduction to Kolmogorov Complexity and Its Applications*, Springer.
- Thomas M. Cover, Joy A. Thomas (1991), *Elements of Information Theory*, Wiley.


`www.ipipan.waw.pl/~ldebowsk`