Dowód pierwszego twierdzenia Gödela o niezupełności arytmetyki oparty o złożoność Kołmogorowa

Grzegorz Gutowski
SMP II rok

opiekun:
dr inż. Jerzy Martyna II UJ

1 Wstęp

Pierwsze twierdzenie o niezupełności arytmetyki zostało udowodnione przez Kurta Gödela w roku 1931[1]. Gödel pokazał, że pod pewnymi dodatkowymi warunkami (ω - niesprzeczności) dowolna niesprzeczna teoria formalna zawierająca arytmetykę musi być niezupełna. Późniejsze wyniki innych matematyków osłabiły założenia i uprościły dowód tego twierdzenia. W najmocniejszym wariancie można pokazać, że dowolna niesprzeczna teoria formalna zawierająca arytmetykę jest nierozstrzygalna, a dodatkowo jeśli jest aksjomatyzowalna, to jest niezupełna.

Złożoność Kołmogorowa została wprowadzona przez rosyjskiego matematyka Andreia Kołmogorowa w 1965 roku. Służy ona do charakteryzacji skończonych obiektów matematycznych przedstawionych jako ciągi binarne. Można ją intuicyjnie opisać jako miarę komplikacji obiektu. Im bardziej obiekt jest skomplikowany, tym jego złożoność jest większa. Złożoność Kołmogorowa znalazła zastosowania w informatyce i rachunku prawdopodobieństwa.

Korzystając ze złożoności Kołmogorowa można udowodnić pewną prostą wersję pierwszego twierdzenia Gödela. Można mianowicie pokazać pewną klasę zdań nad językiem arytmetyki, które są niezależne od każdej aksjomatyzowalnej teorii zawierającej arytmetykę. Pokazanie takich zdań dowodzi, że taka teoria jest teorią niezupełną. Ten ciekawy dowód zostanie przedstawiony po wprowadzeniu niezbędnych definicji i udowodnieniu podstawowoych twierdzeń dotyczących złożoności Kołmogorowa.

2 Złożoność Kołmogorowa

2.1 Definicje

Definicja 1 *Wprowadza się następujący porządek na zbiorze* $\{0,1\}^\star$

$$x \leqslant y \Leftrightarrow (|x| < |y|) \vee (|x| = |y| \wedge x \leqslant_{leks} y)$$

gdzie $|x|$ *jest długością słowa* x*,* $a \leqslant_{leks}$ *jest zwykłym porządkiem leksykograficznym.*

W dalszej części, jeżeli nie jest zaznaczone inaczej, to do porównywania ciągów binarnych jest wykorzystywany ten porządek.

Definicja 2 *Maszyną Turinga* M *nazywamy siódemkę uporządkowaną:*

$$M = (Q, \Sigma, \Gamma, \sigma, q_0, \triangle, F)$$

Gdzie:

Q - *zbiór stanów*

$\Sigma \subset \Gamma$ - *alfabet wejściowy*

Γ - *alfabet taśmy*

q_0 - *stan początkowy*

$\triangle \in \Gamma - \Sigma$ - *znak spacji*

$F \subset Q$ - *zbiór stanów końcowych*

$\sigma\colon Q \times F \mapsto Q \times \Gamma \times \{L, R\}$ - *funkcja przejścia, która może być funkcją częściową*

Sposób obliczania na Maszynie Turinga nie zostanie szczegółowo opisany w tej pracy. Po więcej informacji na ten temat można sięgnąć do [2]. W dalszych rozważaniach zakłada się, że $\Sigma = \{0, 1\}$, a $\Gamma = \{0, 1, \triangle\}$

Definicja 3 *Wprowadza się następujące kodowanie maszyny Turinga do ciągu binarnego:*
Jeżeli $Q = \{q_1, q_2, \ldots, q_n\}$, $q_0 = q_s$, $F = \{q_{i_1}, q_{i_2}, \ldots, q_{i_t}\}$, $\Gamma = \{\gamma_1, \gamma_2, \gamma_3\}$ *(*γ_1 *to* 0, γ_2 *to* 1, *a* γ_3 *to* $\triangle$*), a* $\{L, R\} = \{d_1, d_2\}$, *to funkcję przejścia* σ *można opisać jako zbiór przejść:*

$$\sigma(q_i, \gamma_j) = (q_k, \gamma_l, d_m)$$

i zakodować każde takie przejście jako ciąg binarny:

$$110^i10^j10^k10^l10^m$$

Natomiast ciąg binarny kodujący całą maszynę Turinga to:

$$0^n10^s10^{i_1}10^{i_2}1 \ldots 10^{i_t}$$

skonkatenowany ze wszystkimi przejściami funkcji σ. *Ponieważ w zależności od kolejności numeracji stanów i występowania przejść w konkatenacji może powstać wiele różnych ciągów binarnych opisujących tą samą maszynę Turinga jako jej opis wybiera się najmniejszy z tych ciągów.*

Definicja 4 *Wprowadza się numerację maszyn Turinga, według kolejności ich kodów względem wcześniej wprowadzonego porządku na ciągach binarnych.*

W tej numeracji maszyną M_1 jest maszyna o najmniejszym kodzie binarnym. M_2 to maszyna, która ma drugi w kolejności najmniejszy kod binarny, itd.

Definicja 5 *Mając daną maszynę Turinga M działającą nad alfabetem* $\{0,1\}$ *i oznaczając $M(x)$ funkcję częściową $\{0,1\}^* \to \{0,1\}^*$ określoną przez maszynę M definiuje się złożonośc Kołmogorowa na maszynie M jako*

$$K_M(x) = min\{|y|\colon M(y) = x\}$$

gdzie $|y|$ jest długością ciągu y.

$M(y)$ może być nieokreślone dla konkretnego y, gdyż maszyna M może się nie zatrzymać dla wejścia y. Zbiór $\{|y|\colon M(y) = x\}$ może być zbiorem pustym i należy przyjąc, że $min(\emptyset) = +\infty$.

Definicja 6 *Maszyna Turinga M jest asymptotycznie niegorsza od maszyny Turinga N jeżeli istnieje stała c taka że $K_M(x) \leqslant K_N(x) + c$ dla wszystkich ciągów x.*

Definicja 7 *Maszyna Turinga U jest asymptotycznie optymalna, jeżeli jest asymptotycznie niegorsza od każdej maszyny Turinga M.*

Definicja 8 *Przez $< a, b >$ oznacza się ciąg binarny reprezentujący parę uporządkowaną (a, b) powstający w następujący sposób: Każdy bit reprezentacji a jest podwajany, wynik jest konkatenowany z ciągiem* 01 *i z reprezentacją b.*

Łatwo zauważyć, że z tak zakodowanej pary można odczytać zarówno pierwszą, jak i drugą współrzędną, oraz że zachodzi równość:

$$| < a, b > | = 2 \cdot |a| + 2 + |b|$$

Twierdzenie 9 *Istnieje asymptotycznie optymalna maszyna Turinga.*

Dowód: *Oznaczmy przez U dowolną maszynę uniwersalną działającą na wprowadzonym kodowaniu pary uporządkowanej, czyli taką, że:*

$$\forall_{i \in \mathbb{N}}\colon U(< i, x >) = M_i(x)$$

Dla dowolnej maszyny Turinga M zachodzi $M = M_i$ dla pewnego i. Dla każdego skończonego ciągu binarnego x zachodzi:

$$K_M(x) = K_{M_i}(x) = min\{|y|\colon M_i(y) = x\} =$$

$$= min\{| < i, y > | - 2 \cdot |i| - 2\colon M_i(y) = x\} =$$

$$= min\{| < i, y > | - 2 \cdot |i| - 2\colon U(< i, y >) = x\} \geqslant K_U(x) - 2 \cdot |i| - 2$$

Zatem jeżeli przyjmiemy jako $c = 2 \cdot |i| + 2$ to otrzymamy:

$$K_U(x) \leqslant K_M(x) + c$$

Czyli maszyna U jest asymptotycznie niegorsza od dowolnej maszyny M, co oznacza że jest asymptotycznie optymalna. □

Definicja 10 *Złożoność Kołmogorowa ciągu x definiuje się jako $K(x) = K_U(x)$ przy ustalonej maszynie asymptotycznie optymalnej U.*

Wybór maszyny U jest dla definicji istotny tylko co do stałej, więc w dalszych rozważaniach przyjmuje się, że naszą maszyną U jest dowolna maszyna uniwersalna.

2.2 Podstawowe własności

Lemat 11 *Istnieje stała c, taka że dla każdego skończonego ciągu binarnego x zachodzi:*

$$K(x) \leqslant |x| + c$$

Dowód: *Wystarczy skonstruować maszynę M o następującej własności: $M(x) = x$. Weźmy jako M pierwszą w ciągu maszyn maszynę o tej własności. $M = M_i$ dla pewnego i, a więc:*

$$\forall_x : U(< i, x >) = M_i(x) = M(x) = x$$

Wystarczy zatem przyjąć jako $c = 2 \cdot log_2 i + 2$, gdyż mamy wtedy:

$$min\{|y| : U(y) = x\} \leqslant | < i, x > | = |x| + 2 \cdot log_2 i + 2 = |x| + c$$

□

Lemat 12 *Dla każdej liczby naturalnej n istnieje ciąg binarny x długości n, którego złożoność Kołmogorowa jest większa lub równa n.*

Dowód: *Dla dowodu nie wprost przyjmijmy, że istnieje taka liczba naturalna n, że wszystkie ciągi binarne długości n mają złożoność Kołmogorowa mniejszą od n. Rozważmy dwa zbiory:*

$$X = \{x : |x| = n\}$$

$$Y = \{y : |y| < n\}$$

Zachodzi:

$$\forall_{x \in X} : K(x) < n$$

$$K(x) = min\{|y| : U(y) = x\}$$

Zatem:

$$(K(x) < n) \rightarrow \exists_{y \in Y} : U(y) = x$$

Tak więc:

$$X \subset U \star [Y]$$

A to jest niemożliwe, gdyż zbiór X jest 2^n elementowy, a zbiór Y jest $2^n - 1$. Zatem istnieje ciąg binarny x długości n, którego złożoność Kołmogorowa jest większa lub równa n. □

W ten sam sposób można dowieść, że dla każdej liczby naturalnej n istnieje conajmniej $2^{n-1}+1$ ciągów binarnych, których złożoność Kołmogorowa jest większa lub równa $n-1$.

3 Niezupełność arytmetyki

Definicja 13 *Teorią formalną nazywamy dowolny zbiór formuł elementarnych domknięty dedukcyjnie. Teorię nazywamy:*

> *aksjomatyzowalną, jeżeli zbiór formuł (numerów im odpowiadających) jest rekurencyjnie przeliczalny.*
>
> *rozstrzygalną, jeżeli zbiór formuł (numerów im odpowiadających) jest rekurencyjny.*
>
> *niesprzeczną, jeżeli dla każdej formuły α bez zmiennych wolnych najwyżej jedna z formuł α lub $\neg\alpha$ należy do teorii.*
>
> *zupełną, jeżeli dla każdej formuły α bez zmiennych wolnych conajmniej jedna z formuł α lub $\neg\alpha$ należy do teorii.*

Twierdzenie 14 *Dowolna niesprzeczna, aksjomatyzowalna teoria formalna zawierająca arytmetykę jest niezupełna.*

Dowód: *Dowód przebiega poprzez wskazanie nieskończonej rodziny zdań niezależnych od tak określonej teorii. Można mianowicie pokazać, że tylko dla skończenie wielu stałych c istnieje ciąg x taki że formuła "$K(x) > c$" jest twierdzeniem teorii.*
Będziemy korzystać z faktu, iż każda aksjomatyzowalna teoria ma swój enumerator, czyli taką maszynę M, która wypisuje na taśmie wszystkie twierdzenia teorii. Rozważmy teraz maszynę N, która realizuje następujący algorytm:

1. *Wczytaj liczbę naturalną c zapisaną dwójkowo.*
2. *Przeglądaj taśmę wynikową maszyny M, aż do napotkania pierwszego twierdzenia postaci $K(x) > d$, gdzie x jest dowolnym ciągiem binarnym, a d jest liczbą naturalną większą lub równą c.*
3. *Wypisz ciąg binarny x.*

Zakładając dla dowodu nie wprost, że istnieje dla dowolnie dużych c formuła postaci "$K(x) > c$" będąca twierdzeniem teorii, pętla z kroku 2 musi się zakończyć. Zatem maszyna N dla dowolnej liczby naturalnej c zwraca ciąg x,

o którym jako o pierwszym wiadomo w wyniku przeglądania wyjścia maszyny M, że jego złożoność Kołmogorowa jest większa od c.
Dla pewnej liczby naturalnej i zachodzi: $N = M_i$. Zatem dla każdej liczby c mamy że złożoność Kołmogorowa ciągu $x = N(c)$ jest mniejsza lub równa $| < i, c > |$. Podsumowując mamy dwa oszacowania na złożoność Kołmogorowa ciągu $x = N(c)$:

$K(x) > c$

$K(x) \leqslant | < i, c > | = 2 \cdot |i| + 2 + |c| = loc_2 c + d$, *gdzie stała d nie zależy od liczby c.*

Stwierdzenie, że dla dowolnie dużych c maszyna N znajdzie ciąg x, który ma spełniać obie te nierówności prowadzi do sprzeczności, gdyż dla wystarczająco dużej liczby c musi zachodzić

$$c > log_2 c + d$$

bez względu na wielkość stałej d, która zależy tylko od numeru maszyny N. A w takim wypadku nie mogą zachodzić obie nierówności limitujące K(x), co dowodzi, że istnieje tylko skończenie wiele stałych c, dla których istnieje ciąg binarny x taki że formuła "$K(x) > c$" jest twierdzeniem teorii.

Na mocy lematu 12 można stwierdzić, że dla dowolnie dużej stałej c istnieją ciągi binarne, które mają złożoność Kołmogorowa większą niż c, ale tylko dla skończenie wielu c, możemy udowodnić taki fakt o jakimkolwiek ciągu. Zatem istnieją formuły, które są niezależne od rozważanej teorii, co oznacza, że jest ona niezupełna. □

4 Zakończenie

Korzystając ze złożoności Kołmogorowa można otrzymać dość słabą wersję pierwszego twierdzenia Gödla, ale użyta metoda jest relatywnie łatwa. Wynik można osiągnąć po zdefiniowaniu tylko kilku pojęć i wykorzystaniu podstawowych wiadomości z teorii języków formalnych i teorii obliczalności. Ciekawym aspektem dowodu jest podanie konkretnych formuł o wyraźnej treści matematycznej, które są niezależne od systemu aksjomatycznego.

Literatura

[1] K. Gödel : *Über formal unentscheidbare Sätze der Principia mathematica und verwandter Systeme I* Monasch. Math. Phys. 38 (1931) 173-198.

[2] P.G. Odifreddi : *Classical recursion theory* Elsevier, Amsterdam 1999.

[3] M. Li, P. Vitányi : *An Introduction to Kolmogorov Complexity and Its Applications* Springer-Verlag, New York 1993.