Czego nie może maszyna Turinga, czyli o algorytmach (II)

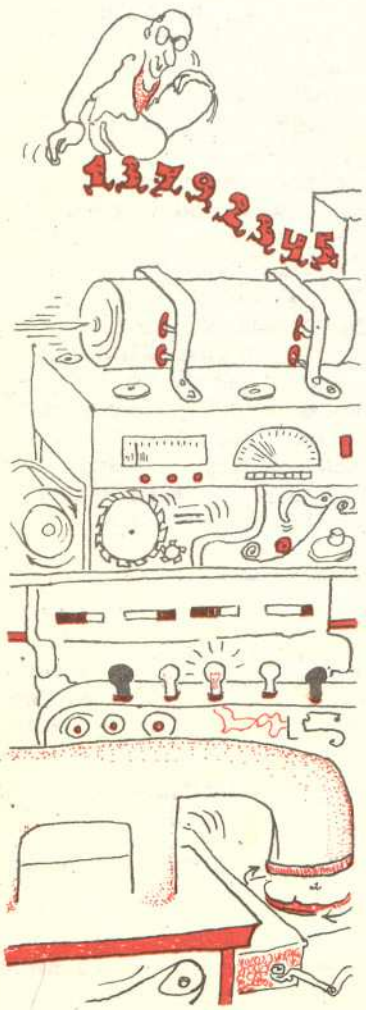
Prof. dr Andrzej MOSTOWSKI, członek rzeczywisty PAN

Działanie każdej maszyny Turinga jest — jak widzieliśmy — wyznaczone przez jej alfabet, to jest zbiór symboli $s_0, s_1, \ldots, s_N$, zbiór stanów $q_0, q_1 \ldots, q_P$ i program. Można je więc w pełni opisać jednym wielkim „słowem", to jest ciągiem znaków: na początku tego ciągu stawiamy symbole $s_0, s_1, \ldots, s_N$, potem znak przestankowy; potem ciąg znaków dla stanów $q_0, q_1, \ldots, q_M$, potem znów znak przestankowy i wreszcie ciąg instrukcji, z których każda jest określona czwórką symboli. Taki opis maszyny wymaga wielu znaków, nie trudno jednak zredukować ich liczbę do dwóch, np. do znaków 0, 1. Wystarczy w tym celu zamiast liter L, P występujących w instrukcjach, pisać ciągi 101, 1001, a zamiast s_j i q_i pisać ciągi 10 ... 01 zawierające odpowiednio $2j+3$ albo $2i+4$ zera. Znak przestankowy możemy zapisywać jako 1.

Powstający w ten sposób ciąg złożony z zer i jedynek nazwiemy kodem maszyny. Kod taki możemy też traktować jak liczbę naturalną zapisaną w układzie dwójkowym. Będziemy oznaczali przez $\overline{M}$ kod maszyny M. W podobny sposób określamy kody wejść i wyjść; przez $\overline{w}$ oznaczamy kod wejścia w.

Nic nie stoi na przeszkodzie, aby za wejście do maszyny M obrać jej kod $\overline{M}$; musimy w tym celu założyć tylko, że symbole 0, 1 należą do zbioru symboli $s_0, s_1, \ldots, s_N$ maszyny. Tak więc $M(\overline{M})$ jest albo nieokreślone, albo też jest pewnym ciągiem symboli $s_0, s_1, \ldots, s_N$ w zależności od tego, czy algorytm opisany przez maszynę M stosuje się do wejścia $\overline{M}$, czy też nie.

Przyjmijmy dla każdego ciągu n złożonego z zer i jedynek $f(n) = 1$, jeśli n nie jest kodem maszyny, $f(n) = 0$, jeśli n jest kodem maszyny M, ale $M(n)$ nie jest określone, oraz $f(n) = M(n),0$ jeśli n jest kodem maszyny i $M(n)$ jest określone (tutaj $M(n),0$ jest ciągiem powstającym przez dopisanie zera na końcu ciągu $M(n)$).



Udowodnimy, że wartości funkcji f nie można obliczyć przy pomocy maszyny Turinga. Inaczej mówiąc udowodnimy, że nie ma takiej maszyny Turinga M_0, że dla każdego ciągu n złożonego z zer i jedynek $M(n)$ jest określone i równe $f(n)$. Przypuśćmy jednak, że taka maszyna M_0 istnieje. Zatem dla każdego n jest $M(n) = f(n)$. W szczególności przyjąć możemy $n = \overline{M}_0$; ponieważ $\overline{M}_0$ jest kodem maszyny i M_0 $(\overline{M}_0)$ jest określone, więc z definicji funkcji f otrzymujemy $f(\overline{M}_0) = M_0(\overline{M}_0), 0$. Zatem $M_0(\overline{M}_0) = f(\overline{M}_0) = M_0(\overline{M}_0), 0$, co jest niemożliwe, gdyż ciągi $M_0(\overline{M}_0)$ i $M_0(\overline{M}_0), 0$ są różne.

Istnienie M_0 prowadziłoby zatem do sprzeczności.

O funkcji f zdefiniowanej wyżej mówimy więc, że nie daje się ona obliczać algorytmicznie.

Istnieje wiele innych funkcji — znacznie naturalniejszych niż powyższa — o których udowodniono, że nie są algorytmicznie obliczalne. Podamy tu dwa przykłady.

W jednym z nich idzie o algorytmiczną odpowiedź na pytanie, czy równanie algebraiczne (wielu zmiennych) o współczynnikach całkowitych ma rozwiązania całkowite. Inaczej mówiąc pytamy, czy istnieje taka maszyna M, że jeśli jako jej wejście obierzemy wielomian F wielu zmiennych o współczynnikach całkowitych, to $M(F)$ istnieje i jest równe 0 lub 1 w zależności od tego, czy istnieją liczby całkowite, które po wstawieniu do F na miejsce zmiennych nadadzą wielomianowi wartość 0. Problem, czy taka maszyna istnieje, był zaproponowany w r. 1900 przez Hilberta; jest to tzw. dziesiąty problem Hilberta. Niedawno, bo w r. 1970, Matjasewicz rozwiązał ten problem i wykazał, że żądana maszyna M nie istnieje, nie mamy więc możności sprawdzać algorytmicznie, czy równanie algebraiczne (wielu zmiennych) ma rozwiązania całkowite. Można nawet pokazać, że już w zakresie wielomianów o co najwyżej 24 zmiennych algorytmu takiego nie ma.

Innym, nie mniej sławnym pytaniem było, czy istnieje maszyna o takiej własności, że jeśli na jej wejściu znajdzie się wzór z arytmetyki liczb całkowitych, to na wyjściu ukaże się 0 lub 1 w zależności od tego, czy wzór ten jest wyprowadzalny z aksjomatów arytmetyki, czy nie.

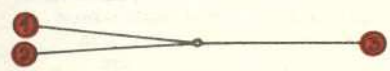
Już w r. 1931 K. Gödel i A. Church dowiedli, że nie ma możliwości algorytmicznego sprawdzania, czy wzory arytmetyki są, czy też nie są wyprowadzalne z jej aksjomatów (pod słowem „wzór" rozumiemy tu zdanie poprawnie zbudowane z równości między wielomianami, łączników rachunku zdań i kwantyfikatorów).

Prace Gödla, Churcha i Matjasewicza są trudne; podstawą ich jest jednak naszkicowany wyżej dowód niemożności algorytmicznego obliczenia funkcji f. Zakończymy artykuł uwagą na temat tego dowodu. Użyty w nim sposób rozumowania nosi nazwę przekątniowego. Jest to sposób często stosowany. Używał go twórca teorii mnogości, Georg Cantor, używał go Bertrand Russell, konstruując swój słynny paradoks, używał go też Kurt Gödel w swej wspomnianej poprzednio pracy z 1931 r. Rzeczywistym jednak odkrywcą tej metody był filozof grecki Eubulides z Miletu, który żył zapewne w III wieku p.n.e. Sformułował on następujący paradoks kłamcy: „To, co teraz piszę, jest fałszywe". Czy napisałem tu prawdę, czy fałsz? Łatwo stwierdzić, że z założenia, iż zdanie w cudzysłowie jest prawdziwe, wynika, że jest ono fałszywe, i na odwrót. I na tym właśnie polega paradoks. W tym paradoksie Eubulides chciał sformułować zdanie, które samo sobie przyporządkowuje własność fałszu. Jest to więc błędne koło — i stąd właśnie pochodzi paradoks. Zdanie Eubulidesa nie jest jednak zdaniem zbudowanym poprawnie. Analogia z funkcją f nie dającą się obliczyć algorytmicznie pochodzi stąd, że f jest określona przez odwoływanie się do wartości $M(\overline{M})$, to jest do wyjścia maszyny, której wejściem jest kod niej samej. Jest to więc też rodzaj koła: kod M wkładamy jako wejście do samego M. W tym jednak przypadku określenie f jest prawidłowe. Paradoks nie powstaje, koło nie jest błędnym kołem; otrzymujemy tylko twierdzenie o niemożności obliczenia f algorytmem.

Jak widzimy, algorytm jest ciekawym pojęciem. Opisując algorytmy używamy języka takiego, jak w nowoczesnej nauce o maszynach liczących. Pojęcie jest jednak stare, sama nazwa prowadzi do dawnej hinduskiej i arabskiej matematyki. A w niektórych dowodach dotyczących algorytmów napotykamy na rozumowania zrodzone w subtelnych umysłach greckich filozofów.

Zadania

Redaguje dr Andrzej ZIEMIŃSKI (według pomysłu J. P.)



F11. Uczyliście się wielokrotnie, że jednym z najbardziej podstawowych praw fizyki jest zasada zachowania energii. Ale czy obowiązuje ona również wtedy, gdy występuje zjawisko interferencji? Pewien sceptyk zaproponował doświadczenie mające obalić zasadę zachowania energii i opisał, jakich spodziewa się rezultatów. Poniżej przytaczamy ten opis.

„Dwie równoległe struny są połączone z trzecią struną, identyczną jak poprzednie, według schematu pokazanego na rysunku 1. W równoległych strunach wywołujemy spójne impulsy poprzeczne o amplitudzie A. W trzeciej strunie biegnące fale interferują ze sobą i wywołują falę o amplitudzie $2A$. Ponieważ struny są identyczne, a energia biegnącej fali jest proporcjonalna do A^2, w opisanym zjawisku zasada zachowania energii została pogwałcona $(2A^2 < (2A)^2)$".

A może wkradł się jakiś błąd do tego rozumowania? Zastanówcie się. Odpowiedź możecie znaleźć na str. 11

Osobom interesującym się rozwiązywaniem zadań z fizyki polecamy zbiory zadań Olimpiad Fizycznych. Dostępne są następujące książki:
1. Tadeusz Pniewski, *Olimpiady Fizyczne XV i XVI*, PZWS, Warszawa 1969 (20 zł).
2. Czesław Ścisłowski, *Olimpiady Fizyczne XVII i XVIII*, PZWS, Warszawa 1971 (14 zł).
3. Waldemar Gorzkowski, *Olimpiady Fizyczne XIX i XX*, WSiP, Warszawa 1973 (24 zł).

Redaguje mgr Andrzej MĄKOWSKI

M31. Mówimy, że w zbiorze A jest określone działanie $*$, gdy każdej parze uporządkowanej (x, y) elementów zbioru A przyporządkowany jest element zbioru A, który oznaczamy $x*y$. Udowodnić, że jeżeli działanie $*$ określone w pewnym zbiorze A spełnia warunki

(1) $$x*(x*y) = y,$$

(2) $$(y*x)*x = y$$

dla wszelkich $x, y \in A$, to jest ono przemienne, tzn. dla wszelkich x, y zachodzi równość $x*y = y*x$.

Rozwiązanie na str. 16

M32. Niech n będzie liczbą całkowitą większą od 1. Udowodnić, że istnieje taki wielomian $P(x, y, z)$ trzech zmiennych o współczynnikach całkowitych, że zachodzi tożsamościowa równość:

$$x = P(x^n, x^{n+1}, x+x^{n+2}).$$

Rozwiązanie na str. 14

M33. Dany jest trapez $ABCD$, w którym $AB \| CD$, $AB = a$, $CD = b$, O jest punktem przecięcia przekątnych trapezu. Wiedząc, że pole trapezu jest równe S, obliczyć pole trójkąta AOB.

Rozwiązanie na str. 5