Twierdzenie Gödla

Dr Leszek PACHOLSKI

Jedną z najistotniejszych cech matematyki współczesnej jest powszechne używanie metody aksjomatycznej. Chociaż metoda ta była znana już w czasach Euklidesa, dopiero na przełomie wieków dziewiętnastego i dwudziestego sformułowano ją jako zasadę i stworzono podstawy jej badania. Jeden z najwybitniejszych matematyków wszystkich czasów, D. Hilbert (1862–1943), opisał podstawowe warunki, które powinien spełniać system aksjomatyczny, aby był użyteczny i słuszny. On też sformułował program, zwany powszechnie programem Hilberta, sprowadzenia całej matematyki do systemu aksjomatycznego. Możliwość realizacji tego programu stała się w naszym stuleciu przedmiotem intensywnych badań naukowych. Wykazały one, że programu Hilberta nie uda się zrealizować. Wynika to z twierdzenia Churcha i Gödla o niezupełności i nierozstrzygalności arytmetyki.

Najstarszy system aksjomatyczny — geometrię Euklidesa — można poznać już na lekcjach geometrii. W systemie tym, podobnie jak w innych systemach aksjomatycznych, istnieją dwa rodzaje prawd. Prawdy jednego rodzaju to te, których środkami matematyki udowodnić nie można. Noszą one nazwę aksjomatów lub pewników. Przyjmuje się je za oczywiste. Są one fragmentem opisu pewnej rzeczywistości fizycznej (np. aksjomaty geometrii są opisem przestrzeni, w której poruszają się ciała niebieskie). Inna grupa prawd to twierdzenia, czyli zdania, które można z aksjomatów wyprowadzić.

Jednym ze starszych systemów aksjomatycznych jest aksjomatyka liczb naturalnych, stworzona przez włoskiego matematyka G. Peano. Opisuje ona własności liczb naturalnych oraz działań na liczbach naturalnych: dodawania, mnożenia etc. Aksjomaty Peana są oczywiste. Aby się o tym przekonać, wystarczy przejrzeć ich listę:

$$x+1 \neq 0;$$

$$\text{jeśli } x+1 = y+1, \text{ to } x = y;$$

$$x+0 = x;\ x+(y+1) = (x+y)+1;$$

$$x \cdot 0 = 0;\ x(y+1) = xy+x.$$

Ostatni, nie wymieniony jeszcze aksjomat indukcji stwierdza, że zawsze, jeśli istnieje choć jedna liczba naturalna o danej własności, istnieje również najmniejsza liczba o tej własności.

Mimo iż podana wyżej aksjomatyka jest bardzo uboga, wszystkie nawet najbardziej skomplikowane twierdzenia teorii liczb można przy jej pomocy udowodnić.

Przypomnijmy, na czym polega dowodzenie twierdzeń. Dowód twierdzenia można podzielić na pewną liczbę elementarnych kroków. W każdym z nich korzysta się z aksjomatów, wcześniej udowodnionych twierdzeń, a także ze zdań, które wyprowadzone zostały we wcześniejszych krokach dowodu. Na ich podstawie wyciąga się wnioski, które powinny być oczywiste. Wniosek otrzymany w ostatnim kroku — to twierdzenie.

Podana wyżej definicja dowodu jest bardzo nieprecyzyjna. Niejasne jest bowiem, co to znaczy „oczywisty". Aby tę nieścisłość usunąć, wyodrębniono niewielką liczbę tak zwanych reguł wnioskowania. Reguła wnioskowania to zasada, która orzeka, że jeśli pewne zdania zwane przesłankami są prawdziwe, to prawdziwe jest też inne zdanie — wniosek. W każdej z reguł liczba przesłanek i ich kształt są ściśle określone, a gdy przesłanki są dane, wniosek jest jednoznaczny. Przykładem takiej reguły jest reguła odrywania. Mówi ona, że zdanie B jest prawdziwe, jeśli prawdziwe są: zdanie A oraz zdanie „jeśli A, to B".

Obecnie możemy podać bardziej precyzyjną definicję dowodu. Dowód jest to ciąg elementarnych kroków polegających na wypisywaniu zdań prawdziwych, przy czym za zdania prawdziwe uznaje się aksjomaty, wcześniej udowodnione twierdzenia i te zdania, które przy pomocy reguł wnioskowania można wyprowadzić ze zdań wypisanych wcześniej. W ten sposób sprawdzenie poprawności dowodu sprowadza się do przejrzenia listy reguł wnioskowania, aksjomatów i wcześniejszej części dowodu.

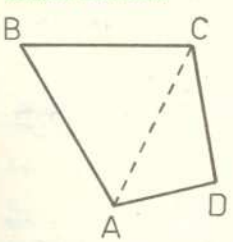
Może nasunąć się pytanie, czy można zbudować kompletną listę reguł wnioskowania, to znaczy taką, aby każde twierdzenie posiadało dowód przy użyciu reguł wnioskowania znajdujących się na tej liście. Odpowiedź na to pytanie jest pozytywna. Wynika to z twierdzenia K. Gödla o zupełności.

Aby reguły wnioskowania mogły precyzyjnie opisać metodę dowodzenia, zdania, do których te reguły stosujemy, muszą być wyrażone w możliwie prostym i jednoznacznym języku. Na szczęście język matematyki jest taki; ponadto, gdy zachodzi potrzeba, język używany na co dzień przez matematyków można zastąpić językiem formalnym, w którym możliwe jest zapisanie najbardziej skomplikowanych zdań wyłącznie przy użyciu symboli.

Podstawowym obiektem języka formalnego jest formuła. Do budowania formuł służą spójniki

Rozwiązanie zadania M43.

Załóżmy, że w czworokącie wypukłym $ABCD$ zachodzi nierówność



(1) $AB \geqslant AC$.

Wówczas (zob. rysunek)
$\sphericalangle BCA \geqslant \sphericalangle ABC$,
skąd $\sphericalangle BCD > \sphericalangle BCA \geqslant \sphericalangle ABC > \sphericalangle DBC$
a więc $BD > CD$. Dodając stronami nierówność ostatnią i (1) otrzymujemy $AB+BD > AC+CD$. Tak więc wykazaliśmy nie wprost żądane twierdzenie. Czytelnik zechce się zastanowić, czy twierdzenie pozostaje prawdziwe bez założenia wypukłości czworokąta $ABCD$.

logiczne, kwantyfikatory i formuły atomowe. Formuły atomowe są różne dla różnych teorii matematycznych. W teorii liczb są to sensowne wyrażenia utworzone z liczb, zmiennych, czyli liter $x, y, z, \ldots$, oraz symboli $+, \cdot, =, 0, 1$ (ew. innych, które używane są w arytmetyce liczb naturalnych). Spójniki logiczne to wyrażenia „oraz" ($\wedge$), „lub" ($\vee$), „nieprawda, że" ($\sim$), „jeśli ..., to" ($\Rightarrow$). W nawiasach wypisane są symbole, których używa się zamiast odpowiednich zwrotów w języku polskim. Kwantyfikatory są to zwroty „dla pewnego a" ($\bigvee_a$) oraz „dla każdego a" ($\bigwedge_a$). Formuła to odpowiednio połączony ciąg formuł atomowych, spójników logicznych i kwantyfikatorów. Jeśli zmienna występuje pod kwantyfikatorem, nazywamy ją zmienną związaną. Jeżeli w formule wszystkie zmienne są związane, to formułę taką nazywamy zdaniem. Jeśli pewna zmienna nie jest związana, to nazywamy ją zmienną wolną. I tak na przykład w formule $\bigvee_z (yz = x)$ oznaczającej, że x jest podzielne przez y, z jest zmienną związaną, natomiast y i x są zmiennymi wolnymi. W formule „dla każdego y, jeśli x jest podzielne przez y, to $x = y$ lub $y = 1$", która oznacza, że x jest liczbą pierwszą, x jest zmienną wolną, y natomiast jest zmienną związaną. Ostatnią formułę można zapisać używając wyłącznie spójników logicznych, kwantyfikatorów i formuł atomowych teorii liczb — $\bigwedge_y (\bigvee_z (zy = x) \Rightarrow x = y \vee y = 1)$. Jeżeli w formule wszystkie zmienne wolne zastąpimy przez liczby, otrzymamy zdanie. Na przykład zdaniem będzie formuła $\bigwedge_y (\bigvee_z (yz = 7) \Rightarrow 7 = y \vee y = 1)$, otrzymana z poprzedniej przez podstawienie liczby 7 w miejsce jedynej zmiennej wolnej x.

Reguły wnioskowania dla języka symbolicznego stają się zasadami, według których ciąg symboli (formułę) uznajemy za „prawdziwy", jeśli prawdziwe są inne ciągi symboli. Można przy tym reguły wnioskowania opisać w sposób na tyle precyzyjny, że posługiwanie się nimi polega na mechanicznym porównywaniu ich budowy. Rozumienie treści formuł jest tu zbędne. Czynnością mechaniczną jest też wypisywanie wniosków otrzymanych przy pomocy ustalonej reguły dowodzenia z danych przesłanek. Można więc wykonanie tych czynności przekazać maszynom liczącym. Odpowiednio zaprogramowana maszyna jest w stanie stwierdzić, czy zadana formuła jest wnioskiem z innych formuł. Potrafi też podać wniosek, gdy ma dane reguły dowodzenia i przesłanki.

Powszechnie znany jest sposób porozumiewania się z maszyną liczącą. Programy, polecenia oraz dane koduje się za pomocą otworów na taśmie papierowej. Na takiej taśmie maszyna drukuje też odpowiedzi na zadane pytania. W podobny sposób można na taśmie zakodować formuły. Jeżeli, tak jak się to często robi, przyjmiemy, że dziurka w taśmie oznacza jedynkę, natomiast brak dziurki oznacza zero, to każdy kod na taśmie stanie się rozwinięciem pewnej liczby naturalnej w systemie dwójkowym. Wobec tego można utożsamić kod formuły z odpowiadającą mu liczbą. Po to, aby otrzymać kod wniosku, gdy dane są kody przesłanek i gdy dana jest reguła dowodzenia, którą należy zastosować, maszyna wykona pewną liczbę operacji arytmetycznych. Z każdą regułą dowodzenia związana jest przeto funkcja całkowitoliczbowa o tej własności, że wartość tej funkcji na kodach przesłanek jest kodem wniosku. Funkcję tę można wyrazić przy pomocy działań arytmetycznych $+$, $\cdot$, etc.

Przyjmijmy dla uproszczenia, że są dwie reguły dowodzenia, każda o dwóch przesłankach. Niech f_1, f_2 będą funkcjami odpowiadającymi tym regułom. Dalej niech $a_1, \ldots, a_n$ będą kodami aksjomatów. Jeśli zadany jest ciąg formuł o kodach $b_1, \ldots, b_k$, to ciąg ten jest dowodem, gdy

$$\bigwedge_{i \leqslant k} (\bigvee_{j \leqslant n} (b_i = a_j) \vee \bigvee_{s < i} \bigvee_{t < i} (f_1(b_s, b_t) = b_i \vee f_2(b_s, b_t) = b_i)).$$

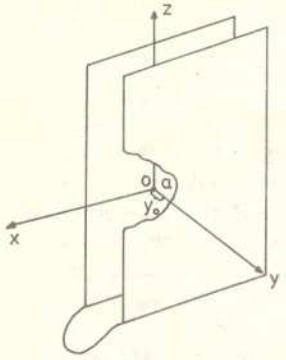
Powyższy wzór w sposób symboliczny opisuje to, że każdy element ciągu $b_1, \ldots, b_k$ jest aksjomatem lub też wynika z wcześniejszych elementów na mocy jednej z reguł dowodzenia. Wyżej opisaną formułę, oznaczającą, że ciąg $b_1, \ldots, b_k$ jest kodem dowodu, oznaczamy przez $E'(b_1, \ldots, b_k)$. Zadany ciąg liczb naturalnych $b_1, \ldots, b_k$ można w prosty sposób zakodować przy pomocy jednej liczby naturalnej $p_1^{b_1} \ldots p_k^{b_k}$, gdzie p_i jest i-tą liczbą pierwszą. W ten sposób nie tylko pojedyncze formuły, ale także ciągi formuł będą utożsamiane z liczbami naturalnymi. Z formuły E' można w łatwy sposób otrzymać formułę $E(x)$ oznaczającą, że x jest kodem ciągu liczb, które są kodami formuł tworzących dowód. Niech f oznacza funkcje taką, że jeśli x jest kodem ciągu, to $f(x)$ jest ostatnim elementem tego ciągu. Oznaczmy przez $D(y)$ formułę $\bigvee_x (E(x) \wedge f(x) = y)$. Nietrudno zauważyć, że $D(y)$ oznacza, iż y jest kodem twierdzenia.

Oczywiście to, że są tylko dwie reguły i skończona liczba aksjomatów, jest dużym uproszczeniem. Wypisanie formuły E oraz D bez tych uproszczeń jest nieco bardziej skomplikowane. Zasada jest jednak ta sama.

W czwartym wieku przed naszą erą, w czasach gdy Kreteńczycy byli sławnymi na cały świat kłamcami, Eubulides, uczeń Euklidesa, postawił pytanie: „Czy Kreteńczyk Epimenides mówił prawdę, gdy mówił «kłamię»?". Na to pytanie nie można udzielić poprawnej odpowiedzi. Jeśli bowiem mówił prawdę, to prawdziwe było zdanie „kłamię", a przeto prawdy nie powiedział. Jeśli natomiast skłamał, to mówiąc „kłamię" mówił prawdę, a więc nie kłamał.

Rozwiązanie zadania F15.

Wprowadźmy układ współrzędnych jak na rys. 1 i przyjmijmy, że ciało o ładunku Q



znajduje się w punkcie o współrzędnych $x = z = 0$, $y = y_0$. Ciało to indukuje na wewnętrznych powierzchniach okładek kondensatora ładunek powierzchniowy o sumarycznej wartości $-Q$. (Zgodnie z twierdzeniem Gaussa). Ładunek na okładkach jest rozłożony nierównomiernie. Jednakże całkowity ładunek zgromadzony na każdej z okładek zależy, przy ustalonych Q i a, tylko od odległości ciała o ładunku Q od danej okładki. Dla naszych celów wystarczy znaleźć tę zależność.

Zgodnie z zasadą superpozycji wypadkowe pole elektrostatyczne pochodzące od wielu ładunków jest sumą pól elektrostatycznych wywołanych przez poszczególne ładunki. Zastosujmy tę zasadę do naszego problemu. Wynika z niej, że np. umieszczenie dodatkowego ciała o ładunku Q w dowolnym punkcie płaszczyzny $y = y_0$, wewnątrz kondensatora, podwaja całkowity ładunek powierzchniowy obu okładek. Można to spostrzeżenie uogólnić stwierdzając, że całkowity ładunek indukowany na okładkach nie zależy od rozmieszczenia ładunków w płaszczyźnie $y = y_0$ wewnątrz kondensatora. Zamiast więc rozpatrywać skomplikowany problem naładowanego ciała punktowego umieszczonego wewnątrz kondensatora, możemy rozwiązać zagadnienie równomiernie naładowanego wycinka płaszczyzny o powierzchni równej powierzchni okładek i o sumarycznym ładunku Q, umieszczonym w płaszczyźnie $y = y_0$. Dla obu przypadków całkowity ładunek na każdej z okładek kondensatora jest taki sam. Oczywiście inny będzie rozkład powierzchniowy ładunku na okładkach, ale to dla naszego zadania nie ma znaczenia. Ponieważ okładki kondensatora są połączone drutem i mają równy potencjał, więc nowy układ jest równoważny układowi dwu równolegle połączonych kondensatorów płaskich. Ładunek zgromadzony na okładkach jest proporcjonalny (przy ustalonej różnicy potencjałów) do pojemności kondensatora, czyli w przypadku kondensatora płaskiego jest odwrotnie proporcjonalny do odległości między okładkami. Stąd stosunek ładunków na okładkach wynosi:

$$\frac{Q_1}{Q_2} = \frac{a - y_0}{y_0}.$$

Ponieważ $-Q = Q_1 + Q_2$, więc

$$Q_2 = -Q\frac{y_0}{a}.$$

Przesuwając ciało o ładunku Q o odcinek Δy zmieniamy ładunek Q_2 o $\Delta Q_2 = -Q\frac{\Delta y}{a}$.

I taki właśnie ładunek ΔQ_2 przepłynie przez drut przy przesunięciu ciała naładowanego o odcinek o długości Δy.

Przytoczone powyżej pytanie nosi nazwę antynomii kłamcy lub paradoksu Epimenidesa i jest jednym z wielu paradoksów, które od starożytności spędzały sen z powiek filozofom i zapładniały ich wyobraźnię, zmuszały do nieustannych rewizji poglądów na znane i często bardzo proste sprawy. Wśród antynomii można wyróżnić bogatą klasę tak zwanych antynomii semantycznych, do których należy antynomia kłamcy. Istota tych antynomii polega na tym, że buduje się je ze zdań autoreferujących, to znaczy orzekających coś o sobie. „Kłamię" Epimenidesa stwierdza, że zdanie „kłamię" jest kłamstwem.

Podam jeszcze jeden przykład antynomii tego samego typu — oczywiście nieznany w starożytności. Przypuśćmy, że mamy do dyspozycji doskonałą maszynę cyfrową z olbrzymią pamięcią, szybko działającą i niezawodną. Na wyjściu maszyny umieszczamy przyrząd, który w chwili gdy maszyna drukuje odpowiedź „nie", wyłącza ją z sieci, natomiast na inne sygnały nie reaguje. Podajemy maszynie informacje o działaniu tego przyrządu i zadajemy pytanie „czy po udzieleniu odpowiedzi na to pytanie zostaniesz wyłączona z sieci?". I cokolwiek maszyna wydrukuje, odpowiedź będzie błędna. Jeśli wydrukuje „tak", przyrząd na tę odpowiedź nie zareaguje i maszyna nie zostanie wyłączona, jeśli natomiast wydrukuje „nie", przyrząd zareaguje i maszyna zostanie wyłączona wbrew temu, co wydrukowała.
Można także zbudować bardziej skomplikowaną antynomię, z pomocą której można otrzymać wspomniane na wstępie twierdzenie Churcha i Gödla. Z twierdzenia tego wynika między innymi, że program Hilberta zaksjomatyzowania całej matematyki nie może zostać zrealizowany. Jakikolwiek rozsądny układ aksjomatów przyjmiemy, zawsze znajdziemy zdanie, którego przy pomocy tych aksjomatów nie uda się ani udowodnić, ani obalić.
Zbiór aksjomatów będziemy nazywali niesprzecznym, jeśli przy jego pomocy nie można udowodnić zdań sprzecznych. Układ aksjomatów nazywamy zupełnym, jeśli każde zdanie można przy jego pomocy udowodnić albo obalić. Układ jest obliczalny, jeśli można tak zaprogramować maszynę, żeby umiała stwierdzić, czy dane zdanie jest twierdzeniem. Używając przed chwilą zdefiniowanych pojęć, można sformułować twierdzenie Gödla: żaden obliczalny i niesprzeczny układ aksjomatów arytmetyki nie jest zupełny.

Istotą obu cytowanych wcześniej antynomii jest występowanie w nich zdań autoreferujących. Kody formuł arytmetyki można utożsamić z liczbami naturalnymi. Zdania arytmetyki opisują własności liczb, może się więc zdarzyć, że formuła orzeka o swoim kodzie, a więc w pewnym sensie o sobie. Fakt, że formuła jest twierdzeniem, jest równoważny z tym, że po podstawieniu jej kodu do formuły D otrzymamy zdanie prawdziwe. A więc tu także istnieje możliwość zbudowania zdania autoreferującego, wystarczy do formuły D podstawić kod tej formuły. Gdy dana jest formuła, odpowiednio zaprogramowana maszyna może podstawić dowolną liczbę w miejsce zmiennej wolnej. W szczególności za tę zmienną maszyna może podstawić kod tej formuły. Mając dany kod x formuły X maszyna będzie mogła wydrukować kod zdania Y, otrzymanego przez podstawienie liczby x do formuły X. Proces obliczania kodu y, gdy dany jest kod x, opisuje pewną funkcję arytmetyczną. Oznaczmy ją literą F.

Niech A będzie zaprzeczeniem zdefiniowanej wyżej formuły D. Wtedy $A(x)$ oznacza, że x nie jest kodem twierdzenia. Z formuły A tworzymy nową formułę podstawiając $F(x)$ w miejsce zmiennej x. Tak otrzymaną formułę oznaczamy literą B, jej kod natomiast literą b. Oczywiście b można obliczyć, gdy tylko dany jest kod f funkcji F oraz kod formuły A. Podstawiając b w miejsce zmiennej wolnej w formule B otrzymujemy zdanie C. Z definicji funkcji F wynika, że kod c zdania C jest równy $F(b)$. Okazuje się, że zdanie C oraz zdanie $A(c)$ są równoważne. Istotnie $A(c)$ to $A(F(b))$, gdyż $c = F(b)$. Natomiast C to $B(b)$. Ale $B(x)$ — to z definicji $A(F(x))$, a więc $B(b)$ jest także równe $A(F(b))$. W ten sposób przez kolejne podstawienie do formuły jej kodu, a więc stosując metodę zasugerowaną przez przytoczone antynomie, znaleźliśmy dla danej formuły A zdanie samoreferujące B, które jest równoważne ze zdaniem $A(c)$.
Jeśli układ aksjomatów jest zupełny, C powinno być twierdzeniem lub zaprzeczeniem twierdzenia. Okazuje się jednak, że jest to niemożliwe. Przypuśćmy bowiem, że C jest twierdzeniem. Wtedy zdanie $A(c)$, które jest z nim równoważne, jest także twierdzeniem. To znaczy twierdzeniem jest fakt opisany przez $A(c)$ — „c jest kodem zdania, które nie jest twierdzeniem", a więc C nie jest twierdzeniem. Z drugiej strony, jeśli założyć, że twierdzeniem jest zaprzeczenie zdania C, to twierdzeniem będzie zdanie „c nie jest kodem twierdzenia", czyli — $A(c)$. Ale $A(c)$ jest równoważne z C, przeto C jest także twierdzeniem. W obu przypadkach z założenia, że pewne zdanie jest twierdzeniem, wynika, że twierdzeniem jest jego zaprzeczenie, co jest niemożliwe, jeśli tylko układ aksjomatów jest niesprzeczny.

Tym samym pokazaliśmy, że nie można podać takiego układu aksjomatów arytmetyki, przy pomocy którego można by rozstrzygnąć prawdziwość wszystkich zdań. W podobny sposób można też udowodnić, że nie ma algorytmu pozwalającego na sprawdzenie czy zdania arytmetyki są, czy nie są twierdzeniami arytmetyki Peana.

Przytoczone powyżej rozumowanie zawiera szereg luk. Przede wszystkim posługiwaliśmy się pojęciem maszyny cyfrowej o nieograniczonych możliwościach. W dowodach podawanych w podręczniku logiki używa się w tym miejscu teorii maszyn Turinga (por. artykuły prof. A. Mostowskiego, «Delta», 1974, 10, 11).

Rozwiązanie zadania M45.

Gdyby liczba $a = \sqrt{2}^{\sqrt{2}}$ była wymierna, żądane twierdzenie byłoby prawdziwe, przyjęlibyśmy bowiem $x = y = \sqrt{2}$. Pozostaje więc do rozpatrzenia przypadek, gdy liczba a jest niewymierna. Wówczas liczba $b = a^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2} \cdot \sqrt{2}} = (\sqrt{2})^2 = 2$ jest wymierna i można przyjąć $x = a, y = \sqrt{2}$.

Uwaga. Wiadomo, że liczba a jest niewymierna i przestępna, tzn. nie jest pierwiastkiem żadnego wielomianu stopnia dodatniego o współczynnikach całkowitych.