Automatyczny matematyk

Doc. dr Lesław W. SZCZERBA

W erze wszechobowiązującej automatyki nasuwa się nieodparcie pytanie, czy wszystko można zautomatyzować. W szczególności w czasopiśmie poświęconym matematyce zupełnie na miejscu jest pytanie

CZY MOŻNA ZAUTOMATYZOWAĆ MATEMATYKĘ?

Pytanie to można postawić również inaczej: Czy można zbudować maszynę, która wykonywałaby czynności wykonywane dotychczas przez matematyków? Odpowiedzieć na tak szeroko postawione pytanie jest o tyle trudno, że nikt dotychczas nie zdefiniował dostatecznie ściśle obowiązków matematyka. Obawiam się zresztą, że podanie takiej definicji znacznie przekracza moje kompetencje. Nie pozostaje zatem nic innego, jak tylko ograniczyć się do pewnego aspektu działalności matematyków. Mogę się tu zresztą oprzeć o autorytet Hilberta, który twierdził, że matematycy powinni rozwiązywać trudne problemy matematyczne. Opuśćmy w tym stwierdzeniu niejasne określenie „trudne" i zastanówmy się nad tym, co to znaczy rozwiązać problem matematyczny. Większość problemów matematycznych daje się sformułować w następującej postaci: Czy takie to, a takie zdanie jest twierdzeniem takiej to, a takiej teorii matematycznej? Można to wypowiedzieć ściślej: Dany jest pewien układ aksjomatów; czy dane stwierdzenie można wyprowadzić z tych aksjomatów posługując się określonymi regułami dowodzenia? Problem zautomatyzowania tak postawionego zagadnienia wzbudził w ostatnich latach ogólne zainteresowanie i znany jest pod nazwą „problem automatycznego dowodzenia twierdzeń". Wchodzi on w skład kompleksu zagadnień związanych ze sztuczną inteligencją. Upraszcza się go zresztą jeszcze bardziej przyjmując, że regułami dowodzenia posługują się istniejące już maszyny liczące: problem sprowadza się do napisania odpowiedniego programu. Budowę zaś samych maszyn matematycznych, czy — jak ostatnio modnie jest mówić z angielska — komputerów, pozostawia się specjalistom.

Jak zatem napisać program, który dawałby odpowiedź na pytanie, czy dane zdanie wynika z podanej aksjomatyki? Dla teorii rozstrzygalnych sprawa jest prosta: należy ściśle opisać metodę rozstrzygania dla danej teorii. Na przykład dla teorii porządku liniowego lub teorii nierówności liniowych można opisać odpowiednie metody eliminacji kwantyfikatorów (omówione w «Delcie», 1974, nry 7 i 9). Dla rachunku zdań — metodę zero-jedynkową, opisaną w większości podręczników logiki (np. H. Rasiowa *Wstęp do matematyki współczesnej*). Gorzej z teoriami, dla których metoda rozstrzygania nie istnieje, to znaczy z teoriami nierozstrzygalnymi (por. artykuły prof. Mostowskiego, «Delta», 1974, nry 10 i 11). Czy wobec takich teorii jesteśmy całkiem bezsilni? Niezupełnie. Istnieją bowiem metody uniwersalne, dające się zastosować do każdej teorii opisanej aksjomatycznie. Omówimy tę metodę na przykładzie rachunku zdań. Aby uczynić sprawę jeszcze prostszą, zajmiemy się taką formalizacją rachunku zdań, w której występują, poza zmiennymi, tylko dwa symbole zwane też funktorami zdaniotwórczymi: negacja $\sim$ i implikacja $\Rightarrow$. (Pozostałe funktory można wtedy zdefiniować; proszę sprawdzić przykłady na marginesie!).

$p \vee q = \sim p \Rightarrow q$

$p \wedge q = \sim (p \Rightarrow \sim q)$

$p \Leftrightarrow q = (p \Rightarrow \sim q) \Rightarrow \sim (\sim p \Rightarrow q)$

Jeśli w naszym przypadku rachunek zdań ma być zaksjomatyzowany — wypadałoby podać jego aksjomaty. Mamy tu dość dużą swobodę. Te, które zostały podane obok na marginesie, cytujemy z książki A. Mostowskiego *Logika matematyczna*; zostały one podane przez J. Łukasiewicza. Aby się przekonać, że jakieś zdanie jest twierdzeniem rachunku zdań (w przypadku rachunku zdań zamiast „twierdzeniem" mówi się często „tautologią"), trzeba je udowodnić. Cóż to jednak oznacza „udowodnić"? Oznacza to, że trzeba podać dowód tego zdania, czyli ciąg, w którym każde zdanie wynika bezpośrednio z aksjomatów lub też ze zdań wypisanych wcześniej, a kończący się zdaniem, które należy udowodnić. Niektórzy wymagają dopisania na końcu literek c.b.d.o. (*co było do okazania*) lub c.n.u. (*co należało udowodnić*), nie jest to jednak absolutnie konieczne.

1) sylogizm warunkowy
$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$,
2) prawo Dunsa-Scotusa
$p \Rightarrow (\sim p \Rightarrow q)$,
3) prawo Claviusa
$(\sim p \Rightarrow p) \Rightarrow p$.

Wszystko byłoby w porządku, gdyby nie zwrot: „wynika bezpośrednio". Przecież na dobrą sprawę „daje się udowodnić" oznacza tyle, co „wynika", czyżbym więc zamierzał wprowadzać czytelników w błędne koło definicji? Nie sposób się dalej wykręcać i muszę teraz podać precyzyjne reguły wnioskowania, które razem stanowić będą definicję terminu „wynika bezpośrednio".

Reguła 1 (trywialna). Każde zdanie wynika bezpośrednio z siebie samego. Reguła jest, zgodnie z nazwą, trywialna (tzn. naiwnie prosta) i służy tylko do

Przykład
$A = p \Rightarrow (q \Rightarrow p)$
$B = r \Rightarrow s$
$C = (r \Rightarrow s) \Rightarrow (q \Rightarrow (r \Rightarrow s))$

tego, aby można było w dowodzie wypisywać aksjomaty. W ten sposób ciąg złożony z jednego aksjomatu jest dowodem. Czego dowodem? Oczywiście tego aksjomatu. Stąd prosty, acz niezgodny ze (złymi) obyczajami wniosek, że aksjomaty są twierdzeniami.

Reguła 2 (podstawiania). Ze zdania A, w którym występuje zmienna zdaniowa p, wynika bezpośrednio zdanie C, powstające ze zdania A przez podstawienie zdania B w miejscu wszystkich wystąpień zmiennej p.

Uf! Tej reguły nie można nazwać trywialną. Stanie się jednak jasna, gdy się rozpatrzy przykład podany na marginesie.

Reguła 3 (odrywania). Ze zdania A postaci $B \Rightarrow C$ oraz zdania B wynika bezpośrednio zdanie C.

Reguła ta w odróżnieniu od poprzednich ma dwie przesłanki: zdanie A, które musi mieć postać implikacji, oraz zdanie B, które musi być poprzednikiem tej implikacji. Wnioskiem okazuje się następnik implikacji.

Wreszcie czas na warunek końcowy: zdanie wynika bezpośrednio z jednego lub dwu zdań tylko wtedy, gdy wynika z nich na mocy przynajmniej jednej z reguł 1–3.

Teraz już wiemy dokładnie, czym jest dowód w rachunku zdań. Ale w tej sytuacji, jak łatwo zauważyć, sprawdzenie, czy przedstawiony nam przez kogoś ciąg zdań jest dowodem, jest sprawą być może mozolną, ale całkowicie mechaniczną. Sprawdzenie zaś, czy jest to dowód żądanego zdania, nie przedstawia żadnej w ogóle trudności. Z tej obserwacji wywodzą się metody automatycznego dowodzenia twierdzeń: maszyna wypisuje jeden po drugim coraz dłuższe ciągi zdań, a następnie sprawdza, czy wypisany ciąg nie jest przypadkiem poszukiwanym dowodem. Jeśli chcemy mieć pewność, że dla każdego twierdzenia otrzymamy po pewnym czasie dowód, musimy tak ułożyć program wypisujący ciągi, aby każdy skończony ciąg zdań, a przynajmniej każdy dowód mógł się po pewnym czasie pojawić. Stanowi to oczywiście pewną dodatkową trudność, ale na szczęście niezbyt wielką.

Tak więc, jeśli wystartowaliśmy z twierdzenia, to wszystko w porządku, po pewnym, być może bardzo długim, ale jednak skończonym, czasie otrzymamy jego dowód. Cóż jednak, jeśli pechowo zaczęliśmy poszukiwać dowodu zdania, które twierdzeniem nie jest? W przypadku rachunku zdań zawsze pojawi się wtedy negacja tego zdania, i po tym będziemy mogli poznać, że się myliliśmy. Dla niektórych jednak innych teorii możemy być zmuszeni do czekania nieskończenie długo, pożerani przez niepewność: ,,A nuż następny dowód będzie tym właściwym?". Ta niedoskonałość metody wynika z jej ogólności. Metoda daje się bowiem przenieść na wszystkie teorie matematyczne. Może być wówczas znacznie bardziej skomplikowana. Zwłaszcza wtedy, gdy w teorii występują kwantyfikatory, wówczas bowiem reguły wnioskowania ulegają znacznej komplikacji. Zasada pozostaje jednak stale ta sama: wypisywać ,,po kolei" ciągi zdań i sprawdzać, czy któryś nie jest przypadkiem pożądanym dowodem. Dotyczy to również teorii nierozstrzygalnych, i to jest przyczyną omawianej wady.

Z punktu widzenia praktyki programowania istniejących maszyn liczących (owych komputerów) metoda ma jeszcze dalsze wady. Jest mianowicie bardzo nieefektywna: dla otrzymania stosunkowo prostych dowodów maszyna musiałaby pracować bardzo długo, a to jak wiadomo jest związane ze znacznymi kosztami. Zaczęto zatem metodę modyfikować i ulepszać. Ulepszenia te polegały na pomijaniu tych dowodów, o których z góry wiadomo, że nie prowadzą do celu. Modyfikacje te miały ten uboczny skutek, iż maszyna musi teraz pamiętać masę informacji, którą w czasie pracy wyprodukuje. Istniejące, przynajmniej dotychczas, maszyny mają pamięć skończoną, to znaczy mogą zapamiętać tylko skończoną liczbę informacji. Co gorsze, pojemność ich pamięci, choć obiektywnie czasem bardzo duża, nie wystarcza do zapamiętania wyników częściowych, potrzebnych przy poszukiwaniu nawet stosunkowo prostych dowodów. Pamięć maszyny ,,zatyka się" i maszyna przestaje pracować lub zaczyna działać nieprawidłowo.

Do metod tego typu należy np. cieszący się ogromnym zainteresowaniem psychologów ,,Ogólny Rozwiązywacz Problemów" (General Problem Solver). Jest to program, skonstruowany przez matematyków amerykańskich. Zob. np. J. Kozielecki: *Z zagadnień psychologii myślenia*).

W tej sytuacji automatyczne dowodzenie twierdzeń stosuje się tylko do zagadnień niezwykle prostych, ale za to w sytuacjach, gdy ingerencja człowieka jest niemożliwa lub niepożądana. Natomiast jeśli idzie o samodzielne dowodzenie interesujących twierdzeń matematycznych przez maszyny, wymagałoby to albo istotnej zmiany metody, albo istotnego postępu w budowie maszyn liczących. Co do pierwszej ewentualności autor może powiedzieć tylko tyle, że dziś zupełnie nie widać takich możliwości. Co zaś tyczy drugiej, to postęp elektroniki musiałby chyba być tak duży, że wymagałby zmiany poglądów na budowę fizyczną świata. Powie ktoś, że to możliwe. No cóż, nie umiem temu zaprzeczyć ani też potwierdzić, i w tej sytuacji nie mogę zrobić nic innego, jak tylko skończyć artykuł, pozostawiając resztę wyobraźni Czytelnika.