ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE XIV (1972)

Ministerstwo Nauki i Szkolnictwa Wyższego

L. W. SZCZERBA (Warszawa)

Automatyczne dowodzenie twierdzeń

Rozwiązanie wielu zagadnień matematycznych sprowadza się do wykonania pewnej ilości rachunków według ściśle określonego algorytmu. Na przykład znalezienie rozwiązań układu równań liniowych sprowadza się do obliczenia pewnej ilości wyznaczników, stwierdzenie, ile pierwiastków w określonym przedziale liczb rzeczywistych ma dany wielomian — do policzenia łańcucha Sturma, a odpowiedź na pytanie, czy określona formuła rachunku zdań jest tautologią można uzyskać tzw. metodą zero-jedynkową. Klasy zagadnień, dla których istnieje efektywna metoda rozwiązywania nazywają się *rozstrzygalnymi*.

Rozwiązanie zagadnienia rozstrzygalnego nie wymaga, w zasadzie, od rozwiązującego żadnej pomysłowości. Dla każdej klasy zagadnień rozstrzygalnych można by ułożyć program na maszynę cyfrową, tak by maszyna sama, bez żadnego dalszego udziału człowieka, rozwiązywała zagadnienie.

Okazuje się jednak, że większość interesujących klas zagadnień jest nierozstrzygalna. Czy oznacza to, że zastosowanie maszyn cyfrowych w matematyce musi ograniczyć się do wykonywania rachunków, że maszyny nie są w stanie dopomóc matematykowi w rozwijaniu nauki? Nie chodzi tu oczywiście o fakt, że maszyny samym swym istnieniem przyczyniły się do rozwinięcia, a nawet powstania wielu teorii matematycznych, lecz o to, czy maszyna cyfrowa może być względnie uniwersalnym narzędziem w ręku matematyka, czy też może mu dopomóc tylko w nielicznych dziedzinach?

Odpowiedź na to pytanie nie wydaje się jednoznaczna. W dalszym ciągu znajduje się kilka uwag na ten temat.

1. Formuły i zdania

Aby uprawiać jakąś dziedzinę matematyki za pomocą maszyny cyfrowej trzeba się porozumiewać z maszyną w sprawach dotyczących tej dziedziny. Na ogół nie można wprowadzać do maszyny tworów mate-

matycznych bezpośrednio (żadna prosta euklidesowa nie zmieściłaby się w maszynie). Trzeba posługiwać się nazwami przedmiotów. Do tego celu służą języki formalne.

Każdy język formalny składa się z formuł, które są skończonymi ciągami liter pewnego alfabetu. W skład alfabetu wchodzą litery oznaczające zmienne $x_0, x_1, \ldots, x_n, \ldots$, spójniki logiczne(1): negacja $\sim$, alternatywa $\vee$, koniunkcja $\wedge$, kwantyfikator egzystencjalny $\bigvee$ oraz kwantyfikator ogólny $\bigwedge$.

Ponadto alfabet zawiera symbole swoiste danego języka: pewną ilość stałych, symboli relacji i symboli operacji.

Na przykład w przypadku arytmetyki mamy dwie stałe: 0 i 1, dwa symbole operacji $+$ i $\cdot$ oraz dwa symbole relacji $=$ i $<$. Napisy oznaczające liczby, tak zwane termy, możemy budować ze stałych i zmiennych za pomocą symboli operacji, np. termami są: x_0, 0, (x_1+1), $\big((1+1)\cdot x_2\big)$ itp. Ścisłą definicję termu, podobnie jak i dalszych pojęć wspomnianych w tym paragrafie, może czytelnik znaleźć na przykład w [8].

Łącząc dwa termy znakiem relacji otrzymujemy formułę atomiczną, na przykład równość

$$\big((x_1\cdot x_1)+(x_1+1)\big) = 0$$

lub nierówność

$$\big(x_4+(1+x_1)\big) < (x_2-1).$$

Łącząc formuły atomiczne spójnikami zdaniotwórczymi otrzymujemy dowolne formuły.

Każda zmienna nie związana kwantyfikatorem nazywa się *zmienną wolną*. Na przykład w formule

$$\big(x_0 < x_1 \vee \bigvee x_1\big(\bigwedge x_2(x_1 < x_2)\big)\big)$$

zmienna x_0 jest wolna, a zmienna x_2 jest związana, natomiast zmienna x_1 występuje raz jako zmienna wolna (w pierwszym członie alternatywy), a drugi raz jako zmienna związana (w drugim członie alternatywy).

Aby mówić o tym, czy jakieś zdanie, np.

$$\bigwedge x_0 \bigvee x_1(x_0 < x_1) \tag{1}$$

jest prawdziwe, należy najpierw ustalić jak będzie się rozumieć znak $<$

---

(1) Zazwyczaj wśród spójników logicznych wymienia się jeszcze implikację $\rightarrow$ i równoważność $\leftrightarrow$. Oba te spójniki są jednak do celów niniejszego artykułu niewygodne, wprowadziłyby znaczną a niepotrzebną komplikację definicji. Ponieważ zaś dają się łatwo wyeliminować: formułę $X \rightarrow Y$ można zastąpić formułą $\sim X \vee Y$, a formułę $X \leftrightarrow Y$ formułą $(X \wedge Y) \vee (\sim X \wedge \sim Y)$, nie będzie się o nich w zasadzie mówić.

oraz zmienne. Innymi słowy należy podać dziedzinę matematyczną. W przypadku zdania (1) musi to być dziedzina postaci

$$\mathfrak{A} = (A, <),$$

gdzie A jest dowolnym zbiorem, a $<$ relacją dwuargumentową określoną na tym zbiorze. (Ewentualnie relacji może być jeszcze więcej, w każdym razie relacja $<$ musi być.) Weźmy na przykład dziedzinę $\mathfrak{A}_1 = (R, <)$, gdzie R jest zbiorem wszystkich liczb rzeczywistych, a $<$ zwykłą relacją mniejszości. Jak wiadomo, zdanie (1) jest prawdziwe w dziedzinie $\mathfrak{A}_1$. Natomiast w dziedzinie $\mathfrak{A}_2 = (S, <')$, gdzie S jest odcinkiem z końcami $\langle 0, 1\rangle$, a $<'$ zwykłą relacją mniejszości ograniczoną do tego odcinka, zdanie (1) nie jest prawdziwe: nie ma na odcinku S liczby większej od 1.

Niektórzy logicy (por. np. [8]) uważają, że o formule, która nie jest zdaniem, nie sposób powiedzieć, czy jest ona prawdziwa, czy fałszywa. Na przykład trudno powiedzieć cokolwiek o formule

$$\bigvee x_0(x_0 < x_1), \tag{2}$$

dopóki nie wiadomo co oznacza x_1.

Jednak wielu logików (por. np. [13]) uważa formuły ze zmiennymi wolnymi za zdania otwarte i operuje nimi tak, jak gdyby wszystkie zmienne wolne były związane kwantyfikatorami ogólnymi stojącymi na początku.

Przy takim ujęciu zamiast zdania (1) można napisać formułę

$$\bigvee x_1(x_0 < x_1).$$

Przy różnych systemach automatycznego dowodzenia twierdzeń stosuje się różne podejścia. Na przykład w przypadku rachunków Gentzena oraz metod podobnych do tego rachunku (patrz np. [6] i [15]) wygodnie jest mówić o prawdziwości formuł otwartych, natomiast przy niektórych innych systemach (patrz np. [18]) wygodnie ograniczać się do zdań, czyli formuł bez zmiennych wolnych. W dalszym ciągu niniejszego artykułu przyjmiemy drugie podejście: formuły otwarte mogą być prawdziwe. W związku z tym terminu zdanie i formuła będziemy używać zamiennie.

Dawno już zauważono, że nie można w nieskończoność redukować twierdzeń matematycznych do twierdzeń wcześniejszych, nie można w nieskończoność pytać „dlaczego?". Pewne twierdzenia trzeba przyjąć bez dowodu. Twierdzenia te nazywają się *aksjomatami*. *Aksjomatyką* nazywa się dowolny zbiór aksjomatów. Wyciągając z aksjomatów wnioski na drodze rozumowań otrzymuje się różne *twierdzenia*.

Przykładem zastosowania rozumowania logicznego może być reguła odrywania, zwana po łacinie *modus ponens*. Pozwala ona przyjąć za udowodnione zdanie B, jeśli wśród aksjomatów lub zdań wcześniej udowodnionych są zdania A i implikacja $A \to B$. Ogólniej, takim rozumowaniem

może być dowód, to znaczy ciąg zdań $\mathsf{D} = \langle P_0, \ldots, P_n \rangle$ taki, że każde zdanie 1° jest aksjomatem lub 2° tautologią lub też 3° wynika ze zdań wcześniejszych na mocy reguły odrywania. Gdyby w rozpatrywanym systemie logicznym przyjąć inne reguły wnioskowania, należałoby odpowiednio zmodyfikować punkt 3°. Mówimy, że D jest dowodem zdania D, jeżeli to zdanie jest ostatnim wyrazem ciągu D. O takim zdaniu mówi się, że ma dowód D. Zbiór wszystkich zdań mających dowód z aksjomatyki A nazywamy *teorią o aksjomatyce* A. Elementy teorii nazywane są też jej *twierdzeniami*. W szczególnym przypadku każdy aksjomat $A \in \mathsf{A}$ jest twierdzeniem teorii o aksjomatyce A. Dowodem tego twierdzenia jest ciąg jednowyrazowy $\langle A \rangle$.

Jeżeli zdanie Z jest prawdziwe w dziedzinie $\mathfrak{A}$, to mówi się również, że $\mathfrak{A}$ jest *modelem* zdania Z. Jeśli istnieje model $\mathfrak{A}$ zdania Z, to mówimy, że zdanie Z jest *spełnialne*, w przeciwnym razie o zdaniu Z mówimy, że jest *niespełnialne*. Jeśli natomiast zdanie Z jest prawdziwe we wszystkich dziedzinach, to mówimy, że Z jest *tautologią*. Oczywiście jeśli zdanie Z jest tautologią, to zdanie $\sim Z$ jest niespełnialne i odwrotnie, jeśli zdanie Z jest niespełnialne, to zdanie $\sim Z$ jest tautologią.

2. Teorie rozstrzygalne i nierozstrzygalne

Teorie, dla których istnieje metoda rozstrzygania czy dane zdanie jest twierdzeniem tej teorii nazywają się *rozstrzygalnymi*(2). Teorie takie mogłyby być w zasadzie uprawiane przez maszynę cyfrową. Oczywiście pod warunkiem ułożenia odpowiedniego programu, który po wprowadzeniu hipotezy do maszyny orzekałby o jej prawdziwości lub fałszywości.

Teoriami rozstrzygalnymi są między innymi: teoria porządku gęstego (por. [10]), elementarna teoria dodawania liczb naturalnych (por. [14]). Jednak już teoria obejmująca jednocześnie dodawanie i odejmowanie liczb naturalnych, tj. arytmetyka liczb naturalnych, jest nierozstrzygalna (por. [7]). Nierozstrzygalnymi okazało się większość interesujących matematycznie teorii, a w tym rachunek predykatów (por. [4]) i teoria mnogości (por. [19]). Co więcej, każda teoria zawierająca którąkolwiek z nich, a więc praktycznie biorąc każda teoria drugiego rzędu, tzn. dopuszczająca mówienie o zbiorach elementów, jest nierozstrzygalna.

Utarło się w tej sytuacji powiedzenie, że wszystkie interesujące teorie matematyczne są nierozstrzygalne. Wydaje się, że takie twierdzenie

(2) Trudno jest podać ścisłą definicję efektywnego postępowania. Definicje takie można znaleźć w literaturze (np. Turing [23], Markow [11], w języku polskim [8]). Pojęcie to jest jednak na tyle intuicyjne, że poprzestaniemy tu na określeniu nie ścisłym, ale intuicyjnym. Postępowanie jest efektywne, jeśli polega na wykorzystywaniu pewnych prostych czynności skończoną ilość razy.

jest trochę przesadzone, gdyż na przykład arytmetyka liczb rzeczywistych jest rozstrzygalna (por. [22]). Oczywiście chodzi tu o arytmetykę elementarną (pierwszego rzędu), to znaczy taką, w której języku można mówić o liczbach i działaniach dokonywanych na liczbach, a nie o zbiorach liczb. Jest to ograniczenie dość istotne, bo na przykład twierdzenie:

1. *Dowolny wielomian nieparzystego stopnia ma pierwiastek*

nie da się wyrazić w języku elementarnej arytmetyki liczb rzeczywistych, gdyż pojęcie wielomianu nieparzystego stopnia jest nieelementarne, aczkolwiek każde ze zdań:

2. *Dowolny wielomian stopnia n ma pierwiastek*

(jeśli tylko n będzie konkretną liczbą naturalną) można w tym języku wyrazić. Oczywiście gdy n jest liczbą nieparzystą, to zdanie 2 jest twierdzeniem arytmetyki liczb rzeczywistych, a gdy n jest liczbą parzystą, to nie.

Tylko niektóre teorie są rozstrzygalne, a zatem tylko dla niektórych teorii istnieje metoda, która zastosowana do dowolnego zdania Z z języka tej teorii, udzieli w skończonym czasie odpowiedzi na pytanie; czy zdanie Z jest twierdzeniem rozpatrywanej teorii? Jeśli zdanie jest twierdzeniem, zostanie przez tę metodę w skończonej ilości kroków potwierdzone, w przeciwnym razie — obalone (również w skończonej ilości kroków). Dla teorii nierozstrzygalnych nie ma takich metod. Tym bardziej nie ma takiej uniwersalnej metody, która rozstrzygałaby czy wskazane zdanie jest twierdzeniem dowolnej zadanej teorii. Jeśli jednak dopuścimy metody, które w skończonej ilości kroków udzielają odpowiedzi pozytywnej, a więc jeśli zdanie jest twierdzeniem, to zostanie potwierdzone w skończonej ilości kroków, rezygnując z żądania, by metoda obalała w skończonej ilości kroków zdania, które nie są twierdzeniem, to okaże się, że istnieje wiele metod uniwersalnych. Dwie takie metody zostaną opisane w dalszym ciągu.

3. Rachunek Gentzena

Jednym z najszerzej znanych sposobów automatycznego dowodzenia twierdzeń jest tzw. *rachunek Gentzena*. Jest to metoda sprawdzania czy dana formuła jest tautologią. Zagadnienie, czy określona formuła jest tautologią, mało interesowałoby przeciętnego matematyka, gdyby do tego typu pytań nie dawało się sprowadzić wielu naturalnych zagadnień matematycznych; pytanie, czy formuła dowolna Z wynika z aksjomatów $Ax_1, \ldots, Ax_n$ jest równoważna pytaniu, czy formuła

$$Ax_1 \wedge \ldots \wedge Ax_n \rightarrow Z$$

jest tautologią. Rachunek Gentzena najdogodniej opisywać w dwu etapach, najpierw dla formuł otwartych, a następnie dla formuł dowolnych.

Jeżeli F jest formułą atomiczną lub jej negacją, to oczywiście nie jest tautologią([3]), jeżeli natomiast F jest alternatywą

$$A_0 \vee \sim A_0$$

(gdzie A_0 jest formułą atomiczną), to F jest tautologią. Co więcej, alternatywa dłuższa też będzie tautologią, jeżeli tylko będzie miała postać

$$A_0 \vee \sim A_0 \vee A_1 \vee \ldots \vee A_n \tag{1}$$

(gdzie A_0 jest formułą atomiczną, a A_i dla $i \geqslant 1$ są formułami atomicznym i lub ich negacjami) lub też różniła się od tej alternatywy tylko kolejnością członów. Innymi słowy formuła

$$F = A_0 \vee A_1 \vee \ldots \vee A_n$$

(gdzie A_i są formułami atomicznymi lub ich negacjami) jest tautologią wtedy i tylko wtedy, gdy w niej występuje formuła atomiczna A i jej negacja, czyli dla pewnych $i, j \leqslant n$, A_i jest negacją A_j.

Załóżmy zatem, że formuła F jest koniunkcją pewnej ilości formuł postaci (1), czyli, że ma postać

$$(A_{00} \vee A_{01} \vee \ldots \vee A_{0m_0}) \wedge \ldots \wedge (A_{n0} \vee A_{n1} \vee \ldots \vee A_{nm_n}) \tag{2}$$

(gdzie jak zwykle A_{ij} oznacza formułę atomiczną lub jej negację. Na to, by formuła F była tautologią logiczną, potrzeba i wystarcza, by każdy z członów koniunkcji był tautologią. Zagadnienie sprawdzania czy formuła postaci (2) jest tautologią, sprowadza się więc natychmiast do skończonej liczby zagadnień typu: Czy formuły postaci (1) są tautologiami? Zagadnienie rozstrzygania czy formuła F jest tautologią zostało więc już rozwiązane dla formuł postaci (2) zwanych *formułami o postaci normalnej koniunkcyjno-alternatywnej*. Jak jednak postępować z formułą otwartą, która nie jest dana w postaci normalnej? Należy ją oczywiście do tej postaci sprowadzić. W tym celu należy formułę powtarzać krok po kroku. Wszystkie spójniki zdaniotwórcze w formule F są złożone cienką czcionką. Dla odróżnienia, te spójniki, które już zostaną do końca, aż do postaci normalnej, składane są czcionką grubą([4]).

Niech Z będzie na przykład formułą

$$\sim(A \vee B) \vee (A \wedge C) \tag{Z1}$$

(gdzie A, B i C są formułami atomicznymi).

([3]) Formuła $x < y$ jest prawdziwa tylko w tych systemach relacyjnych, w których $<$ jest relacją pełną, tzn. zachodzą pomiędzy wszystkimi elementami, a formuła $\sim x < y$ — gdy $<$ jest relacją pustą, czyli nie zachodzi dla żadnych elementów.

([4]) W wielu opracowaniach zamiast grubej alternatywy stosuje się zazwyczaj przecinek (,), a zamiast grubej koniunkcji średnik (;).

Formuła (Z1) jest alternatywą, funktor główny zapisujemy grubą czcionką:

(Z2) $$\sim (A \vee B) \vee (A \wedge C).$$

W pierwszym członie alternatywy wykorzystujemy prawo de Morgana:

(Z3) $$(\sim A \wedge \sim B) \vee (A \wedge C).$$

Korzystamy trzykrotnie z rozdzielności alternatywy względem koniunkcji:

(Z4) $$\big(\sim A \vee (A \wedge C)\big) \wedge \big(\sim B \vee (A \wedge C)\big),$$

(Z5) $$(\sim A \vee A) \wedge (\sim A \vee C) \wedge \big(\sim B \vee (A \wedge C)\big),$$

(Z6) $$(\sim A \vee A) \wedge (\sim A \vee C) \wedge (\sim B \vee A) \wedge (\sim B \vee C).$$

Ponieważ tylko jeden człon koniunkcji jest tautologią, a pozostałe trzy nie są tautologiami, więc formuła (Z6), a co zatem idzie i formuła Z nie są tautologiami.

W całym postępowaniu zostało wykorzystane kilka reguł. Aby zapisać te reguły w najogólniejszej postaci, trzeba przyjąć następujące oznaczenia: A_i oznacza formuły atomiczne lub ich negacje, F, G, X, Y oznaczają dowolne formuły otwarte (spójniki zdaniotwórcze w X, Y mogą być zarówno półgrube jak i cienkie, a ponadto formuły X i Y mogą być formułami pustymi, to znaczy mogą w ogóle nie występować). Poszczególne reguły są zapisane w postaci dwu wierszy przedzielonych kreską. To co jest nad kreską, to jest zastana formuła, na miejsce której należy wpisać formułę wypisaną pod kreską:

(G1) $$\frac{(A_0 \vee \ldots \vee A_n \vee (F \vee G) \vee X) \wedge Y}{(A_0 \vee \ldots \vee A_n \vee F \vee G \vee X) \wedge Y}$$

(G2) $$\frac{(A_0 \vee \ldots \vee A_n \vee (F \wedge G) \vee X) \wedge Y}{(A_0 \vee \ldots \vee A_n \vee F \vee X) \wedge (A_0 \vee \ldots \vee A_n \vee G \vee X) \wedge Y}$$

(G3) $$\frac{(A_0 \vee \ldots \vee A_n \vee \sim\sim F \vee X) \wedge Y}{(A_0 \vee \ldots \vee A_n \vee F \vee X) \wedge Y}$$

(G4) $$\frac{(A_0 \vee \ldots \vee A_n \vee \sim (F \vee G) \vee X) \wedge Y}{(A_0 \vee \ldots \vee A_n \vee (\sim F \wedge \sim G) \vee X) \wedge Y}$$

(G5) $$\frac{(A_0 \vee \ldots \vee A_n \vee \sim (F \wedge G) \vee X) \wedge Y}{(A_0 \vee \ldots \vee A_n \vee (\sim F \vee \sim G) \vee X) \wedge Y}$$

Łatwo zauważyć, że pierwsza reguła odgrywa rolę łączności alternatywy, druga — rozdzielności alternatywy względem koniunkcji, trzecia — prawa podwójnego przeczenia, a czwarta i piąta praw de Morgana. Jak widać, brak przemienności zarówno koniunkcji, jak i alternatywy.

W przytoczonym powyżej przykładzie stosowaliśmy reguły (1)-(5) nie tylko w pierwszym członie koniunkcji (do tego tylko formalnie rzecz biorąc uprawniają nas reguły), ale i w dalszych. Ten chwyt zastąpił oba prawa przemienności. Okazuje się jednak, że jeśli nie jesteśmy zainteresowani w postaci normalnej, a tylko w sprawdzeniu czy formuła Z jest tautologią, to można się w ogóle obejść bez praw przemienności. Już przy formule (Z5) można było zauważyć, że pierwszy człon koniunkcji jest tautologią, a zatem formuła (Z5) jest tautologią wtedy i tylko wtedy, gdy formuła

(Z6a) $$(\sim A \vee C) \wedge (\sim B \vee (A \wedge C))$$

jest tautologią. Takie przejście byłoby zastosowaniem reguły: jeżeli dla pewnych $i, j \leqslant n$ A_i jest negacją A_j, to

(G0) $$\frac{(A_0 \vee \ldots \vee A_n \vee X) \wedge Y}{Y}.$$

Regule tej należy nadać numer wcześniejszy od pozostałych, gdyż jak się później okaże, w takiej właśnie kolejności trzeba będzie stosować reguły. Nie ma to co prawda większego znaczenia (poza pewną oszczędnością czasu) w przypadku formuł otwartych. Może jednak nabrać zasadniczego znaczenia wówczas, gdy w formule pojawią się kwantyfikatory.

Do formuły (Z6a) nie można zastosować już żadnej reguły (G0)-(G5): pierwszy człon koniunkcji jest alternatywą formuł atomicznych lub ich negacji, a jednocześnie nie jest tautologią, wobec czego cała formuła nie jest tautologią.

Rozpatrzmy jeszcze jeden przykład:

(i) $$\sim(A \vee \sim B) \vee (\sim B \vee A),$$

(ii) $$\sim(A \vee \sim B) \vee (\sim B \vee A),$$

(iii) $$(\sim A \wedge \sim \sim B) \vee (\sim B \vee A),$$

(iv) $$(\sim A \vee (\sim B \vee A)) \wedge (\sim \sim B \vee (\sim B \vee A)),$$

(v) $$(\sim A \vee \sim B \vee A) \vee (\sim \sim B \vee (\sim B \vee A)),$$

(vi) $$B \vee (\sim B \vee A),$$

(vii) $$B \vee \sim B \vee A.$$

W krokach (v) i (vii) zastosowaliśmy regułę (G0) i w rezultacie otrzymaliśmy formułę bez żadnych znaków, tzw. formułę pustą.

Z powyższych rozważań wynika, że chcąc sprawdzić czy dana formuła otwarta jest tautologią, należy stosować do niej kolejno reguły (G0)-(G5) póki tylko można. Jeśli w końcu otrzyma się regułę pustą, to formuła wyjściowa jest tautologią, w przeciwnym przypadku nie.

Jeśli chcemy przystąpić do badania dowolnych formuł, a więc takich, w których mogą wystąpić kwantyfikatory, to należy dopuścić w regułach (G0)-(G5), aby i formuły F, G, X, Y były dowolne, a ponadto należy dołączyć cztery reguły odpowiadające kwantyfikatorom. Dwie pierwsze odpowiadają prawom de Morgana dla kwantyfikatorów:

$$\text{(G6)}\quad \frac{(A_0 \vee \ldots \vee A_n \vee \sim \bigwedge x\, F(x) \vee X) \wedge Y}{(A_0 \vee \ldots \vee A_n \vee \bigvee x \sim F(x) \vee X) \wedge Y}$$

$$\text{(G7)}\quad \frac{(A_0 \vee \ldots \vee A_n \vee \sim \bigvee x\, F(x) \vee X) \wedge Y}{(A_0 \vee \ldots \vee A_n \vee \bigwedge x \sim F(x) \vee X) \wedge Y}$$

Trzecia wykorzystuje fakt, że zmienne wolne traktuje się tak jak gdyby były związane kwantyfikatorem ogólnym:

$$\text{(G8)}\quad \frac{(A_0 \vee \ldots \vee A_n \vee \bigwedge x\, F(x) \vee X) \wedge Y}{(A_0 \vee \ldots \vee A_n \vee F(y) \vee X) \wedge Y}$$

W regule tej żąda się dodatkowo, aby zmienna y nie występowała w formule nad kreską.

Najbardziej skomplikowana jest reguła opuszczania kwantyfikatora egzystencjalnego. Aby ją sformułować należy najpierw zbiór wszystkich termów ustawić w ciąg nieskończony. Sama reguła ma następującą postać:

$$\text{(G9)}\quad \frac{(A_0 \vee \ldots \vee A_n \vee \bigvee x\, F(x) \vee X) \wedge Y}{(A_0 \vee \ldots \vee A_n \vee F(t) \vee X \vee \bigvee x\, F(x)) \wedge Y}$$

gdzie t jest najwcześniejszym termem takim, że X nie jest postaci $X' \vee F(t) \vee X''$ ani też $F(t)$ nie występuje wśród A_i.

Warto zwrócić uwagę, że reguła ta nie likwiduje wcale kwantyfikatora egzystencjalnego, tak jak robiły to pozostałe reguły z innymi spójnikami zdaniotwórczymi, a jedynie odsuwa go na koniec pierwszego członu. Jedyny sposób, aby się go pozbyć, to usunąć go wraz z całym pierwszym członem na mocy reguły (G0). Nie zawsze to okazuje się możliwe i bardzo często postępowanie nigdy się nie kończy. Można to jednak udowodnić, że jeśli wyjściowa formuła jest tautologią, a ponadto w każdym kroku będziemy najpierw usiłowali zastosować regułę (G0), a dopiero, gdy nam się nie uda, to jedną z pozostałych, to postępowanie skończy się i to formułą pustą. W dowodzie tego twierdzenia istotną rolę odgrywa fakt, że wszystkie termy zostały ustawione w ciąg nieskończony: W przypadku postę-

powania nieskończonego można mieć pewność, że każdy term został wykorzystany.

Powyższy opis odbiega w wielu szczegółach od oryginalnego rachunku Gentzena opublikowanego w roku 1935 (patrz [6]). Jest to w zasadzie opis modyfikacji rachunku Gentzena dokonanej przez Rasiową i Sikorskiego (patrz [15], str. 299 i następne). Różnice między tym systemem a opisanym powyżej są nieistotne. Jest znanych jeszcze kilka innych modyfikacji rachunku Gentzena. Najbardziej znany jest system zwany „semantycznymi tablicami Betha" (patrz [2]).

Rachunek Gentzena w tej czy innej formie był wielokrotnie podstawą doświadczeń. Układano na jego podstawie programy na różne maszyny cyfrowe i próbowano dowodzić twierdzenia. Najbardziej znane jest doświadczenie Hao Wanga (patrz [24]), który się oparł na oryginalnym systemie Gentzena. Program Hao Wanga był w stanie udowodnić wszystkie tautologie opublikowane przez Russella i Whiteheada w *Principia Mathematicae* (patrz [25]).

Obecnie główny nurt badań w dziedzinie automatycznego dowodzenia twierdzeń przesunął się na zastosowania twierdzenia Herbranda.

4. Twierdzenie Herbranda

Weźmy pod uwagę dowolne zdanie (bez zmiennych wolnych) postaci

$$\bigwedge x \bigvee y \, F(x, y), \tag{1}$$

gdzie $F(x, y)$ jest formułą kwantyfikatorową o dwu zmiennych wolnych x, y. Zdanie to odczytuje się na ogół następująco:

„dla dowolnego x można tak dobrać y, że spełniony jest warunek $F(x, y)$".

Różnym wartościom x odpowiadają na ogół różne wartości y. To co należy wybrać za y zależy od tego co wybrano za x. W każdym modelu zdania (1) można zatem określić funkcję φ taką, że jeśli zmienną x będziemy interpretować jako nazwę elementu x, a y jako nazwę elementu $\varphi(x)$, to formuła F będzie w tym modelu spełniona (prawdziwa). To znaczy, że zdanie (1) jest równoważne zdaniu:

$$\bigwedge x \, F\big(x, f(x)\big),$$

gdzie f jest nazwą funkcji φ. Zgodnie z konwencją, że zmienna wolna — to zmienna związana kwantyfikatorem ogólnym na początku zdania, można powiedzieć, że zdanie (1) jest równoważne formule otwartej

$$F\big(x, f(x)\big).$$

Jeśli jakikolwiek model zdania (1) zawiera jakiś element, powiedzmy x, to musi zawierać również element $\varphi(x)$. W takim razie jednak musi też zawierać element $\varphi(\varphi(x))$ itd., a w modelu muszą być prawdziwe wszystkie formuły:

$$(2) \qquad F(x, f(x)),\ F(f(x),\ f(f(x))),\ F(f(f(x)), f(f(f(x)))),\ \ldots$$

Co więcej, zdanie (1) ma model wtedy i tylko wtedy, gdy wszystkie zdania (2) mają model. To z kolei jest równoważne temu, że każdy skończony zbiór zdań (2) ma model. Zdanie (1) jest zatem sprzeczne wtedy i tylko wtedy, gdy istnieje skończony zbiór zdań (2) taki, że koniunkcja tych zdań jest sprzeczna.

Oryginalne twierdzenie Herbranda (patrz [9]) jest już tylko przeformułowaniem powyższej równoważności: mówi ono, że zdanie jest tautologią logiczną (a więc negacją zdania sprzecznego) wtedy i tylko wtedy, gdy jest tautologią alternatywa pewnej skończonej ilości formuł otwartych bezkwantyfikatorowych, otrzymanych z rozpatrywanego zdania metodą podobną do opisanej powyżej.

Sprawdzanie, czy formuła otwarta bezkwantyfikatorowa jest tautologią czy nie, sprowadza się do zastosowania jednej ze znanych metod roztrzygania dla rachunku zdań. Wobec tego dzięki twierdzeniu Herbranda mamy nową metodę sprawdzania czy dane zdanie jest tautologią: należy w tym celu wypisywać kolejno alternatywy odpowiednio skonstruowanych formuł bezkwantyfikatorowych (zwane alternatywami Herbranda) i badać czy któraś z nich nie jest tautologią. Istnieje bardzo wiele metod automatycznego dowodzenia twierdzeń opartych na twierdzeniu Herbranda. Najbardziej znana jest tzw. metoda rezolucji (patrz [16]), która w tej chwili ma już bogatą literaturę (patrz [17]). Nieco innym podejściem jest metoda odwrotna (patrz [12]). Metody polegają na rozpatrywaniu alternatyw Herbranda, ale tylko niektórych, specjalnie podejrzanych o to, że są tautologiami.

5. Możliwości praktycznych zastosowań

Teoretycznie wszystkie opisane czy wspomniane powyżej metody można zaprogramować na maszynę cyfrową, a następnie zamiast męczyć się nad znajdowaniem dowodów różnych twierdzeń można by ten trud pozostawić maszynom.

Powyższe rozumowanie, pozornie bez zarzutu, nie uwzględnia tego, że istniejące (przynajmniej obecnie) maszyny działają co prawda bardzo szybko, ale na wykonanie każdej operacji potrzebują pewnego czasu, a ponadto, i to jest jeszcze ważniejsze, mają tylko ograniczoną pojemność pamięci. Przy praktycznym zastosowaniu którejkolwiek z metod do sto-

sunkowo prostych zagadnień ilość operacji jest tak wielka, że czas pracy maszyny zaczyna liczyć się w godzinach. Powoduje to nieopłacalność stosowania maszyn matematycznych: człowiek, nawet bardzo wysoko wykwalifikowany, jest ciągle jeszcze tańszy. Co prawda sprawę kosztów można uznać za drugorzędną, praca maszyn tanieje, podczas gdy praca ludzi staje się coraz droższa, a ponadto warto by raz czy kilka razy udowodnić jakieś poważne twierdzenie za pomocą samych maszyn, nawet gdyby to miało kosztować bardzo wiele.

Tu jednak dochodzi do głosu drugie ograniczenie: pojemność pamięci. Jako przykład ostrości tego ograniczenia może służyć następujące doświadczenie:

W geometrii rzutowej istnieje tzw. *twierdzenie Pascala*:

Trzy punkty przecięcia par boków przeciwległych sześciokąta wpisanego w stożkową leżą na jednej prostej (por. [1]).

Dowód w pracy [1] zajmuje mniej więcej stronę druku. Jak wszystkie zdania geometryczne, twierdzenie Pascala ma swój odpowiednik analityczny. W tej postaci dowód twierdzenia Pascala sprowadza się do obliczenia pewnego wyznacznika. Okazało się jednak, że jeżeli nie będzie się stosować wymyślnych tricków upraszczających, to wyznacznik staje się tak skomplikowany, że do zapisania go nie wystarczyło ponad pół miliona słów pamięci maszyny IBM 360/50 (patrz [3]).

Powyższy przykład ilustruje dość ogólną prawidłowość dotyczącą wszystkich metod automatycznego dowodzenia twierdzeń; prowadzą one z reguły do dowodów bardzo skomplikowanych, pomimo że równocześnie często istnieją dowody znacznie prostsze. Istnieją co prawda sposoby upraszczania dowodów, niemniej każda z metod automatycznego dowodzenia twierdzeń wymaga olbrzymiej pamięci. W związku z tym praktyczne wykorzystanie tych metod w całej ich rozciągłości wymagałoby maszyn o pamięci wielokrotnie większej od stosowanych obecnie. Wydaje się natomiast rzeczą całkowicie realną sporządzenie programu, który sprawdzałby poprawność już istniejących dowodów. W przypadku dowodu zapisanego formalnie sprawa jest bardzo prosta. Kłopot tylko w tym, że w praktyce bardzo rzadko wypisuje się dowody formalne. Przyczyną tego jest niewątpliwie długość dowodów, na przykład formalny dowód twierdzenia Rolle'a (patrz [20]) zajmuje 7 stron druku. Dowody publikowane w pracach matematycznych ograniczają się na ogół do wskazania istotnych kroków dowodu, pozostawiając zapełnienie luk domyślności czytelnika. Podobnie można postępować z maszyną. Po opracowaniu odpowiedniego programu można by wprowadzać do maszyny istotne kroki dowodu, a maszyna uzupełniałaby luki i w ten sposób sprawdzała czy dowód został sporządzony poprawnie. Ponieważ w rachunku Gentzena najwięcej miejsca w pamięci zajmuje stosowanie reguły (G8) (dotyczącej kwantyfikatora egzystencjalnego), istotnym krokiem dowodu może być wskazanie,

który term należy podstawić za zmienną związaną kwantyfikatorem egzystencjalnym.

Zagadnienie podziału pracy między maszynę a człowieka jest jeszcze ciągle zagadnieniem otwartym. Po jego rozwiązaniu maszyna stanie się nowym, uniwersalnym narzędziem w ręku matematyka: narzędziem, które będzie szybko i sprawnie sprawdzać stawiane przezeń hipotezy.

Literatura

[1] K. Borsuk, *Geometria analityczna w n-wymiarach*, Warszawa 1966.

[2] E. W. Beth, *The foundations of mathematics*, Amsterdam 1959.

[3] E. Cerutti, P. J. Davis, *FORMAC meets Pappus: some observations on elementary analytic geometry by computer*, Amer. Math. Monthly 76 (1969), str. 895–905.

[4] A. Church, *A note on the Entscheidungsproblem*, J. Symbolic Logic 1 (1936), str. 40–41.

[5] R. Descartes, *Rozprawa o metodzie dobrego powodowania swoim rozumem i szukania prawdy w naukach*, Kraków 1918.

[6] G. Gentzen, *Untersuchungen über das logische Schliessen*, Math. Z. 39 (1934–5), str. 210, 405–431.

[7] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Math. u Phys. 38 (1931), str. 173–198.

[8] A. Grzegorczyk, *Zarys logiki matematycznej*, Warszawa 1969.

[9] J. Herbrand, *Recherches sur la théorie de la démonstration*, Trav. Soc. Sci. Lett. Varsovie Cl. III, 33 (1930), str. 1–128.

[10] C. H. Langford, *Some theorems on deducibility*, Ann. of Math., ser. 2, 28 (1926), str. 16–40.

[11] А. А. Марков, *Теория алгорифмов*, Труды Стеклова 42 (1954).

[12] С. Ю. Маслов, *Обратный метод установления выводимости в классическом исчислении предикатов*, ДАН СССР 159 (1964), str. 17-20.

[13] A. Mostowski, *Logika matematyczna*, Warszawa 1948.

[14] M. Pressburger, *Über die Vollstandigkeit eines gewissen Systems der Arithmetic ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Comptes — rendus du I Congres des Mathématiciens des Pays Slaves, Warszawa 1926, str. 92–101.

[15] H. Rasiowa, R. Sikorski, *The mathematics of metamathematics*, Warszawa 1963.

[16] J. A. Robinson, *A machine-oriented logic based on the resolution principle*, Journal of ACM 12 Jan., 1965, str. 23–41.

[17] — *A review of automatic theorem-proving*, Proc. of Symposia in Applied Mathematics, 19 AMS 1967.

[18] L. W. Szczerba, *Semantic method of proving theorems*, Bull. Acad. Polon. Sci. Ser. sci. math. astr. phys., vol. XVIII, 9 (1970), str. 507–512.

[19] W. Szmielew, A. Tarski, *Mutual interpretability of some essentially undecidable theories*, Proc. of the Int. Congress of Math. Cambridge 1950, I, str. 734.

[20] J. Sleszyński, *Teoria dowodu*, tom II, Kraków 1929.

[21] A. Tarski, *What is elementary geometry?* The axiomatic methods ... Amsterdam 1959, str. 16–29.

[22] A. Tarski, J. C. C. McKinsey, *A decision method for elementary algebra and geometry*, Berkeley and Los Angelos 1951.

[23] A. M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society, Ser. 2, 42 (1936), str. 230–265.

[24] H. Wang, *Towards mechanical mathematics*, IBM J. Res. Develop. 4 (1969), str. 2–22.

[25] A. N. Whitehead, B. Russell, *Principia Mathematicae*, Cambridge 1910.