GREGORY J. CHAITIN

GRANICE MATEMATYKI

KURS NA TEMAT TEORII INFORMACJI

I GRANIC FORMALNEGO DOWODZENIA

W przekładzie z języka angielskiego

PIOTRA CZARNOTY

i

Przedmową do wydania polskiego

JÓZEFA DĘBOWSKIEGO

1. W dotychczasowych dziejach nauki, zanim problem granic matematyki w ogóle został postawiony, zazwyczaj mieliśmy do czynienia z poglądami, według których poznanie typu matematycznego z reguły uchodziło za wzór naukowej doskonałości (racjonalności i wiarygodności), wzór wszelkich naukowych cnót (rzetelności i ścisłości) oraz podstawę poznania każdego innego typu (archimedesowy punkt oparcia). Protopolastów tego typu myślenia bez trudu znajdziemy już w antycznej Grecji. Dość wskazać tu Pitagorasa, Platona, Euklidesa czy Diofantosa. Jednak ów wymodelowany na wiedzy matematycznej ideał poznania naukowego chyba najczęściej zwykło się łączyć z wiekiem siedemnastym i postulowaną przez Kartezjusza (1598-1650) koncepcją nauki jako *mathesis universalis* — koncepcją nauki (filozofii) ufundowanej na matematyce i obejmującej w jednym systemie całość ludzkiej wiedzy o świecie: zarówno o poszczególnych segmentach tego świata, jak całej jego strukturze (hierarchii). Szczęśliwym trafem, w kartezjańskim projekcie nauki jako *mathesis universalis* najmocniej zaakcentowana była jego część czysto metodologiczna. Był to ze strony Kartezjusza bardzo szczęśliwy zabieg, albowiem na tę część programu łatwo godzili się nawet filozoficzni oponenci kartezjanizmu, np. Pierre Gassendi (1592-1655) czy Thomas Hobbes (1588-1679). I to właśnie ona najsilniej oddziałała na wyobraźnię siedemnastowiecznych myślicieli, matematyków i badaczy przyrody. Oddziaływanie to było do tego stopnia silne, że niemal bez reszty podlegały mu umysły tak wielkich postaci jak Benedykt Spinoza (1632-1677), który nawet naukę o moralności usiłował budować *more geometrico*, Gottfried Wilhelm Leibniz (1646-1716) czy Issac Newton (1642-1727).[1]

Oglądając się wstecz, poza Kartezjuszem, warto tu pamiętać zwłaszcza o Leibnizu. Warto o nim pamiętać przynajmniej z dwóch powodów. Po pierwsze, Leibniz, podobnie jak Kartezjusz, był matematykiem wyjątkowo twórczym, a wobec tego własne sukcesy w zakresie matematyki łatwo ośmielały go (poniekąd całkiem uprawnienie) do stosowania metody matematycznej także w innych dziedzinach wiedzy. Nadzieje Leibniza były do tego stopnia rozbudzone, że uważał, iż bezwyjątkowo każdy poważny problem naukowy można rozwiązać przy użyciu rachunku matematycznego i metody czysto kombinatorycznej. Miast tedy spierać się w nieskończoność, wystarczy — jak mniemał — porachować. A więc, jak powiadał, *calculemus!*.

Po drugie, jak wiadomo, Leibniz był nie tylko wytrawnym matematykiem, ale i wybitnym logikiem, może nawet — jak czasami się uważa — logikiem najwybitniejszym pomiędzy Arystotelesem a Fregem.[2] Znakomicie więc pojmował, że metody matematyczne mogą być owocnie stosowalne do rozwiązywania rozmaitych problemów tylko wtedy, gdy wszystkie te problemy będzie można jakoś zunifikować, najlepiej na bazie jednego języka — języka szczególnego, bo uniwersalnego. Łatwo zauważyć, iż w ten sposób, tj. postulując stworzenie takiego uniwersalnego języka (*lingua universalis*), Leibniz stał się w filozofii matematyki prekursorem logicyzmu i formalizmu.

2. Na swój prawdziwy i konkretny sprawdzian pomysły Leibniza musiały jednak jeszcze jakiś czas poczekać. Wszak w szerokich kręgach samych matematyków to dopiero od czasów Davida Hilberta (1862-1943) oczekuje się, by każda poważna teoria matematyczna była nie tylko aksjomatyzowalna, lecz także formalizowalna. Można powiedzieć i tak, że na dobrą sprawę pełna formalizacja całej matematycznej wiedzy samym matematykom zaczęła się marzyć dopiero po spektakularnych sukcesach z przełomu XIX i XX wieku, w szczególności, po zaksjomatyzowaniu arytmetyki liczb naturalnych (G. Peano, 1889), euklidesowej geometrii (D. Hilbert) i teorii mnogości (E. Zermelo, 1908). Jednak to dopiero

[1]Spinoza nawet naukę o moralności usiłował budować *more geometrico.* Newton z kolei swoje główne dzieło zatytułował: *Zasady matematyczne filozofii przyrody* (*Philosophiae naturalis principia mathematica,* 1687).

[2]Por. J. Woleński, *Epistemologia, Tom I. Zarys historyczny i problemy metateoretyczne,* Wydawnictwo „Aureus", Kraków 2000, s. 86.

w 1900 roku David Hilbert — idąc krok dalej niż np. Gotlob Frege (1848-1925) — zaproponował konkretny program metodologiczny, który zamysł pełnej formalizacji wiedzy matematycznej miał skutecznie realizować. W latach 1910-1913 dodatkowej inspiracji dostarczyło ukazanie się trzech tomów monumentalnego dzieła B. Russella (1871-1970) i A. N. Whiteheada (1861-1947) pt. *Principia Mathematica.* W dziele tym po raz pierwszy została przedstawiona konkretna droga wyprowadzenia całej matematyki z czystej logiki. W ten sposób Russell i Whitehead nareszcie pokazali, że istotnie — tak jak przypuszczał Leibniz, a postulował Frege — abstrakcje matematyczne są dokładnie tej samej natury, co abstrakcje logiczne, tyle że niższego piętra.

Oczywiście, D. Hilbert nie miał złudzeń co do tego, że — wobec dotychczasowych sukcesów — całe przedsięwzięcie jest już proste i łatwe do wykonania. Lista najważniejszych problemów, które uprzednio należało rozwiązać — lista tzw. „23 problemów Hilberta" — była wszak wymownie długa. Między innymi należało wykazać, że teorie matematyczne, z którymi mamy do czynienia, choćby te elementarne, istotnie są niesprzeczne i zupełne (drugi problem na liście Hilberta, chyba najbardziej kluczowy w całym programie!). Niestety, opracowana w tym celu teoria dowodu całkowicie zawiodła. Jak się okazało, na podstawie Hilbertowskiej teorii dowodu, a więc w sposób konstruktywny i efektywny (*scil.* finitystyczny), wprawdzie można było udowodnić niesprzeczność euklidesowej geometrii lub niesprzeczność niektórych prostych rachunków logicznych, ale już nie sposób było tego dokonać w wypadku elementarnej (aksjomatycznej) teorii liczb.

3. Wymienione trudności, a także szereg innych, o których Hilbert skłonny był początkowo mniemać, iż ich przezwyciężenie jest tylko kwestią czasu, wkrótce jednak znalazły swoje wyjaśnienie, tyle że czysto negatywne. Dostarczył go Kurt Gödel (1906-1978). W 1930 roku na II Konferencji z Epistemologii Nauk Ścisłych w Królewcu Gödel ogłosił wyniki swoich dotychczasowych badań nad systemami formalnymi. Rok później zostały one opublikowane w *„Monatshefte für Mathematik und Physik"* (1931, Bd. 38, s. 173-198) pt. *Űber formal unentscheidbare Sätze der „Principia Mathematica" und verwandter Systeme.* Poza szeregiem niezwykle pomysłowych szczegółów technicznych (dotyczących m.in. arytmetyzacji składni i tak zwanej „numeracji gödlowskiej"), artykuł Gödla zawierał przede wszystkim dowód twierdzenia o niezupełności arytmetyki. Ściśle biorąc, w rachubę wchodziły dwa twierdzenia o niezupełności. Gdy chodzi o pierwsze z tych twierdzeń, to głosi ono, że każdy system formalny, który zawiera arytmetykę liczb naturalnych, zarazem zawiera też zdania, które nie są ani jego aksjomatami, ani jego tezami. Aksjomatami i tezami owych bogatszych systemów sformalizowanych nie są także negacje tych zdań. Zdania te nazywamy dzisiaj bądź zdaniami nierozstrzygalnymi, bądź zdaniami gödlowskimi. Przy tym, co należy podkreślić, są to zdania całkowicie sensowne (czyli dopuszczone regułami składni), a nadto jeszcze jedno z nich zawsze jest prawdziwe w modelu standardowym tego systemu. Innymi słowy, znaczy to, że — wbrew oczekiwaniom Hilberta — w każdym systemie sformalizowanym zawierającym arytmetykę liczb naturalnych zawsze istnieć będą takie zdania, których przy użyciu środków formalnych tego systemu ani nie będzie można dowieść, ani obalić. Krótko:

(1) Jeśli $AR \subseteq T$ i $T \in NSP$, to istnieje zdanie $A \in J_T$ takie, że $A \notin Cn(T)$ i $\sim A \notin Cn(T)$

I nic tu nie pomoże dopisanie owego nierozstrzygalnego zdania (lub jego negacji) do listy aksjomatów. W takim bowiem wypadku natychmiast pojawiają kolejne zdania nierozstrzygalne.

Istotne ograniczenia każdego formalizmu bodaj jeszcze dobitniej ilustruje *II twierdzenie o niezupełności.* Jego treść jest następująca. Niesprzeczność systemu

sformalizowanego zawierającego arytmetykę liczb naturalnych nie może być okazana za pomocą środków tego systemu. A więc:

(2) Jeśli AR$\subseteq$T i T$\in$NSP, to *Con*(T)$\notin$*Cn*(T), gdzie *Con*(T) znaczy: „T jest niesprzeczna"

Innymi słowy, by przedstawić dowód niesprzeczności takiego systemu, trzeba użyć bogatszych środków formalnych niż te, które mamy do dyspozycji w ramach tego systemu. Szkopuł polega jednak na tym, że nie mamy żadnych gwarancji, iż owe bogatsze systemy formalne, z których środków korzystamy, są niesprzeczne. Aby bowiem udowodnić ich niesprzeczność, trzeba odwołać się do systemów jeszcze bogatszych. I tak dalej — *in infinitum.* Słowem, jak wykazał Gödel, nie istnieje procedura (czytaj: konstruktywny dowód dedukcyjny), dzięki której w skończonej liczbie kroków, a więc w sposób efektywny, można by się przekonać, że systemy sformalizowane zawierające arytmetykę liczb naturalnych są niesprzeczne.[3]

4. Dla naszej wiedzy o granicach formalizmu i naturze wiedzy matematycznej, prócz wymienionych dwu twierdzeń Gödla o niezupełności, istotne znaczenie ma jeszcze kilka dalszych odkryć z lat trzydziestych XX wieku. Poza twierdzeniem Tarskiego o niedefiniowalności prawdy, warto w tym kontekście wymienić przede wszystkim znane twierdzenia Alonzo Churcha o nierozstrzygalności klasycznego rachunku predykatów i, zwłaszcza, nierozstrzygalności arytmetyki. Rozstrzygalność jest bardzo ważną metalogiczną właściwością systemów sformalizowanych — bodaj nie mniej ważną, niż ich niesprzeczność czy zupełność. Krótko można powiedzieć tak: teoria jest rozstrzygalna wtedy i tylko wtedy, gdy istnieje metoda, która o każdym sensownym wyrażeniu tej teorii w sposób efektywny (tj. w skończonej liczbie kroków) pozwala ustalić, czy jest ono twierdzeniem tej teorii. Np. klasyczny rachunek zdań jest rozstrzygalną teorią logiczną, ponieważ dzięki metodzie zerojedynkowej (albo poprzez sprowadzenie do tzw. postaci normalnej) o każdym jej wyrażeniu sensownym jesteśmy w stanie rozstrzygnąć, czy jest ono twierdzeniem tej teorii, czy też nie jest.

Niestety, nie wszystkie teorie logiczne posiadają tę właściwość. W 1936 roku A. Church udowodnił, że klasyczny rachunek predykatów jest nierozstrzygalny. Przedstawiony przez Churcha dowód polegał na wykazaniu, że zbiór twierdzeń klasycznego rachunku predykatów, choć rekurencyjnie przeliczalny, nie jest rekurencyjny. Znaczy to, że nie można skonstruować żadnej takiej procedury decyzyjnej (*scil.* żadnego algorytmu), która umożliwiałaby przetestowanie każdego wyrażenia na okoliczność „bycia twierdzeniem klasycznego rachunku predykatów". W tym samym 1936 roku Church wykazał też, że również arytmetyka liczb naturalnych, o ile jest niesprzeczna, jest nierozstrzygalna.[4]

---

[3] Główny nerw rozumowania i poszczególne kroki procedury dowodowej Gödla jasno i precyzyjnie omawiają m.in. E. Nagel i J. R. Newman. Por. E. Nagel, J. R. Newman, *Twierdzenie Gödla,* tłum. B. Stanosz, PWN, Warszawa 1966, zwł. s. 61-68. Natomiast gdy chodzi o sformalizowany zapis tej procedury, to por. w tej sprawie R. Murawski, *Funkcje rekurencyjne i elementy metamatematyki. Problemy zupełności, rozstrzygalności, twierdzenia Gödla,* Uniwersytet A. Mickiewicza w Poznaniu, Poznań 1990, s. 91-110. Por. też W. Marciszewski (red.), *Logika formalna. Zarys encyklopedyczny z zastosowaniem do informatyki i lingwistyki,* PWN, Warszawa 1987, s. 138-139.

[4] Na marginesie warto może zauważyć, iż 1936 rok był wyjątkowo płodny w ważne odkrycia metamatematyczne (podobnie zresztą jak cała czwarta dekada XX w.). W 1936 r., prócz twierdzeń Churcha i Turinga o nierozstrzygalności AR, zostało również sformułowane głośne twierdzenie Tarskiego o niedefiniowalności prawdy. Krótko można je wyrazić w sposób następujący: Jeśli AR$\subseteq$T i T$\in$NSP, to zbiór zdań prawdziwych w modelu $\mathfrak{M}_T$ jest niedefiniowalny w T. Przedstawiony przez Tarskiego dowód tego twierdzenia polegał na wykazaniu, że podczas definiowania prawdy dla AR w AR pojawiają się antynomie semantyczne typu antynomii kłamcy. Por. A. Tarski, *Der Wahrheitsbegriff in den formalisierten Sprachen,* „Studia Philosophica" 1936, vol. I, ss. 261-405. Przedruk w: A. Tarski, *Collected Papers,* vol. 1, Birkhäuser, Basel 1986, ss. 51-198.

(3) Jeśli AR∈NSP, to AR∈NROZ

Wprawdzie niektóre jej fragmenty, np. arytmetyka tylko z dodawaniem lub tylko z mnożeniem (tzw. arytmetyka Presburgera), są teoriami rozstrzygalnymi, lecz cała arytmetyka, ponieważ zbiór wszystkich jej twierdzeń jest nieobliczalny, jest nierozstrzygalna. Oczywiście, nierozstrzygalne (i niezupełne) jest również każde rozszerzenie arytmetyki. A to znaczy, że wymienionymi defektami odznaczają się te wszystkie teorie matematyczne, które zawierają arytmetykę, a wobec tego praktycznie jest nimi obciążona cała matematyka (ponieważ zawiera AR).

5. Jak wskazuje tytuł niniejszej książki, a przede wszystkim jej zawartość, Gregory J. Chaitin doskonale zdaje sobie sprawę z istnienia wymienionych wyżej ograniczeń — ograniczeń, które dotykają całej usystematyzowanej wiedzy matematycznej. W obrębie dzisiejszej metamatematyki mówią o nich tzw. **twierdzenia limitacyjne.**[5] Krok po kroku, z właściwą sobie swadą, prof. G. J. Chaitin analizuje wymienione ograniczenia. Szczególnie wiele uwagi poświęca kwestii (nie)rozstrzygalności. To skądinąd zrozumiałe. Wprawdzie (nie)rozstrzygalność wydaje się być tylko konsekwencją (nie)zupełności, lecz „praktycznie" to właśnie ona stanowi punkt krytyczny każdego formalizmu. Jako jeden z pierwszych fakt ten wyraźnie dostrzegł także Alan Turing. Jeszcze jakiś czas po roku 1931 jakiś matematyczny hiperoptymista mógł mieć nadzieję, że — zgodnie z oczekiwaniami Hilberta — prędzej czy później zostanie opracowana procedura, która o każdym sensownym wyrażeniu systemu formalnego (nawet gdy jest on niezupełny) umożliwi rozstrzygnięcie, czy wyrażenie to jest prawdziwe w tym systemie, czy też nie jest. Nadzieja owego hiperoptymisty musiała jednak prysnąć po roku 1936. To bowiem w tym roku, posługując się metoda przekątniową Cantora, Turing wykazał, że nie istnieje żadna taka procedura (żaden algorytm, żaden komputerowy program), która umożliwiałaby realizację oczekiwań Hilberta. Nie ma takiej procedury, tak jak nie ma algorytmu, który umożliwiałby ustalenie, czy n-ty program komputerowy kiedykolwiek wygeneruje n-tą cyfrę (i zakończy pracę), czy też nigdy jej nie wygeneruje i wobec tego nigdy się nie zatrzyma (nigdy nie zakończy pracy). Jak wiadomo i jak to dziś mówimy, jest to tzw. „problem stopu" — problem niemożliwy do rozstrzygnięcia z powodu istnienia nieobliczalnej liczby rzeczywistej, którą odkrył Turing posługując się metodą przekątniową Cantora.

Ktoś może pomyśleć, że tzw. „problem stopu" ma jedynie znaczenie lokalne. Wszelako tak można było mniemać tylko do pewnego czasu. Jeśli nawet zignorować twierdzenie Churcha o nierozstrzygalności AR, to należy liczyć się z faktem, iż — jak to w 1970 roku wykazał Jurij Matjasewicz (z Instytutu Matematycznego im. W. A. Stiekłowa w Leningradzie) — Turinga „problem stopu" i dziesiąty problem Hilberta są sobie równoważne. Przypomnijmy, że w swoim dziesiątym problemie Hilbert pytał o algorytm umożliwiający rozstrzygnięcie, czy dowolne (losowo wybrane) równanie diofantyczne posiada rozwiązanie, czy też go nie posiada. W 1970 roku J. Matjasewicz wykazał, że algorytm taki nie istnieje. Znaczy to, że tak jak nie istnieje algorytm umożliwiający rozstrzygnięcie, czy losowo wybrany program komputerowy zakończy pracę, tak nie istnieje również algorytm, który odpowie nam na pytanie, czy losowo wybrane równanie diofantyczne ma rozwiązanie.

Pewnym szczególnym wariantem „dziesiątego problemu Hilberta" zajął się również G. J. Chaitin. Mianowicie, używając jako narzędzia pracy oprogramowania komputerowego

[5] Jak się zdaje, nazwa „twierdzenia limitacyjne" po raz pierwszy została użyta w 1958 roku przez A. Fraenkela i Y. Bar-Hillela w odniesieniu do twierdzeń Gödla o niezupełności, twierdzeń Churcha o nierostrzygalności i twierdzenia Tarskiego o niedefiniowalności prawdy. Por. A. Fraenkel , Y. Bar-Hillel, A. Levy, *Foundations of Set Theory*, II ed., North-Holland, Amsterdam 1973, s. 310. Więcej w sprawie twierdzeń limitacyjnych i innych ważnych ustaleń współczesnej metamatematyki (także ich filozoficznych implikacji) por. w: J. Woleński, *Metamatematyka a epistemologia,* Wydawnictwo Naukowe PWN, Warszawa 1993, s. 51-96, zwł. zaś s. 73-85.

(LISP), które specjalnie zostało przystosowane do celów matematycznych i które chodzi na IBM-ie RS/6000, skonstruował — jak pisze — „przewrotne (niezwykle skomplikowane) 200-stronicowe równanie algebraiczne z parametrem N i 17 tysiącami zmiennych”.[6] Następnie postawił pytanie: „Czy dla każdej całkowitej wartości liczbowej parametru N istnieje skończona czy też nieskończona ilość całkowitych liczbowych rozwiązań?”[7]

Odpowiedź wypadła zdumiewająco. Jeśli bowiem do równania podstawiać kolejne wartości liczbowe parametru N oraz w przypadku skończonej liczby rozwiązań przyjmować 0, zaś w przypadku nieskończonej 1, to jego rozwiązaniem będzie ciąg zer i jedynek, którego w żaden sposób nie można odróżnić od ciągu zestawiającego wyniki nieskończenie wielu rzutów monetą. Nieobliczalną liczbę rzeczywistą z przedziału między 0 i 1, odpowiadającą ciągowi otrzymanych zer i jedynek, G. J. Chaitin nazwał następnie Ω (*Omega*).[8]

$$\Omega = 00101111011001001100 01...$$

Jak się okazuje, jej kolejne cyfry odpowiadają nieskończonej liczbie zupełnie przypadkowych faktów arytmetycznych. Wiemy wprawdzie, że każdy bit *Omegi* **musi być** albo zerem albo jedynką, ale nie wiemy i **nigdy** wiedzieć nie będziemy (!), kiedy i dlaczego wystąpi w niej zero, a kiedy i dlaczego — jedynka. Sytuacja jest więc w maksymalnym stopniu matematycznie nieprzewidywalna. Innymi słowy, *Omega* (Ω), ponieważ stanowi skrajnie nieuporządkowaną sekwencję zer i jedynek, jest nieredukowalna do żadnego algorytmu — jest, jak się powiada, **algorytmicznie nieupraszczalna** (niekompresowalna).[9] Znaczy to, że, mówiąc odrobinę inaczej, ewentualny algorytm (program komputerowy), za którego pośrednictwem moglibyśmy tę sekwencję wiernie odtworzyć, musiałby być równie długi, jak ona sama. Wnioski, które wyprowadza Chaitin w rezultacie odkrycia *Omegi*, są następujące. Cytuję:

> „Normalny pogląd na matematykę jest taki, że jeśli coś jest prawdziwe, to jest prawdziwe z jakiegoś powodu, prawda? W matematyce powodem, dla którego coś uważa się za prawdziwe nazywamy dowodem. I pracą matematyka jest znajdowanie dowodów.
> A zatem, normalnie uważacie, że jeśli coś jest prawdziwe, to jest prawdziwe z jakiegoś powodu. Cóż, Omega pokazuje wam, co odkryłem, że pewne matematyczne fakty są prawdziwe bez żadnego powodu! One są prawdziwe przez przypadek! I w konsekwencji na zawsze wymykają się potędze matematycznego dowodzenia. Każdy bit Omegi musi być 0 lub 1, ale jest to tak delikatnie wyważone, że nigdy nie będziemy wiedzieć jaki to bit.
>
> Wierzyłem kiedyś, że cała matematyczna prawda, całe nieskończone bogactwo matematycznej prawdy może być skompresowane w mały zbiór aksjomatów i metod dowodzenia, co do których my wszyscy możemy się zgodzić i których uczyliśmy się jako studenci matematyki. [...] Niestety, istnienie nieredukowalnych faktów matematycznych dowodzi, że w pewnych przypadkach nie istnieje absolutnie żadna kompresja, żadna struktura czy wzorzec w matematycznej prawdzie. [...] Gdyby Bóg był skłonny odpowiedzieć tak/nie na pytanie, to każdy bit Omegi wymagałby oddzielnego pytania, ponieważ nie istnieje żadna korelacja, nie ma żadnej redundancji! [...] W tym kierunku nieredukowalność matematycznej informacji (*irreducible mathematical information*) nie może już pójść dalej, nieprawdaż?”[10]

6. Cóż można jeszcze w tej sprawie powiedzieć? Istnienie nieobliczalnej liczby Ω — liczby, której odkrycie, jak utrzymuje Chaitin, nie byłoby możliwe bez użycia profesjonalnego komputera i specjalnego języka programowania (zmodyfikowany wariant

---

[6] G. J. Chaitin, *Randomness & Complexity…*, s. 3. Zobacz też G. J. Chaitin, *Randomness in Arithmetic,* s. 83.
[7] Zauważmy, iż Chaitin wcale tu nie pyta, czy skonstruowane przez niego równanie jest w ogóle rozwiązalne. Poniekąd byłoby to bowiem tylko powtórzenie pytania, z którym już wcześniej zmierzył się Turing.
[8] G. J. Chaitin, *Randomness in Arithmetic,* s. 81.
[9] Tamże, *s.* 83-85. Zobacz też G. J. Chaitin, *The Limits of Mathematics*, Singapore 1998, Springer, s. 54.
[10] G. J. Chaitin, *The Limits…,* s. 54-55 (*Conclusion*).

LISP-a) — wskazuje nie tylko na doniosłość matematyki nierekurencyjnej, ale nadto i przede wszystkim zwraca uwagę na wszechobecną **przypadkowość:** przypadkowość (losowość), według Chaitina, przez środowisko samych matematyków ostentacyjnie lekceważoną czy nawet ignorowaną. Tymczasem, jak twierdzi Chaitin, przypadkowość (losowość) nie omija również matematyki. Zawiera się także w czystej matematyce, a nawet w elementarnej arytmetyce liczb naturalnych (dziedzina równań diofantycznych). W związku z tym Chaitin konkluduje:

> „Bóg gra w kości nie tylko w mechanice kwantowej i fizyce klasycznej, ale nawet w czystej matematyce, nawet w elementarnej teorii liczb".[11]

7. Czyżby więc w rezultacie odkrycia *Omegi* zaistniały przesłanki do sformułowania kolejnego twierdzenia limitacyjnego? W każdym razie, gdyby bez reszty oddać się lekturze *Granic matematyki...* i potulnie pozwolić się autorowi prowadzić, to bez wątpienia można by odnieść takie wrażenie. Rzecz jednak w tym, że nie wszystko, co w tak urokliwy sposób Chaitin nam przedstawia, można przyjąć z zaufaniem równie wielkim, jak wielki jest entuzjazm samego autora. Zacytowane przed chwilą zdania niewątpliwie brzmią efektownie. Nie wydaje się jednak, by były równie odkrywcze. Mało odkrywczy wydaje się także wcześniej cytowany wniosek. Wbrew Chaitinowi nie można bowiem uważać, by matematycy byli dzisiaj skłonni utożsamiać (*scil.* traktować ekwiwalentnie) pojęcie „obiektywnej prawdy matematycznej" i pojęcie „dowodliwości". Tego typu pomieszanie było możliwe przed Gödlem, lecz nie dzisiaj. Odkrycie przez Gödla zdań nierozstrzygalnych raz na zawsze położyło kres tego typu uroszczeniom. Kropkę nad „i" postawił Tarski, gdy dowiódł, że pełny opis języka każdej bogatszej teorii matematycznej („bogatszej" znaczy: „zawierajacej AR") nie może być przedstawiony w języku tej teorii, lecz musi korzystać z formalizmu teorii jeszcze bogatszej. Dlaczego? Przede wszystkim dlatego, że pojęcie prawdziwości zdań AR nie może być zdefiniowane w AR.

Myśl tę można wyrazić w sposób jeszcze bardziej ogólny. Prawdziwość nie może być zredukowana do dowodliwości dokładnie z tych samych powodów, z których semantyka nie daje się zredukować do samej tylko składni. Powody tego stanu rzeczy wyłuszczają Gödla *I twierdzenie o niezupełności* i Tarskiego *twierdzenie o niedefiniowalności prawdy.* Zatem:

(4) Jeśli T$\subseteq$AR, to T-semantyka nie jest formalizowalna w T-składni.

Oczywiście, nie trzeba tu dodawać, że pojęcie prawdy — podobnie jak pojęcie spełniania, a w odróżnieniu od pojęcia dowodu lub konsekwencji logicznej — jest właśnie pojęciem semantycznym. Zatem odkrycie *Omegi* jako pewnego „faktu matematycznego" byłoby czymś absolutnie niezwykłym, gdyby w matematyce rzeczywiście sprawy się miały tak, jak je opisuje Chaitin, w szczególności: gdyby pomiędzy pojęciem „obiektywnej prawdy matematycznej" i pojęciem „dowodliwości" można było postawić znak równości, a więc — ostatecznie — semantykę zredukować do składni. Jednak w świetle metamatematycznych ustaleń, w które obfitowała zwłaszcza czwarta dekada XX wieku, tego rodzaju myślenie wydaje się dzisiaj całkowicie archaiczne — równie archaiczne jak stary pogląd Hilberta, że wszystko można sformalizować.

8. W trakcie lektury *Granic matematyki...* u średnio uważnego czytelnika może zrodzić się także wiele innych wątpliwości. Przykładowo, wątpliwości może budzić fascynacja LISP-em jako optymalnym (ba, w wersji Chaitina, najlepszym!) językiem programowania — językiem szczególnie użytecznym, m.in. ze względu na jego elastyczność, zwłaszcza w badaniach matematycznych. Jednak LISP, o czym dobrze wiedzą informatycy,

[11] G. J. Chaitin, *Randomness & Complexity…,* s. 12.

jest stosunkowo „starym" i poniekąd już „zużytym" językiem programowania (choć, czego dobrym przykładem jest Greg Chaitin, wciąż jeszcze ma swoich „wielbicieli"). Jeśli tedy istotnie w rozwiązaniu wielu konkretnych i niebanalnych problemów matematycznych może być użyteczny komputer, to w tym celu można dzisiaj używać języków bardziej wyrafinowanych niż LISP, np. sięgnąć po Prolog czy inne języki, które umożliwiają rozwiązywanie równań nieliniowych. Również z punktu widzenia problematyki zajmującej Chaitina, bardziej interesujące (i użyteczne) wydają się być języki programowania i programy, na których chodzą komputery 5 generacji. A to dlatego, iż stosuje się je przede wszystkim do rozwiązywania problemów złożoności (a nie jedynie obliczalności). Jak się zdaje, złożoność wiąże się z losowością w sposób bardziej podstawowy, niż obliczalność. Wybór przez Chaitina właśnie LISP-a można tedy usprawiedliwić w ten jedynie sposób, że zarówno LISP, jak i rachunek lambda Churcha są stosunkowo „najbliżej" uniwersalnych maszyn Turinga. A skoro rachunku lambda nie da się uruchomić w komputerze, to — jeśli chce się być wiernym głównym ideom komputacjonizmu — pozostaje wybrać LISP-a.

9. W tym miejscu u czytelnika dobrze obeznanego nie tylko z dwudziestowieczną filozofią matematyki, lecz także z najnowszą metodologią informatyki, mogą pojawić się kolejne znaki zapytania. Na przykład: czy w ogóle algorytm (*resp.* myślenie algorytmizowalne) dobrze przylega do formalizmu matematycznego? W szczególności, czy istotnie LISP jest tożsamy z odpowiednim językiem samej matematyki: rachunkiem funkcji czy rachunkiem lambda? Albo: czy jest w ogóle uprawnione, i ew. w jakiej mierze, utożsamienie dowodliwości z obliczalnością, czyli — upraszczając — dowodu (nawet gdy jest to dowód ściśle matematyczny) z samym tylko rachunkiem (nawet gdy jest to rachunek wyjątkowo wyrafinowany)?

Jak wiadomo, pojęcie rekurencyjności trudno jest przecenić: zarówno w badaniach ściśle matematycznych, jak i w rozważaniach metamatematycznych. Wszak pojęcie to pozwala nam uniezależnić się od konkretnych formalizmów, czyli relatywizacji do określonego języka. W rozwiązywaniu problemu definiowalności czy dowodliwości rekurencyjność oznacza tedy istotny postęp, ba, gwarantuje osiągnięcie „matematycznego raju". Jednak z drugiej strony, jak to zauważył m.in. K. Gödel, rekurencyjność może być uznana jedynie za „pewien szczególny rodzaj dowodliwości czy rozstrzygalności"[12] — „pewien szczególny", a więc jeden z wielu, być może wcale nie najważniejszy. W szczególności, gdyby ją utożsamić z konstruktywnością, to łatwo pozwala ona wyprecyzować m.in. pojęcie dowodu w sensie ścisłym. Mianowicie, za w pełni konstruktywne (efektywne) pozwala uznać tylko te pojęcia, definicje, twierdzenia, teorie i dowody matematyczne, które mają charakter rekurencyjny, a więc — praktycznie — nie wykraczają poza arytmetyzację składni i elementarną indukcję matematyczną. Tymczasem w matematyce, także i metamatematyce, bardziej interesujące — tak z pragmatycznego, jak i teoretycznego punktu widzenia — zawsze były przypadki niekonstruktywności. Przy tym, niekonstruktywność i nierekurencyjność — podobnie zresztą jak i nieformalizowalność — wcale nie musi być kojarzona z zagrożeniem sprzecznością lub brakiem należytej precyzji.

Niestety, Chaitin ani nie dyskutuje wymienionych kwestii, ani w ogóle ich nie stawia. Z góry zakłada, iż to, co jest do policzenia i to, co jest zapisane w postaci algorytmu (w LISP-ie), jest tożsame, równoważne, a przynajmniej w sposób istotny zbieżne. Tymczasem założenie to wcale nie jest oczywiste. Rangę wymienionych przed chwilą pytań, a także problematyczność przyjętego przez Chaitina założenia, dobrze widać m.in. z perspektywy przyjętej przez Rogera Penrose'a w książce *Nowy umysł cesarza...* Penrose dobitnie pokazuje tam, iż poznania matematycznego, choćby najskromniej je pojmować, nie sposób jest zredukować do wykonywania algorytmów. Nie sposób przystać na tego rodzaju redukcjonizm

[12] K. Gödel, *Remarks Before the Princeton Bicentennial Conference on Problems in Mathematics,* [w:] idem, *Collected Works,* t. II, Oxford University Press, New York1989, s. 150-153.

m.in. dlatego, ponieważ to pierwsze ma charakter twórczy (odkrywczy). Natomiast w przypadku wykonywania algorytmów, nawet tych najbardziej finezyjnych, twórcze myślenie wcale nie jest potrzebne. Ba, dla skrupulatnego wykonywania algorytmów przestaje być potrzebne jakiekolwiek myślenie. A nawet więcej: tam, gdzie w rachubę wchodzi jedynie i tylko wykonywanie algorytmów (*resp.* implementowanych programów komputerowych), tam w ogóle nie może być śladu jakiegokolwiek myślenia. I odwrotnie: tam, gdzie rzeczywiście mamy do czynienia z myśleniem, tam zawsze będą współwystępować elementy nie poddające się algorytmizacji. Wystarczająco wymowne są tu różne warianty znanego eksperymentu J. R. Searle'a z „chińskim pokojem".

10. Mimo zasygnalizowanych wyżej wątpliwości, z punktu widzenia metamatematyki odkrycie *Omegi,* a więc kolejnej liczby nieobliczalnej, stanowi ważny (meta-)matematyczny rezultat. Ważny, bo po raz kolejny potwierdzający trafność, głębokość i doniosłość dokonanych przez Gödla odkryć. Ważny, bo domagający się gruntownego przemyślenia, a może i zrewidowania, podstaw współczesnej matematyki: tak w sensie czysto teoretycznym, jak i pragmatycznym (operacyjnym). Ważny, a może nawet arcyważny, bo przymuszający także samych matematyków do ponowienia pytań o granice wiedzy matematycznej, a więc pytań typu: Co jeszcze wymyka się potędze rozumu matematycznego i potędze ścisłego matematycznego dowodzenia? Czy poza tymi ograniczeniami wiedzy matematycznej, o których mówią dotychczasowe twierdzenia limitacyjne, jest jeszcze coś, czego rozum matematyczny ogarnąć nie jest w stanie i wobec czego dalej pozostaje bezradny albo ślepy? Czy konstruktywność procedur dowodowych w matematyce dalej należy wiązać z ich formalizowalnością i/lub rekurencyjnością? Co poza dowodliwością może poręczać prawdziwość matematycznych twierdzeń? Czy tradycyjne ujęcie teorii matematycznych, a więc ich ujęcie aksjomatyczno-dedukcyjne, mimo swych atutów, nie wyczerpało swych poznawczych możliwości? Czy nie czas po temu, by należycie przetestować inne (konkurencyjne) sposoby osiągania i porządkowania systematycznej wiedzy matematycznej, np. semantyczny lub strukturalny (nie-zdaniowy)? Etc. Etc.

Jak sądzę, to właśnie mierząc się z tymi pytaniami Greg J. Chaitin sformułował pewne metodologiczne postulaty — postulaty, które, choć dla części matematyków mogą brzmieć nieco osobliwie lub niepokojąco, innej części pozwolą być może nabrać wiatru w żagle. Mianowicie, dostrzegając nieskuteczność (bezowocność, jałowość) prowadzenia pracy badawczej „w dawnym dobrym stylu"[13], Chaitin proponuje nowy metodologiczny paradygmat — paradygmat, opierający się na zwrocie w kierunku „matematyki eksperymentalnej" (*quasi*-empirycznej), nade wszystko zaś uznający przypadkowość (losowość) za istotną i niezbywalną cechę także świata przedmiotów matematycznych.[14] Według Chaitina, ważnym źródłem nowych impulsów w dziedzinie badań matematycznych, a może nawet tych impulsów źródłem najważniejszym, jest dzisiaj informatyka. Stale rosnące możliwości obliczeniowe komputerów stwarzają całkiem nowe warunki eksperymentowania i testowania matematycznych hipotez. Jakkolwiek paradoksalnie by to nie wyglądało, okoliczności tej nie wolno dzisiaj ignorować lub choćby nie doceniać.[15] Jednak, co chciałem wyraźnie odnotować, wbrew komputacjonistom i mimo swych wieloletnich związków z IBM-em, Chaitin nie uważa, by komputery mogły zastąpić w myśleniu samych

[13] Chaitin zauważa w tym kontekście, iż poszukiwania matematyków, którzy pracują jeszcze w starym stylu, a więc ignorują twierdzenia Gödla i jego własne ustalenia (nie uwzględniają przypadkowości w świecie matematycznym), przypominają próbę wydedukowania z praw Newtona np. całej teorii względności albo równań Maxwella czy Schrödingera. Tamże, s. 24 i n.

[14] Tamże, s. 22-26 (*sub. 5, Experimental mathematics*).

[15] Ewentualny paradoks polega tu na tym, że to, co ze swej istoty niealgorytmizowalne, nieobliczalne i niesekwencyjne — np. okazana przez Chaitina przypadkowość świata matematycznego, a nadto dynamika nieliniowa, kwantowa teoria pola, geometria fraktalna itp. — usiłuje się wytropić i opisać właśnie za pomocą algorytmów i obliczeń.

matematyków.[16] Podobnie jak np. J. R. Searle (i zgodnie z programem słabej AI) sądzi tylko, że maszyny obliczeniowe stanowią dzisiaj dla matematyków wyjątkowo skuteczne **narzędzie** pracy badawczej. Tedy wielkim błędem z ich strony byłoby tego faktu należycie nie docenić i należycie nie zdyskontować.[17] Chaitin wskazuje także na nowe matematyczne czasopismo — czasopismo pod nazwą *Journal of Experimental Mathematics,* które najpełniej odpowiada programowi nowej matematycznej szkoły.[18]

Zapewne jeszcze w niejednym punkcie można powątpiewać w rzeczywistą doniosłość (przełomowość, rewolucyjność) faktycznie dokonanych przez Chaitina ustaleń czy w lansowany przez niego, w stylu charakterystycznym dla amerykańskiego rynku idei, obraz przyszłej *quasi*-empirycznej matematyki i program nowej matematycznej szkoły. Jednak jedno wydaje się być pewne. Osiągnięte przez Chaitina wyniki, a przynajmniej częściowo także ich filozoficzna interpretacja, godne są odnotowania i gruntownego przemyślenia. Odnotowania i przemyślenia godna jest również, i to jako temat dla siebie (tutaj wyraźnie przeze mnie nie wyodrębniony), sformułowana przez Chaitina algorytmiczna teoria informacji — teoria umożliwiająca badanie niezupełności systemów aksjomatycznych w kontekście informatycznym (m.in. poprzez odwołanie się do losowych sekwencji binarnych i zjawiska algorytmicznej niekompresowalności).

Jeszcze kilka lat temu, a mam na myśli schyłek lat dziewięćdziesiątych XX wieku, Gregory J. Chaitin był postacią w Polsce niemal nieznaną — nieznaną zarówno samym matematykom, jak i informatykom (także metodologom informatyki). O ile wiem, pierwsze informacje na temat badań Chaitina nad podstawami matematyki i algorytmiczną teorią informacji poczęły się pojawiać najpierw w środowisku filozoficznym — w środowisku filozofów matematyki (R. Murawski), logików (J. Paśniczek) oraz filozofów nauki i epistemologów (jak niżej podpisany).[19] Jednym z pierwszych w tym gronie był autor niniejszego przekładu, pan Piotr Czarnota. Doskonale pamiętam ten jego wielki „ogień w oczach", gdy jeszcze jako student zwrócił mi uwagę na osobę i prace Grega J. Chaitina. Pamiętam również pasję, z jaką referował (i dyskutował) wyniki Chaitina na teoriopoznawczym seminarium, które w roku 1999/2000 prowadziłem dla studentów filozofii UMCS.[20]

Dzisiaj sytuacja się zmieniła i bez wątpienia wygląda dużo lepiej. Dzięki internetowi teksty G. J. Chaitina — zarówno te ważne, jak i mniej ważne — są w całości dostępne niemal każdemu. Z profesorem Chaitinem można wymienić poglądy i opinie także drogą mailową, a — co na marginesie chciałbym zauważyć — jest on wielkim miłośnikiem tej formy

---

[16] Na odnalezienie dowodu i genialnych autorów tego przedsięwzięcia czeka wszak szereg nowych matematycznych twierdzeń — twierdzeń równie interesujących jak niedawno udowodnione wielkie twierdzenie Fermata czy hipoteza Riemanna. G. J. Chaitin, *The Limits…,* s. 55.

[17] G. J. Chaitin, *Randomness & Complexity…,* s. 14-15.

[18] G. J. Chaitin, *The Limits...,* s. 26.

[19] W języku polskim pierwszy tekst samego Chaitina ukazał się w 2002 roku w przekładzie R. Murawskiego. Por. G. Chaitin, *Twierdzenia Gödla a informacja,* [w:] *Współczesna filozofia matematyki. Wybór tekstów,* Wybrał, przełożył, komentarzami opatrzył i wstępem poprzedził Roman Murawski, Wydawnictwo Naukowe PWN, Warszawa 2002, s. 341-358. We wrześniu 2002 r. na konferencji pod hasłem *Filozofia na progu XXI wieku* (jej organizatorem był Wydział Filozofii i Socjologii UMCS) wygłosiłem odczyt, w którym zreferowałem niektóre ustalenia Chaitina. Jego nieco zmodyfikowaną (i rozszerzoną) wersję por. w: J. Dębowski, *Pułapki komputacjonizmu,* „Filozofia Nauki" 2004, Nr 1-2. Por. też J. Dębowski, *Filozofia nauki — jej przedmiot, problemy i stanowiska* [w:] *Podstawy filozofii,* pod red. S. Opary, A. Kucnera i B. Zielewskiej, Wydawnictwo UWM, Olsztyn 2003, s. 169-182.

[20] Swoje ówczesne zainteresowania badaniami G. J. Chaitina pan P. Czarnota zwieńczył pracą magisterską pt. *Algorytmiczna teoria informacji w ujęciu G. J. Chaitina,* obronioną w 2003 roku na Wydziale Filozofii i Socjologii UMCS.

komunikacji. Aby wyeliminować ostatnią poważną barierę ograniczającą dostęp do myśli Chaitina, a tym samym obieg jego pism uczynić jeszcze pełniejszym, wszystkim zainteresowanym (w szczególności, środowisku matematyków, informatyków i filozofów poznania matematycznego) przekazujemy polski przekład bodaj najważniejszej jego książki — książki pod wymownym tytułem *Granice matematyki*. Przy tej okazji pozwalam sobie wyrazić nadzieję, iż jej polskojęzyczne wydanie — wydanie sfinalizowane przede wszystkim dzięki życzliwemu zainteresowaniu Wydawnictwa UWM w Olsztynie i osobiście Pana Prorektora S. Achremczyka — w sposób istotny przyczyni się do ożywienia naukowego dyskursu nie tylko nad podstawami wiedzy matematycznej, lecz podstawami całej ludzkiej wiedzy: naukowej i pozanaukowej, demonstratywnej i niedemonstratywnej, apriorycznej i aposteriorycznej, analitycznej i syntetycznej, dyskursywnej i pozadyskursywnej, pojęciowej i oglądowej, bezpośredniej i pośredniej, zdroworozsądkowej i literacko-artystycznej, potocznej i sapiencjalnej, racjonalnej i irracjonalnej. Wszelkiej.

Józef Dębowski

Olsztyn, marzec 2004.

Przedmowa

Jako nastolatek, Greg utworzył niezależnie od Kołmogorowa i Solomonoffa to, co nazywamy obecnie algorytmiczną teorią informacji, przedmiot, którego jest on głównym architektem. Jego praca naukowa z 1965 roku na temat eksperymentów na automatach, którą napisał będąc w szkole średniej, jest do dziś nadal przedmiotem zainteresowania. Jest on również bardzo zaangażowany w IBM, gdzie pracuje od niemal trzydziestu lat nad rozwojem technologii RISC.

Rezultaty Grega są szeroko cytowane. Moim ulubionym portretem Grega może być ten, odnaleziony u Johna Horgana, pisarza piszącego dla *Scientific American,* w książce *Koniec nauki* z 1996 roku. Greg otrzymał wiele zaszczytów. Był gościem dystyngowanych osób takich jak Prigogine'a, Króla i Królowej Belgii oraz następcy tronu Japonii.

Streszczając się, pozwólcie mi sparafrazować Bette Davis z filmu *Wszystko o Ewie*, która powiedziała „Zapnijcie pasy bezpieczeństwa, zanosi się na wyboistą pogadankę!". Panie i Panowie, Greg Chaitin! (śmiechy i oklaski)

Cristian Calude przedstawiając Gregory'ego Chaitina na spotkaniu DMTCS'96 w The University of Auckland.

Słowo wstępne

Gdyby jakaś katastrofa miała nagle zagrozić zniszczeniem wszystkiego, co kiedykolwiek napisałem, to ta książka jest tym, co chciałbym zachować! To, co zawiera jest podstawą, wszystko inne to szczegóły techniczne. Ta książka jest ostateczną wersją kursu na temat granic matematyki, który prowadziłem kilka razy. Zawiera zapisy moich trzech ulubionych wykładów, w których próbowałem przenieść ten klimat występu na żywo przed audytorium. Przebywanie twarzą w twarz ze słuchaczami daje mi szczególną energię, której nie mam kiedy dyktuję wykład!

Po tych trzech wykładach jest dużo kodu programu języka LISP-a a na końcu trochę kodu programu Mathematica.

Z uwagi na ten kurs musiałem wynaleźć nowy dialekt LISP-a. Niestety nie ma podręcznika dla mojego LISP-a, ale dwa z tych wykładów wyjaśnią go. Jest też długie wykonywanie LISP-a `examples.r`, które zawiera dużo objaśnień i ukazuje każdą cechę tego języka. Zatem uważam, że to, co się tutaj znajduje jest równoważne zajęciom fakultatywnym z wykorzystaniem podręcznika.

Zawarłem również kod programu do mojego interpretera LISP-a. Jest to trzysta wierszy Mathematica i aneks na końcu książki.

Niestety oprogramowanie jest krótkotrwałe, zmienia się w miarę jak je wykonujecie i musicie uruchamiać je tak szybko, jak potraficie, żeby zostać w tym samym miejscu! Kod programu w aneksie to Mathematica Version 2, nie ostatnia wersja Mathematica, która jest Version 3. Zakodowałem również interpretera w C , a C być może zostanie zastąpiony przez Javę w niezbyt odległej przyszłości! Ponieważ ten kurs jest obecnie w swojej wersji ostatecznej, zdecydowałem wycofać się z wyścigu i zamrozić oprogramowanie.

Jednakże możecie zrozumieć podstawowe idee zawarte w tej książce czytając wykłady, bez przechodzenia przez kod programu LISP-a. Możecie czytać mój kod programu LISP-a i testować jego wykonywanie bez posiadania interpretera. Zatem wszystko, co niezbędne znajduje się w tej książce. Możliwość uruchomiania interpretera LISP-a jest z pewnością pomocna. To była cała idea mojego kursu, który powinien być praktycznym kursem komputerowym. Prowadziłem również ten kurs kilka razy bez komputerów i wydawało mi się, że to także działa nawet jeśli nie było równie ekscytujące.

Możecie również uruchomić LISP-a w waszej głowie, co jest sposobem, w jaki matematyka jest tradycyjnie uprawiana. Zatem pomyślcie o tym raczej jak o formalizmie, niż języku programowania.

Ogromnie cieszyłem się dając ten kurs lub jego streszczenia w Maine, prywatnie w moim biurze, w Santa Fe i Albuquerue w Rumunii nad Morzem Czarnym, w Abisko i Rovaniemi pod kołem podbiegunowym, w Helsinkach, Kopenhadze oraz w Auckland. To wspaniała zabawa i jestem bardzo, bardzo wdzięczny za te zaproszenia. Stymulowały mnie do rozwiązywania zadań i tworzenia wielu, wielu wersji tego oprogramowania. Chcę zatem podziękować Georgowi Markowsky'emu, Johnowi Casti, Crisowi Calude, Walterowi Meyersteinowi, Bernardowi Moretowi, Edowi Angelowi, Veikko Kearenowi, Gautamie Sasgupta, Klausowi Sutnerowi, Torowi Nørretrandersowi i Andersowi Karlqvistowi.

Muszę również podziękować the Santa Fe Institute, którego mam przyjemność regularnie odwiedzać. Dwa rozdziały z tej książki są wykładami, które wygłosiłem podczas tamtych wizyt. Nadal pamiętam rozwiązywanie niektórych kluczowych problemów pewnej bezsennej nocy w życzliwym domu Johna i Vivien Casti.

I nic z tego nie mogłoby się stać bez IBM, które wspiera moje badania od trzydziestu lat. W szczególności jestem wdzięczny mojemu obecnemu zarządowi: Lee Nackmanowi i Ambujowi Goyalowi za umożliwienie mi ukończenia tej książki. Podziwiam również tych bardzo bystrych i zdeterminowanych uczestników moich kursów. Odważni pionierzy!

Wszystkim „Merci beaucoup” i „Tusind tak”! Ostatnie podziękowania dla Hansa-Christiana za fotografię na stronie tytułowej, którą zrobił na Viena University w sali, gdzie wykładał Gödel.

Gregory Chaitin, kwiecień 1997

Losowość w arytmetyce oraz schyłek i upadek redukcjonizmu w czystej matematyce

G. J. Chaitin, *chaitin@watson.ibm.com*

Bulletin of the European Association for Theoretical Computer Science, Nr 50 (czerwiec 1993), s. 314-328

Wykład wygłoszony we wtorek 22 października na Mathematics-Computer Science Colloquium w University of New Mexico. Wykład był filmowany na video; to jest zredagowany transkrypt.

1.Hilbert o metodzie aksjomatycznej

W ubiegłym miesiącu byłem mówcą na sympozjum na temat redukcjonizmu w Cambridge University gdzie Turing wykonywał swoją pracę. Chciałbym powtórzyć wykład, który tam wygłosiłem i wytłumaczyć, w jaki sposób moja praca jest kontynuacją i rozwinięciem pracy Turinga. Dwaj poprzedni mówcy mówili przykre rzeczy o Dawidzie Hilbercie. A zatem zacznę od powiedzenia, że pomimo tego, co być może słyszeliście w kilku poprzednich wykładach, Hilbert nie był przygłupem!

Idea Hilberta jest kulminacją dwóch tysięcy lat matematycznej tradycji: nawiązującej do aksjomatycznego traktowania geometrii przez Euklidesa, do marzeń Leibniza o logice symbolicznej, oraz monumentalnego dzieła *Principia Mathematica* Whiteheada i Russella. Marzeniem Hilberta było raz i na zawsze wyjaśnić metody matematycznego dowodzenia. Hilbert chciał sformułować formalny system aksjomatyczny, który obejmowałby całą matematykę.

Formalny system aksjomatyczny

→
→
→

Kładł on nacisk na pewną liczbę kluczowych właściwości, które taki formalny system aksjomatyczny powinien posiadać. Ów system jest podobny do komputerowego języka programowania. Są to ściśle określone instrukcje odnośnie metod dowodzenia, postulatów i reguł wnioskowania, które my jako matematycy akceptujemy. Co więcej, Hilbert ustalił, że formalny system aksjomatyczny obejmujący całą matematykę powinien być niesprzeczny i zupełny.

Formalny system aksjomatyczny

→ niesprzeczny
→ zupełny
→

„Niesprzeczny”- znaczy, że nie powinniście być w stanie udowodnić wyrażenia i zaprzeczenia tego wyrażenia.

Formalny system aksjomatyczny

→ niesprzecznyA~A
→ zupełny
→

Nie powinniście być w stanie udowodnić A i nie-A. To stawiałoby nas w trudnej sytuacji.

„Zupełny"- znaczy, że jeśli utworzycie sensowne wyrażenie, to powinniście być w stanie rozstrzygnąć je w taki czy inny sposób. Znaczy to, że albo A, albo nie-A powinno być twierdzeniem i powinno być dowodliwe z aksjomatów poprzez zastosowanie reguł wnioskowania w formalnym systemie aksjomatycznym.

Formalny system aksjomatyczny

→ niesprzeczny A ~ A
→ zupełny A ~ A
→

Rozważmy sensowne wyrażenie A i jego przeciwieństwo nie-A. Dokładnie jedno z tych dwóch powinno być dowodliwe, jeśli formalny system aksjomatyczny jest niesprzeczny i zupełny.

Formalny system aksjomatyczny jest podobny do języka programowania. Posiada alfabet i reguły gramatyki, innymi słowy formalną składnię. Jest to ten rodzaj rzeczy, z którymi jesteśmy obecnie obeznani. Popatrzcie wstecz na trzy ogromne tomy Whiteheada i Russella pełne symboli a zrozumiecie, że patrzycie na wielki program komputerowy w jakimś niezrozumiałym języku programowania.

A teraz bardzo zadziwiający fakt. Niesprzeczny i zupełny oznacza tylko prawdę i całą prawdę. Te właściwości wydają się być rozsądnymi wymaganiami. Jest jednak zabawna konsekwencja mająca coś wspólnego z tak zwanym problemem decyzji. W języku niemieckim jest to Entscheidungsproblem.

Formalny system aksjomatyczny

→ niesprzeczny A ~ A
→ zupełny A~ A
→ problem decyzji

Hilbert przypisywał bardzo duże znaczenie problemowi decyzji.

HILBERT
Formalny system aksjomatyczny

→ niesprzeczny A ~ A
→ zupełny A~ A
→ problem decyzji

Rozwiązanie problemu decyzji dla formalnego systemu aksjomatycznego daje algorytm, który umożliwia wam rozstrzygnięcie, czy jakieś sensowne wyrażenie jest, czy nie jest twierdzeniem. Rozwiązanie problemu decyzji jest nazywane procedurą decyzyjną.

HILBERT
Formalny system aksjomatyczny

→ niesprzeczny A~ A
→ zupełny A ~A
→ procedura decyzyjna

To brzmi niesamowicie. Formalny system aksjomatyczny, który Hilbert chciał zbudować obejmowałby całą matematykę: elementarną arytmetykę, rachunek, algebrę. Wszystko. Jeśli istnieje procedura decyzyjna, wówczas matematycy są bezrobotni. Ten algorytm, ta mechaniczna procedura może sprawdzić czy coś jest twierdzeniem czy nie, może sprawdzić czy to jest prawdziwe czy nie. A zatem wymaganie istnienia procedury decyzyjnej dla formalnego systemu aksjomatycznego brzmi tak, jak byście prosili o zbyt wiele.

Jednakże bardzo łatwo zauważyć, że jeśli system jest zupełny i niesprzeczny, to pociąga za sobą, iż z konieczności musi istnieć procedura decyzyjna. Oto, w jaki sposób można to zrobić. Macie formalny język ze skończonym alfabetem i gramatyką. Hilbert podkreślał, że całą istotą formalnego systemu aksjomatycznego jest to, iż musi być mechaniczna procedura do sprawdzania czy rzekomy dowód jest poprawny, czy nie, czy jest on podporządkowany regułom, czy nie. Jest to pogląd, że matematyczna prawda powinna być obiektywna po to, aby każdy mógł się zgodzić czy dowód wynika z reguł, czy nie.

Jeśli sprawa tak się przedstawia, to przebiegacie wszystkie możliwe dowody ustawione w porządku według długości. Następnie, badacie wszystkie sekwencje symboli alfabetu o długości jednego, dwóch, trzech, czterech, tysiąca, tysiąca i jednego znaku...o długości stu tysięcy znaków. Stosujecie tę mechaniczną procedurę, która jest istotą formalnego systemu aksjomatycznego, aby sprawdzić czy każdy dowód jest poprawny. Oczywiście przez większość czasu to będzie nonsens, to będzie niegramatyczne. Ale ostatecznie znajdziecie każdy możliwy dowód. Jest to tak, jakby milion małp pisało na maszynach. Znajdziecie każdy możliwy dowód, ale oczywiście tylko w zasadzie. Albowiem ta liczba rośnie wykładniczo i jest to coś, czego nie moglibyście wykonać w rzeczywistości. Nigdy nie dotarlibyście do dowodów, które są na jedną stronę długie.

A zatem tylko w zasadzie moglibyście przebiec wszystkie możliwe dowody sprawdzając, które są poprawne, zobaczyć czego one dowodzą i w ten sposób systematycznie znaleźć wszystkie twierdzenia. Innymi słowy, istnieje algorytm, czyli mechaniczna procedura do generowania jednego po drugim każdego twierdzenia, które może być dowiedzione w formalnym systemie aksjomatycznym. Jeśli dla każdego sensownego wyrażenia wewnątrz tego systemu, albo to wyrażenie jest twierdzeniem, albo zaprzeczenie tego wyrażenia jest twierdzeniem, tylko jedno z nich, to w takim razie macie procedurę decyzyjną. Aby sprawdzić, czy dane wyrażenie jest twierdzeniem czy nie po prostu przebiegacie wszystkie możliwe dowody, aż znajdziecie wyrażenie pojawiające się jako twierdzenie lub udowadniacie przeciwne wyrażenie.

Zatem, wydaje się, że Hilbert w rzeczywistości wierzył, że rozwiąże raz i na zawsze wszystkie matematyczne problemy. To brzmi zdumiewająco, ale on najwyraźniej w to wierzył. Wierzył, że będzie w stanie ustanowić niesprzeczny i zupełny formalny system aksjomatyczny dla i uzyska z niego procedurę decyzyjną dla całej matematyki. To jest właśnie podążanie za formalną, aksjomatyczną tradycją w matematyce.

Ale jestem pewien, że nie sądził on, iż będzie to praktyczna procedura decyzyjna. Ta, którą przedstawiłem w zarysie działałaby tylko w zasadzie. Jest wykładniczo powolna, strasznie powolna! Całkowicie niepraktyczna. Albowiem założenie było takie, że gdyby wszyscy matematycy mogliby się zgodzić czy dowód jest poprawny a system niesprzeczny i zupełny, to w zasadzie uzyskaliby procedurę decyzyjną do automatycznego rozwiązywania

każdego problemu matematycznego. To było wspaniałe marzenie Hilberta, które miało być ukoronowaniem tradycji Euklidesa i Leibniza, Boole'a i Peano oraz Russella i Whiteheada.

Oczywiście jedynym problemem tego inspirującego projektu jest to, że okazał się niemożliwy do realizacji.

2. Gödel, Turing i metoda przekątniowa Cantora

Hilbert jest rzeczywiście inspirujący. Jego sławny wykład z 1900 roku jest wezwaniem do uzbrojenia matematyków w celu rozwiązania listy dwudziestu trzech trudnych problemów. Jako młodzi ludzie stający się matematykami czytaliście listę dwudziestu trzech problemów gdzie Hilbert mówi, że nie ma żadnych ograniczeń w tym, co matematycy mogą robić. Możemy rozwiązać problem, jeśli jesteśmy dość bystrzy i pracujemy nad nim dość długo. Hilbert nie wierzył, że w zasadzie jest jakaś granica tego, co matematycy mogą osiągnąć.

Uważam, że jest to bardzo inspirujące. John von Neumann też tak uważał. Kiedy był młodym człowiekiem próbował przeprowadzić do końca ambitny program Hilberta. Ponieważ Hilbert nie mógł doczekać się kiedy to wszystko będzie działać i zaczął od elementarnej teorii liczb, 1, 2, 3, 4, 5,... nawet nie od liczb rzeczywistych.

Następnie, w 1931 roku, ku wielkiemu zdziwieniu wszystkich (wliczając von Neumanna) Gödel udowodnił, iż jest to niemożliwe, że to nie może być wykonane, jak zapewne wszyscy o tym wiecie.

Gödel 1931

Było to przeciwieństwo tego, czego wszyscy wcześniej oczekiwali. Von Neumann powiedział, że nigdy nie przyszło mu do głowy, że program Hilberta nie może być przeprowadzony.
Von Neumann ogromnie podziwiał Gödla i pomógł mu uzyskać stałą pracę w Institute for Advanced Studies.

Gödel udowodnił co następuje. Przypuśćmy, że mamy formalny system aksjomatyczny zawierający elementarną teorię liczb, 1, 2, 3, 4, 5,... oraz dodawanie i mnożenie. Następnie załóżmy, że jest on niesprzeczny, co jest minimalnym wymaganiem. Jeśli możecie udowodnić fałszywe wyniki to jest naprawdę dość źle. Gödel udowodnił, że jeśli założycie, iż system jest niesprzeczny, to wówczas możecie udowodnić, że jest niezupełny. To był wynik Gödla, a dowód jest bardzo zmyślny i zawiera samo-odniesienie. Gödel był w stanie skonstruować stwierdzenie dotyczące liczb całkowitych, które mówi samo o sobie, że jest niedowodliwe. To był ogromny szok. Gödel musiał być podziwiany za swoją intelektualną wyobraźnię ponieważ wszyscy inni sądzili, że to Hilbert miał rację.

Niemniej jednak uważam,że podejście Turinga z 1936 roku jest lepsze.

Gödel 1931
Turing 1936

Dowód Gödla z 1931 roku jest bardzo pomysłowy, to prawdziwy *tour de force*. Muszę wyznać, że kiedy byłem dzieciakiem próbowałem zrozumieć ten dowód, mogłem go czytać i podążać krok za krokiem, ale jakoś nigdy nie czułem, że go pojmuję. Natomiast Turing ma zupełnie odmienne podejście.

Uważam, że podejście Turinga jest, uczciwie mówiąc, w pewien sposób bardziej podstawowe. Faktycznie, Turing dokonał więcej niż Gödel. Turing nie tylko uzyskał jako wniosek wynik Gödla, ale udowodnił, że nie może istnieć żadna procedura decyzyjna.

Zauważcie- jeśli założycie, że macie formalny system aksjomatyczny dla arytmetyki i jest on niesprzeczny, to z twierdzenia Gödla wiadomo, że nie może być zupełny ale nadal może jeszcze istnieje procedura decyzyjna. Nadal być może istnieje mechaniczna procedura, która umożliwiłaby rozstrzygnięcie, czy dane wyrażenie jest prawdziwe, czy nie. Ta kwestia została pozostawiona otwarta przez Gödla, ale Turing ją rozstrzygnął. Ten fakt, że nie jest możliwe istnienie procedury decyzyjnej jest bardziej fundamentalny i otrzymujecie niezupełność jako oczywisty wniosek.

W jaki sposób zrobił to Turing? Chcę wam opowiedzieć jak to zrobił, ponieważ jest to „trampolina" dla mojej własnej pracy. Sposób, w jaki to przeprowadził, jestem pewien, że wszyscy o tym słyszeliście, ma coś wspólnego z tak zwanym problemem zakończenia pracy. Faktycznie, jeśli wrócicie do rozprawy naukowej Turinga z 1936 roku to nie znajdziecie w niej terminu „problem zakończenia pracy". Ale z pewnością ta idea tam jest.

Ludzie zapomnieli również, że Turing mówił o „liczbach obliczalnych". Tytuł jego pracy jest następujący „On computable numbers with an application to the Entscheidungsproblem." Każdy pamięta, że problem zakończenia pracy jest nierozstrzygalny oraz, że pochodzi z pracy wymienionej powyżej, ale niewielu ludzi pamięta, że Turing mówił także o obliczalnych liczbach rzeczywistych. Moja praca dotyczy obliczalnych i dramatycznie nieobliczalnych liczb rzeczywistych. A zatem chciałbym odświeżyć waszą pamięć i przypomnieć, w jaki sposób idzie dowodzenie Turinga.

Dowodzenie Turinga jest naprawdę tym, co niszczy marzenie Hilberta i jest prostym dowodzeniem. Jest to właśnie metoda przekątniowa Cantora (dla tych z was, co wiedzą co to jest) zastosowana do obliczalnych liczb rzeczywistych. Jest to idea przedstawiona w dużym skrócie, ale wystarczy, aby wykazać, że marzenie Hilberta i ukoronowanie dwóch tysięcy lat tego, co matematycy sądzili o matematyce, jest błędne. Zatem praca Turinga jest ogromnie głęboka.

Jaki jest dowód Turinga? Liczba rzeczywista, wiecie, 3, 1415926..., jej długość jest mierzona z arbitralną precyzją przy pomocy nieskończonej ilości cyfr. Turing powiedział, że liczba rzeczywista obliczalna to taka, dla której istnieje program komputerowy lub algorytm do obliczania cyfr jedna po drugiej. Na przykład, jest program dla π i są też algorytmy do rozwiązywania równań algebraicznych z liczbami całkowitymi jako współczynnikami. Faktycznie, większość liczb, które w rzeczywistości znajdziecie w analizie to liczby obliczalne. Niemniej jednak, jeśli znacie teorię mnogości, to wiadomo, że są one wyjątkami ponieważ obliczalne liczby rzeczywiste są przeliczalne, ale są też liczby rzeczywiste nieprzeliczalne (nie musicie wiedzieć, co to znaczy). To jest istotą pomysłu Turinga.

Ten pomysł wygląda następująco. Sporządzacie listę wszystkich możliwych programów komputerowych. W tamtych czasach nie było żadnych programów komputerowych i Turing musiał wynaleźć maszynę Turinga, co było ogromnym krokiem naprzód. Ale teraz po prostu wyobraźcie sobie napisanie listy wszystkich możliwych programów komputerowych.

p_1
p_2
p_3
p_4
p_5
p_6
…

Gödel 1931
Turing 1936

Jeśli rozważycie programy komputerowe w notacji binarnej, wówczas jest naturalnym myśleć o programie komputerowym, jak o liczbie naturalnej. Obok każdego programu komputerowego- pierwszego, drugiego, trzeciego piszemy tę liczbę rzeczywistą, którą on oblicza, jeśli oblicza liczbę rzeczywistą (być może nie). Lecz jeśli program drukuje nieskończoną liczbę cyfr to zapisujemy je. Zatem być może jest to 3, 1415926 i oto macie następna i następną i następną.

p_1 3,1415926...
p_2
p_3
p_4
p_5
p_6
...

Gödel 1931
Turing 1936

W takim razie sporządzamy tę listę. Być może niektóre z programów nie drukują nieskończonej serii cyfr ponieważ są programami, które zatrzymują się lub takimi, które zawierają wewnętrzny błąd i eksplodują. Wówczas na liście będzie wiersz pusty.

p_1 3.1415926...
p_2 ...
p_3 ...
p_4 ...
p_5
p_6 ...
...

Gödel 1931
Turing 1936

To nie jest naprawdę ważne---zapomnijmy o tej możliwości.

Idąc w ślady Cantora, Turing mówi, aby zejść w dół przekątnej i przyjrzeć się pierwszej cyfrze pierwszej liczby, drugiej cyfrze drugiej liczby, trzeciej...

p_1 -. $\mathbf{d_{11}}$ d_{12} d_{13} d_{14} d_{15} d_{16} ...
p_2 -. d_{21} $\mathbf{d_{22}}$ d_{23} d_{24} d_{25} d_{26} ...
p_3 -. d_{31} d_{32} $\mathbf{d_{33}}$ d_{34} d_{35} d_{36} ...
p_4 -. d_{41} d_{42} d_{43} $\mathbf{d_{44}}$ d_{45} d_{46} ...
p_5
p_6 -. d_{61} d_{62} d_{63} d_{64} d_{65} $\mathbf{d_{66}}$ ...
...
. $\neq d_{11}$ $\neq d_{22}$ $\neq d_{33}$ $\neq d_{44}$ $\neq d_{55}$ $\neq d_{66}$ ...

Gödel 1931
Turing 1936

Cóż, właściwie są to cyfry po przecinku ułamka dziesiętnego. A zatem jest pierwsza cyfra po przecinku pierwszej liczby, druga cyfra po przecinku drugiej liczby, trzecia cyfra trzeciej liczby, czwarta cyfra czwartej liczby. Nie ma znaczenia czy piąty program drukuje piątą cyfrę, to naprawdę nie ma znaczenia.

Potem wykonujecie rzecz następującą- zmieniacie te cyfry. Sprawiacie**,** że są inne. Zmieniacie każdą cyfrę na przekroju. Połączmy te zmienione cyfry razem, tworząc w ten sposób nową liczbę z przecinkiem z przodu, nową liczbę rzeczywistą. To jest metoda przekątniowa Cantora. A zatem macie cyfrę, którą wybraliście i która od pierwszej cyfry różni się pierwszą cyfrą po przecinku od drugiej drugą, od trzeciej trzecią i składacie te cyfry razem w jedną liczbę.

p_1 -. $\mathbf{d_{11}}$ d_{12} d_{13} d_{14} d_{15} d_{16} ...
p_2 -. d_{21} $\mathbf{d_{22}}$ d_{23} d_{24} d_{25} d_{26} ...
p_3 -. d_{31} d_{32} $\mathbf{d_{33}}$ d_{34} d_{35} d_{36} ...
p_4 -. d_{41} d_{42} d_{43} $\mathbf{d_{44}}$ d_{45} d_{46} ...
p_5
p_6 -. d_{61} d_{62} d_{63} d_{64} d_{65} $\mathbf{d_{66}}$ ...
...
. $\neq d_{11}$ $\neq d_{22}$ $\neq d_{33}$ $\neq d_{44}$ $\neq d_{55}$ $\neq d_{66}$ ...

Gödel 1931
Turing 1936

Ta nowa liczba nie może być na liście z powodu sposobu, w jaki została skonstruowana. Dlatego jest to nieobliczalna liczba rzeczywista. W jaki sposób Turing przechodzi stąd do problemu zakończenia pracy? Cóż, zapytajcie samych siebie**, dlaczego** nie możecie obliczyć tej liczby? Wytłumaczyłem wam w jaki sposób otrzymać tę liczbę i wygląda na to, że prawie moglibyście to zrobić. Aby obliczyć *N*-tą cyfrę tej liczby otrzymujecie *N*-ty program komputerowy (z pewnością możecie to zrobić), następnie uruchamiacie go dopóki nie wydrukuje *N*-tej cyfry i w tym momencie zmieniacie ją. Zatem, w czym jest problem? Wydaje się to łatwe.

Problemem jest to, co się stanie jeśli *N*-ty program komputerowy nigdy nie wydrukuje *N*-tej cyfry a wy będziecie siedzieć tam czekając? I to jest właśnie problem zakończenia pracy. Nie możecie rozstrzygnąć czy *N*-ty program komputerowy kiedykolwiek wydrukuje *N*-tą cyfrę! W ten sposób Turing uzyskał nierozstrzygalność problemu zakończenia pracy. Ponieważ gdybyście byli w stanie rozstrzygnąć problem zakończenia pracy, wówczas moglibyście rozstrzygnąć czy *N*-ty program komputerowy kiedykolwiek wydrukuje *N*-tą cyfrę. Gdybyście mogli to zrobić, wówczas bylibyście właściwie w stanie przeprowadzić procedurę przekątniową Cantora i obliczyć liczbę rzeczywistą, która musi różnić się od jakiejkolwiek obliczalnej liczby rzeczywistej. To jest oryginalne dowodzenie Turinga.

Dlaczego spowodowało to obalenie marzenia Hilberta? Co Turing udowodnił? Dowiódł, że nie ma algorytmu, żadnej mechanicznej procedury, która rozstrzygałaby czy *N*-ty program komputerowy wygeneruje *N*-tą cyfrę. Wobec tego niemożliwym jest aby istniał algorytm, który rozstrzygałby czy dany program komputerowy kiedykolwiek zatrzyma się (znalezienie *N*-tej cyfry wygenerowanej przez *N*-ty program komputerowy jest szczególnym przypadkiem). Cóż, to czego pragnął Hilbert to formalny system aksjomatyczny, z którego powinna wywodzić się cała matematyczna prawda i tylko prawda. Gdyby Hilbert mógł tego dokonać to uzyskałby mechaniczną procedurę do rozstrzygania czy dany program komputerowy kiedykolwiek zatrzyma się. Dlaczego?

Przebiegacie przez wszystkie możliwe dowody do momentu gdy, albo znajdziecie dowód, że program zatrzyma się, albo znajdziecie dowód, że program nigdy się nie zatrzyma. Gdyby marzenie Hilberta o skończonym zbiorze aksjomatów, z których cała matematyczna prawda powinna być wywiedziona byłoby możliwe, wówczas poprzez przebiegnięcie wszystkich możliwych dowodów i sprawdzenie, które z nich są poprawne moglibyście rozstrzygnąć, który program komputerowy zatrzyma się. Moglibyście w zasadzie. Ale **nie możecie** z powodu bardzo prostego dowodu Turinga, który jest właściwie dowodem przekątniowym Cantora, zastosowanym do liczb rzeczywistych obliczalnych. Jakie to jest proste!

Dowód Gödla jest pomysłowy i trudny. Dowód Turinga jest tak fundamentalny, tak głęboki, że wszystko wydaje się naturalne i przekonywające. Ale oczywiście Turing korzystał z pracy Gödla.

3. Prawdopodobieństwo zakończenia pracy i algorytmiczna losowość.

Mówiłem wam o Turingu i rzeczywistych liczbach obliczalnych z tego powodu, że zamierzam zastosować inną procedurę aby skonstruować nieobliczalną liczbę rzeczywistą, dużo bardziej nieobliczalną niż to robi Turing.

p_1 -. $\mathbf{d_{11}}$ d_{12} d_{13} d_{14} d_{15} d_{16} ...
p_2 -. d_{21} $\mathbf{d_{22}}$ d_{23} d_{24} d_{25} d_{26} ...
p_3 -. d_{31} d_{32} $\mathbf{d_{33}}$ d_{34} d_{35} d_{36} ...
p_4 -. d_{41} d_{42} d_{43} $\mathbf{d_{44}}$ d_{45} d_{46} ...
p_5
p_6 -. d_{61} d_{62} d_{63} d_{64} d_{65} $\mathbf{d_{66}}$ ...
...
. $\neq d_{11} \neq d_{22} \neq d_{33} \neq d_{44} \neq d_{55} \neq d_{66}$ ...

Gödel 1931
Turing 1936
liczby rzeczywiste nieobliczane

W ten sposób popadamy w dużo gorsze kłopoty.

W jaki sposób otrzymuję dużo bardziej nieobliczalną liczbę rzeczywistą? (Będę musiał wam powiedzieć jak nieobliczalną liczbą jest.) Nie poprzez zastosowanie metody przekątniowej. Liczbę, którą nazywam Omegą, otrzymuję w następujący sposób:

$$\Omega = \Sigma_{p \text{ halts}} 2^{-/p/}$$

Jest to właśnie prawdopodobieństwo zakończenia pracy. Jest to rodzaj matematycznego kalamburu. Zasadniczy wynik Turinga jest taki, że problem zakończenia pracy jest nierozwiązywalny. Nie ma żadnego algorytmu, który rozstrzygałby problem zakończenia pracy. Moim głównym wynikiem jest to, że problem zakończenia pracy jest algorytmicznie nieredukowalny lub algorytmicznie losowy.

Czym dokładnie jest prawdopodobieństwo zakończenia pracy? Poniżej napisałem dla niego wyrażenie:

$$\Omega = \Sigma_{p \text{ halts}} 2^{-/p/}$$

Zamiast przeglądania pojedynczych programów i pytania czy one zatrzymają się wkładacie wszystkie programy komputerowe razem do worka. Jeśli generujecie program komputerowy

w sposób losowy poprzez rzucanie niezafałszowaną monetą dla uzyskania każdego bitu programu, to jakie jest prawdopodobieństwo, że program zatrzyma się? Rozważacie programy, jako ciągi bitów i generujecie każdy bit przez niezależny rzut monetą. Zatem, jeśli program jest *N*-bitów długi, to prawdopodobieństwo, że otrzymacie ten konkretny program wynosi 2^{-N}. Jakikolwiek program *p*, który zatrzymuje się wnosi $2^{-|p|}$ dwa do minus jego wielkości w bitach, liczba bitów, jaką zawiera do tego prawdopodobieństwa zakończenia pracy.

Nawiasem mówiąc, jest szczegół techniczny, który jest bardzo ważny a nie działał we wcześniejszej wersji algorytmicznej teorii informacji. Nie moglibyście napisać w ten sposób:

$$\Omega = \Sigma_{p \text{ halts}} 2^{-/p/}$$

To dałoby nieskończoność. Techniczny szczegół jest taki, że żadne rozszerzenie prawidłowego programu nie jest prawidłowym programem. Zatem ta suma:

$$\Sigma_{p \text{ halts}} 2^{-/p/}$$

jest pomiędzy zerem i jedynką. W przeciwnym razie okazałaby się nieskończonością. Zabrało mi to tylko dziesięć lat dopóki, nie zrobiłem tego jak należy. Pierwotna wersja algorytmicznej teorii informacji z lat sześćdziesiątych jest błędna. Jednym z powodów tego jest to, że nie możecie nawet zdefiniować tej liczby.

$$\Omega = \Sigma_{p \text{ halts}} 2^{-/p/}$$

W 1974 roku ponownie przeformułowałem algorytmiczną teorię informacji z „samo-ograniczającymi" programami i odkryłem prawdopodobieństwo zakończenia pracy Ω.

Dobrze- zatem jest to prawdopodobieństwo pomiędzy zerem a jedynką

$$0 < \Omega = \Sigma_{p \text{ halts}} 2^{-/p/} < 1$$

jak wszystkie prawdopodobieństwa. Pomysł jest taki, że generujecie każdy bit programu przez rzucanie monetą i pytacie, jakie jest prawdopodobieństwo, że program zatrzyma się. Ten numer Ω, prawdopodobieństwo zakończenia pracy jest nie tylko liczbą rzeczywistą nieobliczalną. Już Turing wiedział jak to zrobić. Ta liczba jest nieobliczalna w najgorszy z możliwych sposobów.

Pozwólcie mi podać kilka wskazówek jak nieobliczalną liczbą jest Ω.

A zatem, pierwszą rzeczą jest to, że Ω jest algorytmicznie niekompresowalna. Jeśli chcecie uzyskać pierwsze *N*-bitów Omegi z programu komputerowego, jeśli chcecie, żeby program komputerowy wydrukował wam pierwsze *N*-bitów Omegi i następnie zatrzymał się, to program komputerowy musi być *N*-bitów długi. Zasadniczo drukujecie tylko wielkości stałe, które zawiera program. Nie możecie upakować pierwszych *N*-bitów Omegi. To

$$0 < \Omega = \Sigma_{p \text{ halts}} 2^{-/p/} < 1$$

jest liczba rzeczywista, moglibyście napisać ją w rozwinięciu binarnym. Ale jeśli chcecie wyciągnąć pierwsze *N*-bitów z programu komputerowego to właściwie musicie je tam wprowadzić. Program musi być *N*-bitów długi. Jest to nieredukowalna matematyczna informacja. Nie istnieje bardziej zwięzły opis.

W tej chwili mówimy w sposób skrótowy o tych sprawach. Pozwólcie dać mi więcej konkretnych przykładów jak losowa jest Omega. Émile Borel na początku tego wieku był jednym z założycieli teorii prawdopodobieństwa.

$$0 < \Omega = \Sigma_{p \text{ halts}} 2^{-/p/} < 1$$
Émile Borel

Pytanie: Czy mogę zadać bardzo proste pytanie zanim będzie pan kontynuował?
Odpowiedź: Pewnie.
Pytanie: Nie rozumiem, dlaczego Ω powinna być prawdopodobieństwem. Co się stanie, jeśli oba jedno-bitowe programy zatrzymają się? Mam na myśli co się stanie, jeśli jeden i drugi jedno-bitowy program zatrzyma się a następnie niektóre inne programy zatrzymają się. Zatem Omega wynosi więcej niż jeden i nie jest prawdopodobieństwem.
Odpowiedź: Mówiłem, że żadne rozszerzenie prawidłowego programu nie jest prawidłowym programem.
Pytanie: W porządku. Żaden inny program nie może się zatrzymać.
Odpowiedź: Te dwa jedno-bitowe programy byłyby wszystkimi programami, jakie tam się znajdują. To jest powód, dla którego ta liczba

$$0 < \Omega = \Sigma_{p \text{ halts}} 2^{-/p/} < 1$$

nie może być zdefiniowana, jeśli myślisz o programach w normalny sposób...

A zatem, oto mamy Émila Borela, który mówi o czymś, co nazywał liczbą normalną.

$$0 < \Omega = \Sigma_{p \text{ halts}} 2^{-/p/} < 1$$
Émile Borel---liczby rzeczywiste normalne

Co to jest liczba rzeczywista normalna? Ludzie obliczyli π do miliardowego miejsca po przecinku, być może do dwóch miliardów. Jednym z powodów robienia tego, poza tym, że jest to jak wspinaczka w górach i ustanawianie rekordu świata, jest pytanie czy każda cyfra występuje tą samą ilość razy. Wygląda na to, że cyfry od 0 do 9 występują z 10% częstotliwością w rozwinięciu dziesiętnym π. To wygląda w ten sposób, ale nikt nie może tego udowodnić. Uważam, że to samo dotyczy √2, chociaż nie jest to tak popularna liczba, żeby o nią pytać.

Pozwólcie mi przedstawić część pracy, którą wykonał Borel pod koniec wieku torując drogę nowoczesnej teorii prawdopodobieństwa. Wybierzcie liczbę rzeczywistą w przedziale jednostkowym, liczbę rzeczywistą z przecinkiem z przodu, bez żadnej części liczby całkowitej.

Jeśli wybierzecie liczbę rzeczywistą w przedziale jednostkowym, to Borel udowodnił, że z prawdopodobieństwem wynoszącym jeden liczba ta będzie „normalną". Normalna znaczy, że kiedy piszecie ją w rozwinięciu dziesiętnym to każda cyfra wystąpi w granicy dokładnie 10% częstotliwości w danym okresie czasu. Podobnie będzie w każdej innej podstawie systemu liczenia. Na przykład w systemie binarnym 0 i 1 wystąpią w granicy dokładnie 50% częstotliwości. Podobnie z blokiem cyfr. Borel nazwał to absolutnie normalną liczbą rzeczywistą i udowodnił z prawdopodobieństwem wynoszącym jeden, że jeśli wybierzecie liczbę rzeczywistą w sposób losowy pomiędzy jeden i zero to będzie ona posiadać tę samą właściwość. Jest tylko jeden problem. Borel nie wiedział czy π jest liczbą normalną, nie wiedział czy √2 jest liczbą normalną.
W rzeczywistości, nie mógł wskazać żadnego przykładu normalnej liczby rzeczywistej.

Pierwszy przykład takiej liczby został odkryty przez przyjaciela Alana Turinga z Cambridge Davida Champernowne'a, który nadal żyje i jest dobrze znanym ekonomistą. Turing był pod jego wrażeniem. Sądzę, że nazywał go „Champ", ponieważ Champ opublikował to wcześniej w pracy naukowej jako student. Pozwólcie mi przedstawić wam liczbę Champernowne'a.

$0 < \Omega = \sum_{p \text{ halts}} 2^{-|p|} < 1$
Émile Borel ---liczby rzeczywiste normalne
Champernowne
.01234567891011121314...99100101...

To idzie w ten sposób. Zapisujecie przecinek i następnie piszecie 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, następnie 10, 11, 12, 13, 14 aż do 99, następnie 100, 101. Kontynuujecie dalej w ten zabawny sposób. To się nazywa liczbą Champernowne'a i Champernowne udowodnił, że jest to liczba normalna w systemie dziesiętnym, tylko w systemie dziesiętnym. Nikt nie wie, czy jest to liczba normalna w innych systemach. Myślę, że jest to wciąż otwarty problem. Chociaż w systemie dziesiętnym nie tylko cyfry od 0 do 9 będą występować z 10% częstotliwością. Każdy możliwy blok dwóch cyfr będzie występować dokładnie z 1% częstotliwością a każdy blok trzech cyfr będzie występować dokładnie z 1% częstotliwością etc.
To nazywa się byciem normalnym w systemie dziesiętnym. Ale nikt nie wie, co się dzieje w innych systemach.

Powód, dla którego o mówię o tym wszystkim jest taki, iż to wynika z faktu, że prawdopodobieństwo zakończenia pracy Ω jest algorytmicznie nieredukowalną informacją, że ta liczba

$$0< \Omega = \sum_{p \text{ halts}} 2^{-|p|} < 1$$

jest normalna w każdym systemie. Łatwo można tego dowieść, korzystając z pojęć dotyczących kodowania i kompresji informacji, która sięga wstecz do Shannona. Zatem mamy w końcu przykład całkowicie normalnej liczby. Nie wiem, co sądzicie na temat tego jak naturalna jest ta liczba, ale jest ona ściśle określoną liczbą rzeczywistą, która pojawia się i jest też normalną w najbardziej pożądanym znaczeniu, jakie Borelowi mogło przyjść do głowy. Liczba Champernowne'a zupełnie nie mogłaby tego wykonać.

Liczba Ω jest faktycznie losowa w wielu innych znaczeniach. Powiedziałbym to w ten sposób. Nie może różnić się od wyniku niezależnych rzutów niezafałszowaną monetą. Faktycznie ta liczba

$$0 < \Omega = \sum_{p \text{ halts}} 2^{-|p|} < 1$$

ukazuje, że macie całkowitą losowość, chaos i nieprzewidywalność oraz brak struktury w czystej matematyce! W ten sam sposób, jak Turing posługując się metodą przekątniową Cantora zniszczył marzenia Hilberta, tak też zapiszcie tylko to wyrażenie

$$0< \Omega = \sum_{p \text{ halts}} 2^{-|p|} < 1$$

a wykaże ono, że są obszary czystej matematyki gdzie dowodzenie jest całkowicie bezużyteczne! To jest właśnie prawdopodobieństwo zakończenia pracy.

Dlaczego to mówię? Cóż, powiedzmy, że chcecie zastosować aksjomaty, aby dowieść, jakie są bity liczby Ω. Już wam mówiłem, że jest ona nieobliczalna---prawda?---jak liczba, którą skonstruował Turing korzystając z metody przekątniowej Cantora. Zatem wiemy, że nie

ma algorytmu, który obliczy cyfrę po cyfrze lub bit po bicie liczbę Ω. Jednak spróbujmy dowieść, jakie są pojedyncze bity Omegi używając formalnego systemu aksjomatycznego. Co się dzieje?

Sytuacja jest bardzo, bardzo zła. To wygląda tak. Przypuśćmy, że macie formalny system aksjomatyczny, który jest *N*-bitowym systemem aksjomatycznym. (Wytłumaczę później, co to dokładnie znaczy). Okazuje się, że w formalnym systemie aksjomatycznym o złożoności *N*, to jest o *N*-bitowej wielkości możecie udowodnić jakie jest położenie i wartość co najmniej $N + c$ bitów Ω.

Co mam na myśli mówiąc o *N*-bitowym formalnym systemie aksjomatycznym? Cóż, pamiętacie, że istotą formalnego systemu aksjomatycznego jest mechaniczna procedura służąca do sprawdzania czy dowód formalny wynika z reguł czy nie. Jest to program komputerowy.

Oczywiście w czasach Hilberta nie było żadnych programów komputerowych ale Turing wynalazł maszyny Turinga, za pomocą których moglibyście ostatecznie sprecyzować dokładnie pojęcie programu komputerowego i na pewno obecnie jesteśmy z tym dobrze obeznani.

Zatem algorytm sprawdzający poprawność dowodu będący istotą formalnego systemu aksjomatycznego, w sensie Hilberta jest programem komputerowym i właśnie widzimy jak wiele bitów posiada ten program.[21] Istotnym jest jak wiele bitów on potrzebuje, aby wyszczególnić reguły gry, postulaty, aksjomaty i reguły wynikania. Jeśli jest to wyrażone w bitach to być może będziecie w stanie udowodnić, powiedzmy, że pierwszym bitem Ω w rozwinięciu binarnym jest 0, drugim bitem jest 1, trzecim bitem jest 0 a następnie może być przerwa i być może będziecie w stanie udowodnić, że tysięcznym bitem jest 1. Lecz będziecie mogli rozstrzygnąć tylko *N* przypadków, jeśli wasz formalny system aksjomatyczny jest *N* -bitowym formalnym systemem aksjomatycznym.

Pozwólcie mi lepiej wytłumaczyć, co mam na myśli. To znaczy, że możecie tylko tyle wyciągnąć, ile wprowadziliście. Jeśli chcecie udowodnić, czy poszczególny bit na określonym miejscu w rozwinięciu binarnym liczby Ω jest 0, czy 1, to w gruncie rzeczy jedynym sposobem, aby to udowodnić jest przyjęcie tego jako hipotezy, jako aksjomatu, jako postulatu. Jest to nieredukowalna matematyczna informacja. To kluczowe określenie naprawdę oddaje całą ideę.

Nieredukowalna matematyczna informacja

$0 < \Omega = \sum_{p \text{ halts}} 2^{-|p|} < 1$

Émile Borel --- liczby rzeczywiste normalne

Champernowne

.01234567891011121314...99100101...

Dobrze, co zatem mamy? To raczej prosty matematyczny obiekt, który kompletnie nam się wymyka. Bity Omegi nie mają żadnej struktury. Nie ma żadnego wzorca, nie istnieje żadna struktura, którą my jako matematycy możemy pojąć. Jeśli jesteście zainteresowani udowodnieniem jakie są pojedyncze bity tej liczby na określonym miejscu, czy to są 0 czy 1, to dowodzenie jest kompletnie bezużyteczne. Jest niestosowne i prowadzi donikąd.

Jak powiedziałem wcześniej, jedynym sposobem, aby z formalnego systemu aksjomatycznego uzyskać te wyniki jest w gruncie rzeczy przyjęcie ich jako założeń, co znaczy, że nie stosujecie dowodzenia. Ostatecznie, cokolwiek może być dowiedzione poprzez przyjęcie tego jako postulat, który dodajecie do waszego zbioru aksjomatów. Zatem jest to najgorszy możliwy przypadek. To jest nieredukowalna matematyczna informacja. Oto jest

[21] Uwaga techniczna: w rzeczywistości najlepiej jest rozważać złożoność formalnego systemu aksjomatycznego jako rozmiar wyrażony w bitach tego programu komputerowego, który wylicza zbiór wszystkich twierdzeń.

przypadek, gdzie nie ma żadnej struktury, nie ma żadnych korelacji, nie istnieje żaden wzorzec, który moglibyśmy dostrzec.

4. Losowość w arytmetyce.

W porządku, ale co to ma wspólnego z losowością w matematyce? Teraz wracamy do Gödla.

Turing mówi, że nie możecie posłużyć się dowodem, aby rozstrzygnąć czy program się zatrzyma. Nie możecie zawsze dowieść, czy program zatrzyma się, czy nie. W ten sposób Turing niszczy marzenia Hilberta o uniwersalnej matematyce. Wpakuję nas w jeszcze większe kłopoty poprzez badanie innego rodzaju zagadnienia, mianowicie, czy potraficie udowodnić, że piątym bitem tej szczególnej liczby rzeczywistej

$$0 < \Omega = \sum_{p \text{ halts}} 2^{-|p|} < 1$$

jest 0, czy 1, lub czy ósmym bitem jest 0, czy 1? Są to dziwnie wyglądające zagadnienia.
Kto kiedykolwiek słyszał o problemie zakończenia pracy w 1936 roku? Nie są to tego rodzaju rzeczy o które normalnie martwią się matematycy. Popadamy w kłopoty, ale z zagadnieniem raczej w dużym stopniu oddalonym od normalnej matematyki.

Chociaż nie możecie mieć formalnego systemu aksjomatycznego, który może zawsze udowodnić, czy program zatrzyma się czy nie, to mógłby być dobry do wszystkiego innego, a zatem moglibyście mieć **ulepszoną** wersję marzenia Hilberta. I tak samo z prawdopodobieństwem zakończenia pracy Ω. Jeśli problem zakończenia pracy wygląda trochę dziwacznie, a z pewnością wyglądał tak w 1936 roku, to cóż, Ω jest nową odmianą i z pewnością też wygląda dziwacznie.
Kto kiedykolwiek słyszał o prawdopodobieństwie zakończenia pracy? To nie jest ten rodzaj rzeczy, którym matematycy normalnie się zajmują. Więc dlaczego przejmuję się tymi wszystkimi wynikami niezupełności?

Cóż, Gödel właśnie stanął przed tym problemem ze swoim stwierdzeniem, które jest prawdziwe, lecz niedowodliwe. Jest to stwierdzenie, które mówi samo o sobie, że jest niedowodliwe. Taki rodzaj rzeczy również nie pojawia się w prawdziwej matematyce. Jednym z kluczowych elementów w dowodzie Gödla jest to, że udało mu się skonstruować **arytmetyczne** stwierdzenie, które mówi samo o sobie, że jest niedowodliwe. Otrzymano owo stwierdzenie, które odwołuje się samo do siebie w elementarnej teorii liczb, co wymagało tak dużo pomysłowości.

Było dużo prac opierających się na pracy Gödla, wykazującej, że problemy dotyczące obliczeń są równoważne arytmetycznym problemom dotyczącym liczb całkowitych. Kilka nazwisk przychodzi mi do głowy. Julia Robinson, Hilary Putnam i Martin Davis wykonali trochę ważnej pracy a następnie kluczowy wynik został znaleziony w 1970 roku przez Jurija Matjasewicza. Skonstruował on równanie diofantyczne, które jest algebraicznym równaniem dotyczącym tylko liczb całkowitych z wieloma zmiennymi. Jedna ze zmiennych, *K*, jest wyróżniona jako parametr. Jest to równanie wielomianowe z całkowitymi współczynnikami i wszystkie niewiadome muszą być liczbami całkowitymi---jest to równanie diofantyczne. Jak mówiłem, jedną z niewiadomych jest parametr. Równanie Matjasewicza ma rozwiązanie dla poszczególnej wartości parametru *K* wtedy i tylko wtedy, gdy *K*-ty program komputerowy zatrzyma się.

W 1900 roku Hilbert pytał o algorytm, który rozstrzygnie czy dane równanie diofantyczne, równanie algebraiczne zawierające tylko liczby całkowite, ma rozwiązanie. To był dziesiąty problem Hilberta. Dziesiąty na jego słynnej liście dwudziestu trzech problemów. To, czego dowiódł Matjasewicz w 1970 roku jest równoważne rozstrzygnięciu czy wybrany losowo program komputerowy zatrzyma się. Zatem Turinga problem zakończenia pracy jest

właśnie tak trudny jak dziesiąty problem Hilberta. Jest dokładnie tak trudno ustalić czy losowo wybrany program komputerowy zatrzyma się, jak rozstrzygnąć czy losowo wybrane równanie algebraiczne zawierające liczby całkowite ma rozwiązanie. Dlatego nie istnieje algorytm umożliwiający wykonanie takiej operacji i dziesiąty problem Hilberta nie może być rozwiązany. Taki był wynik Matjasewicza z 1970 roku.

Matjasewicz kontynuował badania w tej dziedzinie. W szczególności jest fragment pracy, którą wykonywał we współpracy z Jamesem Jonesem w 1984 roku. Mogę posłużyć się nią, aby podążać śladami Gödla. Zobaczcie, wykazałem, że istnieje całkowita losowość, że nie ma żadnego wzoru, żadnej struktury oraz że dowodzenie jest całkowicie bezużyteczne jeśli jesteście zainteresowani poszczególnymi bitami tej liczby.

$$0 < \Omega = \sum_{p \text{ halts}} 2^{-|p|} < 1$$

Podążając za Gödlem przekształćmy to na coś w elementarnej teorii liczb. Albowiem, jeśli popadniecie w kłopoty w elementarnej teorii liczb, która stanowi podstawę, to jest problem. Elementarna teoria liczb, 1, 2, 3, 4, 5..., dodawanie i mnożenie sięga wstecz do starożytnych Greków i jest najbardziej solidną częścią całej matematyki. W teorii zbiorów zajmujecie się dziwnymi obiektami takimi jak duże liczby kardynalne, a tutaj nawet nie zajmujecie się pochodnymi, całkami, czy podzielnikiem, ale tylko liczbami całkowitymi. Korzystając z wyników Matjasewicza i Jonesa z 1984 roku, mogę faktycznie nadać Omedze znaczenie arytmetyczne i uzyskać losowość w elementarnej teorii liczb.

To, co mam tutaj to wykładnicze równanie diofantyczne z parametrem. „Wykładnicze równanie diofantyczne" znaczy po prostu, że dajecie zmienne w wykładnikach. Dla porównania- Matjasewicz, aby udowodnić, że dziesiąty problem Hilberta jest nierozwiązywalny zastosował właśnie wielomianowe równanie wykładnicze, co znaczy, że wykładniki potęg są zawsze stałymi liczbami naturalnymi. Ja musiałem uwzględnić X^Y. Jeszcze nie wiadomo, czy rzeczywiście musiałem to zrobić. To mógł być przypadek, że dałem sobie radę z wykładniczym równaniem diofantycznym. Jest to otwarte pytanie. Sądzę, że jeszcze nie zostało rozstrzygnięte. Ale na chwilę obecną to, co mam to wykładnicze równanie diofantyczne z siedemnastoma tysiącami zmiennych. To równanie ma objętość dwustu stron i ponadto jedną zmienną, którą jest parametr.

To równanie, gdzie każda stała jest liczbą całkowitą, liczbą naturalną i wszystkie te zmienne również są liczbami naturalnymi tj. liczbami całkowitymi dodatnimi (właściwie **nie-ujemnymi** liczbami całkowitymi). Jedną z tych zmiennych jest parametr, zmieniacie jego wartość biorąc kolejno 1, 2, 3, 4, 5.... Następnie pytacie, czy równanie ma skończoną, czy nieskończoną liczbę rozwiązań. Moje równanie jest skonstruowane w ten sposób, że ma skończoną liczbę rozwiązań, jeśli poszczególnym pojedynczym bitem Omegi jest 0 i ma nieskończoną liczbę rozwiązań, jeśli tym bitem jest 1. Rozstrzygając, czy moje wykładnicze równanie diofantyczne w każdym indywidualnym przypadku ma skończoną czy nieskończoną liczbę rozwiązań, jest dokładnie tym samym co wyznaczanie pojedynczego bitu

$$0 < \Omega = \sum_{p \text{ halts}} 2^{-|p|} < 1$$

prawdopodobieństwa zakończenia pracy. Jest to całkowicie niemożliwe ponieważ Omega jest nieredukowalną matematyczną informacją.

Pozwólcie mi podkreślić różnicę między tą pracą a pracą Matjasewicza nad dziesiątym problemem Hilberta. Matjasewicz udowodnił, że istnieje wielomianowe równanie diofantyczne z parametrem posiadającym następujące właściwości: zmieniacie parametr i pytacie czy równanie ma rozwiązanie. Okazuje się, że jest to równoważne Turinga

problemowi zakończenia pracy i dlatego wymyka się potędze matematycznego dowodzenia, formalnego aksjomatycznego dowodzenia.

Czym to się różni od tego, czym ja się zajmuję? Stosuję wykładnicze równanie diofantyczne, co znaczy, że uwzględniam zmienne w wykładnikach. Matjasewicz uwzględnia tylko stałe wykładniki. Wielka różnica jest w tym, że Hilbert pytał o algorytm pozwalający rozstrzygnąć czy równanie diofantyczne ma rozwiązanie. Pytanie, które ja muszę postawić, aby uzyskać losowość w elementarnej teorii liczb, w arytmetyce liczb naturalnych jest odrobinę wyrafinowane. Zamiast pytać czy istnieje rozwiązanie ja pytam, czy jest skończona czy nieskończona liczba rozwiązań.

To bardziej abstrakcyjne pytanie. Ta różnica jest istotna.

Moje dwustustronicowe równanie jest skonstruowane tak, aby miało skończoną lub nieskończoną liczbę rozwiązań w zależności od tego, czy poszczególnym bitem prawdopodobieństwa zatrzymania się jest 0 czy 1. Podczas zmiany parametru otrzymujecie każdy pojedynczy bit Omegi. Równanie Matjasewicza jest tak skonstruowane, aby posiadało rozwiązanie wtedy i tylko wtedy, gdy poszczególny program kiedykolwiek zatrzyma się. Podczas gdy zmieniacie parametr uzyskujecie każdy poszczególny program komputerowy.

A zatem nawet w arytmetyce możecie znaleźć absolutny brak struktury Omegi, Omega jest losowa i jest nieredukowalną matematyczną informacją. Dowodzenie jest zupełnie bezsilne w tych obszarach arytmetyki. Moje równanie ukazuje, że tak jest. Jak powiedziałem wcześniej, aby uzyskać to równanie korzystałem z pomysłów Gödla, które miały początek w oryginalnej pracy naukowej z 1931 roku. Ale to prace naukowe Jonesa i Matjasewicza z 1984 roku dały mi ostatecznie narzędzie, którego potrzebowałem.

Więc dlatego mówię, że jest losowość w elementarnej teorii liczb, w arytmetyce liczb naturalnych. Jest to kamienny mur nie do przebicia, jest to najgorszy przypadek.

Od Gödla wiedzieliśmy, że nie możemy mieć formalnego systemu aksjomatycznego, który byłby zupełny. Wiedzieliśmy, że mamy kłopoty i Turing udowodnił nam jak zasadnicze są, ale Omega jest ekstremalnym przypadkiem, gdzie dowodzenie zawodzi całkowicie.

Nie będę wchodził w szczegóły, ale pozwólcie mi powiedzieć w ogólnikowych informatyczno-teoretycznych terminach. Równanie Matjasewicza daje wam N arytmetycznych pytań z odpowiedziami tak/nie, które wydają się być tylko $\log N$-bitami algorytmicznej informacji.

Moje równanie daje wam N arytmetycznych pytań z odpowiedziami tak/nie, które są nieredukowalną, niekompresowalną matematyczną informacją.

5.Matematyka eksperymentalna.

W porządku, pozwólcie mi powiedzieć trochę więcej w kilka minut, które zostawiłem, aby wytłumaczyć, co to wszystko znaczy.

Przede wszystkim, związek z fizyką. Kiedy rozwinięto mechanikę kwantową pojawił się wielki spór, ponieważ mechanika kwantowa jest niedeterministyczna. Einsteinowi nie podobało się to. Twierdził, że: ”Bóg nie gra w kości!”. Ale jestem pewien, iż wszyscy o tym wiecie, że przy pomocy chaosu i dynamiki nieliniowej zdaliśmy sobie obecnie sprawę, że nawet w klasycznej fizyce jest obecna losowość i nieprzewidywalność. Moja praca ma ten sam charakter. Ukazuje, że czysta matematyka a nawet elementarna teoria liczb 1, 2, 3, 4, 5..., arytmetyka liczb naturalnych jest w takiej samej sytuacji. Również tam mamy losowość. Zatem, jak przedstawiłyby to nagłówki gazet, Bóg gra w kości nie tylko w mechanice kwantowej i klasycznej fizyce, ale także w czystej matematyce, w elementarnej teorii liczb. Jeśli wyłania się nowy paradygmat to losowość jest w jego rdzeniu. Nawiasem mówiąc, losowość jest również w rdzeniu kwantowej teorii pola, jak ukazują jasno wirtualne

cząsteczki i Feynmana suma po historiach. A zatem moja praca pasuje do wielu prac w fizyce i dlatego jestem często zapraszany, aby wygłaszać wykłady na spotkaniach fizyków.

Niemniej jednak, najważniejszą kwestią nie jest fizyka, lecz matematyka. Słyszałem, że Gödel pisał listy do swojej matki, która została w Europie. Wiecie, Gödel i Einstein byli przyjaciółmi w The Institute for Advanced Studies. Zobaczylibyście ich wspólnie spacerujących po ulicy. W każdym razie Gödel pisał listy do swojej matki twierdząc, że chociaż praca Einsteina w dziedzinie fizyki miała naprawdę olbrzymi wpływ na to, w jaki sposób ludzie uprawiają fizykę, to był rozczarowany, że jego własna praca nie miała takiego samego wpływu na matematyków.

Nie stanowiło różnicy, w jaki sposób matematycy właściwie kontynuowali swoją codzienną pracę. Zatem uważam, że jest to kluczowe pytanie: jak naprawdę powinniśmy uprawiać matematykę?

Twierdzę, że mam dużo silniejsze wyniki niezupełności. Jeśli tak, to być może będzie bardziej jasne czy matematyka powinna być uprawiana w zwykły sposób. Jaki jest zwykły sposób uprawiania matematyki? Pomimo faktu, iż każdy wie, że jakikolwiek skończony zbiór aksjomatów jest niezupełny, to właściwie w jaki sposób pracują matematycy? Cóż, załóżmy, że macie przypuszczenie nad którym zastanawiacie się od kilku tygodni i wierzycie w nie, ponieważ przetestowaliście wielką liczbę przypadków na komputerze. Być może jest to przypuszczenie o liczbach pierwszych i od dwóch tygodni usiłujecie je udowodnić. Pod koniec tych dwóch tygodni nie powiecie: „No cóż- oczywiście powodem, dla którego nie mogłem tego udowodnić jest twierdzenie Gödla!" Dlatego pozwólcie nam dodać go jako nowy aksjomat! Ale gdybyście potraktowali twierdzenie Gödla bardzo poważnie, być może faktycznie byłby to sposób podążania naprzód. Matematycy będą się śmiać, ale fizycy rzeczywiście postępują w ten sposób.

Spójrzcie na historię fizyki. Zaczynacie od fizyki newtonowskiej. Nie możecie uzyskać równań Maxwella z fizyki newtonowskiej. To nowa dziedzina doświadczenia. Potrzebujecie nowych postulatów, aby sobie poradzić. Jeśli chodzi o szczególną teorię względności, cóż szczególna teoria względności jest prawie w równaniach Maxwella. Lecz równania Schrödingera nie pochodzą z fizyki newtonowskiej, ani równań Maxwella. To nowa dziedzina doświadczenia i znów potrzebujecie nowych aksjomatów. Zatem fizycy są przyzwyczajeni do idei, że kiedy zaczynacie eksperymentować w mniejszej skali lub z nowymi zjawiskami, to być może potrzebujecie nowych zasad, aby zrozumieć i wyjaśnić co się dzieje.

Obecnie pomimo niezupełności matematycy wcale nie postępują tak jak postępują fizycy. Na podświadomym poziomie nadal zakładają, że ta mała liczba zasad, postulatów i reguł wynikania, których nauczyli się wcześniej - jako studenci matematyki jest wystarczająca. Są oni wewnętrznie przekonani, że jeśli nie mogą dowieść wyników to jest to ich własna wina. Jest to prawdopodobnie dobre podejście, aby winę raczej wziąć na siebie niż obwiniać kogoś innego, ale spójrzmy na takie zagadnienie jak hipoteza Riemanna. Fizyk powiedziałby, że jest dość dowodów eksperymentalnych dla hipotezy Riemanna i kontynuowałby dalej, przyjmując ją jako założenie robocze.

Co to jest hipoteza Riemanna? Jest wiele nierozwiązanych zagadnień dotyczących rozmieszczenia liczb pierwszych, które mogą być rozstrzygnięte, jeśli przyjmiemy hipotezę Riemanna. Korzystając z komputerów ludzie sprawdzają te przypuszczenia i one doskonale działają. Są eleganckimi formułami, ale nikt nie może ich udowodnić. Wiele z nich wynika z hipotezy Riemanna. Dla fizyka to wystarczyłoby: hipoteza jest użyteczna, wyjaśnia wiele danych. Oczywiście fizyk też musiałby być przygotowany aby powiedzieć: "Och, zrobiłem poważny błąd!", ponieważ eksperyment może później stać w sprzeczności z teorią. To się zdarza bardzo często.

W fizyce cząstek elementarnych odrzucacie teorie cały czas i większość z nich szybko ginie. Ale matematykom nie podoba się, gdy muszą się wycofywać. Ale jeśli gracie bezpiecznie problem jest taki, że być może przegrywacie i uważam, że tak właśnie jest.

Sądzę, że powinno być jasne, do czego zmierzam. Uważam, że elementarna teoria liczb i reszta matematyki powinna być uprawiana bardziej w duchu nauki eksperymentalnej oraz, że powinniście być gotowi przyjąć nowe zasady. Uważam, że wypowiedz Euklidesa, iż aksjomat jest prawdą oczywistą samą przez się (selfevident) jest wielką pomyłką. Równanie Schrödingera z pewnością nie jest prawdą oczywistą samą przez się! Hipoteza Riemanna również nie jest oczywista sama przez się, ale jest bardzo użyteczna.

Zatem uważam, że matematycy nie powinni ignorować niezupełności. Jest to bezpieczny sposób postępowania, ale tracimy wyniki, które moglibyśmy zyskać. Byłoby to tak, jakby fizycy powiedzieli: dobrze, żadnych równań Schrödingera, żadnych równań Maxwella, trzymamy się Newtona, wszystko musi być wydedukowane z praw Newtona (Maxwell nawet usiłował to zrobić. Posiadał mechaniczny model pola elektromagnetycznego. Na szczęście nie uczą tego w college'u!)

Proponowałem to wszystko dwadzieścia lat temu, kiedy zacząłem otrzymywać informatyczno-teoretyczne wyniki niezupełności. Lecz niezależnie ode mnie wyłania się nowa szkoła filozofii matematyki, zwana „*quasi*-empiryczną" szkołą myśli dotycząca podstaw matematyki. Jest książka Tymoczko pod tytułem *New Directions in the Philosophy of Mathematics*(Birkhauser, Boston, 1986).To dobry zbiór artykułów. Następną książką do przejrzenia jest *Searching for Certainty* Johna Castiego(Morrow, New York, 1990), która ma dobry rozdział na temat matematyki. Ostatnie pół rozdziału mówi właśnie o *quasi*-empirycznym punkcie widzenia.

Nawiasem mówiąc, Lakatosowi, który był jednym z ludzi zaangażowanych w ten nowy ruch przytrafiło się być w tym czasie w Cambridge. Wcześniej wyjechał z Węgier.

Głównymi szkołami filozofii matematyki na początku tego stulecia były: Russella i Whiteheada pogląd, że logika jest podstawą wszystkiego, szkoła formalistyczna Hilberta i „intuicjonistyczna", konstruktywistyczna szkoła Brouwera. Niektórzy ludzie uważają, że Hilbert wierzył, iż matematyka jest nic nie znaczącą grą atramentowych znaków na papierze. Nie było tak! Hilbert właśnie powiedział, iż aby było absolutnie jasne i wyraźne o czym traktuje matematyka, musimy uszczegółowić zasady określające czy dowód jest poprawny w sposób tak dokładnie sprecyzowany, aby stały się one regułami mechanicznymi. Nikt, kto uważałby, że matematyka jest bez znaczenia, nie byłby tak pełen energii, żeby wykonać tak doniosłą pracę i być tak inspirującym przywódcą.

Początkowo matematycy popierali Hilberta. Nawet po Gödlu i jeszcze bardziej zdecydowanie, gdy Turing udowodnił, że marzenie Hilberta nie spełni się. W praktyce matematycy prowadzili badania jak wcześniej, czyli w duchu Hilberta. Podejście konstruktywistyczne Brouwera uważano w większości za niedogodne. Jeśli chodzi o Russella i Whiteheada to mieli oni dużo problemów z wyprowadzeniem całej matematyki z logiki. Jeśli wyprowadzacie całą matematykę z teorii zbiorów odkryjecie, że przyjemnie jest definiować liczby całkowite w terminach zbiorów (von Neumann pracował nad tym). Ale następnie okazuje się, że jest dużo problemów ze zbiorami.
Nie tworzycie liczb naturalnych w sposób bardziej pewny poprzez oparcie ich na czymś, co jest bardziej problematyczne.

Teraz wszystko jest przewrócone do góry nogami. Jest do góry nogami nie z powodu jakiejś filozoficznej dyskusji, nie z powodu wyników Gödla, wyników Turinga czy moich własnych wyników o niezupełności. Jest do góry nogami z bardzo prostego powodu---komputera!

To komputer zmienił sposób, w jaki wszystko wykonujemy. To komputer niezmiernie zwiększył matematyczne doświadczenie. Tak łatwo jest przeprowadzać matematyczne