Krzysztof Wójtowicz

Teoria obliczeń kwantowych – argument w sporze o aprioryczny status matematyki?

Studia Philosophiae Christianae 45/1, 71-91

2009

Studia Philosophiae Christianae
UKSW
45(2009)1

KRZYSZTOF WÓJTOWICZ
Instytut Filozofii UW, Warszawa

TEORIA OBLICZEŃ KWANTOWYCH – ARGUMENT W SPORZE O APRIORYCZNY STATUS MATEMATYKI?[1]

1. WSTĘP

W niniejszym artykule stawiam problem natury dowodu matematycznego (i ogólniej: natury wiedzy matematycznej) w świetle pewnych teoretycznych wyników współczesnej informatyki, dotyczących tzw. algorytmów kwantowych. Problem ów można sformułować w formie następującego pytania:

- Czy wyniki teoretyczne dotyczące algorytmów kwantowych rzucają nowe światło na filozoficzną dyskusję dotyczącą empirycznych aspektów wiedzy matematycznej?

Temat jest złożony, a więc nawet wstępna prezentacja musi z konieczności być stosunkowo obszerna. Dlatego skupię się tutaj na nakreśleniu niezbędnych preliminariów, ukazaniu tła problemu i jego sformułowaniu, nie zaś na szczegółowej analizie problemu.

2. MATEMATYKA – NAUKA APRIORYCZNA?

Epistemologiczny spór między racjonalizmem a empiryzmem znajduje swoje odbicie w sporze dotyczącym natury wiedzy matematycznej. W tradycji filozoficznej dominuje pogląd, przypisujący jej status

[1] Artykuł został napisany w ramach grantu badawczego *Status wiedzy matematycznej w świetle wyników teorii obliczeń i metamatematyki*, N N101 094136.

wiedzy czysto rozumowej. Często więc wiedza matematyczna bywa określana jako: „wiedza aprioryczna", „uzyskana na drodze czysto rozumowej", „konieczna", „dotycząca prawd wiecznych", „nieempiryczna", „analityczna", „dotycząca bytów idealnych", „prawdziwa we wszystkich możliwych światach" *etc.* Tkwi za nimi pewna wspólna wizja matematyki jako wiedzy czysto racjonalnej, zasadniczo różnej od wiedzy uzyskanej na drodze nauk empirycznych.

Klasycznym przykładem przedstawiciela „treściowej" koncepcji dowodu matematycznego (w myśl której podstawą poznania matematycznego jest zdolność rozumu do ujmowania pewnych fundamentalnych prawd jako oczywistych – i zarazem do akceptowania pewnych kroków dedukcyjnych jako oczywistych) jest Kartezjusz. W myśl jego koncepcji poznanie matematyczne (i nie tylko, ale tu interesuje nas głównie matematyka) stanowi pewien akt o charakterze czysto intelektualnym. Oprócz „widzenia oczyma rozumu" oczywistości prawd musimy także być w stanie wyprowadzić z nich wnioski – ale również tutaj mamy do czynienia z odwołaniami do intuicyjnego postrzegania prawomocności owych operacji. Wizja Kartezjusza jest bardzo odległa od wizji formalistycznej: dowody matematyczne w ujęciu Kartezjusza nie mają charakteru symbolicznych, formalnych manipulacji, lecz ich podstawą jest intuicyjny wgląd.

Warto podkreślić (jest to istotne dla dyskusji dotyczącej natury dowodu matematycznego), że Kartezjusz żąda, aby każdy poszczególny etap dowodu był dla nas absolutnie jasny: „Jeśli w szeregu rzeczy, będących przedmiotem badania, napotyka się coś, czego nasz umysł nie może dość dobrze ująć intuicyjnie, należy przy tym zatrzymać się i nie badać rzeczy następnych, ale powstrzymywać się od daremnej pracy"[2]. Jednak żąda jeszcze czegoś więcej: tego, aby móc dostrzec strukturę dowodu w jednym akcie intelektualnym. Kartezjusz pisze bowiem: „Dla uzupełnienia nauki należy wszystkie i poszczególne rzeczy, które odnoszą się do naszego celu, przeglądnąć ciągłym i nieprzerwanym ruchem myśli i objąć je w dostatecznym i uporządkowanym wyliczeniu"[3]. Taki pogląd jest z pewnością

[2] R. Descartes, *Prawidła kierowania umysłem; poszukiwanie prawdy przez światło przyrodzone rozumu*, tłum. z łac. i franc. L. Chmaj, PWN, Warszawa 1958, 36.

[3] Tamże, 31. Kartezjusz pisze też o rozumowaniach: „Dlatego przebiegnę je kilkakrotnie swego rodzaju ciągłym ruchem wyobraźni, która widzi od razu człony po-

bliski sercu wielu matematyków, którzy podkreślają konieczność rozumienia idei dowodu, a nie jedynie poszczególnych kroków dowodowych. Matematykowi jest o wiele łatwiej zaakceptować dowód, którego strukturę (jako pewnej całości) ogarnia, niż dowód, który postrzega jako ciąg poprawnych kroków, które jednak nie są powiązane pewną wspólną ideą[4].

Poglądy Kartezjusza można uznać za modelowe dla pewnego stylu myślenia o matematyce, wiedzy matematycznej i źródłach tej wiedzy. Podstawową rolę odgrywa w tej wizji posiadanie intelektualnego wglądu – czyli swoistej intuicji matematycznej. Do takiej kategorii intuicji matematycznej, czyli swoistej zdolności poznawczej umożliwiającej wgląd w świat prawd matematycznych, odwoływał się również Gödel[5]. Jest on matematycznym realistą: jego zdaniem, matematyczna rzeczywistość jest od nas niezależna, nie jest bynajmniej wytworem naszego intelektu. Gödel zdecydowanie odrzuca więc psychologistyczne interpretacje matematyki. Rzeczywistość

---

szczególne w chwili, gdy do innych przechodzi, aż się nauczę od pierwszego stosunku do ostatniego tak szybko przechodzić, iż będę mógł niemal zupełnie bez pomocy pamięci objąć jednym spojrzeniem całość" (tamże, 31–32).

[4] O. Bassler w pracy *The surveyability of mathematical proof: a historical perspective*, Synthese (2006)148, 99–133, analizuje problem, czy dowody matematyczne dają się „ogarnąć", rozróżniając „ogarnialność lokalną" (oczywistość poszczególnych kroków) od globalnej (oczywistość rozumowania jako całości, które intuicyjnie ujmujemy). Postulat globalnej ogarnialności dowodów matematycznych przypisuje właśnie Kartezjuszowi. O *Cartesian story* pisze także Fallis w pracy *Intentional gaps in mathematical proofs*, Synthese (2003)134, 45–69 – nazywając tak koncepcję, w myśl której dowody matematyczne są pozbawione luk, zaś matematyk jest w stanie ująć wszystkie kroki dowodowe.

[5] Mówi o tym wyraźnie w następującym fragmencie: „Pomimo ich [obiektów teorii mnogości – K.W.] oddalenia od danych zmysłowych mamy coś w rodzaju percepcji obiektów teorii mnogości, co widać z faktu, że aksjomaty narzucają się nam jako prawdziwe. Nie widzę powodu, aby mieć mniej zaufania do tego rodzaju percepcji, tj. do intuicji matematycznej, niż do percepcji zmysłowej, która pozwala nam budować teorie fizyczne, w oczekiwaniu, że przyszłe dane zmysłowe będą z nią zgodne, i co więcej oczekiwać, że problem, który teraz nie jest rozstrzygalny, jest mimo to sensowny i może zostać rozstrzygnięty w przyszłości". K. Gödel, *What is Cantor's Continuum Problem?*, w: *Philosophy of Mathematics*, red. P. Benacerraf, H. Putnam, Prentice–Hall, Englewood Cliffs, New Jersey 1964, 258–273, 271.

matematyczną możemy poznawać i opisywać, zaś dostęp poznawczy do owej obiektywnej sfery bytów matematycznych zapewnia nam właśnie intuicja matematyczna – swoista zdolność naszego umysłu. Dzięki temu pewne zdania matematyczne możemy uznać za pierwotne, podstawowe prawdy.

Nie ma tu miejsca na szczegółową analizę stanowiska Gödla, w szczególności tego, jak doszedł do swej silnej i radykalnej formy matematycznego platonizmu. Warto jednak wspomnieć, że Gödel przyjmuje swoisty postulat o charakterze metodologicznym, w myśl którego dopuszczalne (a nawet konieczne!) jest wzmacnianie założeń, tworzenie coraz silniejszych systemów pozwalających na rozwiązywanie otwartych (a nierozwiązywalnych słabszymi środkami) problemów. Należy przy tym podkreślić, że nie chodzi tutaj wyłącznie o formalne wyprowadzanie wniosków w danych systemach aksjomatycznych. Rozwiązywanie problemów może polegać także na poszukiwaniu coraz silniejszych aksjomatów, wykraczających poza dotychczas przyjmowane formalizmy. Jest to możliwe dzięki odwołaniu do intuicji matematycznej. Gödel pisze więc, że „zdania teorioliczbowe nierozstrzygalne w danym formalizmie są zawsze rozstrzygalne przez oczywiste wnioskowania niewyrażalne w danym formalizmie. Jeśli chodzi o te nowe wnioskowania, to okazują się one być równie oczywiste jak te, które dane są wewnątrz formalizmu. Nie jest więc raczej możliwe sformalizowanie rozumowań matematycznych nawet w dziedzinie teorii liczb, jednak przekonanie, o którym mówi Hilbert pozostaje nienaruszone”[6].

Gödel twierdzi, że nasza intuicja podlega rozwojowi. Dzięki temu możemy coraz lepiej rozumieć sens pojęć matematycznych i ustanawiać nowe aksjomaty[7]. Można więc mówić o swoistej otwartości (niewyczerpalności) naszej intuicji, która pozwala nam

[6] K. Gödel, *Undecidable diophantine propositions*, w: *Collected Works*, vol.3., red. S. Feferman i. in., Oxford University Press 1995, 164–175. Gödel nawiązuje tutaj do optymistycznych stwierdzeń Hilberta, w myśl których w matematyce nie ma problemów zasadniczo nierozwiązywalnych.

[7] W tym kontekście mówi się niekiedy o programie Gödla. Sam Gödel poszukiwał aksjomatów, które miałyby pomóc w rozwiązaniu hipotezy continuum. Por. np. K.Wójtowicz, *O tzw. programie Gödla*, Zagadnienia Filozoficzne w Nauce XXVIII–XXIX(2001), 100–117.

na intuicyjne ujęcie pewnych treści wymykających się formalizmom. Przy dyskusji tego problemu Gödel odwołuje się do udowodnionych przez siebie twierdzeń. Przypomnijmy, że zgodnie z II twierdzeniem Gödla nie można udowodnić niesprzeczności arytmetyki w niej samej (dotyczy to również teorii silniejszych od arytmetyki, które spełniają pewne warunki techniczne)[8]. Posługując się standardowymi oznaczeniami (por. ostatni przypis), II twierdzenie Gödla mówi, że Con(PA) jest niedowodliwe wewnątrz PA. Zarazem jednak mamy silne poczucie prawdziwości owego zdania: skoro stwierdza ono, że PA jest niesprzeczna, a jest w PA niedowodliwe, to znaczy, że **naprawdę** PA jest niesprzeczna (bo gdyby PA była sprzeczna, to dałoby się w niej udowodnić każde zdanie, w szczególności zdanie Con(PA)). Intuicyjnie postrzegamy więc prawdziwość zdania Con(PA), choć owej prawdziwości nie możemy formalnie udowodnić. Intuicja prowadzi nas zatem do sformułowania nowej teorii: dołączamy do PA jako nowy aksjomat zdanie Con(PA), otrzymując teorię T=PA+Con(PA). Ową teorię T postrzegamy intuicyjnie jako nie mniej wiarygodną od teorii PA[9]. Skoro zaś teorię T uznajemy za nie mniej wiarygodną niż PA, to również zdanie Con(T) powinniśmy uznać za nie mniej wiarygodne od (już wcześniej zaakceptowanego) zdania Con(PA). Jednak zdanie Con(T) nie jest dowodliwe w ramach teorii T (zgodnie z II twierdzeniem Gödla, gdyż stosuje się ono nie tylko do PA, ale również do teorii silniejszych). Powtarzając rozumowanie, które przeprowadziliśmy w stosunku do zdania Con(PA), możemy również zdanie Con(T) uznać za nie mniej wiarygodne od teorii

[8] Dalej będziemy się posługiwać skrótem PA dla arytmetyki (od *Peano Arithmetic*), zaś zdanie wyrażające niesprzeczność arytmetyki oznaczać przez Con(PA). W ogólnym wypadku teorii T, zdanie wyrażające jej niesprzeczność oznaczamy przez Con(T). Nie wnikam tu w szczegóły techniczne dotyczące kodowań, arytmetyzacji składni *etc.*, należy jednak podkreślić, że dzięki tej procedurze możliwe jest wyrażanie metamatematycznych faktów dotyczące PA **wewnątrz** PA (bo tylko wtedy jest sens stawiać pytanie, czy Con(PA) daje się udowodnić w PA).

[9] Intuicyjnie: jeśli uznamy teorię PA za niesprzeczną, to mamy prawo do PA dołączyć zdanie wyrażające jej niesprzeczność. Sęk w tym, że to zdanie Con(PA) nie jest twierdzeniem PA, a nowym, silniejszym aksjomatem. Jednak na poziomie intuicji mamy pełne prawo ów nowy aksjomat dołączyć.

T. Tym samym teorię T_1 = T+Con(T) możemy uznać za równie wiarygodną, co T. Taka argumentacja stosuje się również do kolejnych teorii z ciągu teorii: $T_2=T_1+Con(T_1)$, $T_3=T_2+Con(T_2)$ *etc.* Za każdym razem odwołujemy się do naszej intuicji, która pozwala nam dostrzec intuicyjny sens i wiarygodność owych zdań. Te rozważania pokazują, iż systemy formalne nie są w stanie adekwatnie uchwycić naszych przekonań – zawsze bowiem możemy odwołać się do pozateoretycznego, intuicyjnego rozumienia sensu pojęć matematycznych.

Gödel w wyraźny sposób wpisuje się więc w nurt tradycji racjonalistycznej. W takim duchu formułowane są też jego argumenty na rzecz matematycznego realizmu. Abstrahują one całkowicie od problemu zastosowań matematyki w naukach empirycznych. Zaś kryteria prawdziwości zdań matematycznych nie mają nic wspólnego z empirią – prawdy matematyczne i prawdy empiryczne mają bowiem inne źródła i dotyczą innych sfer rzeczywistości. „Wypowiedź matematyczna nie mówi nic na temat fizycznej ani psychicznej rzeczywistości istniejącej w przestrzeni i czasie, ponieważ jest prawdziwa już na mocy znaczeń występujących w niej pojęć, niezależnie od świata rzeczy”[10]. Rola matematyki w procesie tworzenia wiedzy fizycznej (z której oczywiście Gödel sobie doskonale zdawał sprawę) nie ma znaczenia z punktu widzenia argumentacji Gödla[11]. Wiedza matematyczna zaś zdobywana jest na drodze czysto intelektualnych aktów.

[10] K. Gödel, *Some basic theorems on the foundations of mathematics and their implications*, w: *Collected Works*, vol.3., dz. cyt., 304–323, 320.

[11] Gödel twierdzi wprost: „Można powiedzieć, że 99,9% współczesnej matematyki zawiera się w pierwszych trzech szczeblach hierarchii mnogościowej. A zatem z praktycznego punktu widzenia, cała matematyka może zostać zredukowana do skończonej ilości aksjomatów. Jest to jednak jedynie pewien historyczny zbieg okoliczności (*historical accident*), który nie ma znaczenia dla samej zasady”. K. Gödel, *Some basic theorems on the foundations of mathematics and their implications*, art. cyt., 304–323, 307.

3. WĄTKI EMPIRYSTYCZNE

Wizji matematyki Kartezjusza czy Gödla nie mogą oczywiście zaakceptować empiryści. Nie przypisują oni rozumowi statusu odrębnej władzy poznawczej, która daje nam wiedzę niezależną od empirycznych źródeł. Dotyczy to w szczególności również wiedzy matematycznej. Ich zdaniem, ta wiedza musi być w pewien (choćby pośredni) sposób ugruntowana w doświadczeniu zmysłowym. Do przyjęcia poglądu o takich empirycznych źródłach wiedzy matematycznej może nas skłaniać istnienie głębokich związków między matematyką a naukami empirycznymi, dla których matematyka stanowi potężne narzędzie. Należy pamiętać o tym, że tworzenie nowych pojęć, koncepcji i teorii matematycznych miało silny związek z rozwojem fizyki (oczywistym przykładem jest rachunek różniczkowy i całkowy). Te obserwacje prowadzą nas w naturalny sposób do pytania o empiryczne aspekty wiedzy matematycznej.

Skrajnym przykładem matematycznego empirysty był Mill, który uważał matematykę za wiedzę empiryczną, zawierającą uogólnienia wyników obserwacji. I tak na przykład prawa arytmetyki – zdaniem Milla – wyrastają z codziennej praktyki liczenia przedmiotów. Geometria zaś dotyczy po prostu fizycznych własności naszej przestrzeni fizycznej, a jej źródłem jest obserwacja. Oczywiście wszelkie obserwacje są obarczone błędem – ale stosujemy idealizacje i abstrahujemy od nieistotnych własności badanych przedmiotów. W trakcie tworzenia wiedzy matematycznej dokonujemy uogólnień, w wyniku których zapominamy o pierwotnych źródłach naszej wiedzy i zaczynamy sądzić, że wiedza ta ma charakter aprioryczny. Wiedza matematyczna ma jednak charakter wiedzy empirycznej i tym samym nie może mieć charakteru wiedzy apriorycznej, pewnej i czysto racjonalnej.

Stanowisko Milla jest skrajne, jednak oczywiście nurt empirystyczny w matematyce ma reprezentantów, których stanowiska są znacznie lepiej uzasadnione. Przykładem jest Quine. Jest on konsekwentnym empirystą. W myśl jego koncepcji, punktem wyjścia w procesie tworzenia naszej wiedzy są dane zmysłowe, które następnie są poddawane „teoretycznej obróbce", aby uzyskać możliwie spójny obraz świata. W tym porządkowaniu danych odwołujemy się do mechanizmu postulowania istnienia przedmiotów – przykładem

jest postulowanie istnienia przedmiotów fizycznych jako źródeł naszych wrażeń. Zakładamy przecież, że podobne wrażenia zmysłowe wiążą się z tym samym, obiektywnie istniejącym i trwającym w czasie przedmiotem. Procedura reifikacji umożliwia nam stworzenie prostszego i operatywnego obrazu świata[12].

Quine posługuje się metaforą sieci, do której porównuje system naszych przekonań o świecie. Poszczególne zdania tego systemu tworzą coś w rodzaju węzłów w tej sieci – i dotyczy to zarówno zdań obserwacyjnych, jak i takich, które zawierają terminy teoretyczne i matematyczne. Można więc powiedzieć, że również wiedza matematyczna stanowi fragment takiego całościowego systemu przekonań (ugruntowanego w empirii)[13].

Zabieg reifikacji ma miejsce na każdym poziomie tworzenia wiedzy – w przypadku wiedzy zdroworozsądkowej postulujemy istnienie przedmiotów makroskopowych, w przypadku wiedzy naukowej postulujemy istnienie przedmiotów teoretycznych, ale też – i to należy podkreślić – przedmiotów matematycznych. Takie wzbogacanie ontologii występuje na każdym etapie tworzenia naszej wiedzy, zaś ostatecznym kryterium przyjęcia danej teorii jest jej zgodność (od-

[12] Wygodniejszy jest np. obraz fizykalistyczny niż fenomenalistyczny – i dlatego wybieramy ten pierwszy. Quine pisze o tym tak: „Łącząc oddzielne doznania zmysłowe i traktując je jako percepcję jednego przedmiotu, ujmujemy bogactwo naszych doznań w prostym i operatywnym schemacie pojęciowym. Przyporządkowywanie danych zmysłowych przedmiotom zewnętrznym jest (...) podyktowane zasadą prostoty: wcześniejsze i późniejsze wrażenie okrągłości łączymy z tą samą monetą lub z dwiema różnymi monetami, kierując się postulatem maksymalnej prostoty naszego całościowego obrazu świata". W. van O. Quine, *O tym, co istnieje*, w: Z *punktu widzenia logiki*, tłum. z ang. B. Stanosz, PWN, Warszawa 1969, 31.

[13] „Całokształt naszej tzw. wiedzy czy też przekonań, od najbardziej przypadkowych prawd geografii i historii aż po najgłębsze prawa fizyki atomistycznej, a nawet czystej matematyki i logiki formalnej, jest tworem człowieka i styka się z doświadczeniem tylko wzdłuż swoich krawędzi. Mówiąc inaczej, nauka jako całość podobna jest do pola siły, którego warunkami brzegowymi jest doświadczenie. Konflikt z doświadczeniem na brzegach pola powoduje odpowiednie przystosowania w jego wnętrzu. (...) Żadne poszczególne świadectwo doświadczenia nie jest związane z jakimś określonym zdaniem z wnętrza pola; związek ten ma co najwyżej charakter pośredni, za sprawą równowagi pola jako całości". W. van O. Quine, *Dwa dogmaty empiryzmu*, w: Z *punktu widzenia logiki*, dz. cyt., 65.

powiednie teoretyczne dopasowanie koncepcji) z doświadczeniem (czyli ze strumieniem wrażeń zmysłowych). Oznacza to w szczególności, że kryteria istnienia przedmiotów wykraczają poza obserwowalność[14]. Dotyczy to także przedmiotów matematycznych i ma istotne znaczenie z punktu widzenia dyskusji ontologicznej. Quine twierdzi, że skoro w przyjmowanych przez nas teoriach występują zdania stwierdzające istnienie obiektów matematycznych, to trzeba konsekwentnie przyjąć istnienie obiektów matematycznych[15].

Z punktu widzenia tematyki niniejszego artykułu należy zwrócić uwagę na fakt, że w myśl koncepcji Quine'a wiedzy matematycznej nie można oczywiście uznać za wiedzę aprioryczną. Punktem wyjścia naszej wiedzy są dane zmysłowe: one podlegają owej „teoretycznej obróbce", w której w szczególności pojawiają się wypowiedzi dotyczące matematyki. Wiedza matematyczna wyrasta zatem – w pośredni sposób – z doświadczenia empirycznego, a nie z żadnego czysto intelektualnego oglądu. Należy tu też podkreślić, że Quine przypisuje status **wiedzy** właśnie (a nie jedynie status niezinterpretowanego systemu formalnego) tylko tym fragmentom matematyki, które mają zastosowanie w naukach empirycznych[16].

4. ALGORYTMY KWANTOWE

Nie ulega oczywiście wątpliwości, że matematyka jest niezbędna dla zdobywania wiedzy fizycznej. Pojawia się jednak pytanie niejako odwrotne: czy wiedza fizyczna może być przydatna w zdobywaniu wiedzy matematycznej? Uszczegółowiając, zapytajmy: czy może-

[14] „Przedmioty fizyczne są pojęciowo wnoszone do sytuacji jako wygodne ogniwa pośredniczące – nie przez definiowanie ich w terminach doświadczenia, lecz jako nieredukowalne byty postulowane". Tamże, 67.

[15] Quine odwołuje się do tzw. kwantyfikatorowego kryterium istnienia. W szczególności nie różnicuje sposobów istnienia, odrzuca więc wyjaśnienia statusu ontycznego obiektów matematycznych odwołujące się do takich rozróżnień.

[16] Podstawą argumentu z niezbędności Quine'a są dwa założenia: (1) ontologia teorii naukowych winna być przyjmowana w całości na podstawie kryterium kwantyfikatorowego; (2) matematyka jest niezbędna w naukach empirycznych (czyli nie jest możliwe takie sformułowanie teorii empirycznych, w których brak byłoby odniesień do obiektów matematycznych).

my wykorzystać prawa fizyki, aby wspomagały nas w zdobywaniu nowej wiedzy matematycznej? Chcę tu zwrócić uwagę na pewne istotne w kontekście tego zagadnienia punkty, związane z dowodami komputerowymi oraz z tzw. kwantową teorią obliczeń.

Postawione tu pytanie wiąże się z problemem standardów matematycznej argumentacji – kiedy uznamy ją dostatecznie przekonującą, aby na jej podstawie przyjąć nowe twierdzenie? Takie sformułowanie pytania może wydać się nieco zaskakujące: przecież badane w teorii dowodu pojęcie dowodu formalnego jest jasne i klarowne: jest to stosowny (najczęściej skończony) ciąg formuł $\alpha_1,...,\alpha_n$, taki, że... (tu następuje wyliczenie stosownych reguł wnioskowania charakteryzujących dany system logiczny). Oczywiście w takim rozumieniu pojęcia dowodu nie ma miejsca na odwołania do intuicji w sensie Kartezjusza czy Gödla, wyeliminowane są czynniki subiektywne. Na dowód patrzymy jak na obiekt czysto syntaktyczny, o jego prawomocności decyduje wyłącznie zgodność z regułami składniowymi, zaś w trakcie prowadzenia samego dowodu nie jest konieczny żaden wgląd w treść operacji.

Jednak taka wizja dowodu matematycznego jest odległa od codziennej praktyki matematycznej. Dowody, jakie znamy z wykładów czy publikacji naukowych, są oczywiście ścisłe, precyzyjne, pozbawione luk. Jednak nie są to dowody formalne w rozumieniu teorii dowodu. Dowód formalny jest raczej pewną idealizacją standardowego pojęcia dowodu. Mamy oczywiście przekonanie, że jest to poprawna idealizacja – tzn. że każdy standardowy dowód matematyczny daje się sformalizować w odpowiednim języku formalnym (przy czym takie najogólniejsze ramy dopuszczalnej formalizacji – przynajmniej standardowo – wyznacza teoria mnogości ZFC). Pojawia się jednak zasadne pytanie: kiedy powinniśmy zaakceptować dany (niesformalizowany) dowód matematyczny jako przekonujący?[17] A jeszcze inaczej: jakie argumenty matematyczne są przekonujące? I gdzie są granice **matematycznej** argumentacji? Kiedy mamy prawo uznać, że faktycznie wzbogaciliśmy naszą wiedzę matematyczną o nowe,

[17] Odpowiedź, iż powinniśmy uznać za „legalne" takie dowody, które dają się sformalizować, niewiele mówi: skąd bowiem mamy wiedzieć, czy dowód daje się sformalizować, nie formalizując go faktycznie? Chodzi nam o podjęcie takiej decyzji **bez** faktycznego formalizowania dowodu.

właśnie udowodnione twierdzenie? Problem ten z punktu widzenia klasycznej koncepcji matematyki jako wiedzy czysto apriorycznej ma dobrze określone rozwiązanie (w duchu kartezjańsko-gödlowskim): to nasz intelektualny wgląd pozwala nam na akceptację danego dowodu jako poprawnego[18]. Trudno uznać takie rozwiązanie za bezdyskusyjne – rozumienie dowodu matematycznego podlegało bowiem pewnej ewolucji i precyzacji, i dziś kładziemy większy nacisk raczej na jego formalną poprawność niż na nasze intuicje[19].

Problem granic dopuszczalnej matematycznej argumentacji nabiera szczególnej aktualności w związku z praktycznymi i teoretycznymi osiągnięciami informatyki. Standardowym przykładem problemu, jaki pojawia się w kontekście tych dyskusji, jest zagadnienie czterech barw. Chodzi o postawione już w 1852 roku przez Francisa Guthrie pytanie, czy każdą mapę można pokolorować czterema kolorami tak, aby żadne dwa sąsiadujące państwa nie były tego samego koloru. Hipoteza czterech barw głosi, że tak właśnie jest. Przez wiele lat uzyskiwano wyniki cząstkowe, dotyczące ograniczonej ilości państw; dowód ogólny potwierdzający hipotezę podano dopiero w roku 1976[20].

---

[18] Oczywiście nie w takim naiwnym sensie, że matematyk patrzy na dowód, zamyka oczy i oto nagle przeszywa go intuicyjne poczucie jego poprawności. Konieczne jest prześledzenie całego toku rozumowania, wszystkich poszczególnych kroków dowodowych *etc*. Jednak na poziomie tych analiz odwołujemy się do pewnych czysto apriorycznych zasad, a ostatecznie musimy zgodzić się na prawomocność pewnych kroków argumentacyjnych.

[19] Problemowi tej ewolucji rozumienia pojęcia dowodu matematycznego poświęcone są prace: K. Wójtowicz, *Dowód matematyczny z punktu widzenia formalizmu matematycznego. I*, Roczniki Filozoficzne 55(2007)2, 123–138; tenże: *Dowód matematyczny z punktu widzenia formalizmu matematycznego. II*, Roczniki Filozoficzne 55(2007)2, 139–153.

[20] K. Appel, W. Haken, *Every planar map is four colorable, part I: discharging*, Illinois Journal of Mathematics 21(1977), 429–490; K. Appel, W. Haken, J. Koch, *Every planar map is four colorable, part II: reducibility*, Illinois Journal of Mathematics 21(1977), 491–567. Twierdzenie o czterech barwach nie jest jedynym, które zostało udowodnione za pomocą komputera, ale ograniczę się do tego przykładu, gdyż jest dostatecznie klarowny (i ten właśnie przykład jest najczęściej przywoływany w dyskusjach filozoficznych).

Dowód Appela, Hakena i Kocha wpisywał się w dotychczasowy nurt badań, korzystając z technik wypracowanych przez zmagających się z problemem matematyków. Miał jednak szczególny charakter – w nieuchronny sposób odwoływał się do wyników obliczeń komputera. Okazało się bowiem, że twierdzenie o czterech barwach można udowodnić w ten sposób, że sprawdzi się zachodzenie pewnego warunku dla bardzo wielu szczególnych przypadków (w pierwszej wersji blisko 1500) – a w każdym z tych przypadków obliczenia były(by) zbyt żmudne i skomplikowane, aby można je było kiedykolwiek przeprowadzić ręcznie. Pierwszy program komputerowy wymagał około 1200 godzin pracy komputera. Później algorytmy zostały poprawione, a komputery stały się szybsze – nie zmienia to jednak faktu, że wykonanie tej pracy jest poza zasięgiem człowieka.

Nie ulega wątpliwości, że w takim dowodzie odwołujemy się do wyniku działania pewnego elektronicznego urządzenia – a więc do wyniku pewnego eksperymentu fizycznego. Pojawia się tu szereg naturalnych pytań o charakterze filozoficznym i metodologicznym: Czy faktycznie dysponujemy dowodem twierdzenia o czterech barwach? Czy komputerowy dowód twierdzenia o czterech barwach stanowi nowy rodzaj dowodu matematycznego? Czy twierdzenie o czterech barwach jest nowym typem twierdzenia matematycznego, zaś wiedza o 4–barwności map stanowi nowy typ wiedzy matematycznej?

Entuzjaści dowodów komputerowych skłonni są udzielić odpowiedzi pozytywnej na pierwsze, a negatywnej na pozostałe pytania. Ich zdaniem, dowód komputerowy nie niesie w sobie żadnej specyfiki – nie różni się co do swej istoty niczym od dowodu za pomocą kartki i ołówka. Znamy bowiem zasadę działania komputera (podobnie jak znamy zasadę działania kartki i ołówka – np. wiemy, że kartka samodzielnie nie dopisuje żadnych znaków). Dowód komputerowy jest całkowicie przejrzysty – wiemy, co się dzieje w dowolnym momencie obliczenia (a w każdym razie potencjalnie możemy się tego dowiedzieć, przeglądając wydruk). Dowód komputerowy jest nawet lepszy niż dowód ludzki – bo komputery rzadziej się mylą w obliczeniach. W tym więc sensie dowód komputerowy nie niesie w sobie żadnej nowej jakości; zaś pojawienie się tego typu dowodu nie ma żadnego znaczenia z punktu widzenia dyskusji dotyczącej apriorycznej *versus* empirycznej genezy i natury matematyki.

A gdyby uznać, że użycie komputera ma znaczenie dla tej dyskusji, to konsekwentnie należałoby uznać, że również użycie ołówka ma takie znaczenie.

Z kolei przeciwnicy uznania dowodów komputerowych za pełnoprawne dowody matematyczne wskazują na fakt, że nasz dostęp do zachowania komputera istotnie się różni od dostępu do zachowania kartki i ołówka. Wprawdzie mamy silnie potwierdzone hipotezy dotyczące działania komputera (opieramy się tutaj na naszym zaufaniu do praw fizyki i techniki, w szczególności elektroniki), jednak oczywiście nie jesteśmy w stanie z całą pewnością stwierdzić, jak przebiega obliczenie. Nie możemy przecież przejrzeć całości obliczeń. Nasze zaufanie do twierdzenia o czterech barwach nie może więc być większe niż zaufanie do praw fizyki. To jednak powoduje, że oto nagle twierdzenie matematyczne przestaje mieć charakter aprioryczny, a staje się hipotezą empiryczną potwierdzaną w wyniku pewnego testu (a właściwie wielu testów). Nie możemy mieć jednak całkowitej pewności, którą powinniśmy mieć w przypadku wiedzy apriorycznej.

Niezależnie jednak od tego, co sądzimy na temat twierdzenia o czterech barwach, uważam, że istotna jakościowa zmiana w dyskusji pojawia się, kiedy zaczniemy rozważać problematykę algorytmów kwantowych. Przypuśćmy bowiem – na potrzeby dyskusji – że uznajemy argumentację zwolennika dowodu o czterech barwach za przekonującą: wprawdzie faktycznie nie sprawdzamy obliczeń krok po kroku (bo w końcu po to mamy komputer, aby nie musieć tego robić), to jednak w przypadku wątpliwości możemy przejrzeć dowolnie wybrany fragment dowodu. Można powiedzieć swobodnie, że w dowolnym momencie możemy zatrzymać komputer i zajrzeć do środka. Wygodnie w tym kontekście mówić o teoretycznym modelu komputera, czyli o maszynie Turinga[21]. Wprawdzie nie śle-

[21] Maszynę Turinga można wyobrażać sobie jako potencjalnie nieskończoną taśmę, na którą „patrzy" głowica. Głowica może odczytać z taśmy symbol, zastąpić go innym i wykonać ruch; może przy tym nastąpić zmiana stanu wewnętrznego maszyny. Krok działania maszyny Turinga można zatem symbolicznie przedstawić jako przejście: $(q_i, s_j) \rightarrow (q_k, s_l, R)$, gdzie q – stan wewnętrzny, s – symbol, R – ruch w lewo lub ruch w prawo lub pozostanie na miejscu. Maszyna Turinga wykonuje kolejne kroki tej postaci, aż do zatrzymania się maszyny – wtedy na taśmie znajduje

dzimy wszystkich kroków obliczenia maszyny Turinga dowodzącej twierdzenia o czterech barwach, ale przecież w każdej chwili możemy maszynę zatrzymać, sprawdzić jej stan wewnętrzny i następnie dalej puścić w ruch. Sytuacja wygląda jednak inaczej w przypadku algorytmów kwantowych.

Zanim przejdę do omówienia tego modelu obliczeń, zauważmy, że przy algorytmicznym rozwiązywaniu problemów podlegamy pewnym ograniczeniom o charakterze praktycznym: po prostu niektóre problemy, które teoretycznie dają się rozwiązać za pomocą komputera (tzw. problemy rozstrzygalne), wymagają zbyt wiele czasu, aby **faktycznie** takie obliczenie przeprowadzić. Standardowy przykład (jeden z wielu tego typu) to problem sprawdzania, czy dana formuła klasycznego rachunku zdań jest tautologią. Metoda zerojedynkowa (tabelkowa) jest bardzo prosta z pojęciowego punktu widzenia: po prostu trzeba obliczyć wartość logiczną tej formuły dla wszystkich wartościowań. Algorytm sprawdzający tautologiczność musiałby więc obliczać wartość logiczną formuły dla kolejnych wartościowań. Jednak algorytm ten ma wykładniczą złożoność: dla formuł zawierających n zmiennych musimy sprawdzić 2^n wartościowań. Dla n=10 jest to 1024, jednak dla n=300 ilość przypadków przekracza ilość cząstek elementarnych we wszechświecie. A więc choć algorytm sprawdzania tautologiczności jest pojęciowo bardzo prosty, to z praktycznych powodów nie jest on użyteczny dla bardziej skomplikowanych formuł.

Tu warto wspomnieć o problemie, który okazał się bardzo inspirujący dla kwantowej teorii obliczeń – a mianowicie problemie faktoryzacji, czyli rozkładu liczby na czynniki pierwsze. Jest oczywiste, że znacznie łatwiej jest pomnożyć dwie liczby przez siebie (np. 17 i 23) niż znaleźć czynniki pierwsze np. liczby 391. W ogólnym przypadku, czas potrzebny na przeprowadzenie rozkładu liczby na czynniki pierwsze wykładniczo zależy od rozmiaru tej liczby. Z obliczeniowego punktu widzenia problem faktoryzacji jest problemem trudnym (złożonym). Ten fakt wykorzystywany jest w krytografii i dzięki niemu możemy bezpiecznie kodować informacje.

---

się wynik obliczenia (niekiedy maszyna się nie zatrzymuje, tylko prowadzi obliczenie w nieskończoność, czyli „pętli się").

W roku 1994 Peter Shor podał algorytm, który jest w stanie szybko rozłożyć daną liczbę na czynniki pierwsze. Jednak nie był to algorytm klasyczny, ale algorytm kwantowy. Nie da się go zaimplementować na zwykłym komputerze, wymagałby on komputera kwantowego (który na razie nie został jeszcze skonstruowany). Algorytm kwantowy – jak sama nazwa wskazuje – odwołuje się do praw mechaniki kwantowej. Postaram się w uproszczony sposób wyjaśnić istotę tego modelu obliczeń.

Podstawowym pojęciem klasycznej teorii obliczeń (lub teorii informacji) jest bit – czyli jednostka informacji. Bit może przyjmować jeden z dwóch stanów 0 lub 1. Kwantowym odpowiednikiem bitu jest tzw. kubit. W przeciwieństwie do klasycznych bitów (które przyjmują **tylko** jedną z dwóch wartości 0 lub 1), specyfika świata kwantowego pozwala kubitom znajdować się również w tzw. superpozycji stanów 0 i 1 – czyli pewnej ich kombinacji (typ tej kombinacji jest opisany przez dwa współczynniki α i β). Jeśli zatem stany 0 i 1 wyróżnimy jako tzw. stany bazowe (często zapisujemy je w postaci $|0\rangle$ oraz $|1\rangle$), to każdy kubit można zapisać w postaci kombinacji $\alpha|0\rangle+\beta|1\rangle$. Trudno podać intuicje, które kryją się za takim opisem, gdyż współczynniki α oraz β są liczbami zespolonymi. Spełniają one dodatkowo warunek $|\alpha|^2+|\beta|^2=1$ (gdzie $|z|$ oznacza moduł danej liczby zespolonej z[22]). Warunek ten związany jest z postulatem dotyczącym pomiaru kwantowego, o którym wspomnę później. Z punktu widzenia teorii obliczeń ważne jest natomiast to, że aby opisać stan jednego kubitu, musimy podać dwa parametry, będące liczbami zespolonymi[23].

---

[22] Ów moduł liczby zespolonej to po prostu długość wektora (liczba zespolona z ma zawsze postać $z=a+bi$, gdzie i jest jednostką urojoną, czyli liczbą, której kwadrat wynosi –1: $i^2=-1$). Liczbę zespoloną wygodnie utożsamić z wektorem na płaszczyźnie, którego początek leży w (0,0), zaś koniec w punkcie (a,b). Moduł z, czyli długość tego wektora, obliczamy zgodnie z twierdzeniem Pitagorasa: $|z| = \sqrt{(a^2+b^2)}$

[23] Fizyczna realizacja klasycznego bitu to np. moneta, która leży do góry orłem lub reszką, lub przegródka, która jest pusta albo nie (w obu wypadkach możliwe są tylko dwa stany). Fizyczną realizacją kubitu jest np. foton, którego spin opisujemy. Oprócz dwóch stanów bazowych ($|0\rangle$ oraz $|1\rangle$), taki foton może przyjmować szereg wartości „mieszanych”.

W obliczeniach kwantowych odwołujemy się nie tylko do pojedynczych kubitów, ale także do ich układów – tzw. rejestrów. Opis rejestrów jest bardziej złożony. Przypuśćmy, że mamy rejestr dwóch kubitów, z których pierwszy jest w stanie $a_0|0\rangle+a_1|1\rangle$, zaś drugi w stanie $b_0|0\rangle+b_1|1\rangle$. Wówczas stan całego rejestru możemy zapisać po prostu jako iloczyn obu tych stanów:

$(a_0|0\rangle+a_1|1\rangle)(b_0|0\rangle+b_1|1\rangle)$

Po wykonaniu zwykłego mnożenia czynników (jak w przypadku wyrażeń algebraicznych) otrzymujemy:

$a_0b_0|0\rangle|0\rangle + a_0b_1|0\rangle|1\rangle + a_1b_0|1\rangle|0\rangle + a_1b_1|1\rangle|1\rangle$

Uprościmy notację, pisząc $|00\rangle$ zamiast $|0\rangle|0\rangle$, $|01\rangle$ zamiast $|0\rangle|1\rangle$ *etc.* Otrzymujemy zapis:

$a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$

Wektory $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ stanowią więc bazę układu (rejestru) 2–kubitowego[24]. Wektor $a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$ odpowiada więc układowi dwóch kubitów, z których pierwszy jest w stanie $a_0|0\rangle+a_1|1\rangle$, zaś drugi w stanie $b_0|0\rangle+b_1|1\rangle$. Ogólnie, stan każdego dwukubitowego układu będziemy zapisywać w postaci sumy: $c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$ (gdzie zespolone współczynniki c_{00}, c_{01}, c_{10}, c_{11} spełniają warunek $|c_{00}|^2+|c_{01}|^2+|c_{00}|^2+|c_{11}|^2=1$)[25].

W przypadku rejestru trzech kubitów $a_0|0\rangle+a_1|1\rangle$, $b_0|0\rangle+b_1|1\rangle$, $c_0|0\rangle+c_1|1\rangle$ sytuacja wygląda podobnie. Jeśli chcemy opisać stan całego tego układu, wystarczy je przez siebie pomnożyć jak zwykłe wyrażenia algebraiczne. Szczegóły techniczne nie są tu istotne, ważne jest natomiast to, że dla opisania układu 3–kubitowego potrzeba

[24] Układ dwóch kubitów będzie zatem traktowany jako całość, i jako całość jest w superpozycji stanów $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ (ze współczynnikami a_0b_0, a_0b_1, a_1b_0, a_1b_1).

[25] Należy tutaj dodać, że nie zawsze stan układu dwóch kubitów daje się zapisać w formie iloczynu. Taki zapis mówi nam bowiem, że oto pierwszy kubit jest w określonym stanie i drugi też jest w określonym stanie. Tymczasem – niezależnie od tego, jak dziwne to może się nam wydawać – niekiedy nie ma sensu mówić o stanach poszczególnych kubitów. Można jedynie mówić o stanie układu jako całości. Mówimy wówczas o stanach splątanych – i ten efekt kwantowy nie ma klasycznego odpowiednika.

nam $2^3=8$ parametrów[26]. W ogólnym przypadku, układ *n* kubitów wymaga do opisania 2^n parametrów. Jest to przyczyna, dla której komputerowa symulacja ewolucji układu kwantowego jest bardzo trudna. Liczba parametrów niezbędnych do opisania takiego układu rośnie bowiem bardzo szybko; aby opisać ewolucję układu *n* kubitów konieczne byłoby opisanie jednoczesnej ewolucji 2^n parametrów. W przypadku większych wartości *n* jest to niemożliwe z praktycznego punktu widzenia.

Czym jest algorytm kwantowy? Klasyczne algorytmy operują na ciągach 0–1. Algorytmy kwantowe operują na kubitach, a elementarne operacje to tzw. bramki kwantowe. Taka bramka dokonuje modyfikacji kubitu, zgodnie z ogólnym schematem V: $a_0|0\rangle + a_1|1\rangle \rightarrow b_0|0\rangle + b_1|1\rangle$. Oznacza to, że kubit, który przed przejściem przez bramkę był w stanie $a_0|0\rangle + a_1|1\rangle$, po przejściu przez tę bramkę znajdzie się w nowym stanie $b_0|0\rangle + b_1|1\rangle$.[27] Z czysto fizycznego punktu widzenia taką bramką kwantową może być np. przejście fotonu przez półprzepuszczalne lustro, jednak nas interesuje tu jedynie teoretyczna strona zagadnienia.

Zgodnie z tym, co już powiedziano wcześniej, opis ewolucji układu kwantowego jest bardzo złożony – aby opisać ewolucję układu *n* kubitów musimy symulować ewolucję 2^n współczynników. A zatem komputerowy opis procesu fizycznego (np. zachowania się grupy 100 fotonów w urządzeniu optycznym) wymagałby opisu ewolucji 2^{100} współczynników, co jest oczywiście praktycznie niemożliwe. Ewolucji stosunkowo prostego nawet układu fizycznego odpowiada niezwykle złożone obliczenie. To utrudnia – a nawet uniemożliwia – komputerową symulację tej ewolucji. Można jednak na ten fakt spojrzeć z zupełnie innego punktu widzenia, traktując to jako okazję do tego, aby niejako zaprząc naturę do pracy. Z taką ideą wystą-

---

[26] Otrzymujemy (po dokonaniu oczywistych uproszczeń – zamiast $|0\rangle|1\rangle|0\rangle$ piszemy $|010\rangle$ *etc.*) następujący wynik: $a_0b_0c_0|000\rangle + a_0b_0c_1|001\rangle + a_0b_1c_0|010\rangle + a_0b_1c_1|011\rangle + a_1b_0c_0|100\rangle + a_1b_0c_1|101\rangle + a_1b_1c_0|110\rangle + a_1b_1c_1|111\rangle$. Wektory $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$ tworzą bazę rejestru 3–kubitowego i ogólny stan układu 3–kubitowego można zapisać jako: $a_{000}|000\rangle + a_{001}|001\rangle + a_{010}|010\rangle + a_{011}|011\rangle + a_{100}|100\rangle + a_{101}|101\rangle + a_{110}|110\rangle + a_{111}|111\rangle$.

[27] Pomijam tutaj nieistotne dla naszych rozważań warunki techniczne.

pił Feynman blisko 30 lat temu. Punktem wyjścia jest obserwacja, że zachodzi odpowiedniość:

• ewolucja układu kwantowego ↔ (złożone) obliczenie

Oznacza to, że wyniki owych bardzo długich obliczeń odpowiadają końcowym stanom ewolucji układu kwantowego. W szczególności oznacza to, że tego, czego możemy dowiedzieć się w wyniku symulacji komputerowej, możemy znacznie szybciej dowiedzieć się, po prostu obserwując ów układ.

No cóż – nie ma nic dziwnego w fakcie, że np. zamiast obliczać na komputerze, gdzie upadnie pocisk, możemy po prostu przeprowadzić odpowiedni eksperyment fizyczny. Często ów eksperyment pozwala na znacznie szybsze znalezienie odpowiedzi – i tak bywa też w przypadku fizyki klasycznej. Jednak szczególnie wyraźnie ów efekt jest widoczny w wypadku komputerowej symulacji układów kwantowych. W wielu wypadkach taka symulacja nie ma najmniejszego sensu, bo zanim by się zakończyła, to w międzyczasie wyginęłaby ludzkość. Jednak pomysł Feynmana był genialny w swej prostocie: wyobraźmy sobie, że jest jakiś naturalny trudny problem obliczeniowy (np. rozkład liczby na czynniki pierwsze) i że da się znaleźć taki układ kwantowy, że ów problem obliczeniowy stanowi jego symulację. Innymi słowy: może się zdarzyć, że skądinąd ciekawy (i obliczeniowo trudny) problem jest równoważny opisowi ewolucji jakiegoś układu kwantowego. Skoro jednak przy przejściu *układ kwantowy* → *symulacja komputerowa* na ogół tracimy wykładniczo dużo czasu, to znaczy, że przy przejściu odwrotnym (*symulacja komputerowa* → *układ kwantowy*) możemy **zyskać** wykładniczo dużo czasu. W szczególności, zamiast wykonywać np. 2^{100} kroków symulacji komputera, wystarczy przeprowadzić proste doświadczenie z układem 100 kubitów. Ważne jest to, że wynik owego kwantowego eksperymentu będzie po prostu odpowiadał wynikowi owego obliczenia. Tym samym nasz problem obliczeniowy będzie mógł zostać rozwiązany dzięki stosownemu doświadczeniu kwantowemu.

Oczywiście, podstawowe pytanie, jakie się pojawia w tym kontekście, brzmi: czy faktycznie istnieją kwantowe odpowiedniki **naturalnych** problemów obliczeniowych? Nie chodzi przecież o trywialny i bezużyteczny fakt, że każde doświadczenie kwantowe odpowiada obliczeniu, które jest symulacją owego doświadczenia. Chodzi nam o to, aby – mając dany **już uprzednio** pewien problem obliczenio-

wy – móc zaplanować stosowny eksperyment kwantowy dający nam wykładniczy zysk czasowy. Otóż odpowiedź jest pozytywna, a najbardziej spektakularnym przykładem jest wspomniany już algorytm Shora z roku 1994, dzięki któremu można szybko rozłożyć liczbę na czynniki pierwsze. Oznacza to w szczególności, że gdyby ów algorytm został zaimplementowany, klasyczne protokoły kryptograficzne odeszłyby do lamusa. Stworzenie owego algorytmu wywołało ogromne zainteresowanie i dało bardzo silny impuls rozwojowi teorii obliczeń kwantowych. Należy jednak od razu dodać, że algorytmy kwantowe są czysto teoretyczne – budowa komputera kwantowego napotyka na nieprzezwyciężalne – jak na razie – trudności techniczne.

5. ALGORYTMY KWANTOWE A PROBLEM WIEDZY MATEMATYCZNEJ

Nas interesuje tu jednak filozoficzny aspekt ewentualnego zastosowania takich algorytmów. Wyobraźmy sobie, iż jakiś matematyczny problem P zostanie rozwiązany dzięki użyciu algorytmu kwantowego. Z punktu widzenia dyskusji filozoficznej nie jest istotne, czy jest to problem słynny, czy mało znaczący (choć oczywiście bardzo spektakularne byłoby stworzenie algorytmu kwantowego rozwiązującego ważny otwarty problem matematyczny). Istotne jest natomiast pytanie, jaki byłby status tak uzyskanej wiedzy. Sama procedura zastosowania algorytmu kwantowego do rozwiązywania problemu matematycznego przebiegałaby następująco:

(1) Przygotowujemy układ (rejestr) kwantowy w odpowiednim stanie początkowym.

(2) Uruchamiamy algorytm kwantowy (a ściśle: jego fizyczną implementację w komputerze kwantowym).

(3) Po zakończonej ewolucji dokonujemy pomiaru stanu końcowego.

(4) Na tej podstawie ustalamy, czy postawiona przez nas hipoteza matematyczna jest prawdziwa.

A zatem to eksperyment kwantowy stanowiłby argument na rzecz matematycznej tezy T. Jaki jest status tak uzyskanej wiedzy? Czy jej akceptacja jako pełnoprawnej wiedzy matematycznej jest do pogodzenia z poglądem głoszącym aprioryczny status ma-

tematyki? Co powiedzieliby przywołani wcześniej przedstawiciele matematycznego aprioryzmu, tacy jak Kartezjusz czy Gödel?

Użycie komputera kwantowego w dowodzie podważa kartezjańską koncepcję „jasności i wyraźności" widzenia każdego kroku rozumowania matematycznego. Kartezjusz pisał wszak o przeglądaniu rozumowań ruchem myśli, o tym, że konieczne jest nie tylko rozumienie poszczególnych kroków, ale także swoiste ogarnięcie całości jako takiej. Ten warunek wydaje się nie być spełniony w przypadku dowodów komputerowych, a już zwłaszcza w przypadku algorytmów kwantowych, gdzie nie jesteśmy w stanie nawet teoretycznie sprawdzić, jak przebiega obliczenie. Zatrzymanie obliczenia niszczy je – a gdybyśmy chcieli je odtwarzać niejako krok po kroku, uruchamiając wciąż na nowo i sprawdzając kolejne etapy, to będziemy otrzymywać losowe wyniki (ponieważ pomiar kwantowy ma charakter probabilistyczny). W tym więc sensie nie wiemy, w jakim dokładnie stanie znajduje się komputer kwantowy dowodzący naszego twierdzenia.

Czy jednak warunek *surveyability* dowodu jest kluczowy dla apriorycznej koncepcji matematyki? Nie jest on wyartykułowany w tak wyraźny sposób u Gödla – co więcej, Gödel w swoich analizach abstrahuje od problemu długości dowodu i tego, czy jest on praktycznie wykonalny. Interesuje się raczej teoretyczną stroną zagadnienia. Czy jednak zgodziłby się na to, że nową wiedzę matematyczną możemy uzyskać, uruchamiając urządzenie probabilistyczne i czekając, czy na wyświetlaczu pojawi się 0 czy 1? Wydaje się to być bardzo odległe od koncepcji intuicyjnego oglądu pojęć matematycznych. Warto przypomnieć, że Gödel czerpał inspiracje z pism Husserla i uważał fenomenologię za obiecującą metodę w analizie znaczeń pojęć matematycznych. Czyżby redukcję ejdetyczną można było zastąpić eksperymentem fizycznym, w którego przebieg nie ma się nawet **teoretycznie** pełnego wglądu? Szczegółowa analiza tych kwestii wykracza poza ramy niniejszego artykułu, jednak uważam tę problematykę za ważną z punktu widzenia fundamentalnego sporu w filozofii matematyki, jakim jest spór o źródła wiedzy matematycznej.

QUANTUM COMPUTATION THEORY AND THE APRIORICITY OF MATHEMATICS

Summary

In the article I discuss the problem of the nature of mathematical knowledge in the context of quantum computation theory. The main question is, if theoretical results concerning quantum algorithms shed a new light on this discussion. I shortly present the "received view" concerning mathematical knowledge (in the tradition of Descartes or Gödel), present the main ideas of quantum computation theory, and formulate the problem.