EDUKACJA FILOZOFICZNA
Vol. 42 2006

KRZYSZTOF WÓJTOWICZ
Uniwersytet Warszawski

CO TO JEST TEORIA OBLICZEŃ KWANTOWYCH?

Moim celem jest zapoznanie Czytelnika z pewnym teoretycznym modelem obliczeń, wykorzystującym specyfikę świata kwantowego oraz zwrócenie uwagi na ważne pytania filozoficzne, dotyczące statusu uzyskanej w drodze kwantowych obliczeń wiedzy matematycznej. Ponieważ teoria obliczeń kwantowych nie jest powszechnie znana w środowisku filozoficznym, pozwalam sobie na dość szczegółowe i zarazem elementarne wprowadzenie w tematykę. W artykule omawiam więc tylko wybrane, najprostsze zagadnienia, które pokazują specyfikę tego podejścia. Mam nadzieję, że lektura zachęci Czytelników do bliższego zapoznania się z tą problematyką i do podjęcia refleksji filozoficznej na jej temat[1].

I. OBLICZENIA KLASYCZNE. 1. Teoretyczny model obliczeń. W życiu codziennym i w praktyce naukowej mamy do czynienia z różnego typu obliczeniami. Intuicyjne pojęcie liczenia nie jest jednak w pełni jasne – mówimy o liczeniu ilości osób w sali, o obliczeniu trajektorii ruchu kamienia, o obliczeniu sumy stu liczb, o obliczeniu ryzyka danej inwestycji *etc.* – mamy więc do czynienia z różnego typu procedurami. Nie możemy mieć *a priori* pewności, że wszystkie procedury obliczeniowe mają podobny charakter, i że istnieje uniwersalny model obliczeń. Naszą uwagę ograniczymy tu jednak do modelu, który leży u podłoża współczesnej informatyki – modelu maszyny Turinga[2]. Jest to mo-

[1] W języku polskim dostępne są popularne książki [Johnson 2005], [Milburn 2000], oraz bardziej techniczne [Giaro K., Kamiński M 2003], [Hirvensalo 2004]. Przystępne wprowadzenie w problematykę zawiera praca [Deutsch D,. Ekert A., Lupacchini R. 2000]. W Internecie dostępnych jest mnóstwo prac o każdym poziomie zaawansowania – poszukiwania można rozpocząć np. od strony http://www.qubit.org/.

[2] Maszynę Turinga można wyobrażać sobie jako mechaniczne urządzenie, które składa się z trzech podstawowych części: (1) jednostki sterującej (która zawsze jest w jednym ze skończenie wielu stanów wewnętrznych); (2) taśmy (potencjalnie nieskończonej), podzielonej na komórki, na której zapisywane są symbole; (3) głowicy, która potrafi odczytać z taśmy symbol i wpisać na taśmę symbol. Elementarna operacja ma-

model dostatecznie ogólny, aby objąć nasze czynności obliczeniowe dokonywane na obiektach skończonych, a zarazem dostatecznie silny, aby stać się teoretycznym modelem działania komputera.

Działanie maszyny Turinga ma lokalny charakter – w tym sensie, że w każdej chwili maszyna bierze pod uwagę tylko aktualny stan wewnętrzny oraz symbol na taśmie w tej klatce, na który akurat „patrzy" głowica. Dzięki prostemu kodowaniu (którego szczegóły nie są istotne), możemy każdy ogólny przypadek sprowadzić do maszyny Turinga korzystającej z dwóch symboli: 0 oraz 1 (dalej zakładamy więc, że maszyna Turinga operuje na zerach i jedynkach).

Jaka jest relacja pomiędzy tym modelem obliczenia, a naszym intuicyjnym pojęciem obliczenia? Teza Churcha (Churcha-Turinga) głosi, że ten model adekwatnie ujmuje nasze intuicyjne pojęcie obliczenia, a więc że każda funkcja, którą intuicyjnie uznamy za obliczalną, jest też funkcją obliczalną w sensie Turinga. Stwierdzenie, że możliwe jest algorytmicznie rozwiązanie pewnego problemu jest więc równoważne stwierdzeniu, że można zdefiniować stosowną maszynę Turinga, rozwiązującą ten problem (czyli dokonującą stosownych obliczeń po „nakarmieniu" jej danymi). Oczywiście teza Churcha nie jest twierdzeniem matematycznym, ale tezą o charakterze metodologicznym[3].

W tym artykule będę miał na myśli obliczenia w sensie Turinga[4]. Należy tu podkreślić mechaniczność obliczenia maszyny Turinga i to, że składa się ono z pewnej ilości elementarnych kroków, z których każdy

maszyny Turinga polega na odczytaniu z danej komórki taśmy symbolu, i następnie – w zależności od tego, jaki to jest symbol, i w jakim stanie wewnętrznym jest maszyna – ew. zmianie stanu wewnętrznego, ew. wpisaniu na taśmę symbolu, i ew. ruchu głowicą w lewo lub w prawo. Działanie maszyny Turinga polega na wykonywaniu kolejnych elementarnych kroków tej postaci, aż do zatrzymania się maszyny – jeśli takowe nastąpi – lub w nieskończoność (wtedy mówimy o zapętleniu się maszyny Turinga). Istnieją też inne modele obliczeń, równoważne modelowi Turinga. Nie jest to istotne dla naszej dyskusji.

[3] Wokół tezy Churcha narosła ogromna literatura. Zainteresowany Czytelnik może rozpocząć np. od hasła http://plato.stanford.edu/entries/church-turing/, gdzie znajduje się obszerna bibliografia.

[4] Kiedy więc będziemy zastanawiać się nad pytaniem, czy istnieje algorytm rozwiązania danego problemu, będziemy odwoływać się do intuicyjnego pojęcia algorytmu – bowiem zgodnie z tezą Churcha, istnieje odpowiednik takiego algorytmu w postaci maszyny Turinga. Do tej pory wszystkie procedury intuicyjnie uznawane za algorytmiczne okazywały się obliczalne w sensie Turinga (co stanowi swoisty indukcyjny argument na rzecz wiarygodności tej tezy).

jest dla nas krokiem oczywistym i zarazem dalej nierozkładalnym. Będzie to ważne później.

2. Ograniczenia w obliczeniach. Jednym z podstawowych pojęć teorii obliczeń jest pojęcie problemu rozstrzygalnego – czyli takiego, dla którego daje się zdefiniować maszyna Turinga rozwiązująca ten problem. Problemem rozstrzygalnym jest np. sprawdzenie, czy dana liczba a jest sumą dwóch danych innych liczb b,c, czy dana liczba naturalna n jest liczbą pierwszą, czy złożoną lub czy dana formuła rachunku zdań jest tautologią[5]. W każdym z tych przypadków możemy podać ogólny algorytm, który działa dla dowolnej instancji problemu. Liczne przykłady problemów rozstrzygalnych możemy znaleźć w teorii liczb, kombinatoryce, teorii grafów, logice *etc.*

Nie wszystkie problemy są rozstrzygalne – czasami nie istnieje ogólny algorytm (maszyna Turinga), który potrafi rozwiązać problem danego typu[6]. Jednak w tym artykule interesować nas będą tylko problemy rozstrzygalne. Można wśród nich wskazać naturalną hierarchię trudności. Jest oczywiste, że mniej obliczeń trzeba wykonać, aby dodać do siebie dwie liczby, niż aby np. znaleźć ich najmniejszą wspólną wielokrotność. Łatwiej podnieść liczbę do kwadratu, niż rozłożyć ją na czynniki pierwsze. Te intuicyjne obserwacje mają swoje formalne odpowiedniki – problemy klasyfikujemy ze względu na ich złożoność obliczeniową, czyli czas potrzebny do ich rozwiązania. Czas mierzymy zaś ilością kroków wykonanych przez daną maszynę Turinga.

Obliczeniowa trudność problemu nie polega więc na tym, że trudno jest nam go zrozumieć, ale na tym, że trzeba wykonać dużą ilość obliczeń. Prostym przykładem obliczeniowo trudnego problemu jest to, czy dana formuła rachunku zdań jest tautologią. Znana ze szkoły metoda tabelkowa polega na tym, że prowadzimy stosowne obliczenia dla wszystkich wartościowań. W szkole najczęściej robimy to dla formuł z dwoma, najwyżej trzema zmiennymi – stosowna tabelka ma wtedy 4 lub 8 rzędów. W ogólnym przypadku, jeśli formuła ma n zmiennych, to stosowna tabelka ma 2^n rzędów (a więc w przypadku 10 zmiennych – 1024 rzędy, 20 zmiennych –1048576 rzędów *etc.*). W przypadku formuły li-

[5] Intuicyjnie: algorytm polega na sprawdzeniu, czy któraś z liczb mniejszych od n (a tak naprawdę wystarczy $\sqrt{n}+1$) jest dzielnikiem n; algorytm liczy wartość logiczną formuły po kolei dla wszystkich wartościowań.

[6] Znany przykład problemu nierozstrzygalnego to problem stopu: nie istnieje maszyna Turinga, która otrzymując jako dane wejściowe: (1) opis innej maszyny Turinga M; (2) dane początkowe x; byłaby w stanie stwierdzić, czy maszyna M dla danych wejściowych x zatrzyma się, czy zapętli.

czącej 1000 zmiennych, sprawdzenie tautologiczności formuły metodą klasyczną nie jest fizycznie możliwe,

Być może istnieje szybszy algorytm sprawdzania, czy dana formuła rachunku zdań jest tautologią[7]. Gdyby się to udało, byłoby to ważne nie tylko ze względu na rachunek zdań, ale ze względu na fakt, że rozwiązanie to dałoby się „przetłumaczyć" na rozwiązanie bardzo wielu problemów kombinatorycznych. Znając stosowny algorytm sprawdzania tautologiczności formuły rachunku zdań, moglibyśmy podać (prawie równie szybki) algorytm dla wielu innych trudnych obliczeniowo problemów. Przykładem takiego problemu z tej bogatej kolekcji jest problem komiwojażera[8].

Komputerowe rozwiązanie problemu komiwojażera czy tautologii KRZ jest więc wprawdzie teoretycznie możliwe (algorytmy są pojęciowo bardzo proste: przelicz wszystkie ścieżki, przelicz wszystkie wartościowania *etc.*), ale żaden komputer nie jest w stanie - w ogólnym przypadku - przeprowadzić takich obliczeń. Obrazowo mówiąc, Wszechświat jest za mały i trwa zbyt krótko, aby zmieścił się w nim dostatecznie duży komputer i zdążył przeprowadzić obliczenia, więc fizyczna realizacja algorytmu nie jest możliwa[9].

Fakt, że pewne problemy są bardzo złożone, i nie są nam znane szybkie algorytmy pozwalające na ich rozwiązanie, ma także swoje dobre strony. Dzięki temu, że problem faktoryzacji (rozkładu liczby na czynniki pierwsze) jest problemem trudnym obliczeniowo, możemy korzystać z szyfrowania wiadomości. Popularna metoda szyfrowania RSA opiera się właśnie na tym, że trudno jest rozłożyć liczbę na czynniki pierwsze. Najbardziej znany z algorytmów kwantowych (algorytm Shora, podany w roku 1994) dotyczy właśnie tego zagadnienia i pozwala na szybkie złamanie kodu (ściśle: pozwalałby, gdyby istniały komputery kwantowe). Nic więc dziwnego, że wzbudził duże emocje i dał istotny impuls dla teorii obliczeń kwantowych.

---

[7] Należy tu podkreślić, że chodzi o ogólną metodę, działającą dla wszystkich formuł. Jest mało prawdopodobne, aby faktycznie taki algorytm istniał. Na razie jednak nikt nieistnienia takiego szybszego algorytmu nie udowodnił.

[8] Problem komiwojażera ma proste sformułowanie: mamy n miast połączonych drogami, z których każda ma pewną długość (koszt przebycia). Należy znaleźć najkrótszą (najtańszą) drogę łączącą wszystkie miasta.

[9] W praktyce w wielu wypadkach korzysta się z algorytmów probabilistycznych, które wprawdzie nie dają gwarancji dobrej odpowiedzi, ale udzielają tej odpowiedzi z prawdopodobieństwem dostatecznie dużym, aby można było je stosować w praktyce.

Ważny jest dla nas następujący morał: niektóre problemy są teoretycznie rozstrzygalne, ale w praktyce jest to zbyt złożone, aby można je było rozwiązać w klasycznym modelu obliczeń, tj. za pomocą maszyny Turinga (*scil.* komputera). Tworzone są jednak modele obliczeń wykorzystujące specyfikę świata kwantowego, które pozwalają na szybsze rozwiązanie niektórych problemów. Prezentacji tego modelu poświęcona jest następna część artykułu[10].

II. OBLICZENIA W ŚWIECIE KWANTÓW[11]. Klasyczne obliczenie polega na mechanicznym przekształcaniu ciągów 0 i 1 i nie odwołuje się do specyfiki świata kwantowego[12]. Inaczej jest w przypadku obliczeń kwantowych.

1. Dwukrotne losowanie z deterministycznym wynikiem. Zacznijmy od prostego przykładu. Wyobraźmy sobie urządzenie (czarną skrzynkę) *U*, która działa w sposób losowy: otrzymuje na wejściu 0 lub 1, zaś na wyjściu z jednakowym prawdopodobieństwem (czyli ½) i niezależnie od wejścia podaje 0 lub 1.

Wyobraźmy sobie teraz dwa takie urządzenia, i dwukrotne wykonanie operacji *U*. Schemat działania byłby więc następujący:

1. Wybieramy daną wejściową (np. 0) i zadajemy ją pierwszej maszynie *U*.
2. Uruchamiamy maszynę *U*.
3. Wynik działania pierwszej maszyny *U* przekazujemy do drugiej maszyny *U*.
4. Obserwujemy wynik działania drugiej maszyny *U*.

Co wyszło? Każdy człowiek wychowany w świecie fizyki klasycznej (*scil.* każdy człowiek) odpowie, że nie wiadomo - wyszło losowo 0 lub 1 - niezależnie od tego, co zadaliśmy pierwszej maszynie na wejściu. Wiedza na temat danej wejściowej nic nie daje, bo i tak zostaje ona utracona w wyniku losowania.

W świecie klasycznym nie można skonstruować takiej maszyny *U*, która działa losowo (jak rzut monetą), ale która ma tę własność, że jej dwukrotne zastosowanie daje wynik w pełni deterministyczny (gdy za-

[10] Należy tu podkreślić, że jest to model teoretyczny. Nie zostały na razie skonstruowane komputery kwantowe, które umożliwiłyby praktyczną implementację tych algorytmów.

[11] Rezygnuję z wielu szczegółów technicznych, wychodząc z założenia, że zainteresowany nimi Czytelnik i tak sięgnie do literatury. Prezentacja nie jest więc bynajmniej kompletna, chodzi raczej o wprowadzenie Czytelnika w stosowny nastrój.

[12] Dlatego w popularyzatorskich pracach mówi się o tym, że maszyny Turinga można (teoretycznie) budować np. z drewna.

czynamy od 0, otrzymujemy zawsze 1, gdy zaczynamy od 1, otrzymujemy zawsze 0)? Natomiast w świecie kwantów takie urządzenie U istnieje! Moglibyśmy je nazwać „pierwiastkiem z negacji", gdyż $U^2(p) = \neg p$. Aby wyjaśnić zasadę działania tego urządzenia, konieczne będzie wprowadzenie pewnych pojęć.

2. Elementarne pojęcia kwantowej teorii obliczeń. W klasycznej teorii informacji mówimy o bitach, które przyjmują wartości 0 i 1. Jedna liczba (0 lub 1) stanowi więc pełen opis danego bitu. Natomiast podstawowym pojęciem kwantowej teorii obliczeń jest kubit (ang.: *qubit*) - kwantowy bit informacji, czyli kwantowy odpowiednik klasycznego bitu. Kubity są tworami nieco bardziej złożonymi niż bity, do ich opisania nie wystarczy tylko 0 i 1.

Wyobraźmy sobie, że pewien układ fizyczny (od tej pory będziemy mówić tylko o układach kwantowych) może występować w różnych stanach, wśród których wyróżnimy dwa ważne stany, które tworzą swoistą bazę dla wszystkich pozostałych stanów. Oznaczymy je przez $|0\rangle$ oraz $|1\rangle$[13]. Ważne jest to, że układ kwantowy występuje zawsze w stanie, który można opisać jako swoistą „mieszaninę" tych dwóch wyróżnionych stanów bazowych. Mówiąc obrazowo, układ jest np. w 87% w stanie $|0\rangle$, zaś w 13% w stanie $|1\rangle$. Jest to oczywiście sprzeczne z naszymi intuicjami ukształtowanymi w świecie klasycznym, ale tak właśnie jest sformułowana mechanika kwantowa.

Przykładem takiego układu jest elektron, którego spin opisujemy[14]. W popularyzatorskich pracach pojawiają się niekiedy rysunki przestawiające kulkę wirującą w jedną lub w drugą stronę - zadaniem Czytelnika jest wyobrażenie sobie spinu elektronu jako kierunku obrotu takiej kulki. Kiedy mamy przed oczyma obraz wirującej kulki, to niewątpliwie naszej wyobraźni trudno pogodzić się z faktem, że układ może być w takiej dziwnej „mieszaninie" stanów (np. elektron kręci się w 87% w lewo, zaś w 13% w prawo). Sądzę, że lepiej nie wyobrażać sobie elektronu jako kulki wirującej jednocześnie w dwie przeciwne strony, ale przyjąć, że jest to obiekt fizyczny opisywany matematycznie w określony sposób. Mechanika kwantowa opisuje układy kwantowe właśnie w taki sposób, niezależnie od naszej możliwości wyobrażenia sobie tego

[13] Dla usunięcia ewentualnych nieporozumień chcę podkreślić, że omawiam tutaj tylko sytuację ważną z punktu widzenia teorii obliczeń kwantowych. W ogólnym przypadku tych bazowych stanów może być więcej, a opis układu kwantowego znacznie bardziej skomplikowany.

[14] Inny przykład to np. spolaryzowany foton. Nie interesują nas tu jednak fizyczne realizacje kubitów – ważne jest to, że faktycznie takie obiekty istnieją.

faktu. Każdy stan można więc zapisać w postaci $a_0|0\rangle + a_1|1\rangle$, gdzie a_0 i a_1 są współczynnikami, które odgrywają rolę „wag"[15]. Współczynniki te są liczbami zespolonymi, spełniającymi warunek $|a_0|^2+|a_1|^2=1$ (gdzie $|z|$ oznacza moduł danej liczby zespolonej z[16]). Mówiąc bardziej oficjalnie, kubit jest wektorem długości 1 w dwuwymiarowej przestrzeni Hilberta[17].

Obliczenie klasycznej maszyny Turinga polega na tym, że początkowy ciąg zer i jedynek na taśmie jest przetwarzany zgodnie z instrukcjami maszyny. Obliczenie kwantowe polegać będzie natomiast na tym, że przetwarzany będzie stosowny ciąg kubitów (czyli swoistych „mieszanek" zer i jedynek z zespolonymi współczynnikami)[18].

Obliczenie kwantowe składa się z kwantowych kroków, które różnią się od klasycznych. Z fizycznego punktu widzenia krok obliczenia kwantowego polega na tym, że pewien układ kwantowy został poddany pewnej operacji (na przykład grupa fotonów zostaje wpuszczona w układ półprzepuszczalnych luster). Nas tu nie interesują fizyczne szczegóły, ale teoretyczna strona zagadnienia. Z punktu widzenia opisu matematycznego krok działania kwantowego urządzenia liczącego polega na tym, że kubit (lub zestaw – tzw. rejestr – kubitów) zostanie przekształcony zgodnie z pewną opisaną matematycznie kwantową procedurą. Obliczenie kwantowe to ciąg takich kroków, zaś elementarne przekształcenie nazwiemy „bramką kwantową".

---

[15] Mówiąc bardzo swobodnie, współczynnik określa „udział" danego stanu bazowego w stanie układu.

[16] Liczbę zespoloną z można przedstawić w postaci $z=a+bi$, gdzie i jest jednostką urojoną - jest to liczba, której kwadrat wynosi -1: $i^2=-1$. Na płaszczyźnie wygodnie liczbę zespoloną z przedstawić w formie wektora o początku w (0,0) i końcu w punkcie (a,b). Moduł z, czyli $|z|$ to po prostu długość tego wektora, którą obliczamy zgodnie z twierdzeniem Pitagorasa: $|z| = \sqrt{(a^2+b^2)}$.

[17] Fakt, że „wagi" są liczbami zespolonymi, a nie rzeczywistymi może stanowić dodatkową trudność pojęciową (możemy sobie wyobrazić, że coś jest w 50% czarne, ale co znaczy, że coś jest czarne w stopniu $(1+i)/2$?). Jednak formalizm mechaniki kwantowej opisuje stany układów kwantowych w taki właśnie sposób, niezależnie od naszych początkowych trudności z zaakceptowaniem tego faktu.

[18] To, że wektory bazowe oznaczamy przez $|0\rangle$ oraz $|1\rangle$ nie jest oczywiście przypadkiem. Kiedy będziemy chcieli wykorzystać urządzenia kwantowe do obliczeń, i jako wyjściową daną chcemy zadać 0, to musimy przygotować układ kwantowy w początkowym stanie $|0\rangle$. Jeśli chcemy przetwarzać n-elementowy ciąg 0-1, to musimy przygotować układ n kubitów w stosownym stanie początkowym.

Jeśli wyjściowy kubit ma postać $a_0|0\rangle + a_1|1\rangle$, to po jego przejściu przez bramkę kwantową V znajdzie się on na ogół w nowym stanie $b_0|0\rangle + b_1|1\rangle$. Schematycznie:

$$V: a_0|0\rangle + a_1|1\rangle \rightarrow b_0|0\rangle + b_1|1\rangle.$$

Nie wszystkie takie przejścia są możliwe - współczynniki a_0, a_1, b_0, b_1 muszą spełniać stosowne warunki techniczne, których nie ma potrzeby tu omawiać. Ważne dla nas jest to, że taka ewolucja układu kwantowego („podróż" kubitów przez ciąg bramek kwantowych) pozwala na wykorzystanie specyfiki świata kwantowego, która jest źródłem efektywności kwantowych algorytmów.

3. Układy wielu kubitów. Potencjał obliczeń kwantowych ujawnia się, gdy rozważymy układy złożone z większej ilości kubitów. Odpowiadają one układom kwantowym złożonym z większej ilości układów prostszych - może być to np. układ 10 fotonów traktowanych i opisywanych jako jeden układ kwantowy.

Przypomnijmy, że jeden foton opisujemy jako kubit postaci $a_0|0\rangle + a_1|1\rangle$ - potrzebne do jego opisania są więc dwie liczby zespolone. Ile liczb potrzeba do opisania stanu układu złożonego z 10 kubitów? Odruchy wyniesione ze świata klasycznego podpowiadają nam, że powinno wystarczyć 20 liczb (dla każdego z kubitów – po dwie). Tak jednak nie jest. Dla opisania układu n kubitów potrzeba 2^n współczynników (mówimy, że wymiar przestrzeni stanów wynosi 2^n). Aby opisać stan układu składającego się z 10 fotonów, musimy podać 1024 współczynniki, zaś dla opisania układu 20 fotonów potrzeba 1 084 576 współczynników. Opis układu złożonego z 1000 kubitów nie zmieściłby się we Wszechświecie.

Przestrzeń stanów układu n-kubitowego jest więc bardzo złożona. Aby zrozumieć mechanizm prowadzący do takiej komplikacji rozważmy przykład układu złożonego z dwóch kubitów (np. fotonów), z których pierwszy jest w stanie $a_0|0\rangle + a_1|1\rangle$, zaś drugi w stanie $b_0|0\rangle + b_1|1\rangle$. Stan układu mieszanego możemy zapisać jako swoisty iloczyn obu tych stanów:

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

Wykonajmy zwykłe mnożenie czynników (traktując je po prostu jak wyrażenie algebraiczne). Otrzymamy

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

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

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

Możemy więc uznać $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ za wektory bazowe dla układu 2-kubitowego[19]. 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 $|c_{00}|^2+|c_{01}|^2+|c_{00}|^2+|c_{11}|^2=1$).

Jak zapisać stan układu złożonego z trzech kubitów: $a_0|0\rangle+a_1|1\rangle$, $b_0|0\rangle+b_1|1\rangle$, $c_0|0\rangle+c_1|1\rangle$? Wystarczy je przez siebie pomnożyć (oraz skrócić zapis: zamiast $|0\rangle|1\rangle|0\rangle$ piszemy $|010\rangle$ *etc.*). Stan tak powstałego układu można zapisać jako:

$$a_0b_0c_0|000\rangle + a_0b_0c_1|001\rangle + a_0b_1c_0|010\rangle + a_0b_1c_1|011\rangle + a_1b_0c_0|100\rangle + a_1b_0c_1|101\rangle + a_1b_1c_0|110\rangle + a_1b_1c_1|111\rangle$$

Wektory $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$ tworzą więc bazę układu 3-kubitowego i ogólny stan układu 3-kubitowego można zapisać jako:

$$a_{000}|000\rangle + a_{001}|001\rangle + a_{010}|010\rangle + a_{011}|011\rangle + a_{100}|100\rangle + a_{101}|101\rangle + a_{110}|110\rangle + a_{111}|111\rangle$$

W ogólnym przypadku, kiedy mamy układ n kubitów, to ogólny stan takiego układu musimy zapisać w postaci sumy 2^n składników. Wymiar przestrzeni stanów takiego układu wynosi więc 2^n. To pokazuje, dlaczego tak bardzo trudna jest komputerowa symulacja ewolucji układu kwantowego. Aby opisywać układ n kubitów, trzeba opisywać jednoczesną ewolucję 2^n współczynników (z których każdy jest liczbą zespoloną). Nie jest to wykonalne w przypadku 1000 kubitów.

4. Przykład bramek kwantowych. **Rozważmy bramkę kwantową H, która działa w następujący sposób:**

[19] Mówiąc obrazowo, układ dwóch kubitów (traktowanych jako całość) jest w stopniu a_0b_0 w stanie $|00\rangle$, w stopniu a_0b_1 w stanie $|01\rangle$, w stopniu a_1b_0 w stanie $|10\rangle$, w stopniu a_1b_1 w stanie $|11\rangle$.

$|0\rangle \rightarrow 1/\sqrt{2}\,(|0\rangle + |1\rangle)$
$|1\rangle \rightarrow 1/\sqrt{2}\,(|0\rangle - |1\rangle)$[20].

Informacja, jak zachowują się wektory bazowe 0 i 1 wystarczy do obliczenia, jak zachowuje się dowolny wektor, ponieważ operatory opisujące ewolucję układów kwantowych działają w sposób liniowy, co znaczy po prostu, że:
$H(a_0|0\rangle + a_1|1\rangle) = a_0 H|0\rangle + a_1 H|1\rangle$

Operator H to często spotykany w teorii obliczeń kwantowych operator (bramka) Hadamarda. Łatwo obliczyć, że dwukrotne wykonanie bramki Hadamarda prowadzi układ do stanu wyjściowego.

Rozważmy inny operator U, zdefiniowany jako:

$U: |0\rangle \rightarrow \frac{1}{2}(1-i)|0\rangle + \frac{1}{2}(1+i)|1\rangle$
$U: |1\rangle \rightarrow \frac{1}{2}(1+i)|0\rangle + \frac{1}{2}(1-i)|1\rangle$

Krótkie obliczenie pokazuje, że $UU|0\rangle = 1$, zaś $UU|1\rangle = 0$. Zatem definiowany tak operator U jest pierwiastkiem z negacji, o którym była mowa wcześniej ($U^2(p) = \neg p$). Możemy go oznaczyć jako √NOT.

Dlaczego twierdzimy, że √NOT działa losowo? Nie widać tego w powyższym równaniu. Rzeczywiście, operator √NOT działa na przestrzeni Hilberta w sposób deterministyczny. Jednak aby dowiedzieć się czegoś o stanie układu kwantowego, musimy dokonać pomiaru, który ma charakter probabilistyczny, zgodnie z jednym z podstawowych postulatów mechaniki kwantowej. Na nasze potrzeby wystarczy tu uproszczona wersja postulatu mówiącego o pomiarze, odnosząca się do kubitów:

POSTULAT: Jeśli dokonujemy pomiaru układu kwantowego znajdującego się w stanie $a_0|0\rangle + a_1|1\rangle$, to możliwe są dwa wyniki pomiaru: 0 oraz 1, przy czym prawdopodobieństwo uzyskania wyniku pomiaru 0 wynosi $|a_0|^2$, zaś prawdopodobieństwo pomiaru wyniku 1 wynosi $|a_1|^2$. Po pomiarze układ znajduje się w stanie odpowiadającym wynikowi pomiaru[21].

[20] Z fizycznego punktu widzenia ta bramka opisuje np. przez foton przechodzący przez interferometr, opis znaleźć można np. w [Deutsch, Ekert, Lupaccini 2000] lub w [Milburn 2000].

[21] Współczynniki a_0 i a_1 nazywamy amplitudami prawdopodobieństwa. Jest teraz jasne, dlaczego żądamy, aby w równaniu opisującym kubity spełniony był warunek

Jeśli więc układ jest w ogólnym stanie $a_0|0\rangle+a_1|1\rangle$, i pomiar pokazał 0, to o stanie układu sprzed pomiaru możemy wywnioskować jedynie, że $a_0\neq 0$. Po pomiarze układ znajdzie się w stanie 0 (i tym samym następny pomiar już na pewno da wynik 0).

Powróćmy do pierwiastka z negacji. Operator √NOT przekształca $|0\rangle$ na $1/\sqrt{2}(1-i)|0\rangle + 1/\sqrt{2}(1+i)|1\rangle$. Prawdopodobieństwo, że pomiar układu znajdującego się w takim stanie da wynik 0 wynosi ½; takie samo jest prawdopodobieństwo, że da wynik 1. A zatem procedura polegająca na:

1. Przygotowaniu układu kwantowego w stanie $|0\rangle$;
2. zastosowaniu operatora √NOT do tego układu;
3. pomiarze stanu;

jest procedurą całkowicie losową. Natomiast jeśli po pierwszym √NOT nie wykonamy pomiaru, ale drugi raz przeprowadzimy √NOT, to otrzymamy procedurę deterministyczną, która początkowy stan 0 z pewnością przeprowadzi na stan 1, zaś początkowy stan 1 na stan 0.

Pojawia się pewna pojęciowa trudność: obliczenia, które pozwalają na wyliczenie prawdopodobieństw są elementarne i łatwo je prześledzić. Zarazem wydaje się rzeczą niepokojącą, że złożenie dwóch czynności losowych daje czynność deterministyczną. Pamiętajmy jednak, że nie dokonujemy pomiaru po pierwszym wykonaniu √NOT, ale od razu przekazujemy wynik do drugiego √NOT – zaś pomiar dokonywany jest dopiero na samym końcu. Gdybyśmy dokonali pomiaru po pierwszym √NOT, i układ poddali drugiemu działaniu √NOT, to drugi √NOT otrzymałby na wejściu stan $|0\rangle$ lub stan $|1\rangle$ (a nie stan $1/\sqrt{2}\,((1-i)|0\rangle + (1+i)|1\rangle)$, i pomiar układu po drugim √NOT dałby już wynik losowy.

Pomiar nie daje nam – w ogólnym przypadku – informacji na temat tego, w jakim stanie był układ przed pomiarem. Jeśli więc wykonamy obliczenie kwantowe i następnie wykonamy pomiar, to najczęściej nie dowiemy się, w jakim stanie był układ po wykonaniu obliczenia kwantowego. W ogólnym przypadku tracimy więc informację zawartą w wyniku obliczenia. Jednak czasem zdarza się, że znajomość wyniku pomiaru wraz z pewnymi dodatkowymi informacjami dotyczącymi ewolucji układu pozwoli na wywnioskowanie, jaki był stan układu przed pomiarem.

$|a_0|^2+|a_1|^2=1$ – chodzi o to, aby suma prawdopodobieństw poszczególnych pomiarów wynosiła 1.

Rozważmy prosty przykład: dany jest jeden kubit, o którym z góry wiemy, że znajduje się w jednym ze stanów bazowych 0 lub 1 (ale nie wiemy, w którym). Jeśli dokonamy pomiaru, to otrzymamy w ten sposób pełną informację na temat stanu (jeśli np. pomiar dał wynik 0, to znaczy, że kubit musiał być w stanie 0). Podobnie, jeśli mamy układ dwóch kubitów, i wiemy o nich np., że znajdują się w jednym z dwóch stanów:

$$\Phi_0: 1/\sqrt{2}(|00\rangle+|01\rangle)$$
$$\Phi_1: 1/\sqrt{2}(|10\rangle+|11\rangle)$$

i dokonamy pomiaru na pierwszym kubicie, to pomiar ten informuje nas o stanie układu. Tylko stan Φ_0 mógł dać wynik 0, tylko stan Φ_1 mógł dać wynik 1. Jeśli więc wiemy o stanie układu po ewolucji na tyle dużo, że pomiar pozwala na stwierdzenie, jaki był stan przed pomiarem, to można to wykorzystać w praktyce. Z taką sytuacją mamy do czynienia w najprostszym algorytmie kwantowym – algorytmie Deutcha.

5. Najprostszy algorytm kwantowy. W swobodnym sformułowaniu chodzi o problem, czy posiadana przez nas moneta jest zwykła (tzn. orzeł i reszka), czy oszukana (dwa orły lub dwie reszki). Ile stron monety musimy obejrzeć, aby się o tym przekonać? Oczywiście dwie.

Matematyczne sformułowanie tego problemu brzmi: dana jest funkcja f: $\{0,1\} \rightarrow \{0,1\}$, zaś naszym zadaniem jest przekonanie się, czy $f(0) = f(1)$ (moneta jest oszukana), czy też $f(0) \neq f(1)$ (moneta jest prawdziwa). Przypuśćmy, że mamy czarną skrzynkę, która oblicza wartość funkcji f (intuicyjnie, skorzystanie z tej skrzynki odpowiada obejrzeniu jednej ze stron monety). Ile razy trzeba skorzystać z tej funkcji, aby odpowiedzieć na pytanie o typ funkcji? Klasycznie – oczywiście dwa razy: trzeba zapytać o wartość $f(0)$, a następnie o wartość $f(1)$. W świecie kwantowym można zrobić to szybciej – wystarczy jednokrotne odwołanie się do czarnej skrzynki.

Naszej „czarnej skrzynce" odpowiada procedura U_f, która działa na dwóch kubitach w następujący sposób:

$$U_f: |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle,$$

gdzie symbol $\oplus$ oznacza dodawanie *modulo* 2 ($0\oplus0=0$; $0\oplus1=1$; $1\oplus0=1$; $1\oplus1=0$). Intuicyjnie, na drugim kubicie przechowujemy wartość funkcji f, gdzie argumentem jest pierwszy kubit. Algorytm Deutscha wygląda tak (dalej pomijam wszystkie współczynniki typu $1/\sqrt{2}$, ½ *etc.* aby uprościć zapis):

1. Startujemy od układu w stanie: pierwszy kubit $-|0\rangle$; drugi kubit $-|0\rangle - |1\rangle$. Stan całego układu można więc zapisać jako $|0\rangle(|0\rangle-|1\rangle)$. Poddajemy pierwszy kubit działaniu bramki Hadamarda, otrzymując:

$$H: |0\rangle(|0\rangle-|1\rangle) \rightarrow (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

2. Układ poddajemy działaniu procedury U_f:

$$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \rightarrow ((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)(|0\rangle - |1\rangle)$$[22]

Pierwszy kubit znajdzie się więc w stanie $(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$. Są dwie możliwości:

(1) Jeśli $f(0)=f(1)$, to stanem pierwszego kubitu jest $|0\rangle + |1\rangle$ lub $-(|0\rangle + |1\rangle)$
(2) Jeśli $f(0) \neq f(1)$, to stanem pierwszego kubitu jest $|0\rangle - |1\rangle$ lub $-(|0\rangle - |1\rangle)$

Poddajemy pierwszy kubit transformacji Hadamarda, otrzymując:

- w przypadku (1): stan $|0\rangle$ lub $-|0\rangle$
- w przypadku (2): stan $|1\rangle$ lub $-|1\rangle$

Teraz pomiar dokonany na pierwszym kubicie daje nam już pewność co do tego, jaki był stan sprzed pomiaru. Tym samym dowiadujemy się, czy zachodzi sytuacja (1) czy (2).

Zauważmy, że algorytm Deutscha składa się z wykonania trzech operacji: bramki Hadamarda na pierwszym kubicie; zastosowania procedury U_f, powtórnej bramki Hadamarda na pierwszym kubicie. Pomiar może zostać wykonany dopiero na końcu – gdyby bowiem dokonać pomiaru w trakcie, wówczas stan kubitu ustaliłby się. Nie można zatem kontrolować przebiegu obliczenia w jego trakcie, bo to zaburzy obliczenie w nieodwracalny sposób. Podkreślmy, że w tym algorytmie korzystaliśmy z operacji U_f tylko raz!

Uogólnieniem algorytmu Deutscha jest algorytm Deutscha-Jozsy, w którym mamy funkcję $f:\{0,1\}^n \rightarrow \{0,1\}$ (każdemu ciągowi 0-1 długości n przypisuje 0 lub 1). Wiemy z góry, że funkcja jest stała, lub że taką samą ilość razy przyjmuje wartość 0, co 1. Klasycznie, musimy skorzystać z

[22] Czytelnik ma do wyboru: (1) obliczyć, traktując to jako ćwiczenie; (2) uwierzyć.

obliczenia wartości funkcji f około 2^{n-1} razy[23]. Algorytm Deuscha-Jozsy rozwiązuje problem w czasie wielomianowym. Również w przypadku tego algorytmu nie można kontrolować poszczególnych etapów eksperymentu.

Artykuł jest z założenia elementarny, więc nie będę tu opisywał innych algorytmów kwantowych. Z punktu widzenia dalszej dyskusji ważne jest to, że działają one w sposób wykładniczo szybszy, niż algorytmy klasyczne, i że opierają się na specyfice zjawisk kwantowych.

Opisane zjawiska skłaniają do podjęcia refleksji filozoficznej, dotyczącej statusu wiedzy uzyskanej na drodze eksperymentu kwantowego. Problem staje się szczególnie ciekawy w przypadku pytania o status uzyskanej w ten sposób wiedzy matematycznej. Temu zagadnieniu poświęcona jest ostatnia część artykułu.

III. INSPIRACJE DLA FILOZOFII[24]**.** Tradycyjny pogląd na wiedzę matematyczną przypisuje jej status wiedzy apriorycznej, dotyczącej niezmiennych, pozaczasowych bytów abstrakcyjnych. W myśl tego poglądu intuicyjnie postrzegamy pewne pierwotne prawdy jako oczywiste; intuicyjnie postrzegamy też fakt, że dowody matematyczne stanowią właściwe narzędzie „transmisji prawdy" od prawd pierwotnych do twierdzeń. Źródłem wiedzy matematycznej jest więc rozum. W przypadku dowodów matematycznych opartych na obliczeniu kwantowym pojawia się jednak zasadniczo nowa jakość.

Przypomnijmy krótko dyskusję dotyczącą statusu komputerowych dowodów twierdzeń matematycznych (np. twierdzenia o czterech barwach)[25]. W toczącej się na ten temat dyskusji podejmowano problem, czy odwołanie do elementów empirycznych (działania pewnego urządzenia elektronicznego w określonym miejscu i czasie) nie wprowadza do matematyki elementów, które naruszają status dowodu matematycznego jako bytu pozaczasowego, idealnego, opisywanego w kategoriach czysto rozumowych *etc.* W tej sprawie można – w uproszczeniu – wyróżnić dwa skrajne stanowiska:

(1) Dowód komputerowy jest czymś istotnie nowym, ponieważ odwołuje się do przeprowadzonego eksperymentu.

---

[23] Jeśli mamy szczęście, to już za drugim razem otrzymamy różne wyniki, i wiemy, że funkcja nie jest stała. Jeśli mamy pecha, to 2^{n-1} razy otrzymamy ten sam wynik, i musimy zapytać jeszcze raz, aby rozstrzygnąć, czy funkcja jest stała, czy nie.

[24] Ponieważ celem artykułu jest zwrócenie uwagi Czytelnika na pewne zagadnienia, a nie ich szczegółowa analiza, więc uwagi te mają charakter szkicowy.

[25] Zainteresowanego Czytelnika odsyłam do pracy [Tymoczko 1979].

(2) Dowód komputerowy nie jest niczym nowym, ponieważ znamy zasadę działania komputera i w zasadzie (choć nie w praktyce) możemy prześledzić krok po kroku całe obliczenie wykonane przez komputer[26].

Kiedy mówimy o obliczeniach, o procedurach mechanicznych, to mamy na myśli właśnie takie procedury, dla których modelem jest maszyna Turinga. Taki proces składa się z elementarnych kroków, mamy wgląd w obliczenie na każdym jego etapie. Teoretycznie, możemy więc prześledzić dowód 4CT, możemy rozłożyć obliczenie na elementarne kroki i poddać je analizie. Jak natomiast przebiegałby kwantowy dowód twierdzenia matematycznego[27]? Schematycznie, możemy taki dowód przedstawić w następujący sposób:

1. Faza koncepcyjna:
Należy zdefiniować układ kwantowy (i obliczenie kwantowe) tak, aby zachodziła odpowiedniość między jego ewolucją a obliczeniem komputera (i aby ewolucja kwantowa dawała odpowiedź na postawione pytanie). W szczególności obejmuje to ustalenie zależności między wynikami pomiaru po skończonej ewolucji, a odpowiedzią na nasze pytanie.

2. Faza eksperymentalna:
2.1. Przygotowanie układu kwantowego w odpowiednim stanie początkowym.
2.2. Przeprowadzenie ewolucji układu kwantowego.
2.3. Po skończonej ewolucji wykonanie pomiaru.

Dzięki temu, że ewolucja układu kwantowego została zdefiniowana w odpowiedni sposób, pomiar pozwala na znalezienie odpowiedzi na pytanie. Można powiedzieć, że taki kwantowy dowód realizuje ideę sformułowaną przez Feynmana w [Feynman 1982]: to nie obliczenie komputerowe symuluje proces fizyczny, ale skonstruowany został proces fizyczny, który prowadzi do takiego samego wyniku, jak obliczenie komputera (jednak w czasie wykładniczo szybszym). Wprawdzie nie doczekamy się więc końca obliczeń komputera (Słońce zgaśnie wcze-

[26] Możemy na przykład zażyczyć sobie wydruku operacji od numeru 100.000 do 110.000 i sprawdzić je krok po kroku.

[27] Nie jest tu istotne, czy byłoby to twierdzenie głębokie i doniosłe, czy twierdzenie matematycznie mało ciekawe, jak np. twierdzenie, że dana formuła rachunku zdań jest tautologią. Chodzi o samą zasadę.

śniej), ale dzięki eksperymentowi kwantowemu wiemy, jaki byłby wynik tych obliczeń[28].

Zauważmy, że dokonanie pomiaru w trakcie ewolucji spowoduje ustalenie stanu kwantowego i zniszczy całą operację. W przypadku klasycznych dowodów komputerowych mamy (teoretycznie) wgląd w każdy krok obliczenia. Możemy lokalnie sprawdzić, czy faktycznie urządzenie liczące działa zgodnie z naszymi oczekiwaniami. Jesteśmy więc przekonani o tym, że komputer robi dokładnie to, co robiłby człowiek (bardzo skrupulatny pod względem formalnej poprawności), tyle że znacznie szybciej[29]. Jednak w wypadku obliczenia kwantowego powstaje jakościowa różnica w stosunku do obliczenia klasycznego. nie możemy kontrolować przebiegu ewolucji układu kwantowego, w przeciwieństwie do obliczenia komputera.

Z naszego punktu widzenia, elementarną operacją jest cała ewolucja kwantowa (która może polegać na przejściu 1 kubitu przez jedną bramkę, ale też na przejściu 1000 kubitów przez system 1000 bramek kwantowych) – i taką ewolucję należy traktować jako niepodzielną całość, jako – obrazowo mówiąc – swoistą „czarną skrzynkę". Dowód matematyczny opierający się na obliczeniach kwantowych opierałby się więc na zaufaniu do działania takich kwantowych czarnych skrzynek. Pomiar jest wykonywany dopiero na końcu całego ciągu operacji, nie możemy więc „zaglądać" do układu kwantowego w trakcie jego ewolucji. Ewolucja układu nie przebiega zgodnie z instrukcjami jakiejkolwiek maszyny Turinga – nie jest to więc obliczenie w klasycznym sensie tego słowa. Nie można twierdzić, że układ fizyczny wykonuje to samo, co człowiek, tyle że szybciej – działanie tego układu opiera się bowiem na zupełnie innej zasadzie, niż klasyczny proces obliczeniowy. Na obliczenie nie możemy już patrzeć jako na pewien wyidealizowany proces logiczny (zaimplementowany w komputerze), ale jako na pewien proces fizyczny, którego ewolucja związana jest w fundamentalny sposób ze specyfiką świata kwantowego. Realizacja tego procesu jest możliwa tylko w świecie kwantowym i tylko eksperyment kwantowy dostarczy nam tej nowej wiedzy matematycznej. Jest to fakt, który skłania do podjęcia filozoficznej refleksji. Jeśli uznamy kwantowe dowody za prawomocne, to problem wiedzy matematycznej zostaje uwikłany w cały

[28] Ta uwaga ma oczywiście charakter hipotetyczny - na razie nie ma komputerów kwantowych, ze względu na trudności techniczne dotyczące chronienia układów kwantowych przed zaburzeniami zewnętrznymi.

[29] Nie znaczy to bynajmniej, że bagatelizuję trudności filozoficzne związane z klasycznymi dowodami komputerowymi, por. [Wójtowicz ?].

splot trudności filozoficznych związanych z mechaniką kwantową: problem pomiaru, problem interpretacji mechaniki kwantowej *etc.* Filozofia matematyki zaciąga więc poważny dług u filozofii fizyki.

Zakończę kilkoma uwagami dotyczącymi problemu mechanizacji myślenia i komputacyjnej teorii umysłu. Główną tezą komputacyjnej teorii umysłu jest to, że umysł działa (na stosownie głębokim poziomie) jak maszyna Turinga[30]. Postawmy następujące pytanie: co by było, gdyby mózg w swoim działaniu wykorzystywał specyfikę kwantowego przetwarzania informacji?[31]. Zauważmy, że opisane wyżej algorytmy kwantowe mogą być symulowane poprzez algorytmy klasyczne (w ogólnym przypadku) z wykładniczą stratą czasu. Jednak jeśli umysł miałby być maszyną Turinga, to jego działanie winno odbywać się (z definicji) w czasie rzeczywistym. Gdyby więc dla naszego myślenia znaczenie miały zjawiska kwantowe, to powstałaby następująca sytuacja:

1. Umysł działa kwantowo.
2. Można to (teoretycznie) symulować na maszynie Turinga.
3. Ale umysł nie może tego symulować w czasie rzeczywistym.

Czy w tej sytuacji zasadne byłoby stwierdzenie, że wprawdzie umysł faktycznie nie działa jak maszyna Turinga, ale co do zasady działa jak maszyna Turinga?[32]. Ten problem wymaga analizy. Sądzę więc, że problematyka obliczeń kwantowych jest też ważna z punktu widzenia (nie tylko komputacyjnej) teorii umysłu.

[30] Por. np. http://plato.stanford.edu/entries/computational-mind/.

[31] Tezę, że dla opisania ludzkiej świadomości znaczenie mogą mieć zjawiska kwantowe od dawna stawia np. Penrose (popularną prezentację zawiera [Penrose 2000]).

[32] Przypuśćmy, że ktoś mnoży (w standardowy sposób na kartce) dwie duże liczby, a następnie twierdzi, że co do zasady on wcale nie mnoży, tylko dodaje – bo przecież zamiast mnożyć liczby *n* oraz *m* przez siebie, wystarczy dodać do siebie *m* razy liczbę *n*. Czy ktoś, kto zgadł, jaki jest poprawny wynik obliczenia ma prawo powiedzieć, że co do zasady on obliczył – po przecież wynik jest taki sam i jego zgadywanie jest funkcjonalnie nieodróżnialne od obliczenia?

BIBLIOGRAFIA:

Deutsch D,. Ekert A., Lupacchini R.
[2000] *Machines, Logic and Quantum Physics.* "The Bulletin of Symbolic Logic", 6 (3), 265-283.
Feynman R.P.
[1982] *Simulating physics with computers.* "International Journal of Theoretical Physics", 21, 467-488.
Johnson G.
[2005] Na skróty przez czas. Prószyński i S-ka, Warszawa.
Giaro K., Kamiński M.
*[2003] Wprowadzenie do algorytmów kwantowych. Akademicka Oficyna Wydawnicza EXIT, Warszawa.
Hirvensalo M.
[2004] Algorytmy kwantowe. Wydawnictwa Szkolne i Pedagogiczne S.A., Warszawa.
Milburn G.
[2000] Procesor Feynmana. Wydawnictwo CiS, Warszawa.
Penrose R.
[2000] Nowy umysł cesarza. PWN, Warszawa.
Tymoczko T.
[1979] *The four-color problem and its philosophical significance.* "The Journal of Philosophy", 76 (2), 57-83. Przekład polski *Problem czterech barw i jego znaczenie filozoficzne*, w: *Współczesna filozofia matematyki*, Murawski R. (red.), PWN, Warszawa, 2002, 310-340.
Wójtowicz K.
Eksperyment komputerowy – źródło wiedzy matematycznej?, w przygotowaniu.