Piotr FORMANOWICZ
Instytut Informatyki, Politechnika Poznańska

O ZŁOŻONOŚCI OBLICZEŃ KWANTOWYCH

Streszczenie. W ciągu ostatnich lat rozwój komputerów kwantowych istotnie przyspiesza i stają się one dostępne dla coraz szerszych grup użytkowników. Istnieją oczekiwania, że niezwykła moc obliczeniowa tego typu komputerów pozwoli na rozwiązywanie problemów trudnych do rozwiązania za pomocą komputerów klasycznych. Równolegle do rozwijania komputerów kwantowych od strony sprzętowej od lat badana jest złożoność obliczeń kwantowych. Uzyskanie w tej dziedzinie wyniki wskazują, że możliwości obliczeniowe tego rodzaju komputerów mogą nie być tak imponujące, jak się tego niekiedy oczekuje. W niniejszym artykule przedstawione zostało krótkie omówienie obecnego stanu wiedzy na temat możliwości obliczeniowych komputerów kwantowych.

ON COMPLEXITY OF QUANTUM COMPUTING

Summary. In recent years the development of quantum computers is considerably increasing and they are becoming available for growing groups of users. There are expectations that their enormous computing power will allow to solve problems very hard for classical computers. In parallel to the development of quantum computing hardware the complexity of quantum computations is investigated for years. The obtained results in this area indicate, that the real computing power of quantum computers may be not so impressive as sometimes expected. In this paper a brief overview of the current knowledge about the computational abilities of quantum computers is presented.

1. Wprowadzenie

Komputery kwantowe stają się w ostatnich latach coraz bardziej popularne w tym sensie, że coraz więcej się o nich mówi, rosną oczekiwania związane z ich potencjalnymi zastosowaniami, a w wielu ośrodkach można uzyskać dostęp do systemów umożliwiających przeprowadzanie obliczeń za pomocą komputerów tego rodzaju lub symulatorów komputerów kwantowych. Można powiedzieć, że trwa wyścig do zbudowania komputera kwantowego mającego znaczenie komercyjne, w którym biorą udział największe firmy z szeroko rozumianego świata informatycznego, takie jak IBM czy Google. Innymi słowy, jesteśmy świadkami bardzo ważnego momentu w historii informatyki oraz nauk pokrewnych.

Warto zatem pamiętać o kilku sprawach ściśle związanych z obliczeniami kwantowymi, które pozwolą docenić to, co właśnie obserwujemy, ale też właściwie ocenić rodzące się nowe możliwości obliczeniowe. A zatem warto zwrócić uwagę na fakt, że idea

obliczeń kwantowych nie jest nowa, gdyż mówił o niej już Richard Feynman w 1981 roku [8]. Niestety, w tamtym okresie jego idee nie miały żadnych szans na realizację, jednak kilkanaście lat później, na początku ostatniej dekady XX wieku nastąpił wyraźny wzrost zainteresowania przeprowadzaniem obliczeń w sposób bezpośrednio wykorzystujący mechanikę kwantową. Warto zauważyć, że podobnie jak to było w przypadku klasycznej informatyki, rozwój teorii informatyki kwantowej znacznie wyprzedził (i nadal wyprzedza) rozwój sprzętu, za pomocą ktorego można by tę teorię implementować.

Drugą sprawą, którą należy mieć na uwadze, są trudności związane z budową komputerów kwantowych, wynikające wprost z mechaniki kwantowej. Jednym z głównych ich źródeł jest dekoherencja, czyli znikanie kwantowej superpozycji (będącej źródłem mocy obliczeniowej komputerów kwantowych) przy oddziaływaniu układu kwantowego z jego otoczeniem. Oczywiście, oddziaływania takiego nie można całkowicie wyeliminować, a gdy zachodzi ono w sposób nieporządany, jest przyczyną powstawania błędów. Błędy te można korygować, jednak by taka korekcja była efektywna, jej tempo musi być większe niż tempo powstawania nowych błędów. Jest to nadal jedno z głównych wyzwań stojących przed konstruktorami komputerów kwantowych.

Trzecią sprawą, której należałoby być świadomym, jest fakt, że nie wszystkie kwantowe urządzenia umożliwiające przeprowadzanie obliczeń i nazywane komputerami kwantowymi, są w rzeczywistości komputerami. Komputer powinien umożliwiać wykonywanie dowolnych operacji przetwarzania danych, a nie wszystkie urządzenia określane jako komputery kwantowe spełniają ten warunek.

Wreszcie czwartą, niezwykle ważną kwestią, są rzeczywiste możliwości i ograniczenia komputerów kwantowych. Panuje dosyć powszechne przekonanie o ich niezwykłej mocy obliczeniowej wynikającej z przetwarzania wszystkich potencjaalnych rowiązań jednocześnie dzięki kwantowej równoległości. Wyobrażenia te czasami mijają się z rzeczywistością, a kwantowa rónoległość ma swoje granice, które stanowi proces odczytywania rozwiązania. Spośród wszystkich potencjalnych rozwiązań odczytywane jest wtedy tylko jedno, losowo wybrane w wyniku zajścia zjawiska, które mimo stu lat badań nad mechaniką kwantową nadal pozostaje zagadką, czyli redukcji funkcji falowej. Ujmując rzecz bardzo ogólnie, idea algorytmów kwantowych polega na tym, by w trakcie ich wykonywania spośród potencjalnych rozwiązań przetwarzanych równolegle wyeliminowane zostały te (albo przynajmniej ich większość), które nie odpowiadają poszukiwanemu rozwiązaniu. Wtedy w momencie odczytu rozwiązania jest duża szansa na uzyskanie rozwiązania właściwego. Nie należy jednak zapominać o tym, że obliczenia kwantowe mają naturę probabilistyczną. Innymi słowy, komputery kwantowe nie są urządzeniami magicznymi i mają swoje ograniczenia, choć nie zostały one do końca poznane.

Przedstawieniu obecnego stanu wiedzy na temat tych ograniczeń poświęcony jest niniejszy artykuł.

2. Złożonośc obliczeniowa

Komputery kwantowe postrzega się czasem jako urządzenia, które dokonają wielkiego przełomu w obliczeniach, gdyż będą w stanie rozwiązywać problemy **NP**-zupełne lub **NP**-trudne w czasie wielomianowym. Do powstania takich oczekiwań względem tych komputerów przyczynił się prawdopodobnie w dużym stopniu algorytm Shora za-

proponowany w 1994 roku, który rozwiązuje problem faktoryzacji (tj. rozkładu liczb na czynniki pierwsze) na komputerze kwantowym w czasie wielomianowym [12]. Algorytm ten pobudza wyobraźnię, gdyż gdyby można go stosować w praktyce, wiele z powszechnie stosowanych zabezpieczeń kryptograficznych opartych na kluczu publicznym stałoby się co najmniej mało skutecznych. Należy jednak zwrócić uwagę, że istnienie algorytmu Shora nie oznacza, że za pomocą komputera kwantowego można rozwiązać w czasie wielomianowym problem **NP**-zupełny, gdyż nie wiadomo, czy problem faktoryzacji (w wersji decyzyjnej) należy do klasy problemów **NP**-zupełnych. Przypuszcza się, że nie należy on do tej klasy, mimo że nie jest znany dla niego klasyczny algorytm wielomianowy. Jeżeli miałoby się okazać, że za pomocą komputerów kwantowych można rozwiązywać w czasie wielomianowym problemy **NP**-zupełne, oznaczałoby to, że klasa **NP** jest zawarta w klasie problemów rozwiązywalnych w czasie wielomianowym przez tego rodzaju komputery. By móc prowadzić ścisłe rozważania na ten temat, należy określić odpowiedni model obliczeń oraz oparte na nim klasy złożoności związane z obliczeniami kwantowymi. W literaturze zostało to zrobione już wiele lat temu [6].

Ze względu na fakt, że obliczenia kwantowe mają naturę probabilistyczną, warto przypomnieć definicję probabilistycznej maszyny Turinga (por. [9]):

Definicja 1
Probabilistyczna maszyna Turinga (PTM) jest uporządkowaną szóstką $M = (Q, \Sigma, \Gamma, \delta, q_s, F)$, w której wszystkie składniki oprócz δ, są takie same jak w przypadku deterministycznej maszyny Turinga (DTM), natomiast δ jest rozkładem prawdopodobieństwa przejść, tzn. $\delta : Q \times \Gamma \times Q \times \Gamma \times \{\leftarrow, -, \rightarrow\} \rightarrow [0, 1]$. Dla każdej pary $(q_1, s_1) \in Q \times \Gamma$ musi być spełniony warunek $\Sigma_{(q_2,s_2,r)\in(Q\times\Gamma\times\{\leftarrow,-,\rightarrow\})}\delta(q_1, s_1, q_2, s_2, r) = 1$. □

W Definicji 1 $\delta(q_1, s_1, q_2, s_2, r)$ jest prawdopodobieństwem tego, że maszyna będąc w stanie q_1 i odczytując z taśmy symbol s_1 przejdzie w stan q_2, zapisze symbol s_2 i przesunie głowicę w kierunku r.

Kwantowa maszyna Turinga zdefiniowana jest bardzo podobnie do PTM (por. [6]):

Definicja 2
Kwantowa maszyna Turinga (QTM) jest uporządkowaną szóstką $M = (Q, \Sigma, \Gamma, \delta, q_s, F)$, w której wszystkie składniki oprócz δ, są takie same jak w przypadku DTM, natomiast δ jest funkcją amplitud prawdopodobieństwa przejść, tzn. $\delta : Q \times \Gamma \times Q \times \Gamma \times \{\leftarrow, -, \rightarrow\} \rightarrow \mathbb{C}$. Dla każdej pary $(q_1, s_1) \in Q \times \Gamma$ musi być spełniony warunek $\Sigma_{(q_2,s_2,r)\in(Q\times\Gamma\times\{\leftarrow,-,\rightarrow\})}|\delta(q_1, s_1, q_2, s_2, r)|^2 = 1$. □

W Definicji 2 $\delta(q_1, s_1, q_2, s_2, r)$ jest amplitudą prawdopodobieństwa tego, że maszyna będąc w stanie q_1 i odczytując z taśmy symbol s_1 przejdzie w stan q_2, zapisze symbol s_2 i przesunie głowicę w kierunku r. Amplituda prawdopodobieństwa jest liczbą zespoloną taką, że jej moduł podniesiony do kwadratu jest prawdopodobieństwem.

Przed przytoczeniem definicji klas złożoności problemów decyzyjnych związanych z obliczeniami kwantowymi warto przypomnieć definicje kilku klas złożoności związanych z obliczeniami klasycznymi, które mają z nimi ścisły związek (por. [9, 11, 10]).

Definicja 3
BPP jest klasą wszystkich języków L, dla których istnieje wielomianowa PTM M taka, że jeżeli $x \in L$, to M akceptuje x z prawdopodobieństwem równym co najmniej $\frac{2}{3}$, natomiast jeżeli $x \notin L$, to M odrzuca x z prawdopodobieństwem równym co najmniej $\frac{2}{3}$. □

Klasę **BPP** można też zdefiniować w oparciu o niedeterministyczną maszynę Turinga (NDTM) w nastepujący sposób:

Definicja 4
BPP jest klasą wszystkich języków L, dla których istnieje wielomianowa NDTM M taka, że jeżeli $x \in L$, to co najmniej $\frac{2}{3}$ ścieżek obliczeń maszyny M prowadzi do zaakceptowania x, natomiast jeżeli $x \notin L$, to co najwyżej $\frac{1}{3}$ ścieżek obliczeń maszyny M prowadzi do zaakceptowania x. □

Definicja 5
ZPP jest klasą wszystkich języków L, dla których istnieje wielomianowa PTM M taka, że dla ciągu wejściowego x maszyna M zatrzymuje się z prawdopodobieństwem równym co najmniej $\frac{1}{2}$ i w takim przypadku, jeżeli $x \in L$, to maszyna M akceptuje x z prawdopodobieństwem równym 1, natomiast jeżeli $x \notin L$, to M odrzuca x z prawdopodobieństwem równym 1. □

Definicja 6
PP jest klasą wszystkich języków L, dla których istnieje wielomianowa NDTM M taka, że jeżeli $x \in L$, to co najmniej $\frac{1}{2}$ ścieżek obliczeń maszyny M prowadzi do zaakceptowania x, natomiast jeżeli $x \notin L$, to mniej niż $\frac{1}{2}$ ścieżek obliczeń maszyny M prowadzi do zaakceptowania x. □

Definicja 7
P/poly jest klasą problemów decyzyjnych rozwiązywalnych przez rodzinę układów logicznych o wielomianowych wielkościach. Rodzina ta może być niejednorodna, co oznacza, że dla różnych wielkości instancji danego problemu może ona zawierać różne układy. □

Spośród wymienionych klas złożoności warto zwrócić szczególną uwagę na klasę **BPP**, gdyż jest ona ściśle związana z podstawową kwantową klasą złożoności, tj. klasą **BQP** zdefiniowaną w następujący sposób [6].

Definicja 8
BQP jest klasą wszystkich języków L, dla których istnieje wielomianowa QTM M taka, że jeżeli $x \in L$, to M akceptuje x z prawdopodobieństwem równym co najmniej $\frac{2}{3}$, natomiast jeżeli $x \notin L$, to M odrzuca x z prawdopodobieństwem równym co najmniej $\frac{2}{3}$. □

Jak nietrudno zauważyć, klasa **BQP** jest kwantowym odpowiednikiem klasy **BPP**. Ponadto, warto przytoczyć definicje dwóch innych kwantowych klas złożoności, tj. klas **EQP** i **ZQP** [13].

Definicja 9
EQP jest klasą wszystkich języków L, dla których istnieje wielomianowa QTM M taka, że jeżeli $x \in L$, to M akceptuje x z prawdopodobieństwem równym 1, natomiast jeżeli $x \notin L$, to M odrzuca x z prawdopodobieństwem równym 1. □

Definicja 10
ZQP jest klasą wszystkich języków L, dla których istnieje wielomianowa QTM M taka, że dla ciągu wejściowego x maszyna M zatrzymuje się z prawdopodobieństwem równym co najmniej $\frac{1}{2}$ i w takim przypadku, jeżeli $x \in L$, to M akceptuje x z prawdopodobieństwem równym 1, natomiast jeżeli $x \notin L$, to M odrzuca x z prawdopodobieństwem równym 1. □

Klasa **EQP** jest kwantowym odpowiednikiem klasy **P**, natomiast klasa **ZQP** to kwantowy odpowiednik klasy **ZPP**.

Ze wzgledu na fakt, że klasa **BQP** jest klasą problemów decyzyjnych, które komputery kwantowe rozwązują w czasie wielomianowym, dla oceny możliwości tego rodzaju komputerów istotne są związki tej klasy z innymi klasami złożoności.

Najważniejsze jest oczywiście pytanie, czy **NP**⊆**BQP**? Gdyby tak było, oznaczałoby to, że komputery kwantowe mogą rozwiązywać w czasie wielomianowym wszystkie problemy z klasy **NP**, a więc również problemy **NP**-zupełne. Niestety, nie wiadomo, czy klasa **NP** jest zawarta w klasie **BQP**, ale wiele wskazuje na to, że jest to mało prawdopodobne. Nie wiadomo też, czy **BQP**⊆**NP**.

Warto wrócić na chwilę do klasy, której kwantowym odpowiednikiem jest **BQP**, czyli klasy **BPP**. Można powiedzieć, że jest to klasa problemów rozwiązywalnych w czasie wielomianowym za pomocą klasycznych komputerów, przy czym należy zwrócić uwagę na fakt, że błąd obliczeń, który pojawia się w definicji tej klasy (prawdopodobieństwo uzyskania błędnej odpowiedzi równe $\frac{1}{3}$), można uczynić dowolnie małym przez powtórzenie obliczeń odpowiednią liczbę razy [1].

Podobnie jak nie wiadomo, czy **BQP**⊆**NP**, nie wiadomo również, czy **BPP**⊆**NP**, choć wiadomo, że **BPP**⊆$\mathbf{NP^{NP}}$ (czyli **BPP** jest zawarta w klasie problemów rozwiązywalnych przez NDTM z wyrocznią **NP**). Natomiast nie wiadomo, czy **BQP**⊆$\mathbf{NP^{NP}}$ (por [1]).

Ponieważ wspomniany wcześniej błąd związany z obliczeniami probabilistycznymi można uczynić dowolnie małym, może pojawić się pytanie, czy nie jest tak, że klasa problemów rozwiązywalnych w czasie wielomianowym za pomocą algorytmów probabilistycznych nie jest w rzeczywistości klasą problemów rozwiązywalnych w takim czasie za pomoca algorytmów deterministycznych, tj. czy **BPP=P**? Niestety, nie wiadomo, czy ta równość zachodzi, choć przypuszcza się, że tak.

Warto zwrócić również uwagę na związek klasy **BQP** z inną wcześniej zdefiniowaną klasą obliczeń probabilistycznych, tj. klasą **PP**. Otóż wiadomo, że **BQP**⊆**PP** oraz $\mathbf{PP^{BQP}}$**=PP** (przy czym **PP**⊆**PSPACE**⊆**EXP**) [4].

Należy zdawać sobie sprawę z tego, że niejednorodność obliczeń jest ściśle związana z losowością. Zauważmy, że **BPP**⊂**P/poly**, tzn. niejednorodność obliczeń daje większe możliwości niż losowość. Zauważmy dalej, że gdyby zachodziła inkluzja **NP**⊆**BPP**, to ze względu na **BPP**⊂**P/poly**, zachodziłoby też zawieranie **NP**⊂**P/poly**,

a to z kolei oznaczałoby, że **PH** (hierachia wielomianowa) zapadałaby się do drugiego poziomu. Jeżeli jednak **PH** jest nieskończona, oznacza to, że problemy **NP**-zupełne nie są rozwiązywalne w wielomianowym czasie przez algorytmy probabilistyczne [11, 10].

Jaki jest jednak konkretnie związek klasy **BPP** z klasą **BQP**? Nasuwa się naturalne przypuszczenie, że wszystkie problemy, które można rozwiązać za pomocą algorytmów probabilistycznych w czasie wielomianowym można rozwiązać w takim czasie za pomocą komputerów kwantowych, czyli że **BPP**$\subseteq$**BQP**. Nie wiadomo jednak, czy **BPP**$\neq$**BQP**. Znana jest jednak wyrocznia, względem której **BPP**$\neq$**BQP** oraz taka, względem której **BQP**$\not\subset$**P/poly**. Co ciekawe, $\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$, czyli wielomianowa QTM z wyrocznią **BQP** ma taką samą moc obliczeniową, jak bez tej wyroczni [6].

Jak było wspomniane wcześniej, przypuszcza się że **BPP** $=$ **P**, jednak sądzi się, iż w przypadku obliczeń kwantowych analogiczna równość nie zachodzi, tzn. przypuszcza się, że **BQP** $\neq$ **P**. Jeżeli faktycznie tak jest, to **P** $\neq$ **PSPACE**, a pytanie o to, czy ta nierówność zachodzi, jest jednym z najważniejszych, nadal otwatych pytań teorii złożoności obliczeniowej.

Wiadomo, że **BQP**$\subseteq$**EXP**, czyli wszystkie problemy decyzyjne, które mogą być rozwiązane za pomocą komputerów kwantowych w czasie wielomianowym, mogą być również rozwiązane za pomocą klasycznych deterministycznych algorytmów w czasie wykładniczym. Oznacza to, że komputery kwantowe mogą dawać co najwyżej wykładnicze przyspieszenie (ale czy rzeczywiście dają wykładnicze przyspieszenie, pozostaje kwestią otwartą).

Jednym z najbardziej istotnych, dotąd nierozwiązanych problemów dotyczących złożoności obliczeń kwantowych, jest pytanie, czy zachodzi inkluzja **BQP**$\subseteq$**PH**? Nie tylko nie wiadomo, czy ta inkluzja zachodzi, ale nie wiadomo też, czy istnieje wyrocznia, względem której zachodzi **BQP**$\not\subset$**PH**. Mimo prawie trzydziestu lat badań tego problemu, na pytanie to nie udało się dotąd znaleźć odpowiedzi.

Jak było wspomniane wcześniej, nie wiadomo, czy **NP**$\subseteq$**BQP**, a co więcej, nie wiadomo, jak można by udowodnić, że **NP**$\not\subset$**BQP** przy założeniu, iż **P**$\neq$**NP**. Wiadomo natiomiast, że istnieje wyrocznia, względem której **NP**$\not\subset$**BQP** [5].

Wcześniej było wspomniane, że algorytmem, który w znacznym stopniu przyczynił się do rozbudzenia oczekiwań względem komputerów kwantowych już na samym początku rozwoju informatyki kwantowej, był kwantowy wielomianowy algorytm Shora dla problemu rozkładu liczb na czynniki pierwsze. Gdyby decyzyjna wersja tego problemu była problemem **NP**-zupełnym, istnienie algorytmu Shora byłoby dowodem na to, że za pomocą komputerów kwantowych można tego typu problemy rozwiązywać w czasie wielomianowym, tzn. zachodziłaby zależność **NP**$\subseteq$**BQP**. Niestety, nie wiadomo, czy decyzyjna wersja tego problemu należy do klasy problemów **NP**-zupełnych. Jest ona elementem klasy **NP**$\cap$**coNP**. A zatem, gdyby ten problem był **NP**-zupełny, oznaczałoby to, że **NP=coNP**, co wydaje się być mało prawdopodobne.Warto przy tym zwrócić uwagę na fakt, że pytanie o równość klas **NP** i **coNP** jest co najmnej tak trudne jak pytanie o równość klas **P** i **NP** (por. [1]).

3. Algorytmy

Na podstawie znanych zależności między klasami złożoności opisanych w poprzednim rozdziale widać, że istnieją ścisłe związki między podstawową klasą związaną

z obliczeniami kwantowymi, czyli **BQP**, oraz wieloma innymi, badanymi od lat klasami. Co więcej, związki te są tego rodzaju, że gdyby okazało się, iż za pomocą komputerów kwantowych można rozwiązywać problemy **NP**-zupełne w czasie wielomianowym, to wiele podstawowych, otwartych od lat problemów teorii złożoności obliczeniowej zostałoby rozwiązanych, przy czym niektóre z nich w sposób niezgodny z oczekiwaniami większości specjalistów z tej dziedziny. Widać więc, że pytanie o to, czy korzystając z komputerów kwantowych można rozwiązywać problemy **NP**-zupełne w czesie wielomianowym jest kolejnym fundamentalnym problemem dotyczącym natury obliczeń.

Znanych jest niewiele algorytmów kwantowych dających wykładnicze przyspieszenie w stosunku do ich najlepszych znanych odpowiedników klasycznych, jednak żaden z nich nie rozwiązuje problemu **NP**-zupełnego. Jednym z takich algorytmów jest algorytm Shora. Zauważmy, że w przypadku tego algorytmu wykorzystane zostały pewne szczególne własności problemu faktoryzacji, które pozwoliły na konstrukcję efektywnego algorytmu kwantowego. Wiele wskazuje na to, że w przypadku problemów **NP**-zupełnych, w celu uzyskania efektywnego algorytmu kwantowego również należałoby skorzystać z pewnych szczególnych własności tych problemów. Innymi słowy, sama kwantowa równoległość najprawdopodobniej nie wystarczy, by w przypadku tych problemów uzyskać efektywne algorytmy. Trudność polega jednak na tym, że dotąd nikomu nie udało się odkryć odpowiednich własności tych problemów. Warto zauważyć, że sytuacja ta niewiele różni się od tej, z którą mamy do czynienia w przypadku komputerów klasycznych – tutaj również prawdopodobnie potrzebna byłaby znajomość pewnych szczególnych własności problemów **NP**-zupełnych, by móc zaprojektować dla nich algorytmy wielomianowe. Być może jednak problemy te nie mają własności, na których można by oprzeć konstrukcję efektywnych algorytmów, ani klasycznych, ani kwantowych.

Warto w tym miejscu wspomnieć, iż już ponad 20 lat temu zostało pokazane, iż każdy kwantowy algorytm działający na zasadzie czarnej skrzynki ma złożoność co najmniej $O(2^{\frac{n}{2}})$, gdzie 2^n jest wielkością przestrzeni rozwiązań danego problemu [5]. Nie jest to oczywiście wykładnicze przyspieszenie w stosunku do algorytmu klasycznego, który ma złożoność $O(2^n)$.

4. Rozszerzenia

Wiele wskazuje na to, że komputery kwantowe powodują, iż zbliżyliśmy się do granic możliwości obliczania tego, co jest możliwe do obliczenia zgodnie z obowiązującymi prawami fizyki. Na ogół teoria obliczeń i teoria złożoności obliczeniowej postrzegane są jako dziedziny nauki odległe od fizyki, a jedyny punkt wspólny między nimi stanowi sprzęt, za pomocą którego obliczenia są wykonywane. Jednak, jak wiadomo, obie te teorie abstrahują od konkretnych realizacji komputerów wykorzystywanych do przeprowadzania obliczeń. A zatem fizyka nie ma (albo raczej nie miała) żadnego związku z oboma tymi obszarami informatyki teoretycznej. Sytuacja ta jednak istotnie się zmieniła wraz z pojawieniem się idei komputerów kwantowych. Metody wykonywania obliczeń za pomocą tego typu komputerów wprost odwołują się do jednej z dwóch fundamentalnych teorii fizycznych, czyli do mechaniki kwantowej. A zatem wykonując obliczenia za pomocą komputerów kwantowych korzysta się wprost z podstawowych praw opisujących funkcjonowanie Wszechświata i wpływają one bezpośrednio na to, co

można obliczyć dysponując określonymi zasobami (na ogół są nimi czas i pamięć). Tak jest, jeśli mechanika kwantowa poprawnie opisuje własności Wszechświata.

Można zadać jednak pytanie, co by było, gdyby mechanika kwantowa w obecnie uznawanej postaci nie była teorią poprawnie opisującą świat, w którym żyjemy? Pytania tego typu stawiane są od dawna i można przykładowo rozważać, jak ewentualna nieliniowość równań mechaniki kwantowej wpłynęłaby na możliwości komputerów kwantowych (równania tej teorii w wersji obecnie uznawanej są liniowe). Okazuje się, że taka nieliniowość miałaby poważne konsekwencje, gdyż powodowałaby, że za pomocą tego typu komputerów można by rozwiązywać w czasie wielomianowym problemy **NP**-zupełne. Niestety, powodowałaby ona również, że nie byłaby zachowana zasada nieoznaczoności oraz że informacja mogłaby być przesyłana z szybkością większą niż szybkość światła, co powoduje, iż wydaje się być mało prawdopodobne, że mechanika kwantowa jest nieliniowa [3].

Inną, wydawałoby się dosyć egzotyczną możliwością, która mogłaby istotnie wpłynąć na własności komputerów kwantowych, jest istnienie zamkniętych krzywych czasoposobnych. Ich istnienie oznacza, że możliwe byłyby podróże w czasie. Choć może się to kojarzyć bardziej z literaturą SF niż z informatyką teoretyczną, to obecnie znane prawa fizyki nie wykluczają istnienia takich krzywych. Gdyby one faktycznie istniały, teoretycznie możliwe byłoby uruchomienie obliczeń na komputerze kwantowym i otrzymanie po niedługim czasie odpowiedzi z przyszłości. Na pierwszy rzut oka daje to niezwykłe możliwości, ale pojawia się znany problem związany z podróżami w czasie, tzn. po otrzymaniu odpowiedzi można by wyłączyć komputer, więc nie mógłby on dokończyć wykonywania obliczeń, a więc i wynik nie mógłby zostać przysłany z przyszłości. Okazuje się jednak, ze w przypadku wykonywania tego typu obliczeń za pomocą komputera kwantowego, paradoks ten można rozwiązać [7]. Co ciekawe jednak, nawet komputer kwantowy korzystający z zamkniętych krzywych czasopodobnych (a zatem bardzo silnego, hipotetycznego, mechanizmu) mógłby w czasie wielomianowym rozwiązywać problemy co najwyżej z klasy **PSPACE**. Ponadto, w przypadku możliwości korzystania w obliczeniach z zamkniętych krzywych czasopodobnych komputery kwantowe i komputery klasyczne miałyby taką samą moc obliczeniową [2].

Przytoczone dwa przykłady hipotetycznego zwiększenia możliwości komputerów kwantowych pokazują, jak mocno obliczalność i złożoność obliczeniowa związane są z naturą wszechświata, w którym żyjemy. Nie powinno to jednak dziwić, gdyż informacja jest obok materii i energii podstawowym składnikiem Wszechświata i jest z nimi ściśle związana.

5. Podsumowanie

W niniejszej pracy podjęto próbę przedstawienia obecnego stanu wiedzy na temat możliwości obliczeniowych komputerów kwantowych. Oczywiście, nie jest to zagadnienie proste, a ze względu na ograniczoną objętość pracy, próba ta mogła być nieco ryzykowna z powodu konieczności ostrej selekcji omawianych zagadnień. Tym niemniej, ponieważ badania możliwości komputerów kwantowych (tzn. złożoności obliczeń kwantowych) znacznie wyprzedziły ich skonstruowanie, wiele w tej dziedzinie już wiadomo, zwłaszcza na temat związków złożoności obliczeń kwantowych ze złożonością obliczeń klasycznych. Obecnie pytanie o to, czy komputery kwantowe mogą rozwiązywać pro-

blemy **NP**-zupełne w czasie wielomianowym pozostaje otwarte i dołączyło do wielu innych istotnych, nierozwiązanych od lat, problemów teorii złożoności obliczeniowej. Dosyć powszechne jest jednak przekonanie, że odpowiedź na nie jest negatywna. Jednakże, nawet jeśli tak jest w rzeczywistości, mogą one dawać istotne przyspieszenie w stosunku do komputerów klasycznych dla pewnych klas problemów. Z pewnością warto śledzić ich rozwój, gdyż mogą one odegrać istotną rolę w rozwoju informatyki, a także fizyki, prowadząc do lepszego zrozumienia procesów przetwarzania informacji na poziomie kwantowym oraz umożliwiając rozwiązywanie coraz bardziej złożonych problemów, podobnie jak to ma miejsce w przypadku nowych generacji komputerów klasycznych.

LITERATURA

1. Aaronson S.: Quantum Computing Since Democritus. Cambridge University Press, Cambridge, 2013.
2. Aaronson S., Watrous J.: Closed Timelike Curves Make Quantum and Classical Computing Equivalent. Proceedings of the Royal Society A, 465, 2009, p. 631–647.
3. Abrams D. S., Lloyd S.: Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems. Physical Review Letters, 81, 1998, p. 3992–3995.
4. Adleman L. M., DeMArrais J., Huang M.-D. A.: Quantum Computability. SAIM Journal on Computing, 6, 1977, p. 675–695.
5. Bennett Ch. H., Bernstein E., Brassard G., Vazirani U.: Strengths and Weaknesses of Quantum Computing. SAIM Journal on Computing, 26, 1997, p. 1510–1523.
6. Bernstein E., Vazirani U.: Quantum Complexity Theory. SAIM Journal on Computing, 26, 1997, p. 1411–1473.
7. Deutsch D.: Quantum Mechanics Near Closed Timelike Lines. Physical Review D, 44, 1991, p. 3197–3217.
8. Feynman R. P.: Simulating physics with computers. International Journal of Theoretical Physics, 21, 1982, p. 467–488.
9. Gill J.: Computational Complexity of Probabilistic Turing Machines. SAIM Journal on Computing, 26, 1997, p. 1524–1540.
10. Moore C., Mertens S.: The Nature of Computations. Oxford University Press, Oxford, 2011.
11. Papadimitriou C. H.: Computational Complexity. Addison-Wesley, Reading, Massachusetts, 1994.
12. Shor P. W.: Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science (1994), p. 124–134.
13. Yanofsky N. S., Manucci M. A.: Quantum Computing for Computer Scientists. Cambridge University Press, Cambridge, 2008.