ISSN 1230-3801

Zeszyt 158 nr 3-4/2021, str. 65- 89
Volume 158 No. 3-4/2021, pp. 65-89

ELEMENTY INFORMATYKI KWANTOWEJ W NOWYCH TECHNOLOGIACH OBLICZENIOWYCH

EXAMPLES OF QUANTUM IT IN NEW TECHNOLOGIES OF COMPUTATION

Tomasz KUCZERSKI

Wojskowy Instytut Techniczny Uzbrojenia, ul. Wyszyńskiego 7, 05-220 Zielonka
Military Institute of Armament Technology, 7 Wyszynski St., 05-220 Zielonka, Poland
Author's e-mail address: kuczerskit@witu.mil.pl.; ORCID: 0000-0001-7595-726X

Mateusz MAJCZAK

DOI 10.5604/01.3001.0015.6777

Streszczenie: Artykuł zawiera definicje elementów informatyki kwantowej w odniesieniu do klasycznych technologii obliczeniowych. Wyjaśnia zasady transformacji algorytmów obliczeniowych do dziedziny obliczeń kwantowych z wykorzystaniem optymalizacji i rachunku macierzowego. Przedstawia przykładowe zastosowania klasycznych algorytmów i ukazuje możliwości ich realizacji w dziedzinie informatyki kwantowej. Autor wskazuje na możliwość zastosowania algorytmów kwantowych w nowych technologiach obliczeniowych w zakresie kryptografii kwantowej i złożonych obliczeniowo analiz danych.

Słowa kluczowe: informatyka kwantowa, obliczenia kwantowe, bramki kwantowe

Abstract: The paper includes definitions of elements of quantum IT referred to classical technologies of computation. It explains the principles of transformation of calculating algorithms to the domain of quantum computations using the optimisation and matrix calculus. Exemplary applications of classical algorithms are presented with possibilities of their realisation in domain of quantum IT. Autor presents some possibilities for using quantum algorithms in new computation technologies concerning quantum cryptography and data analyses with complex computations.

Keywords: quantum information technologies (IT), quantum computations, quantum gates

1. Wstęp

Obliczenia z udziałem kubitów różnią się istotnie od obliczeń wykonywanych przez tradycyjne komputery, operujące na bitach. Komputer kwantowy w swoim funkcjonowaniu zbliża się do idei komputera analogowego, bo operuje wciąż na tym samym zbiorze

1. Introduction

Computations using the qubits are essentially different than those made on traditional computers and using the bits. Operation of quantum computer is closer to the idea of analogue computer as it operates on the same set of qubits without storing the

kubitów, nie odkładając pośrednich wyników na stosie pamięciowym.

Schemat obliczeń w komputerze kwantowym jest następujący:

1) kubity są inicjalizowane na określony stan początkowy – np. |0 0 0 ...0>,
2) na kubity aplikowane są, związane z danym algorytmem bramki kwantowe, dzięki czemu wartość kubitów podlega ewolucji,
3) po zakończeniu obliczeń kwantowych odczytywane są stany kubitów – ściślej nie kompletna wartość tych stanów, lecz pomiary kubitów, dające zredukowany wynik: 0 bądź 1, dla każdego odczytywanego kubitu,
4) W celu uzyskania statystyki odczytywanych pomiarów całą procedurę 1 – 3 powtarza się tyle razy, ile jest niezbędne dla osiągnięcia żądanej dokładności. Wyniki podczas kolejnych powtórzeń oczywiście nie będą identyczne, co wynika z tego, że pomiar zwraca 0 i 1 z prawdopodobieństwem określonym przez stan odczytywanego kubitu.

2. Problem dekoherencji kubitów

Kubit, który został zmierzony, traci superpozycję, stając się bezużytecznym dla dalszych obliczeń kwantowych. To zjawisko, choć z jednej strony jest pożądane i planowane, gdy jest odczytem stanu kubitu, ma swoją negatywną stronę, jeśli zachodzi w sposób niekontrolowany, poza intencją osób wykorzystujących obliczenia kwantowe. Samoistne, wynikające z różnych zaburzeń w układzie, jak też po prostu z samorzutnej deekscytacji stanu wzbudzonego, utraty właściwości kubitów określane są mianem **dekoherencji**. (ang. quantum decoherence).

Jakość obliczeń kwantowych bardzo ściśle

intermediate results in memory.

Scheme of computations on the quantum computer is following:

1) Qubits are initiated in a specific original state – e.g. |0 0 0 ...0>,
2) Quantum gates connected with a specific algorithm are applicated into qubits and in effect the value of qubit evolves ,
3) States of qubits are read out after termination of quantum computations – and more precisely, not a complete value of those states, but the measurements of qubits which provide the reduced result: 0 or 1, for each qubit being read out,
4) In order to get a statistics of measurements which were read out the whole procedure 1 – 3 is repeated many times until a required accuracy is received. The results of consecutive repetitions are not identical, of course, due to the fact that the measurement returns 0 and 1 with the probability determined by the state of the qubit being read out.

2. Qubits Decoherence Problem

Qubit which was measured is deprived of the superposition and by the same is useless for further quantum computations. This effect is expected and planned when it is a readout of the qubit state, but it has a negative notation if it happens in uncontrolled way, beyond intention of operators using the quantum computations. Autonomous losses of properties by qubits are caused by different disturbances in the system, or by a self-deexcitation of the excited state and are named as quantum **decoherence**.

Quality of quantum computations depends strictly on possibilities for limiting

wynika z możliwości ograniczenia dekoherencji. Jeśli kubity będą co chwila same się „psuły", to obliczenia kwantowe o nie oparte nie będą stabilne, będą występowały w nich błędy. Dlatego podejmuje się szereg działań zmierzających do ograniczenia wszelkich wpływów zewnętrznych na kubity, chłodzi się owe kubity, próbuje kontrolować wzajemne oddziaływania między kubitami.

W celu ograniczenia dekoherencji w komputerze kwantowym stosuje się:

- ekranowanie układu od pól zewnętrznych – elektrycznych i magnetycznych,
- chłodzenie kubitów i całego układu kwantowego,
- powiązanie kubitów z możliwie najtrwalszymi (o najdłuższym czasie życia) stanami wzbudzonymi atomów, jonów. Jak podaje Wikipedia: *w 2012 roku udało się stłumić dekoherencję na ok. 2 sekundy w temperaturze pokojowej. Rok później czas ten wyniósł już 39 minut*.

Dodatkowo uzupełnieniem powyższych technik jest korekcja błędów, nadmiarowość obliczeń, mechanizmy diagnostyki potencjalnych czynników zakłócających, aby w większym stopniu panować nad kubitami, uniemożliwiając ich samorzutne redukcje.

3. Algorytmy kwantowe

Algorytm kwantowy polega na zastosowaniu na zbiorach kubitów zadanej sekwencji bramek kwantowych.

Przykłady algorytmów kwantowych:

- algorytm Deutscha-Jozsy (odróżniania funkcji zrównoważonej od stałej) 1992[4],
- algorytm Shora (faktoryzacji, czyli rozkładu liczb na czynniki pierwsze) 1994,
- algorytm Kitajewa (szybkiej kwanto-

decoherence. If the qubits become defective by themselves too often, then the quantum computations basing on them will not be stable, and errors will be present. For this reason many actions are undertaken to limit external impacts into qubits, the qubits are chilled, and attempts are made to control mutual interactions between them.

Following steps are made to reduce decoherence in quantum computer:

- Screening the system against external electric and magnetic fields,
- Chilling qubits and overall quantum system,
- Creating qubits from possibly most durable (with the longest life cycle) excited states of atoms, or ions. Along Wikipedia: *in 2012 decoherence was suppressed for ca. 2 seconds at the ambient temperature. A year later this time was 39 minutes.*

Additionally these techniques are supplemented by correction of errors, excessiveness of computations, and diagnosis mechanisms for potential interference agents to control the qubits in greater degree and prevent their self-reduction..

3. Quantum Algorithms

Quantum algorithm is a deployment of a specific sequence of quantum gates on the sets of qubits.

Examples of quantum algorithms:

- Deutsch-Jozsy's algorithm (distinguishing equivalent function from permanent one) 1992[4],
- Shor's algorithm (factorisation, or decomposition of numbers on the original factors) 1994,
- Kitajew's algorithm (fast Fourier quan-

wej transformacji Fouriera) 1995,
- algorytm Grovera (przeszukiwania bazy danych) 1995,
- algorytm Simona (znajdowania maski XOR funkcji 2-na-1) 1997,
- algorytm estymacji fazy kwantowej (estymacja fazy, bądź wartości własnej operatora),
- algorytm Bernstein–Vazirani (odmiana algorytmu Deutscha-Jozsy) 1992,
- algorytmy oparte o błądzenie kwantowe,
- i inne.

3.1. Rejestr kwantowy

Komputer kwantowy działa najczęściej nie na jednym kubicie, a na całym ich zbiorze, tworzącym rejestr kwantowy. Kubity w takim rejestrze będą przekształcane, splątywane ze sobą, a ostatecznym krokiem na nich wykonywanym będzie pomiar. Stosowane są tu definicje formalne.

3.2. Obwód kwantowy – definicja formalna

Obwodem kwantowym na m kubitach nazywamy odwzorowanie unitarne w przestrzeni Hilberta H_m, które można przedstawić w postaci złożenia skończonej liczby bramek kwantowych.

3.3. Rejestr kwantowy – definicja formalna

Rejestrem kwantowym o długości m nazywamy uporządkowany układ m kubitów. Przestrzenią stanów jest $H_m = H \otimes \cdots \otimes H$ (m razy). Stany bazowe dane są przez $\{|x\rangle : x \in \{0, 1\}\ m\}$. Jeśli utożsamimy je z zapisem binarnym liczb, odpowiada to liczbom $\{0, 1, \ldots, 2^m - 1\}$.

Im większą ilość kubitów zawiera rejestr kwantowy, tym bardziej skomplikowane operacje będzie mógł wykonywać dany komputer kwantowy. Komputery o rejestrach kilkukubi-

tum transform) 1995,
- Grover's algorithm (searching the data base) 1995,
- Simon's algorithm (finding a mask XOR for function 2-on-1) 1997,
- Estimation algorithm for quantum phase (estimation of phase, or the own value of operator),
- Bernstein–Vazirani's algorithm (version of Deutsch-Jozsy's algorithm) 1992,
- Algorithms based on quantum erroring,
- and other ones.

3.1. Quantum Register

Quantum computer usually operates on a set of qubits, instead a one qubit, creating a quantum register. The qubits in such register will be transformed, entangled with each other, and the measurement will be a final operation made on them. Formal definitions are used here.

3.2. Quantum Circuit – Formal Definition

Quantum circuit on m qubits is a unitary reconstruction in the Hilbert's space H_m, which may be represented in the form of composition of a finished number of quantum gates.

3.3. Quantum Register – Formal Definition

Quantum register of length m is an arranged set of m qubits. The space of states is $H_m = H \otimes \cdots \otimes H$ (m times). The ground states are given by $\{|x\rangle : x \in \{0, 1\}\ m\}$. If we identify them with the binary recording of numerals it corresponds to numbers $\{0, 1, \ldots, 2^m - 1\}$.

The greater number of qubits is included in the quantum register the more sophisticated operations would be performed by the quantum computer. Com-

towych mają raczej niewielkie praktyczne zastosowania, służąc głównie celom szkoleniowym. Dopiero kilkadziesiąt, a jeszcze lepiej kilkaset kubitów w rejestrze daje możliwość tworzenia systemów obliczeniowych, które w realny sposób mogłyby zagrozić komputerom tradycyjnym, ponieważ byłyby w stanie dużo szybciej znajdować rozwiązanie części problemów obliczeniowych.

4. Operacje na kubitach, bramki i algorytmy kwantowe

Komputery kwantowe realizują swoje działania obliczeniowe za pomocą bramek kwantowych (ang. gate). Ogólnie bramką kwantową może być każdy prosty proces, który w sposób kontrolowany – poddający się planowemu działaniu, zmienia stan kubitu. Bramka kwantowa stanowi prosty obwód kwantowy, służący do przeprowadzania obliczeń kwantowych na jednym, bądź niewielkiej liczbie kubitów.

Z bramek kwantowych buduje się złożone obwody kwantowe, wykonujące serię operacji obliczeniowych na kubitach.

4.1. Bramka kwantowa – formalna definicja

Bramką kwantową na m kubitach nazywamy odwzorowanie unitarne w przestrzeni $H_m = H \otimes \cdots \otimes H$ (m razy), działające na ustalonej liczbie kubitów.

Bramki kwantowe są zapisywane najczęściej na dwa sposoby – symbolicznie (każda bramka ma przypisany odpowiedni symbol), lub w postaci macierzy.

Bramki kwantowe, użyte w zaplanowany sposób pozwalają na kontrolowanie ewolucji układu kwantowego. Wszystkie bramki są odwracalne, a więc i sama ewolucja bramkami wyznaczona jest odwracalna. Projektant obwodu kwantowego będzie starał się dobrać taką sekwencję bramek kwantowych, aby

puters with register capacities of a few bits have rather limited practical applications, and may be used for training. Just a few dozen, or better a few hundred qubits in the register give a chance for creating computation systems which could challenge traditional computers by solving some computational problems significantly quicker.

4. Operations on Qubits, Gates and Quantum Algorithms

Quantum computers perform their computations using quantum gates. In general, a quantum gate may be every simple process, which in a controlled way, that may be subjected to planned operation, changes the state of qubit. The quantum gate is a simple quantum circuit used for simple quantum computations on one or a low number of qubits.

The quantum gates are used to build complex quantum circuits performing a series of computing operations on qubits.

4.1. Quantum Gate – Formal Definition

The quantum gate on m qubits is a unitary reconstruction in space $H_m = H \otimes \cdots \otimes H$ (m times), operating on a settled number of qubits.

Quantum gates are usually recorded on two ways: a symbolic way (each gate has an adequate symbol ascribed), or a matrix.

Quantum gates used in a planned way can control the evolution of a quantum system. All gates are reversable, and therefore the evolution itself as defined by the gates is reversable. Designer of a quantum circuit will try to select such sequence of quantum gates to reach the objective by realisation of the quantum algorithm. The algorithm of

osiągnąć cel w postaci zrealizowania algorytmu kwantowego (ang. quantum algorithm). Algorytm tego rodzaju oprze się zwykle o następujący schemat:

- kubity zostaną zainicjowane na ustaloną wartość początkową – zwykle |000...0> (wszystkie kubity na start mają początkową wartość |0>). Inicjalizacja ustawia kubity na wyznaczony stan, niszcząc historię poprzednich stanów kubitu;
- na kubitach zostanie zrealizowana właściwa dla danego algorytmu sekwencja bramek kwantowych, rejestr kwantowy będzie ewoluował w sposób zaprogramowany;
- efektem końcowym będzie osiągnięcie docelowego stanu wszystkich kubitów, które teraz powinny zostać zmierzone. Gdy kubity zostają zmierzone, wtedy wszystkie ich funkcje falowe ulegną redukcji, zwracając przy okazji 0 albo 1 – wynik pomiaru. W tym momencie niszczone są wszystkie właściwości kwantowe osiągnięte ewolucją rejestru kwantowego;
- powyższa sekwencja działań zostanie powtórzona tyle razy, ile jest niezbędne dla osiągnięcia zaplanowanej dokładności wyniku. Efektem tych powtórzeń będzie uzyskanie statystyki dla każdego z kubitów – ile razy zwrócił on 0, a ile 1, co następnie trzeba będzie zinterpretować w kontekście idei danego algorytmu.

Bramki kwantowe wykonują różne operacje na kubitach – np.:

- odwracają kubit podmieniając jego bazę, zamieniając |0 > z |1 >.
- zmieniają fazę kubitu
- wywołują interferencję kubitów, splątują kubity
- ogólnie mogą w różny sposób przesuwać punkt na sferze Blocha, zmieniając w ten sposób stan kubitu.

Przykładami bramek kwantowych są:

this type will usually operate on the following scheme:

- qubits will be initiated into a settled original value – usually |000...0> (all qubits on the start have the original value |0>). Initialisation sets the qubits on the settled state, and destroys the history of qubit's former states;
- a sequence of quantum gates, specific for a given algorithm, will be performed on qubits, and the quantum register will be evolving in a programmed way;
- Final effect will be in reaching the target states for all qubits, which at this instant have to be measured. After the measurement all wave functions of qubits are reduced and by the same they return 0 or 1 – the result of measurement. At this moment all quantum properties produced in effect of the quantum register evolution are damaged;
- The above sequence of steps will be repeated so many times as is required for reaching the accepted accuracy of the result. The effect of these repetitions gives a statistics for each qubit saying how many times it returned 0, and 1, what later is interpreted in the context of the specific algorithm idea.

Quantum gates perform various operations on qubits – e.g.:

- Reversing the qubit by replacing its base and changing |0 > to |1 >,
- Changing the phase of qubit,
- Enforcing the interference of qubits by entangling them,
- In general, they may in different way shift the point on the Bloch sphere and change the qubit state in this way,

There are following examples of quantum gates:

- bramka sigma x
- bramka Hadamarda
- bramka fazy
- bramka CNOT.

Te cztery bramki stanowią bazę, z której można skonstruować dowolną inną bramkę kwantową.

4.2. Bramka Pauli-X (bramka NOT)

Dla wyjaśnienia idei bramek kwantowych, jak też i samego kubitu, dobrze byłoby rozpatrzyć na początek działanie bramki Pauli-X. Bramkę tę określa się często jako bramkę NOT, bądź bramkę sigma x (σ_x). Działanie tej bramki można porównać do działania bramki NOT, dla komputerów tradycyjnych - klasycznej. Klasyczna bramka NOT działa w ten sposób, że odwraca stan bitu, czyli jeśli bit zawierał wartość 0, to bramka zamieni go na 1, a jeśli miał wartość 1, to zamieni ją na 0.

Bramka kwantowa NOT działa nie na konkretny stan, lecz na superpozycję stanów kwantowych, co oznacza, iż zamieni obie (!) amplitudy prawdopodobieństwa stanów |0> i |1>. Jeśli amplituda prawdopodobieństwa stanu |0> miała wartość α zaś amplituda prawdopodobieństwa stanu|1> miała wartość β, to po zadziałaniu bramką NOT amplituda prawdopodobieństwa stanu |0> uzyska wartość β, zaś amplituda prawdopodobieństwa stanu |1> będzie miała wartość α. Można to zapisać jako:

$|\Psi> = \alpha\,|0> + \beta\,|1>$

$|\Psi'> = \beta\,|0> + \alpha\,|1>$.

Warto zwrócić uwagę na to, że bramka kwantowa wciąż utrzymuje superpozycję stanów |0> i |1>. W odróżnieniu od klasycznej bramki NOT, żadna wartość stanu bazowego (ani |0>, ani |1>) tutaj nie znikła. Jedynie „stany bazowe wymieniły się amplitudami”. Macierz kwantowej bramki NOT ma postać:

- Gate sigma x
- Hadamard’s gate
- Phase gate
- CNOT gate.

These four gates are a base for creating any other quantum gate.

4.2. Pauli-X Gate (Gate NOT)

The idea of quantum gates and of the mere qubit may be well explained by the operation of Pauli-X gate. This gate is often named as NOT gate, or sigma x (σ_x) gate. Operation of this gate can be compared to operation of gate NOT in traditional computers. Conventional gate NOT works in such way that it reverses the state of bit, i.e. if bit has value 0 then the gate reverses it into 1, and if it has value 1, it changes it into 0.

The quantum gate NOT acts not against a specific state but on the superposition of quantum states, what means that it replaces the amplitudes of probability for both states (!) |0> and |1>. If the amplitude of probability for state |0> was α, and the amplitude of probability for state |1> was β, then after applying the gate NOT, the amplitude of probability for state |0> becomes β, and the amplitude of probability for state |1> becomes α. It may be written as:

$|\Psi> = \alpha\,|0> + \beta\,|1>$

$|\Psi'> = \beta\,|0> + \alpha\,|1>$.

It is worth to note that the quantum gate still maintains the superposition of states |0> and |1>. Just opposite to the classical gate NOT, none of the basic state values (neither |0>, neither |1>) does not disappear here. Only the “basic states have replaced their amplitudes”.

Matrix of quantum gate NOT has the form m:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Oznaczenie dla bramki Pauli X: 

Designation of gate Pauli X: 

4.3. Bramka Pauli Y

Bramka Pauli Y jest bramką jednokubitową (nazywaną niekiedy bramką sigma -y (σ_y)), która przekształca kubit źródłowy obracając go na sferze Blocha wokół osi Y o kąt π radianów. Jest reprezentowana przez macierz (jedną z macierzy Pauliego) o postaci:

4.3. Pauli Y Gate

Gate Pauli Y is a one-qubit gate (it is sometime named as gate sigma -y (σ_y)), which transforms the original qubit by rotating it on the Bloch sphere around axis Y by the angle of π radians. It is represented by a matrix (one of Pauli's matrixes) in the form:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Oznaczenie dla bramki Pauli Y: 

Designation of gate Pauli Y: 

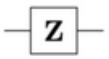
4.4. Bramka Pauli Z

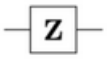
Bramka Pauli Z jest bramką jednokubitową (nazywaną niekiedy bramką sigma -z (σ_z)), która przekształca kubit źródłowy obracając go na sferze Blocha wokół osi Z o kąt π radianów. Jest reprezentowana przez macierz (jedną z macierzy Pauliego) o postaci:

4.2. Pauli Z Gate

Gate Pauli Z is a one-qubit gate (it is sometime named as gate sigma -z (σ_z)), which transforms the original qubit by rotating it on the Bloch sphere around axis Z by the angle of π radians. It is represented by a matrix (one of Pauli's matrixes) in the form:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Oznaczenie dla bramki Pauli Z: 

Designation of gate Pauli Z: 

Te trzy bramki – macierze Pauliego – Pauli X, Pauli Y, Pauli Z, wraz z bramką jednostkową, która nie zmienia kubitu (opisywana macierzą jednostkową), tworzą bazę, a więc w pełni rozpinają przestrzeń przekształceń obrotu kubitów.

These three gates – Pauli's matrixes – Pauli X, Pauli Y, Pauli Z, together with the unitary matrix which does not change the qubit (described by the unitary qubit), create a base, as they completely fill the space of rotational transformations of qubits.

4.5. Bramka fazy

Bramka fazy jest uniwersalną bramką kwantową, która zmienia tylko fazę kubitu. W ogólnej postaci, określanej jako shift (R_φ) jej macierz ma postać:

$$R_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

Tutaj φ jest fazą, o którą zmieniana jest faza pierwotna kubitu. Bramka fazy obraca kubit wokół osi Z na sferze Blocha o kąt φ.

Rozważa się też przypadki szczególne bramki fazy, dla różnych zadanych kątów φ:

1) Dla $\varphi = \pi$ bramka fazy daje nam, opisaną wyżej bramkę Pauliego Z

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

2) Dla $\varphi = \pi/2$ bramka fazy daje nam bramkę S

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = \sqrt{Z},$$

3) Dla $\varphi = \pi/4$ bramka fazy daje nam bramkę T

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} = \sqrt{S}.$$

4.6. Bramka Hadamarda

Bramka Hadamarda może być porównana do kodowania sygnałów mono i stereo w radioodbiornikach FM. Tam z dwóch kanałów – lewego i prawego – konstruuje się dwa sygnały – jeden sumacyjny (który jest odczytywany gdy odbiór jest monofoniczny), a drugi różnicowy. W przypadku bramki Hadamarda mamy tu jednak sumowanie i różnicowanie stanów |0> i |1> kubitu.

Macierz bramki Hadamarda ma postać:

4.5. Phase Gate

Phase gate is an universal quantum gate which changes exclusively the phase of qubit. In general form determined as shift (R_φ) its matrix has a form:

$$R_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

Here, φ is the phase by which the original phase of qubit is shifted. The phase gate rotates the qubit on the Bloch sphere around axis Z by angle φ.

Particular cases are also considered for the phase gate at different given angles φ:

1) For $\varphi = \pi$ the phase gate is the gate Pauli Z, described above

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

2) For $\varphi = \pi/2$ the phase gate gives gate S

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = \sqrt{Z},$$

3) For $\varphi = \pi/4$ the phase gate gives gate T

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} = \sqrt{S}.$$

4.6. Hadamard's Gate

Hadamard's gate may be compared to coding mono and stereo signals in radio sets. In that case two signals are created from two channels – one being a sum (which is used at monophonic transmission), and the second as a differential one. In the case of Hadamard's gate we have summing and subtraction of qubit's states |0> and |1>.

Matrix of Hadamard's gate has a form:

$$H = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Bramka ta przekształca bazowy stan |0> do postaci $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$,
a bazowy stan |1> do postaci $\frac{|1\rangle-|0\rangle}{\sqrt{2}}$.

Symbolem bramki Hadamarda jest 

This gate transforms the basic state |0> to the form $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$,
and a basic state |1> to form $\frac{|1\rangle-|0\rangle}{\sqrt{2}}$.

Symbol of Hadamard's gate is 

4.7. Splątanie kwantowe

Cechą układów stosowanych do obliczeń kwantowych wykorzystywaną w obliczeniach kwantowych jest splątanie (ang. entanglement). W tym wypadku najczęściej splątanie dotyczy kubitów. Kubity splątane ze sobą, nawet będąc rozdzielone przestrzennie, zachowują się w części jakby były nie dwoma oddzielnymi, lecz jednym bytem kwantowym. Objawia się to między innymi tym, że pomiar wykonany na jednym kubicie ze splątanej pary ma natychmiastowy skutek w postaci redukcji funkcji falowej drugiego kubitu. Do tego redukcje funkcji falowych obu kubitów z pary są ściśle skorelowane. Przy maksymalnym splątaniu dwóch kubitów, mierząc stan jednego kubitu ze splątanej pary zyskujemy pewność jaki jest stan drugiego kubitu z owej pary.

Ogólnie splątanie kwantowe polega na tym, że dwie (lub więcej) cząstki, bądź właściwości różnych układów kwantowym dzielą niejako pewien wspólny aspekt. Np. dwa splątane fotony mogą mieć zawsze prostopadłe polaryzacje. Wtedy mierząc polaryzację jednego fotonu ze splątanej pary możemy mieć pewność, że polaryzacja drugiego fotonu z tej pary będzie prostopadła do tej pierwszej. I wszystkie doświadczenia potwierdzają, iż tak rzeczywiście jest, jakby owe fotony „wiedziały", czy drugi foton ze splątanej pary został zmierzony pod kątem jego polaryzacji. Jeśli pomiar któregokolwiek fotonu z pary został zrealizowany, to drugi foton błyskawicznie przyjmie prostopadłą do pierwszego polaryzację.

Splątanie nie musi być pełne. Czasami

4.7. Quantum Entanglement

Entanglement is a feature of systems used for quantum computations. In this case the entanglement mostly refers to qubits. The entangled qubits behave partially as they were not two separate quantum bodies, but like one body, even if they are spatially separated. This is manifested among others in the fact that the measurement made on one of qubits from this entangled couple has an instant effect in reduction of the wave function of the second qubit. Moreover, the reductions of wave functions of two qubits are strictly correlated. At maximal entanglement of two qubits we can measure the state of one of them to have a complete certainty about the state of the second qubit of the couple.

In general the quantum entanglement is based on sharing a certain common aspect between two (or more) particles, or by properties of different quantum systems. For instance, two entangled photons may have always vertical polarisations. Then by measuring the polarisation of one photon we are sure that polarisation of the second photon from this couple will be positioned vertically to the first one. And all experiments confirm that it really is the fact, and it seems that the photons would "know" if polarisation of second photon from the entangled couple was measured. If measurement of any photon from the couple was made, then the second photon immediately takes vertical polarisation against the first one.

The entanglement must not necessarily

cząstki kwantowe, kubity są splątane tylko częściowo. Stany maksymalnego splątania określane są jako „stany Bella" (ang. Bell states).

4.8. Bramka CNOT

Bramka CNOT (ang. controlled NOT gate) jest bramką dwukubitową, co oznacza, że działa naraz na rejestrze kwantowym składającym się z dwóch kubitów. Jest to niezwykle ważna w obliczeniach kwantowych bramka, co wynika z tego, iż efektem jej zadziałania jest splątanie, bądź rozplątywanie kubitów. Zastosowanie tej bramki, w powiązaniu z działaniami bramek jednokubitowych, obracających kubity pozwala na zrealizowanie (przynajmniej w teorii, bo fizyczna realizacja tej bramki nie jest sprawą prostą) dowolnego obwodu kwantowego. Pierwszy kubit z tego rejestru kontrolny, (ang. control), a drugi Target.

Bramka CNOT powoduje odwrócenie (zadziałanie pod bramką typu NOT, omawianą wyżej) kubitu Target wtedy i tylko wtedy, gdy kubit kontrolny jest ustawiony na stan |1>.

be complete. Sometimes quantum particles are entangled only partially. States of complete entanglement are described as Bell states.

4.8. CNOT Gate

Gate CNOT (controlled NOT gate) is a two-qubit gate what means that it operates concurrently on the quantum register consisting of two qubits. This is an especially important gate for quantum calculations what is caused by its operation enforcing the entanglement, or disentanglement of qubits. Application of this gate, in connection with operations of one-qubit gates rotating the qubits, allows for building any (at least in theory, as a physical realisation of the gate is not simple) quantum circuit. The first qubit in this register is a control qubit and second a Target qubit.

The gate CNOT effects the reversing (acting by the sub-gate of NOT type, presented above) of Target qubit only, and exclusively, when the control qubit is set on state |1>.

Przed / *Before*		**Po / *After***	
Sterujący *Control*	**Docelowy *Target***	**Sterujący *Control***	**Docelowy *Target***
|0>	|0>	|0>	|0>
|0>	|1>	|0>	|1>
|1>	|0>	|1>	|1>
|1>	|1>	|1>	|0>

Można to też przedstawić za pomocą macierzy:

It may be also represented by matrix:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Bramka dwukubitowa będzie generowała stany mieszane pierwszego kubitu z drugim. Zatem mamy już teraz do czynienia nie tylko

Double-qubit gate will generate mixed states of the first qubit with the second. Then, we have here not only the states *a* |0>

ze stanami a |0> i b |1> lecz ze stanami kombinującymi każdy stan pierwszego kubitu z każdym drugiego kubitu: a' |00>, b' |01>, c |10>, d |11>.

Bramka ta stan: a |00> + b |01> + c |10> + d |11>

przekształca w stan: a |00> + b ||01> + c |11> + d |10> jednak…

tylko dla części kubitu sterującego o wartości |1>.

Oznaczenie dla bramki CNOT: 

4.9. Zrozumienie splątania dla bramki CNOT

Warto tu zauważyć, że zrozumienie tego dlaczego bramka ta w ogóle splątuje kubity, jest dość ciekawym testem na pojmowanie koncepcji superpozycji w fizyce kwantowej. Opis splątania, zrozumiany w duchu klasycznym prowadzi bowiem do konfuzji. Przecież przed redukcją funkcji falowej nie wiadomo, jaki „wybór" daje nam kubit sterujący – nie wiemy, czy jest on 0, czy 1. Zatem nie wiemy właściwie co się realizuje w splątaniu, czy bit docelowy zostanie odwrócony, czy też nie. Kubit sterujący jest przecież w superpozycji obu stanów, więc też i tą właśnie superpozycją wysterowuje kubit docelowy.

Tak więc, podana wyżej tabela wartości kubitów nie opisuje nam stanów albo – albo, lecz zawarte w kubitach jednocześnie. To zaś oznacza, że jeśliby pierwszy kubit miał dokładnie równe sobie współczynniki a i b, czyli jeśli prawdopodobieństwo zwrócenia w pomiarze 0 i 1 byłoby dla niego dokładnie po 50%, to także odwrócenie kubitu docelowego będzie nie albo – albo, lecz JEDNOCZEŚNIE będzie – z prawdopodobieństwem po 50% – stanu odwróconego z nieodwróconym. Bo mamy tu superpozycję stanu zadziałania bramki NOT na docelowym kubicie z jej niezadziałaniem. Dlatego też w tym kontekście mówimy o splątaniu kubitów.

and b |1> but the states combining each state of the first qubit with every state of the second qubit: a' |00>, b' |01>, c |10>, d |11>.

The gate transforms the state: a |00> + b |01> + c |10> + d |11> into the state: a |00> + b ||01> + c |11> + d |10> but…

only for the part of the controlling qubit having the value |1>.

Designation of gate CNOT: 

4.9. Understanding of Entanglement for Gate CNOT

It is worth to note that understanding why the gate at all entangles the qubits is an interesting test for comprehension of concept of superposition in the quantum physics. Description of entanglement interpreted in a classical way leads to a confusion. Before reduction of the wave function we cannot know what "choice" is offered to us by the controlling qubit – we do not know if it is 0, or 1. Finally, we do not know what really is realised in the entanglement, if the Target bit will be reversed, or not. The controlling qubit is in the superposition of both states, and it controls the Target qubit just through this superposition.

Hence, the table of qubit values presented above does not describe the states or – or, but the states included simultaneously in qubits. And it means that if the first qubit could have exactly equal coefficients ***a*** and ***b***, i.e. the probability of returning at the measurement 0 and 1 would be for it exactly equal to 50%, then the reversing of the Target qubit will be not or – or, but it will be SIMULTANEOUSLY – with probability divided evenly by 50% – to the state reversed and unreversed. Here, we have a superposition of the state when the gate NOT works on the target qubit with the state when it fails to work. In this

Tabela stanów kubitu, choć stosowana w literaturze, może prowokować mylne jej zrozumienie, sugerując, iż kubit docelowy zawsze (w końcu tak zapisano w tabeli) jest odwracany. A tymczasem owa tabela opisuje tak naprawdę tylko tę opcję (właściwie to w tej części stanu kubitu), w której pierwszy kubit zrealizuje się na stan |1>. Jeśli pierwszy kubit zrealizuje się na stan |0>, to zamiast powyższej tabeli i macierzy mielibyśmy macierz jednostkową (z samymi jedynkami na przekątnej), bo mielibyśmy brak zanegowania drugiego kubitu.

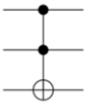
W tabeli 1 przedstawiono oznaczenia i macierze najważniejszych bramek kwantowych.

context we can say about entanglement of qubits.

Then, the table of qubit states, even if presented in publications, may provoke its false interpretation by suggesting that the target qubit (at least it is put in the table) is always reversable. But the truth is that the table describes only this option (in fact in this part of qubit's state) when the first qubit was realised in state |1>. If the first qubit realises itself into the state |0>, then instead of the above table and matrix we could have a unitary matrix (with the ones at diagonal) due to failed negation of the second qubit.

Table 1 includes designations and matrixes for most important quantum gates.

Tabela 1. Podstawowe bramki kwantowe - oznaczenia, macierze (źródło – Wikipedia)
Table 1. Basic quantum gates – designations, matrixes (source – Wikipedia)

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

5. Fizyczne działanie na kubity i realizacja bramek kwantowych

Bramki kwantowe fizycznie są najczęściej w odmienny sposób realizowane w zależności od tego, jaką technologię kubitów przyjęto. W przypadku gdy kubity tworzone są w oparciu o stany wzbudzone atomów, czy jonów, realizacja bramek będzie opierała się zwykle o odpowiednie wzbudzenia promieniami lasera.

W tym opracowaniu nie przewidziano dokładnej analizy procesów fizycznych realizacji bramek kwantowych, co jest związane z tym, że właściwie każde zastosowanie pod tym względem będzie jakoś odmienne. Każda technologia bramki kwantowej jest ściśle związana z tym, jakie kubity wykorzystujemy, jakie zjawiska je budują. Zatem inaczej zafunkcjonuje ona na kubicie opartym o magnesy nadprzewodzące, inaczej na zimnych atomach, inaczej w pułapce jonowej.

Do uzyskiwania żądanych stanów kubitów, szczególnie stanów splątanych często stosuje się efekty nieliniowe. Efekt nieliniowy jest niejako naturalnym źródłem splątania, bo jego opis matematyczny zawiera człony, które nie dają się sprowadzić do sumy pierwszego i drugiego stanu, zawierając też stany mieszane.

Działanie na kubity zwykle będzie realizowane techniką laserową – odpowiednio dobrane impulsy, mogą dokonywać różnych postaci przekształceń obwodów kwantowych:

1) naświetlenie jonu promieniem lasera o odpowiedniej częstotliwości powoduje przejście do stanu wzbudzonego. Ten stan może być interpretowany jako |0> bądź |1> kubitu,
2) w przypadku gdy stany kubitu |0> i |1> realizowane są za pomocą wzbudzania promieniami lasera i wiadomo, że przejście od jednego stanu do drugiego wyma-

5. Physical Actions on Qubits and Realisation of Quantum Gates

Quantum gates are usually realised in different physical forms depending on accepted technology of qubits. In the case when the qubits are created on the base of excited states of atoms, or ions, the realisation of gates is usually based on adequate excitations by laser beams.

This paper does not provide any detailed analysis of physical processes for realisation of quantum gates, what is caused by the fact that each such application is a different one. Each technology of quantum gate is closely connected with the used qubits and effects they harness. Then it will work differently for the qubit based on superconductive magnets, or for the chilled atoms, or in the ion trap.

Nonlinear effects are sometimes used to get desired states of qubits, often the entanglement states. The nonlinear effect is a natural source of the entanglement because its mathematical description includes some components which cannot be reduced to the sum of the first and the second state, but also include the mixed states.

Operations on qubits are usually performed using the laser technique – suitably matched pulses may effect different forms of transformations of quantum circuits:

1) Exposition of an ion by the laser beam with adequate frequency effects transition into the excited state. This state of qubit may be interpreted as |0> or |1>,
2) In the case when the qubit states |0> and |1> are realised by the laser beam excitation, and when it is known that transition from one state to another requires the pulse duration of T, then application of the pulse with duration

ga impulsu o czasie T, to zastosowanie impulsu o czasie T/2, spowoduje wygenerowanie stanu kwantowego pośredniego, czyli wprowadzenie kubitu w superpozycję stanów,
3) czasem naświetlania impulsu można też osiągnąć efekt zmiany fazy kubitu,
4) do sprzęgania ze sobą kubitów mogą być wykorzystane siły coulombowskie,
5) sam pomiar kubitu realizuje się np. w technologii pułapek jonowych optyczną obserwacją po oświetleniu promieniami lasera. Pobudzane fotonami jony swoim zaświeceniem sygnalizują stan, w którym się znajdują.

Bardziej złożone operacje wymagają niekiedy zastosowania, oprócz laserów, także odpowiednio dobranych pól elektromagnetycznych.

6. Algorytmy kwantowe – przykłady z różnych obszarów zastosowań

Aktualne realizacje komputerów kwantowych praktycznie nigdy nie występują samodzielnie, stanowiąc tylko koprocesor kwantowy do komputerów tradycyjnych. Podobnie jest ze sterowaniem układami kwantowymi – są one realizowane za pomocą tradycyjnych komputerów, ewentualnie wspomaganych układami FPGA, czy inną formą elektroniki – częściowo cyfrowej, częściowo analogowej. Algorytmy kwantowe są (i takimi pozostaną) tylko częścią w pewnej całości; druga część będzie realizowana tradycyjnie.

6.1. Kwantowa transformata Fouriera

Kwantowa transformata Fouriera (ang. *quantum Fourier transform,* QFT) – kwantowym analogiem odwrotnej dyskretnej transformaty Fouriera. Ten algorytm kwantowy ma ogromne znaczenie w obliczeniach kwantowych, ponieważ jest składnikiem wielu bardziej złożonych algorytmów.

T/2 causes generation of an intermediate quantum state, i.e. introduction of the qubit into superposition of states,
3) Exposition time of the pulse may also produce the change of qubit's phase,
4) Coulomb forces may be also used for coupling the qubits,
5) The mere measurement of qubit is realised, for instance in technology of ion traps, through optical observation after illumination by laser beams. The luminating of ions excited by photons signalise their state.

More sophisticated operations sometimes require that beside the lasers also suitably matched electromagnetic fields have to be used.

6. Quantum Algorithms – Examples of Applications

Currently, the quantum computers nowhere exist independently and in practice they work only as a quantum coprocessor of traditional computers. Similar situation is with controlling of quantum systems – it is made by traditional computers which could be assisted by FPGA systems, or other form of electronics – partially digital and partially analogue. The quantum algorithms are (and they will remain such ones) only a part of a whole system, and the second part will be realised in traditional way.

6.1. Quantum Fourier Transform

Quantum Fourier transform (QFT) is a quantum equivalent of the reverse discrete Fourier transform. This quantum algorithm is extremely important in quantum computations as it is a part of many more sophisticated algorithms.

Fourier transform provides a spectrum

Transformata Fouriera pozwala na otrzymanie widma sygnału z przebiegu tego sygnału. Ta właściwość została np. w algorytmie Shora w pomysłowy sposób zaaplikowana funkcji potęgowej, umożliwiając odnajdowanie dzielników zadanej liczby naturalnej.

Kwantowa transformata Fouriera może być zrealizowana z użyciem dwóch bramek:

- bramki Hadamarda
- kontrolowanej wersji bramki fazy R_{m}.

$$H = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{i } R_m = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^m}} \end{bmatrix}$$

6.2. Kryptografia kwantowa

Aktualnie myśli się o użyciu komputerów kwantowych w obszarze kryptografii w kontekście dwóch najważniejszych zastosowań:

1) łamanie kluczy kryptograficznych szybciej, niż komputerami tradycyjnymi,
2) kwantowa dystrybucja klucza szyfrowego (ang. *Quantum Key Distribution*, *QKD*) – zespół procedur, których zadaniem jest przekazanie pomiędzy stronami klucza szyfrującego z wykorzystaniem praw kwantowych, gwarantujących poufność tej operacji.

6.3. Wyżarzanie kwantowe

Jedną z technologii obliczeń kwantowych, które wykorzystują własności kwantowe w sposób wykraczający poza standardowe wykorzystanie bramek kwantowych jest wyżarzanie kwantowe (ang. Quantum annealing (QA)). Technika ta służy do znajdowania minimów funkcji na sposób podobny do symulowanego wyżarzania. W technice tej fluktuacje kwantowe są wykorzystywane jako motor odchyleń od początkowego położenia argumentu funkcji, w celu poszukiwania minimalnych wartości dla owej funkcji.

Kwantowe wyżarzanie jest algorytmem jaki stosowany jest w rozwiązaniach obliczeń kwantowych firmy D-WaVe Systems. To bardzo

of the signal on the base of its form. This property was applied for instance in a clever way in Shor algorithm into an exponential function to find out divisors for a given natural number.

Quantum Fourier transform may be realised by using two gates:

- Hadamard gate
- Controlled version of phase gate R_{m}.

$$H = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{i } R_m = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^m}} \end{bmatrix}$$

6.2. Quantum Cryptography

Currently, some trends are visible to use the quantum computers in domain of cryptography in two most important applications:

1) A quicker breaking of cryptographic keys than by traditional computers,
2) Quantum distribution of decipher key (*Quantum Key Distribution* - *QKD*) – a set of procedures aimed to transfer a deciphering key between the sides using the quantum principles warranting the confidentiality of this operation.

6.3. Quantum Annealing

Quantum annealing is one of technologies of quantum computations which goes beyond standard applications of quantum gates. The technique is used to find out the minimums of function in a way which is similar to the simulated annealing. In this technology the quantum fluctuations are used for producing declinations of function argument from the original position in order to find out the minimal values of this function.

Quantum annealing is an algorithm used for solutions of quantum computations of D-WaVe Systems. This application, which is well known in domain of imple-

znane w świecie wdrożeń technik kwantowych zastosowanie ma jednak tę wadę, że nie implementuje zastosowania bramek kwantowych. To oznacza, że wielu specjalistów odmawia temu wdrożeniu miana komputera kwantowego. Bo choć w technice wyżarzania stosunkowo łatwo można zwiększać liczbę kubitów, to ogólnie owa technika ma bardzo limitowane obszary zastosowań. W oparciu o nią nie da się zrealizować (przynajmniej na aktualnym poziomie rozwoju) ani algorytmu Shora, ani innych – bardziej uniwersalnych – algorytmów.

6.4. Pojęcie supremacji kwantowej

W kontekście rozwoju komputeryzacji kwantowej definiuje się pojęcie supremacji kwantowej. Polegać ona miałaby na takim udoskonaleniu się komputerów kwantowych, że obliczenia w tej technologii stały by się szybsze, niż ich odpowiedniki przy użyciu tradycyjnych komputerów. Aktualnie (wiosna 2021) znane doniesienia o uzyskaniu supremacji kwantowej raczej okazywały się przechwałkami, choć mającymi pewne przesłanki do uznania sukcesu w jakimś limitowanym zastosowaniu. Przykładem jest choćby to doniesienie:https://spidersweb.pl/2020/12/chiny-supremacja-kwantowa.html.

W przyszłości jednak (być może nawet tej najbliższej) można się spodziewać osiągnięcia na tyle istotnego postępu na polu obliczeń kwantowych, że zapewnią one znaczącą przewagę temu ośrodkowi, tej organizacji, państwu, które pierwsze tę technologię opanuje w postaci kwantowej supremacji.

Istotnym ograniczeniem na praktyczne wdrożenia kwantowych technik obliczeniowych jest to, że im bardziej uniwersalny miałby być budowany komputer kwantowy, co oznacza zdolność do stosowania wielu różnych bramek, tym trudniej jest go skalować do wykorzystania wielu kubitów. Aktualne wdrożenia oferują bowiem albo więcej kubitów, ale mniej

mentations of quantum techniques, has anyway a drawback caused by the lack of implementation for quantum gates. It makes many experts deny the name of quantum computer for this implementation. Even if it is quite easy to increase the number of qubits in the annealing technique, it has very limited domains of application, in general. It is not possible (at least at the current stage of development) to realise Shor algorithm, neither the other – more universal - algorithms.

6.4. Notion of Quantum Supremacy

Concerning the development of quantum IT a notion of quantum supremacy is defined. It could refer to such improvements of quantum computers that the computations in this technology would be faster than on traditional computers. Now, (in the spring of 2021) the known information about reaching a quantum supremacy is rather premature even if there were some premises of a success in a limited application. Following announcement may be an example of it:

https://spidersweb.pl/2020/12/chiny-supremacja-kwantowa.html.

In the future (maybe not so far) it can be expected that a sufficiently essential progress happens in quantum computations to secure the quantum supremacy for a centre, organisation, or state which as the first one could manage this technology.

Practical implementation of quantum computation techniques encounters an essential limitation in the fact that more universal quantum computer is designed, what means the capacity for using many different gates, the more difficult is to calibrate it for using many qubits. The present implementations offer solutions with greater number of qubits but less number of gates for them,

bramek do nich, czyli mniejsze możliwości wdrożenia algorytmów kwantowych, albo co prawda większą możliwość manipulacji kubitami, lecz realnie z niewielką ilością samych kubitów.

7. Potencjalne zastosowania komputerów kwantowych w dziedzinie obronności

Podstawową korzyścią z zastosowania komputera kwantowego w obronności jest możliwość wykonania znacząco szybciej, niż ma to miejsce dla komputerów tradycyjnych pewnych rodzajów obliczeń. Niektóre problemy o dużej złożoności obliczeniowej, nawet z zastosowaniem superkomputerów, wymagają tak wielkiej ilości obliczeń, że ich wykonanie trwałoby wiele lat – niekiedy na poziomie setek, tysięcy, czy nawet milionów lat. Te same problemy obliczeniowe przekształcone do postaci algorytmów kwantowych mogłyby być rozwiązywane w takim czasie, który daje już szanse na realne sukces w postaci na przykład:

- łamania kluczy szyfrowych – np. dzięki wykorzystaniu algorytmu Shora;
- wspomagania w jakimś zakresie innych, szczególnie złożonych obliczeniowo analiz danych.

8. Łamanie kluczy szyfrowanych opartych o złożoność obliczeniową faktoryzacji liczb

Złożoność obliczeniowa rozkładu bardzo dużych liczb na czynniki pierwsze (faktoryzacja) jest dla tradycyjnego komputera problemem rozwiązywanym w czasie wykładniczym względem długości liczby. To oznacza, że dla wchodzących w grę zastosowań czas faktoryzacji bardzo szybko rośnie do wartości porównywalnych nawet z przyjmowanym powszechnie wiekiem Wszechświata.

Tymczasem kwantowy algorytm Shora faktoryzacji liczb umożliwia (przynajmniej teoretycznie, bo wciąż nie mamy praktycznych

what reduces the application of quantum algorithms, or a greater possibility for manipulating the qubits, but in reality with a small number of the qubits.

7. Possible Use of Quantum Computers in Defence Sector

Major benefit from the use of a quantum computer in defence sector is that some computations may be made significantly faster than on traditional computers. Some problems of high computational complexity require the years, or even hundred, or thousand, or even million years of computations even if supercomputers could be used. The same computational problems transformed into the form of quantum algorithms would be solved within the time which offers a chance for a real success like in the case of:

- Breaking the coded keys – e.g. using Shor algorithm,
- Assisting, in some degree, the other data analyses which are especially complicated in computations.

8. Breaking the Coded Keys Based on Computational Complexity of Factorisation of Numbers

Computational complexity of decomposition of great numbers into original factors (factorisation) by traditional computers makes the time needed for solution increase exponentially with the length of the number. It means that for possible applications the time of factorisation increases rapidly to values which can be even compared to the existence of the Universe.

The quantum Shor algorithm for factorisation of numbers can make this factorisation (at least theoretically as this algorithm is still not commercially availa-

wdrożeń tego algorytmu w komercyjnym wymiarze) tę faktoryzację w czasie $O((\log N)^3)$. Dla bardzo dużych N (a to o takie właśnie przypadki praktycznie chodzi) różnica jest ogromna na korzyść komputera kwantowego.

Z racji na to, że faktoryzacja liczb jest podstawą łamania wielu asymetrycznych algorytmów kryptograficznych – np. najczęściej chyba aktualnie stosowanego algorytmu RSA – zastosowanie na pełną skalę komputerów kwantowych zmieniłoby układ sił w zakresie całych wielkich obszarów kryptografii.

Problemem jednak jest praktyczne wykorzystanie algorytmu Shora. Dla zastosowań, które mają realne znaczenie we współczesnej kryptografii, wymagane jest wykorzystanie tylu kubitów oraz takich bramek kwantowych, jakich aktualne komputery kwantowe nie są w stanie obsłużyć. Szczytowym osiągnięciem, na razie, jest faktoryzacja przez komputer kwantowy… liczby 15.

9. Zapewnienie poufności informacji dzięki kwantowym technikom dystrybucji klucza

Bardziej praktyczne zastosowanie właściwości układów kwantowych jest aktualnie dostępne w obszarze QKD czyli Quantum Key Distribution (dystrybucja klucza kwantowego).

W tym wypadku kwantowy aspekt kryptografii związany jest z możliwością uzgodnienia/przekazania klucza szyfrowego w sposób absolutnie odporny na przechwycenie, ewentualnie podsłuchanie. Później tak przekazany klucz może posłużyć do zaszyfrowania komunikatu tradycyjnymi, symetrycznymi algorytmami szyfrowymi.

Istotą QKD jest oparcie metody o **splątanie kwantowe**. Splątanie cząstek ustanawia pomiędzy nimi szczególny rodzaj połączenia, powodującego iż odczyt splątanego parametru

ble) within the time $O((\log N)^3)$. For very great numbers N (and these are the real cases) there is an immense difference in favour of the quantum computer.

Due to the fact that the factorisation of numbers is a base for breaking many asymmetrical cryptographic algorithms – for instance RSA which is recently mostly used – the application of quantum computers in the full scale would change the configuration of power in the range of huge areas of cryptography. But the practical deployment of Shor algorithm is still a problem. For applications with real meaning in the present cryptography the use of so many qubits, and such quantum gates, is required that quantum computers of today cannot provide. Up to now a top achievement is factorisation of number… 15 by the quantum computer.

9. Securing Confidence of Information by Quantum Techniques of Key Distribution

More practical application of properties of quantum systems is currently available in domain of QKD - Quantum Key Distribution.

In this case the quantum aspect of cryptography is connected with a possibility for acceptation/transfer of coded key in the way which is absolutely resistant against interception, or possible tapping. Later, the key transferred in such way may be used for coding messages in traditional and symmetrical coding algorithms.

The essence of QKD is the **quantum entanglement**. Entanglement of particles settles a particular way of connection between them causing that the readout of the entangled parameter of the first particle is strictly

pierwszej cząstki jest ściśle skorelowany z odczytem (podczas pomiaru) drugiej cząstki z pary. Przykładowo dwa splątane ze sobą fotony podczas pomiaru będą miały dokładnie przeciwne polaryzacje – jeśli jeden wykaże podczas pomiaru polaryzację prawoskrętną, to drugi z pewnością będzie miał polaryzację lewoskrętną. Jaka ta polaryzacja jest, okazuje się dopiero podczas pomiaru.

Strony pragnące być pewne poufności wspólnie wykorzystywanego klucza szyfrowego mogą ów klucz zakodować w cząstkach splątanych. Wtedy, niezależnie od dzielącej ich odległości, a także bez konieczności jakiegokolwiek kanału komunikacji między nimi, pomiar dokonany na którejkolwiek z cząstek ze splątanej pary, będzie skutkował wiedzą o tym, jaką wartość odpowiadającego pomiaru uzyska druga strona. A to oznacza, iż strony mają dostęp do tego samego ciągu wartości (najczęściej ciągu bitów). Ten ciąg może posłużyć do zaszyfrowania informacji tradycyjnym algorytmem symetrycznym. Metoda ta (przy założeniu, że sama splątana cząstka nie była przechwycona) jest stuprocentowo bezpieczna, ponieważ jakikolwiek odczyt stanu splątanej cząstki przez potencjalnego napastnika i tak niszczy splątanie, czyniąc ten kanał dystrybucji klucza bezużytecznym. Przy zastosowaniu dodatkowych protokołów kontrolnych, możliwe jest dodatkowo zdekonspirowanie napastnika.

Ten efekt jest podstawą licznych protokołów wymiany/negocjacji klucza szyfrowego.

10. Teleportacja kwantowa

Cząstki splątane mogą być użyte do tzw. teleportacji kwantowej. Teleportację tę należy rozumieć, jako przeniesienie stanu kwantowego na odległość – przekazanie tego stanu z jednego układu kwantowego na inny.

Warto zauważyć w tym kontekście, że nie

correlated with the readout (during the measurement) of the second particle of the couple. For instance, two mutually entangled photons will have exactly opposite polarisations at the measurement – if one of them will show the right-turning polarisation, then the second one will certainly have the left-turning polarisation. What the polarisation is, can be disclosed only during the measurement.

The parties which want to be sure of the confidence represented by the mutually used coded key may code this key in the entangled particles. Then, independently on the distance separating them, and moreover without any necessity of a communicating channel between them, the measurement made on any particle from the entangled couple will effect in the knowledge about the value the second party will receive at the measurement. It means that the parties have access to the same series of values (usually a series of bits). This series can be used to code the information using traditional symmetrical algorithm.This method (assuming that the entangled particle was not intercepted) is absolutely safe, because any readout of the state of the entangled particle by a potential enemy destroys the entanglement and this channel of distribution of the key becomes useless. By using additional checking protocols it is possible to discover the attacker.

This effect is a principle of many protocols for exchange/negotiation of coding key.

10. Quantum Teleportation

Entangled particles may be used for the so called quantum teleportation. Teleportation has to be interpreted as transfer of quantum state in space from one quantum system to another one.

It is worth to note in this context that

jest możliwe po prostu skopiowanie stanu kwantowego w celu przeniesienia go do nowej lokalizacji.

10.1. Twierdzenie Wootersa – Żurka o nieklonowaniu

Treść twierdzenia o nieklonowaniu: Nie istnieje kwantowa maszyna zdolna do tworzenia kopii nieznanego stanu kwantowego.

Brak możliwości skopiowania stanu kwantowego nie oznacza, iż tego stanu nie da się przenieść. Bowiem jest możliwe przekazanie stanu kwantowego, o ile stan źródłowy zostanie przy okazji zniszczony.

Protokoły teleportacji kwantowej działają właśnie w ten sposób, że przekazują stan kwantowy, niszcząc informacje o tym stanie w cząstce źródłowej (ogólniej: obiekcie źródłowym). Dodatkowo należy zauważyć, iż w protokołach tych używane są także klasyczne kanały komunikacji. Inaczej, czyli bez połączenia komunikacji na poziomie kwantowym i klasycznym, nie dałoby się przenieść całości stanu kwantowego na nowy obiekt.

11. Wspomaganie komputerami kwantowymi zaawansowanych obliczeń

Moc obliczeniowa komputerów kwantowych potencjalnie może być wykorzystana do najbardziej wymagających pod względem obliczeniowym analiz sygnałów radarowych. W szczególności radary pasywne, czyli nie posiłkujące się nadajnikami, a korzystające z komercyjnych nadajników infrastruktury radiofalowej na danym terenie, stawiają bardzo wysokie wymagania pod względem mocy przetwarzania. Uwzględnienie wszystkich czynników jakie związane są propagacją fal elektromagnetycznych, stanowi ogromne wyzwanie dla tradycyjnych komputerów. Jak podaje o radarach pasywnych Wikipedia: *Ponieważ radar pasyw-*

it is not possible to do a simple copy of the quantum state in order to move it into a new localisation.

10.1. Wooters – Żurek Theorem of Non-cloning

Theorem of non-cloning goes: there is no quantum device able for making a copy of an unknown quantum state.

Lack of possibility for copying the quantum state does not mean that this state cannot be transferred. Transfer of the quantum state is possible provided that the original state is destroyed by the same.

Protocols of quantum teleportation operate just in this way that they transfer the quantum state and destroy information about this state in the source particle (in general: in the source object). Additionally, it has to be noted that in these protocols the classical channels of communication are also used. There is no other way, i.e. without combining the communication on the quantum and classical levels, for transporting the whole quantum state on a new object.

11. Assisting Advanced Computations by Quantum Computers

Computation power of quantum computers may be potentially used for analyses of radar signals which are the most challenging in computations. Especially the passive radars which do not use any transmitters, but harness the commercial transmitters of radio infrastructure of the area, have high requirements for the processing power. Considering all factors connected with propagation of electromagnetic waves is an enormous challenge for traditional computers. Wikipedia comments the passive radars: *Because passive radar demands the use of complex correlating processes, the tech-*

ny wymaga zastosowania złożonych procesów korelacyjnych, dlatego ta technika poszła w zapomnienie na wiele lat, wyparta przez prostsze radary impulsowe. Od początku XXI wieku w związku z szybkim wzrostem mocy obliczeniowej komputerów, procesorów sygnałowych i układów logiki programowalnej wrócono do idei radarów pasywnych i je się rozwija.

Warto zauważyć, że technologia radarów pasywnych ma ogromne zalety w porównaniu do radarów aktywnych. Przede wszystkim nie zdradza położenia nadajnika, a nawet nie zdradza, że obiekty są w ogóle namierzane. Oznacza to, że radary pasywne mogą penetrować wrogie terytoria, samemu pozostając w ukryciu. Problemem są tu jednak ogromne wymagania względem mocy obliczeniowych.
Można przypuszczać, że pewne właściwości komputerów kwantowych – szczególnie związane z algorytmami dyskretnej transformaty Fouriera, stosowanej w technikach radarowych, a mające swoje odpowiedniki w postaci kwantowej transformaty Fouriera, mogłyby zapewniać wsparcie do szczególnie złożonych obliczeń.

12. Obliczenia kwantowe, a informatyka tradycyjna

W podsumowaniu do niniejszego raportu niezbędne wydaje się rozważenie pytania: dlaczego w ogóle mielibyśmy inwestować czas, energię, zasoby w dziedzinę obliczeń kwantowych. Co jest tutaj korzyścią?

Aby odpowiedzieć sobie na powyższe pytanie, warto jest zauważyć, że istnieją symulatory komputerów kwantowych, realizowane w oparciu o zwykłe komputery. Naturalnym jest więc zadanie nowego pytanie: czy symulator by nie wystarczył? Krótka odpowiedź brzmi: nie. Symulator kwantowy nie zastąpi realnej realizacji fizycznej procesu kwantowego. Nie zastąpi go z dwóch podstawowych powodów:

nique was forgotten for many years and was replaced by simpler pulse radars. The idea of passive radars has returned since the beginning of 21st century along with a rapid increase of computation power of computers, signal processors, and systems of programmable logics, and it still has been developing.

It is worth to note that the idea of passive radars has great advantages comparing to active radars. First of all it does not disclose the location of transmitter, and even it does not betray that the objects are targeted. It means that the passive radars may penetrate the territories of enemy and remain undetected. Anyway, the huge requirements for the computational power are problematic questions here. It may be expected that certain properties of quantum computers – especially connected with algorithms of the discrete Fourier transform used in radar technologies, and having their counterparts in the form of the quantum Fourier transform, would provide assistance for especially complex computations.

12. Quantum Computations and Traditional IT

Summing up the paper it is necessary to put a question: why in general we have to invest time, energy, and resources into quantum computations. What the benefits are?

To answer that question it is worth to note that there are simulators of quantum computers built from standard computers. Then, a natural question is if the simulator could not be sufficient? A short answer is: not. Quantum simulator cannot replace any real physical form of quantum process. It cannot be done because of two reasons:

– Simulator cannot perform the quantum entanglement in a proper way,

– symulator nie jest w stanie zrealizować poprawnie splątania kwantowego,
– symulator nie umożliwia realizacji prawdziwej superpozycji stanów kwantowych.

Obie te własności procesów kwantowych można przybliżać modelowaniem w zwykłych komputerach, jednak takie przybliżenie będzie zawsze niedoskonałe. Może być zatem użyte do celów szkoleniowych, może pomóc w projektowaniu prawdziwych komputerów kwantowych, lecz nie może tych komputerów kwantowych zastąpić. Bo to właśnie w tych dwóch aspektach – splątaniu i superpozycji – zawiera się siła i sens obliczeń kwantowych, a także ich przewaga nad komputerami tradycyjnymi, a tych żaden symulator nie zrealizuje.

Patrząc na samą naturę zjawiska, w jedynym tylko kubicie zaszyte są dwie liczby rzeczywiste, opisywane na sferze Blocha przez kąty φ i θ. Liczba rzeczywista zawiera w sobie nieskończoną liczbę cyfr rozwinięcia. To oznacza, że w porównaniu z tradycyjnym bitem, który rozgranicza tylko dwa stany, kubit jest nośnikiem nieskończenie większej ilości informacji. Teoretycznie wewnątrz, w strukturze kwantowej sam tylko jeden kubit gromadzi niejako więcej informacji, niż wszystkie komputery świata, dla których przecież liczba bitów jest skończona.

Oczywiście tylko takie porównanie byłoby względem tradycyjnych komputerów niesprawiedliwe. Bo jednak nasz dostęp do tej nieskończonej ilości informacji w kubicie jest też jednocześnie nieskończenie trudny, wymagałby nieskończonej ilości prób, jako że do wartości kubitu i tak realnie możemy sięgnąć dopiero poprzez pomiar, redukujący stany kwantowe, do odpowiedzi bitowej. W ten sposób tracimy owo bogactwo nieskończonej ilości informacji, redukując do odpowiedzi: 0 lub 1. To nie zmienia jednak samego faktu, że nawet najprostszy kubit – przynajmniej w teorii – wewnętrznie

– Simulator cannot provide realisation of real superposition of quantum states.

These two properties of quantum processes may be approximated by modelling on standard computers, but such approximation will be always imperfect. It may be used for training, or it may be helpful at designing real quantum computers, but it could not replace these quantum computers. It is just in this two aspects – entanglement and superposition – where the power and sense of quantum computations makes their advantage over standard computers, and any simulator cannot do it instead.

Just regarding the mere nature of the phenomenon, there are two real numbers coded in one qubit which are described in the Bloch sphere by angles φ and θ. Any real number includes infinite numbers of numerals in evolution. It means that comparing it to the traditional bit, which distinguishes only two states, the qubit is a carrier of infinitely greater volume of information. Theoretically, inside of only one qubit there is more information included in its quantum structure than in all computers in the world which anyway have a limited number of bits.

Of course, limiting the comparison only to this question is unfair to traditional computers. Anyway, the access to that unlimited volume of information inside the qubit is also infinitely difficult as it could require an infinite number of trials, as in reality we can get the access to qubit's value only through the measurement by reducing the quantum states to the answer expressed in bits. In this way we lose this abundance of infinite volume of information by reducing it to the answer: 0 or 1. But it does not change the fact that even the simplest qubit – at least in theory – works intrinsically as it would use "an

działa jakby na „nieskończonym prywatnym rejestrze", na strukturze informacyjnej nie mającej ograniczeń komputerów tradycyjnych, dla których bit zawsze ma jedynie dwa możliwe stany. Pod tym względem obliczenia wykorzystujące procesy kwantowe noszą znamiona podobieństwa do obliczeń analogowych. Jednak o ile typowy procesor analogowy jest projektowany ściśle pod konkretne zastosowanie, to w przypadku obliczeń na kubitach, możliwe jest o wiele bardziej dowolne projektowanie algorytmów obliczeniowych.

Fundamentalną przewagą obliczeń kwantowych nad tradycyjnymi jest to, że proces kwantowy w jednym przebiegu ewolucji rejestru kwantowego sprawdza jednocześnie wszystkie możliwości jego realizacji. Cząstka elementarna – np. elektron w atomie – ostatecznie realizując jakiś swój stan, czyli np. przechodząc na określony poziom wzbudzony – podczas tego przejścia w pewien sposób „bierze pod uwagę" wszystkie istniejące stany, jakie mogłaby zrealizować, uwzględnia w jakimś sensie nieskończoną liczbę czynników (choć na koniec i tak realizuje tylko jeden z branych pod uwagę stanów). Można by obrazowo powiedzieć, że najprostszy nawet kubit, który został potraktowany sekwencją bramek kwantowych, z punktu widzenia tradycyjnej informatyki patrząc, „dokonał nieskończonej ilości obliczeń w znaczeniu komputera klasycznego". Z tego też powodu, żaden symulator kwantowy na komputerach tradycyjnych nie jest w stanie w pełni odwzorować zachowania rzeczywistego układu kwantowego.

Aktualnie techniki obliczeniowe oparte o prawa kwantowe rozwijają się bardzo dynamicznie. Co kilka miesięcy pojawiają się przełomowe odkrycia. To powoduje, że nie sposób jest ściśle przewidzieć ani konkretnej daty w pełni komercyjnego wdrożenia obliczeń kwantowych, ani nawet w jakiej z aktualnie opraco-

infinite private register", or an information structure which has no limitations of traditional computers which can only use bits with two possible states. In this aspect, the computations using the quantum processes are similar to analogue computations. But, whereas a typical analogue processor is designed for a specific application, in the case of computations using the qubits it is possible to design the computation algorithms in a more independent way.

Fundamental advantage of quantum calculations over the traditional ones is that the quantum process at one run of the quantum register evolution is checking at the same time all possibilities of its realisation. An elementary particle – e.g. electron in atom – finally realises one of its states, for instance by jumping into a specific excited level – and during this transferring "it takes into account", in certain degree, all existing states which it could realise, or it considers a boundless number of factors (even if at the end it realises only one from considered states). It may be illustrated in other words by saying that even the simplest qubit which was treated by a sequence of quantum gates has performed, from the point of view of traditional IT, an infinite number of computations of a traditional computer. For this reason any quantum simulator built on traditional computers cannot replicate completely the operation of a real quantum system.

Now, the computation technologies based on quantum principles have been developing intensively. Mile stone discoveries are made at every few months. For this reason it is not possible to predict exactly any specific date for commercial implementation of quantum computations, nor to say what technologies could be used for this breakthrough. The investigations

wywanych technologii nastąpi ten kluczowy przełom. Bo badania prowadzone są wielotorowo, w wielu ośrodkach na świecie. Co do jednego fachowcy raczej są zgodni: ten ośrodek, państwo, organizacja które jako pierwsze opanują technologie kwantowe do poziomu pozwalającego na supremację kwantową, będzie miał znaczącą przewagę nad resztą świata.

are made by many centres in the world, and in many parallel domains. There is one prevailing opinion of experts that the centre, or state, or organisation which manage to handle the quantum technologies on the level securing the quantum supremacy will get a significant advantage over the rest of the world.

Literatura / *Literature*

[1] Wikipedia – różne tematy – w szczególności: kubit, pułapka jonowa, Quantum logic gate i inne.

[2] Świat nauki, Christopher R. Monroe, David J. Wineland „Jonowe maszyny cyfrowe” 16.12.2012 https://www.swiatnauki.pl/8,675.html

[3] Chiński komputer osiąga supremację kwantową: https://spidersweb.pl/2020/12/chiny-supremacja-kwantowa.html

[4] ZDNET, What is quantum computing today? The how, why, and when of a paradigm shift, Scott Fulton III | 10 listopada 2020 https://www.zdnet.com/article/what-is-quantum-computing-understanding-the-how-why-and-when-of-quantum-computers/

[5] ZDNET Quantum computers are coming. Get ready for them to change everything, Daphne Leprince-Ringuet | 2 listopada 2020 https://www.zdnet.com/article/quantum-computers-are-coming-get-ready-for-them-to-change-everything/

[6] ZDNET We're hacking the process of creating qubits.' How standard silicon chips could be used for quantum computing Daphne Leprince-Ringuet, 31 marca, 2021m https://www.zdnet.com/article/were-hacking-the-process-of-creating-qubits-how-standard-silicon-chips-could-be-used-for-quantum-computing/

[7] Neil Gershenfeld i Isaac L. Chung, Molekularne komputery kwantowe, Świat Nauki, Nr 8 (sierpień), 1998

[8] Udostępniono pierwszy opensource'owy komputer kwantowy. Można korzystać za darmo 17 marca 2021, https://kopalniawiedzy.pl/QSCOUT-komputer-kwantowy-platforma-kwantowa-Quantum-Scientific-Computing-Open-User-Testbed,33492

[9] Jak znaleźć „kwantową igłę” w stogu spinów? Ważny krok ku kwantowemu internetowi 3 marca 2021, https://kopalniawiedzy.pl/kwantowy-internet-kubit-informacja-komputer-kwantowy,33427

[10] Urojona część mechaniki kwantowej naprawdę istnieje, 26.03.2021 https://naukawpolsce.pap.pl/aktualnosci/news%2C87076%2Curojona-czesc-mechaniki-kwantowej-naprawde-istnieje.html

[11] Scientists take step towards quantum supremacy March 18, 2021 by National University of Science and Technology MISIS https://phys.org/news/2021-03-scientists-quantum-supremacy.html

[12] Physicists transmit data via Earth-to-space quantum entanglement, July 11, 2017 report by Bob Yirka , Phys.org https://phys.org/news/2017-07-physicists-transmit-earth-to-

space-quantum-entanglement.html

[13] Researchers discover a way to avoid decoherence in a quantum system March 8, 2013 by Bob Yirka , Phys.org https://phys.org/news/2013-03-decoherence-quantum.html

[14] A Two Qubit Logic Gate in Silicon, M. Veldhorst, C.H. Yang, J.C.C. Hwang, W. Huang, J.P. Dehollain, J.T. Muhonen, S. Simmons, A. Laucht, F.E. Hudson, K.M. Itoh, A. Morello, and A.S. Dzurak, November 25, 2014, http://arxiv.org/pdf/1411.5760.pdf