STUDIA INFORMATICA 2000
Volume 21 Number 1 (39)

Stefan WĘGRZYN, Jerzy KLAMKA
Instytut Informatyki Teoretycznej i Stosowanej PAN

KWANTOWE SYSTEMY INFORMATYKI

Streszczenie. W historii rozwoju informatyki jako dyscypliny naukowej wykorzystywano w obszarze jej badań doświadczalnych najpierw makroukłady, a więc przekaźniki, później lampy elektronowe, tranzystory, a następnie obwody scalone o dużej i bardzo dużej skali integracji. Zwrócenie uwagi na możliwość wykorzystania obecności atomów i molekuł jako symboli do kodowania programów informatyki dało początek badaniom nad nanosystemami informatyki. W obecnie prowadzonych pracach nad kwantowymi systemami informatyki bada się możliwości wykorzystania jako symboli do kodowania, a zarazem środka do wykonywania obliczeń, kierunków spinów atomowych i zjawisk magnetycznego rezonansu jądrowego. W artykule omówiono istotę tych zjawisk i sposób ich opisu przydatny na potrzeby informatyki kwantowej. Omówiono działanie kwantowej bramki logicznej i podstawowych elementów komputera kwantowego. Podano matematyczne podstawy obliczeń kwantowych i zasady programowania.

QUANTUM COMPUTER SYSTEMS

Summary. In the development of computer science as a scientific discipline there was a time period during which experimental research were based on macrosystems like relays, then electronics tubes, transistors and recently large scale and very large scale integrated systems. Research studies directed towards computer nanosystems have been initiated by focusing attention on the possibility of using atoms and molecules as coding symbols for computer programs. In the present studies on quantum computer systems possibility of using direction of atomic spin and phenomena of magnetic nuclear resonance as coding symbols is investigated. In the paper the fundamentals of the magnetic nuclear resonance and possibilities of using them to data coding and processing are discussed. Principles of quantum logic gates and basic elements of a quantum computer are described. Mathematical bases of quantum computation and principles of programming are also given.

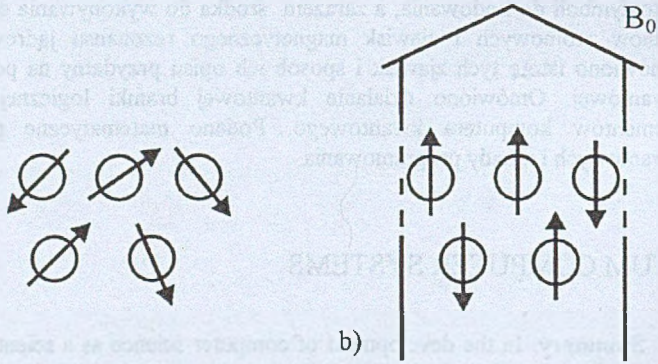
1. Jądrowy rezonans magnetyczny

Podstawowym zjawiskiem fizycznym branym pod uwagę w aktualnie prowadzonych pracach nad komputerami kwantowymi jest specyficzne, opisywane za pomocą mechaniki kwantowej, zachowanie się jąder atomów, zwane *jądrowym rezonansem magnetycznym*.

Zjawisko to polega na, zachodzącym w niektórych przypadkach, rezonansowym pochłanianiu energii elektromagnetycznej w ciałach stałych, cieczach i gazach, a związane jest z posiadaniem przez jądra pierwiastków o nieparzystej liczbie protonów lub neutronów wewnętrznego momentu pędu, zwanego *spinem*, oraz momentu magnetycznego.

Przy braku zewnętrznego pola magnetycznego kierunki momentów magnetycznych jąder są ustawione przypadkowo.

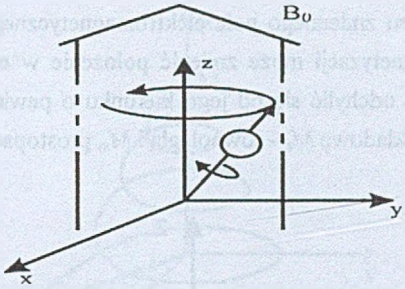
Jeżeli badany obiekt umieścimy w stałym polu magnetycznym o indukcji B_0, to niektóre z jąder o początkowo przypadkowym ustawieniu kierunków momentów magnetycznych zostaną uporządkowane w odniesieniu do kierunku B_0, przyjmując położenie równoległe, które oznaczać będziemy symbolem↑, lub antyrównoległe, które oznaczać będziemy symbolem ↓ (rys. 1).



Rys. 1. Położenie wektorów momentów magnetycznych jąder przed i po wprowadzeniu stałego pola elektromagnetycznego B_0

Fig. 1. Position of the nuclear magnetic momentum vectors before and after introduction of constant magnetic field B_0

Niezależnie od tych dwóch możliwych położeń wektor momentu pędu każdego jądra wykonuje w przestrzeni ruch obrotowy, zakreślając stożek, którego wierzchołek stanowi jądro atomu. Ruch taki nosi nazwę *precesji* i jest wywołany działaniem zewnętrznej siły magnetycznej – rys. 2.



Rys.2. Precesja wektora momentu magnetycznego
Fig. 2. Precession of the vector of magnetic momentum

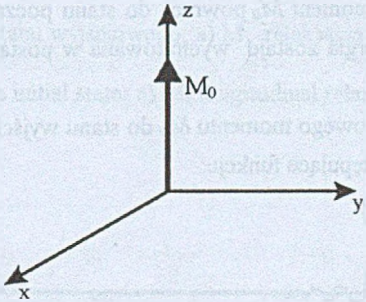
Częstotliwość ruchu precesyjnego f_0 i związana z nią prędkość kątowa ω_0 zależą od indukcji pola magnetycznego B_0 i określone są wzorem Larmora:

$$f_0 = \gamma B_0 / 2\pi \qquad \text{lub} \qquad \omega_0 = \gamma B_0 \tag{1}$$

gdzie: γ – współczynnik żyromagnetyczny,

B_0 mierzone w teslach, $1T = 10\,000$ Gs.

W warunkach równowagi termodynamicznej liczba jąder ustawionych zgodnie z kierunkiem B_0 (co odpowiada niższemu poziomowi energetycznemu stanu magnetycznego) oznaczonych symbolem ↑ jest większa od liczby jąder ustawionych przeciwnie, antyrównolegle i oznaczonych symbolem ↓. W badanym obiekcie wystąpi niewielkie, wypadkowe namagnesowanie (wypadkowy moment magnetyzacji) M_0, tak jak to ilustruje rys. 3.

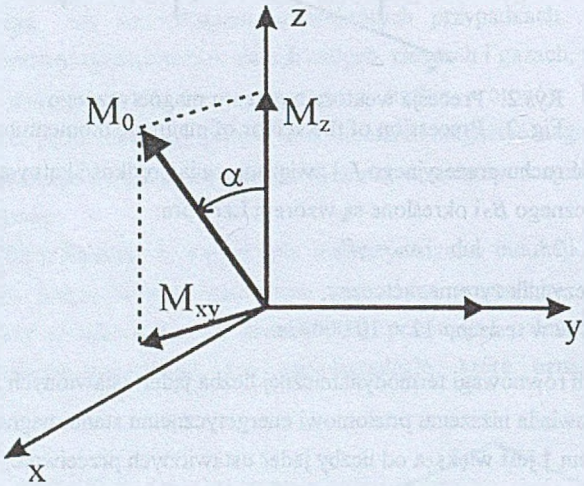


Rys. 3. Wypadkowy wektor magnetyzacji obiektu jako wypadkowe wektorów momentów magnetycznych jąder
Fig. 3. Resultant vector of system magnetization as the resultant of the nuclear magnetic momentum vectors

Taki układ może pochłonąć energię dostarczoną z zewnątrz, gdy częstotliwość zewnętrznego wzbudzającego pola elektromagnetycznego jest równa częstotliwości Larmora.

Częstotliwość ta leży w przedziale częstotliwości radiowych, dlatego mówi się potocznie o impulsach radiowych.

Po otrzymaniu impulsu zmiennego pola elektromagnetycznego o częstotliwości Larmora wypadkowy wektor magnetyzacji może zmienić położenie w odniesieniu do zewnętrznego pola magnetycznego B_0 i odchylić się od jego kierunku o pewien kąt α. Wektor M_0 można wtedy rozłożyć na dwie składowe M_z – równoległą i M_{xy} prostopadłą do linii pola B_0, tak jak to pokazuje rys. 4.



Rys.4. Rozkład wektora M_0 na dwa wektory M_z oraz M_{xy}
Fig. 4. Decomposition of the vector M_0 onto two vectors M_z and M_{xy}

Po ustaniu pobudzenia moment M_0 powraca do stanu początkowego, tak jak to ilustruje rys. 5, a nagromadzona energia zostaje wyemitowana w postaci tak zwanego *sygnału swobodnej relaksacji* lub *echa*.

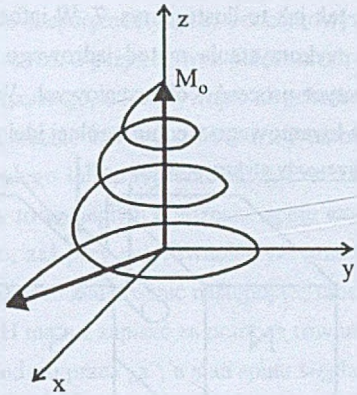
Proces powrotu wypadkowego momentu M_0 do stanu wyjściowego opisują dla przypadku odchylenia o kąt α = 90° następujące funkcje:

$$M_z = M_0\left(1 - e^{-t/T_1}\right)$$

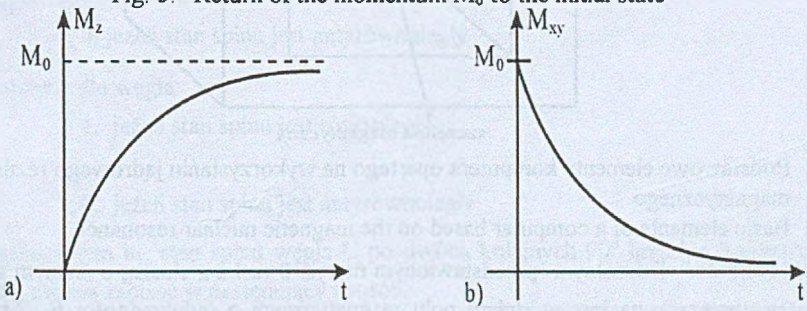
$$M_{xy} = M_0\, e^{-t/T_2} \tag{2}$$

tak jak to ilustruje rys. 6.

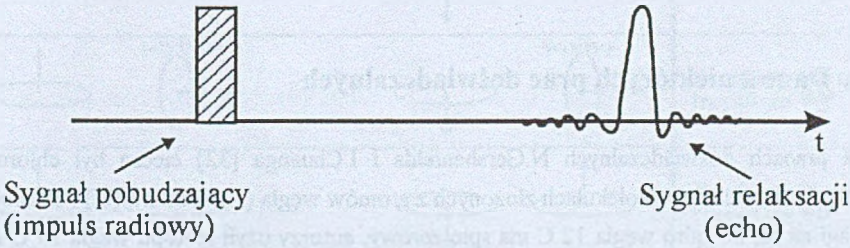
Istotą metod opartych na wykorzystaniu jądrowego rezonansu magnetycznego jest nadawanie, za pomocą cewki nadawczej, skierowanych na badany obiekt impulsów elektromagnetycznych o odpowiednio dobranych częstotliwościach i czasach trwania oraz odbieranie za pomocą cewki odbiorczej nadchodzącego z badanego obiektu echa, czyli sygnałów relaksacji – tak jak to ilustruje rys. 7.



Rys.5. Powrót momentu M_0 do stanu początkowego
Fig. 5. Return of the momentum M_0 to the initial state



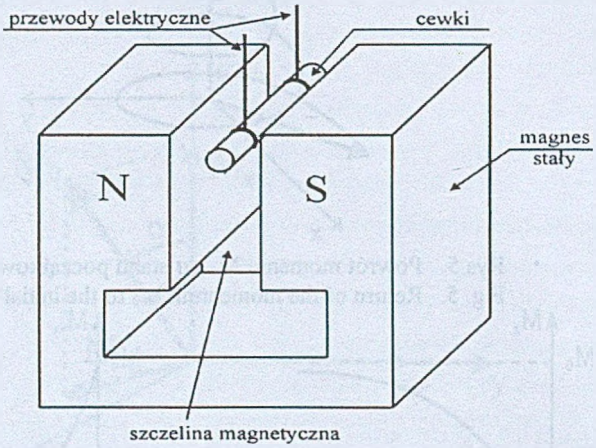
Rys.6. Proces powrotu do stanu wyjściowego: a) M_z relaksacja podłużna, b) M_{xy} relaksacja poprzeczna
Fig.6. Return process to the initial state: a) M_z longitudinal relaxation, b) M_{xy} transversal relaxation



Rys.7. Sygnał pobudzający i jego echo
Fig. 7. Stimulating signal and its echo

W zastosowaniach jądrowego rezonansu magnetycznego do badań materiałów w technice i fragmentów organizmów żywych w medycynie chodzi o wnioskowanie o strukturze wewnętrznej badanych obiektów, na podstawie porównania sygnałów pobudzających i otrzy-

manych sygnałów relaksacji, tak jak to ilustruje rys. 7. W informatyce natomiast prowadzi się badania nad możliwościami wykorzystania metod jądrowego rezonansu magnetycznego do realizacji właściwych informatyce procesów obliczeniowych. W szczególności bada się możliwości konstrukcji komputera kwantowego według ogólnej idei przedstawionej na rys. 8.



Rys.8. Podstawowe elementy komputera opartego na wykorzystaniu jądrowego rezonansu magnetycznego

Fig. 8. Basic elements of a computer based on the magnetic nuclear resonance

W układzie doświadczalnym przedstawionym na rys. 8 rurka z cieczą, o znanym składzie i strukturze, umieszczona jest w stałym polu magnetycznym o indukcyjności B_0. Momenty poszczególnych atomów molekuł cieczy znajdującej się w rurce traktuje się jako symbole elementarnych jednostek obliczeniowych (qubitów), a proces obliczeniowy polega na realizacji programu, którym jest wprowadzenie serii odpowiednio dobranych impulsów elektromagnetycznych i odczytanie wyniku.

2. Dane z niektórych prac doświadczalnych

W pracach doświadczalnych N.Gershenfelda i I.Chuanga [32] cieczą był chloroform ($CHCl_3$), a więc ciecz o molekułach złożonych z atomów węgla (C), wodoru (H) i chloru (Cl). Z uwagi na to, że jądro węgla 12 C ma spin zerowy, autorzy użyli izotopu węgla 13 C z jednym dodatkowym neutronem, który dostarczył jądru niezbędny spin.

Atomy C i H występują w molekule chloroformu obok siebie, co powoduje wzajemne uzależnienie reakcji każdego z nich od stanu sąsiedniego.

Przeprowadzono następujące eksperymenty: przy początkowym równoległym, w stosunku do kierunku B_0 spinie C, wprowadzono przy różnych położeniach spinu H - jeden po drugim - impulsy zmiennego pola magnetycznego, oddziaływując na położenie spinu C.

Pierwszy impuls odchyla położenie spinu C o 90°, drugi natomiast odchyla go o dalszych 90°, ale do położenia równoległego lub antyrównoległego, w zależności od kierunku spinu wodoru (H). Mianowicie – przy równoległym położeniu spinu wodoru odwraca spin C o 180° od jego położenia wyjściowego, zaś przy antyrównoległym położeniu spinu H przywraca go do położenia wyjściowego. Można to zilustrować następującą tabelką (rys. 9).

Zachowanie się spinów C i H można zapisać za pomocą równań logicznych.

Oznaczmy np. stan spinu wodoru przez „a", a stan spinu węgla przez „b" i przyjmijmy:

$$a = \begin{cases} 1, \text{ jeżeli stan spinu jest równoległy} \\ 0, \text{ jeżeli stan spinu jest antyrównoległy} \end{cases}$$

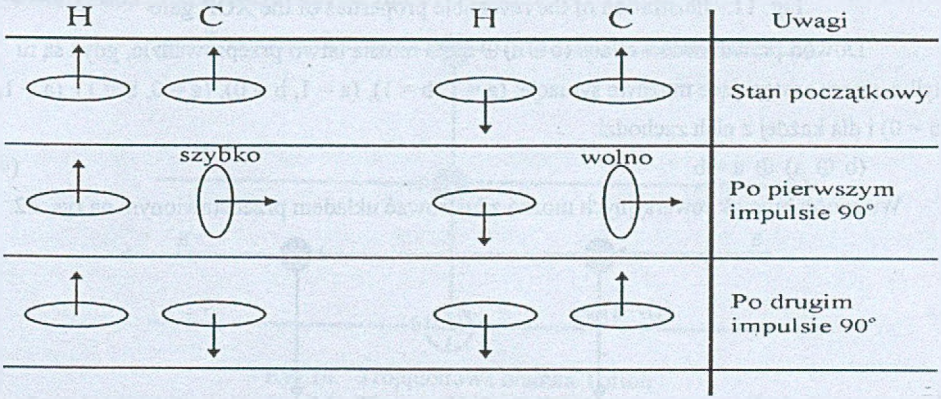
i podobnie dla węgla:

$$b = \begin{cases} 1, \text{ jeżeli stan spinu jest równoległy} \\ 0, \text{ jeżeli stan spinu jest antyrównoległy} \end{cases}$$

W związku z tym b_1, stan spinu węgla C po dwóch kolejnych 90° impulsach elektromagnetycznych, można zapisać w następujący sposób:

$$b_1 = b \oplus a \tag{3}$$

gdzie symbol $\oplus$ oznacza sumę modulo dwa.

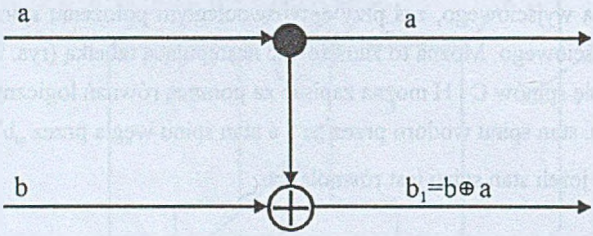


Rys.9. Zależność między spinami wodoru H i węgla C w molekule chloroformu w reakcji na dwa kolejne zewnętrzne impulsy

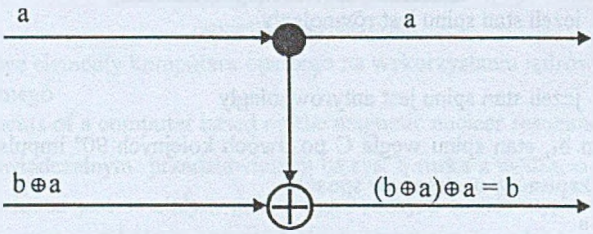
Fig. 9. Relations between spins of hydrogen H and carbon C in chloroform molecule as the reaction for two successive external impulses

Równanie (3) jest równaniem tak zwanej bramki logicznej XOR, oznaczanej również CNOT (tak zwana kontrolowana negacja), którą można zilustrować schematem przedstawionym na rys. 10.

Przedstawiona na rys.10. bramka XOR ma własności rewersyjne, to znaczy, że gdy na jej wejściu wprowadzimy zmienne wyjściowe, to na wyjściu otrzymamy poprzednie wejścia, tak jak to ilustruje rys. 11.



Rys.10. Oznaczenie bramki XOR
Fig. 10. Notation of the XOR gate

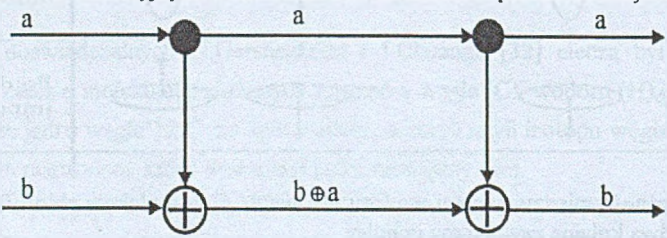


Rys.11. Ilustracja rewersyjnych własności bramki XOR
Fig. 11. Illustration of the reversible properties of the XOR gate

Dowód prawdziwości relacji $(b \oplus a) \oplus a = b$ można łatwo przeprowadzić, gdyż są tu tylko cztery następujące możliwe sytuacje: $(a = 1, b = 1)$, $(a = 1, b = 0)$, $(a = 0, b = 1)$, $(a = 1, b = 0)$ i dla każdej z nich zachodzi:

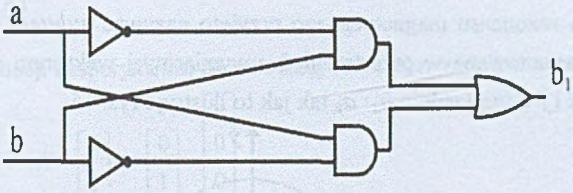
$$(b \oplus a) \oplus a = b \tag{4}$$

Własności bramek rewersyjnych można zilustrować układem przedstawionym na rys. 12.



Rys.12. Łańcuchowe połączenie dwóch bramek o własnościach rewersyjnych
Fig. 12. Chain connection of two gates with reversible properties

Bramka XOR może być zrealizowana nie tylko przy wykorzystaniu zjawisk jądrowego rezonansu magnetycznego, czyli w sposób kwantowy, ale również w sposób klasyczny, tak jak to ilustruje rys.13.



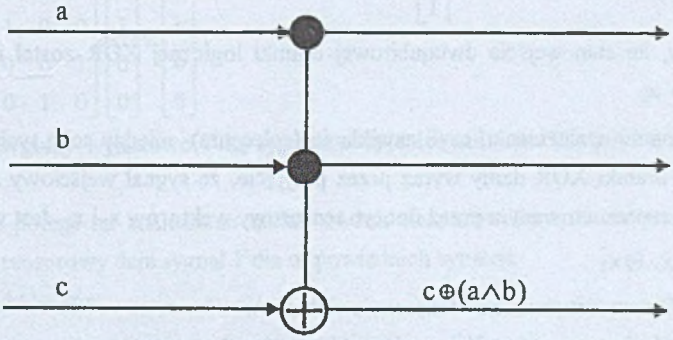
Rys.13. Bramka XOR w realizacji klasycznej
Fig. 13. XOR gate in classical realization

Porównując dwa rozwiązania bramki XOR, a więc kwantowe przedstawione na rys.10 i klasyczne przedstawione na rys. 13 możemy powiedzieć, że:

- w rozwiązaniu klasycznym potrzebne do zrealizowania takiej bramki operacje rozmieszcza się w przestrzeni, a przepływ do nich odpowiednich zmiennych binarnych realizuje się poprzez przeprowadzone przewody (ścieżki prowadzące),
- w rozwiązaniu kwantowym potrzebne do zrealizowania takiej bramki operacje rozmieszcza się w czasie i realizuje się przez kolejne impulsy o odpowiednich częstotliwościach i czasach trwania.

Stąd program w przypadku komputerów kwantowych jest realizowany poprzez oddziaływanie na układ czasowym ciągiem impulsów zmiennego pola elektromagnetycznego.

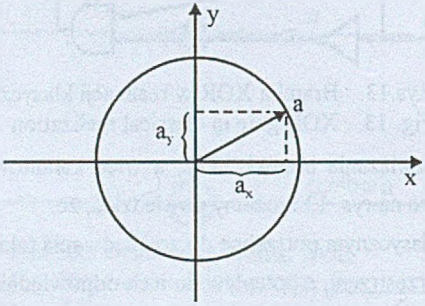
W literaturze można spotkać propozycje różnych bramek, np. w [27] – trójqubitową bramkę Toffoli przedstawioną na rys. 14.



Rys.14. Trójqubitowa bramka Toffoli
Fig. 14. Three-qubit Toffoli gate

3. Własności kwantowej bramki logicznej XOR w zapisie analitycznym

Elementarna jednostka obliczeniowa, którą w przypadku obliczeń wykorzystujących metody jądrowego rezonansu magnetycznego przyjęto nazywać q*ubitem,* może być w prostym przypadku reprezentowana w przestrzeni dwuwymiarowej wektorem a o długości 1 i składowych na osi x i y odpowiednio a_x: a_y, tak jak to ilustruje rys. 15.



Rys.15. Ilustracja qubitu w przestrzeni dwuwymiarowej
Fig. 15. Illustration of the qubit in two-dimensional space

Jest więc $a = \begin{bmatrix} a_x \\ a_y \end{bmatrix}$ w szczególnych przypadkach:

gdy $a_x = 1$ $\quad a = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

gdy $a_y = 1$ $\quad a = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Załóżmy, że stan wejścia dwuqubitowej bramki logicznej XOR został określony przez wektory x_1 i x_2.

Wzajemnemu uzależnieniu, czyli zawikłaniu (spleceniu) między sobą tych dwóch stanów w działaniu bramki XOR damy wyraz przez przyjęcie, że sygnał wejściowy X jest sygnałem splecionym, reprezentowanym przez iloczyn tensorowy wektorów x_1 i x_2. Jest więc:

$$X = x_1 \otimes x_2 \tag{5}$$

gdzie: $\otimes$ oznacza mnożenie tensorowe wektorów.

Wtedy spleciony sygnał wyjściowy bramki jest określony przez wzór:

$$Y = U \cdot X \tag{6}$$

gdzie: U – tak zwana macierz unitarna, która w przypadku dwuwejściowej bramki XOR ma postać:

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{7}$$

Dla dwóch sytuacji eksperymentu zilustrowanych na rys. 9 będzie więc odpowiednio:

Sytuacja 1: $$X = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \tag{8}$$

Sytuacja 2: $$X = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{9}$$

a stąd

dla Sytuacji 1:

$$Y = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \tag{10}$$

a dla Sytuacji 2:

$$Y = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{11}$$

Otrzymane sygnały wyjściowe Y są sygnałami splecionymi (zawikłanymi) z sygnałów y_1 oraz y_2.

Rozwikłanie polega na znalezieniu takich dwóch wektorów dwuelementowych y_1 i y_2, których iloczyn tensorowy daje sygnał Y dla odpowiednich sytuacji.

Zauważmy, że będzie:

dla Sytuacji 1:

$$y_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{i} \quad y_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{12}$$

$$\text{bo} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \tag{13}$$

a dla Sytuacji 2:

$$y_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{i} \quad y_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{14}$$

$$\text{bo} \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{15}$$

a więc wyniki zgodne z wynikami podanymi na rys. 9.

Rozpatrywana w tym rozdziale bramka kwantowa XOR ma własności rewersyjne.

Zauważmy, że w takim przypadku iloczyn dwóch macierzy unitarnych jest równy macierzy jednostkowej.

Jest bowiem:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{16}$$

Jest to matematyczna ilustracja własności łańcuchowego połączenia dwóch bramek o własnościach rewersyjnych, przedstawionego na rys. 12.

4. Matematyczne podstawy informatyki kwantowej

4.1. Qubity

Podstawy teoretyczne informatyki kwantowej wynikają bezpośrednio z podstawowych zasad nierelatywistycznej mechaniki kwantowej. W klasycznej informatyce pojedynczy bit może przyjmować tylko dwie ustalone wartości logiczne, to znaczy 0 lub 1. Natomiast elementarną jednostką kwantowej informacji jest kwantowy bit, w skrócie zwany qubitem, który w ogólnym przypadku może być traktowany jako element zespolonej przestrzeni Hilberta H^2. Dwa

ortogonalne stany pojedynczego qubitu mają postać $\{|0\rangle,|1\rangle\}$ i tworzą one bazę ortogonalną $\left\{\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right\}$ przestrzeni H.

Tak więc dowolny qubit $|\psi\rangle\in H^2$ może być przedstawiony w postaci liniowej kombinacji wektorów bazowych $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$, gdzie liczby zespolone α oraz β nazywane są amplitudami stanu, a wektor $|\psi\rangle$ jest znormalizowany, to znaczy $|\alpha|^2+|\beta|^2=1$ [1, 4, 5]. Oznacza to, że qubit $|\psi\rangle\in H^2$ przyjmuje wartość logiczną 0 z prawdopodobieństwem $|\alpha|^2$ oraz wartość logiczną 1 z prawdopodobieństwem $|\beta|^2$.

Stosowane tutaj oznaczenia są zaczerpnięte bezpośrednio z terminologii stosowanej w mechanice kwantowej. Wektory bazowe $|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}\in H^2$ oraz $|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}\in H^2$ reprezentują odpowiednio wartości logiczne 0 oraz 1 klasycznego bitu. Zatem pojedynczy qubit jest superpozycją tych dwóch wartości logicznych.

W przypadku klasycznego bitu pomiar jego aktualnej wartości logicznej, która może być tylko 0 lub 1, nie nastręcza żadnych trudnosci. Natomiast inaczej jest w przypadku kwantowego qubitu. Pomiar jego aktualnej wartości może zniszczyć fizykalną strukturę qubitu. Podczas pomiaru wartości qubitu dokonuje się ortogonalnej projekcji wektora $|\psi\rangle\in H^2$ na wektory bazowe $|0\rangle\in H^2$ oraz $|1\rangle\in H^2$.

Fundamentalną zasadą mechaniki kwantowej jest to, że przestrzenią stanów kwantowych dla dwóch qubitów jest iloczyn tensorowy przestrzeni stanów kwantowych dla pojedynczych qubitów. Zatem w przypadku dwóch qubitów jest to 4-wymiarowa zespolona przestrzeń Hilberta $H^4=H^2\otimes H^2$. Elementami tej przestrzeni są wszystkie możliwe superpozycje stanów kwantowych reprezentowane iloczynami tensorowymi odpowiednich wektorów.

Ogólnie, kwantowy układ złożony z n qubitów można rozpatrywać jako element 2^n –wymiarowej zespolonej przestrzeni Hilberta H^{2^n} będącej iloczynem tensorowym n przestrzeni H^2, czyli:

$$H^{2^n}=\underbrace{H^2\otimes H^2\otimes\ldots\otimes H^2}_{n-razy}$$

Zatem przestrzeń stanów dla n qubitów posiada 2^n wzajemnie ortogonalnych stanów postaci $\{|i\rangle\}$, gdzie i jest n-bitową liczbą binarną, $i=0,1,2,\ldots,2^n-1$. Ponadto, wektory 2^n-elementowe:

$$|i\rangle=[\underbrace{0,0,\ldots,0,1}_{i-razy},\ \underbrace{0,0,\ldots,0}_{(2^n-i-1)-razy}]^T\in H^{2^n}$$

tworzą bazę ortogonalną w zespolonej przestrzeni Hilberta H^{2^n}. Elementami tej przestrzeni są wszystkie możliwe superpozycje stanów kwantowych reprezentowane iloczynami tensoro-

wymi odpowiednich wektorów. Ponieważ wszystkie stany kwantowe są niezmiennicze względem mnożenia przez dowolny skalar, więc bez utraty ogólności odpowiadające im wektory mogą być znormalizowane o normie 1.

Zatem układ n qubitów jest znormalizowanym wektorem $|\psi\rangle$ w przestrzeni H^{2^n}, który może być przedstawiony w postaci liniowej kombinacji 2^n ortonormalnych wektorów bazowych $|0\rangle$, $|1\rangle$, $|2\rangle$,..., $|i\rangle$,..., $|2^n-1\rangle$. Stąd:

$$|\psi\rangle = \sum_{i=0}^{i=2^n-1} \alpha_i |i\rangle \text{ , gdzie } \sum_{i=0}^{i=2^n-1} |\alpha_i|^2 = 1$$

Przykładowo, dla układu kwantowego złożonego z dwóch qubitów cztery wektory bazowe wzajemnie ortonormalne $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ w zespolonej przestrzeni Hilberta H^4 mają następującą postać:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \in H^4$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \in H^4$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \in H^4$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \in H^4$$

Iloczyn tensorowy dwóch dowolnych qubitów postaci $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \in H^2$ oraz $|\phi\rangle=\gamma|0\rangle+\delta|1\rangle \in H^2$, będący wektorem w zespolonej przestrzeni Hilberta H^4, dany jest następującym wzorem:

$$|\psi\phi\rangle = |\psi\rangle \otimes |\phi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle = \begin{bmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{bmatrix} \in H^4$$

Natomiast dla układu złożonego z trzech qubitów bazowe stany wzajemnie ortonormalne w zespolonej przestrzeni Hilberta H^8 mają postać $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$.

Przykładowo, bazowy stan kwantowy $|010\rangle$ jest reprezentowany w przestrzeni Hilberta H^8 następującym wektorem 8-elementowym:

$$|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \in H^8$$

W podobny sposób można przedstawić pozostałe ortonormalne wektory bazowe w zespolonej przestrzeni Hilberta H^8.

4.2. Bramki kwantowe

Podstawowe operacje wykonywane na pojedynczym qubicie, nazywane kwantowymi bramkami logicznymi, reprezentowane są 2×2 -wymiarowymi macierzami unitarnymi U będącymi liniowymi bijekcjami w zespolonej przestrzeni Hilberta H^2. Macierze unitarne spełniają następującą podstawową równość: $U^{-1} = U^*$, gdzie U^* oznacza transponowaną macierz sprzężoną. Ponadto, macierze te reprezentują w zespolonej przestrzeni Hilberta H^2 obroty wokół początku układu współrzędnych, które nie zmieniają długości wektorów. Zatem, dla pojedynczego qubitu teoretycznie istnieje nieskończenie wiele różnych kwantowych bramek logicznych, odpowiadających poszczególnym macierzom unitarnym U realizujących zadaną kwantową operację matematyczną [1, 28, 29, 31].

W praktyce wystarczy jednak posługiwać się kilkoma odpowiednio wybranymi podstawowymi kwantowymi bramkami logicznymi, którym odpowiadają pewne macierze unitarne. Ponieważ macierze U reprezentujące poszczególne operacje kwantowe są macierzami unitarnymi, a więc z definicji są one odwracalne, a zatem odpowiadające im operacje kwantowe są operacjami rewersyjnymi.

Należy zaznaczyć, że w przypadku klasycznej algebry Boole'a w odniesieniu do jednego bitu istnieją tylko dwie operacje logiczne, to znaczy identyczność I oraz negacja NOT. W układach kwantowych operacje te są reprezentowane odpowiednio następującymi macierzami unitarnymi:

$$U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{dla operacji identyczności } I\text{, oraz}$$

$$U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{dla operacji negacji NOT.}$$

Przykładowo, działanie bramki NOT dla ortogonalnych wektorów bazowych $|0\rangle \in H^2$ oraz $|1\rangle \in H^2$ można przedstawić następująco: $|0\rangle \to |1\rangle$ oraz $|1\rangle \to |0\rangle$. Ogólnie, działanie bramki NOT dla dowolnego znormalizowanego stanu kwantowego $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in H^2$, reprezentowanego wektorem o współczynnikach zespolonych α, β, można przedstawić następująco:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \to \alpha|1\rangle + \beta|0\rangle = |\neg\psi\rangle$$

gdzie symbol $\neg$ oznacza negację.

Biorąc pod uwagę postać macierzy unitarnej U reprezentującej operację negacji oraz stosując zapis wektorowy, otrzymuje się następującą zależność:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

Do podstawowych operacji kwantowych wykonywanych na jednym qubicie, oprócz opisanych powyżej operacji identyczności I oraz operacji negacji NOT, należy także operacja realizowana przez tak zwaną bramkę Hadamarda i oznaczoną w skrócie symbolem H. Bramka kwantowa Hadamarda jest reprezentowana następującą macierzą unitarną o wymiarach 2×2:

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

Przykładowo, działanie bramki Hadamarda H dla ortogonalnych wektorów bazowych $|0\rangle \in H^2$ oraz $|1\rangle \in H^2$ można przedstawić następująco: $|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \in H^2$ oraz $|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \in H^2$.

Ogólnie, działanie bramki Hadamarda H dla dowolnego znormalizowanego stanu kwantowego $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in H^2$ reprezentowanego wektorem o współczynnikach zespolonych α, β, można przedstawić następująco:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \to \frac{1}{\sqrt{2}}(\alpha + \beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha - \beta)|1\rangle$$

Biorąc pod uwagę specyficzną postać macierzy unitarnej U reprezentującej kwantową bramkę Hadamarda oraz stosując zapis wektorowy, otrzymuje się następującą zależność:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}}\alpha + \frac{1}{\sqrt{2}}\beta \\ \frac{1}{\sqrt{2}}\alpha - \frac{1}{\sqrt{2}}\beta \end{bmatrix}$$

W przypadku układu kwantowego złożonego z dwóch qubitów podstawowe operacje reprezentowane są macierzami unitarnymi o wymiarach 4×4. W tym przypadku spośród wszystkich możliwych podstawowych operacji wykonywanych na parze qubitów w przestrzeni H^4 szczególne znaczenie ma operacja, której działanie można matematycznie przedstawić jako $|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U$, gdzie symbol $\otimes$ oznacza iloczyn tensorowy, I jest operacją identycznościową na pojedynczym qubicie oraz U jest dowolną operacją na pojedynczym qubicie reprezentowaną przez unitarną macierz U o wymiarach 2×2. Operacja ta nosi nazwę "sterowalnej bramki U", gdyż operacja wykonywana na drugim qubicie zależy od tego, czy pierwszy qubit jest w stanie kwantowym $|0\rangle\in H^2$, czy też w stanie kwantowym $|1\rangle\in H^2$.

W szczególnym przypadku, gdy macierz unitarna U jest macierzą odpowiadającą operacji negacji NOT, uzyskuje się bramkę kwantową o nazwie *sterowalna negacja,* oznaczaną symbolem CNOT (ang. *controlled NOT*). Przykładowo, działanie 2-qubitowej bramki kwantowej CNOT dla czterech ortonormalnych wektorów bazowych $|00\rangle\in H^4$, $|01\rangle\in H^4$, $|10\rangle\in H^4$, $|11\rangle\in H^4$ można przedstawić następująco:

$$|00\rangle\to|00\rangle,\ |01\rangle\to|01\rangle,\ |10\rangle\to|11\rangle,\ |11\rangle\to|10\rangle$$

Ogólnie, działanie 2-qubitowej bramki CNOT dla dowolnego znormalizowanego stanu kwantowego

$$|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle\in H^4$$

reprezentowanego wektorem odpowiednio o współczynnikach zespolonych $\alpha,\beta,\gamma,\delta$, można przedstawić następująco:

$$|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \to \alpha|00\rangle + \beta|01\rangle + \delta|10\rangle + \gamma|11\rangle$$

Zatem macierz unitarna U o wymiarach 4×4, odpowiadajaca operacji CNOT jest postaci następującej:

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

Biorąc pod uwagę specyficzną postać macierzy unitarnej U reprezentującej kwantową bramkę CNOT oraz stosując zapis wektorowy, otrzymuje się następującą zależność:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \delta \\ \gamma \end{bmatrix}$$

Elementarne operacje można również zdefiniować dla dowolnej liczby qubitów, powiększając odpowiednio wymiary unitarnych macierzy U reprezentujących poszczególne operacje kwantowe. W przypadku układu kwantowego zawierającego n qubitów będą to unitarne macierze o wymiarach $2^n \times 2^n$. Macierze te zatem zawierają tyle wierszy oraz tyle kolumn, ile jest wzajemnie ortogonalnych stanów kwantowych w 2^n -wymiarowej zespolonej przestrzeni Hilberta.

Należy wyraźnie podkreślić, że w odróżnieniu od klasycznego nierewersyjnego boolowskiego funktora logicznego o n wejściach posiadającego jedno wyjście, kwantowa bramka logiczna o n wejściach jest elementem rewersyjnym, posiadającym n wyjść. Zatem kwantowa bramka logiczna w przypadku podania na jej wejście stanów kwantowych odpowiadających wartościom logicznym 0 lub 1 może realizować jednocześnie n funkcji logicznych n-argumentowych.

Podobnie jak w przypadku jednego qubitu, także w przypadku układu n qubitów teoretycznie istnieje nieskończenie wiele różnych kwantowych bramek logicznych reprezentowanych odpowiednio macierzami unitarnymi o wymiarach $2^n \times 2^n$. Niemniej podstawową kwatową bramką logiczną dla układu kwantowego zawierającego n qubitów jest tak zwana bramka Toffoli reprezentowana następującą macierzą unitarną o wymiarach $2^n \times 2^n$:

$$U = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & \dots & 0 & 1 & 0 \end{bmatrix}$$

Niech $x_1, x_2, \dots, x_k, \dots, x_n$ oznacza n wejść, natomiast $y_1, y_2, \dots, y_k, \dots, y_n$ odpowiednio n wyjść bramki Toffoli, wówczas: $y_k = x_k$ dla $k=1,2,\dots, n-1$, oraz

$$y_n = (x_1 \wedge x_2 \wedge \dots \wedge x_k \wedge \dots \wedge x_{n-1}) \oplus x_n$$

Zatem w przypadku n=2 bramka Toffoli dla dowolnych wektorów bazowych realizuje na drugim wyjściu znaną klasyczną funkcję logiczną dwóch zmiennych "suma modulo dwa" $x_1 \oplus x_2$, zwaną inaczej *kontrolowaną negacją* CNOT lub w skrócie bramka XOR.

W przypadku gdy $x_n = 1$, wówczas wyjście y_n zachowuje się. jak klasyczny funktor logiczny NAND. Natomiast w przypadku, gdy $x_n = 0$, wówczas wyjście y_n reprezentuje funktor lo-

giczny AND. Zatem n-wejściowa kwantowa bramka logiczna Toffoli jest bramką uniwersalną, za pomocą której można zrealizować dowolną n-argumentową funkcję logiczną. Szczególnym przypadkiem bramki Toffoli dla $n = 2$ jest, jak wspomniano uprzednio, bramka sterowalnej negacji CNOT.

Uogólnieniem bramki Toffoli jest kwantowa bramka oznaczona symbolem U_D, której działanie reprezentuje macierz unitarna o wymiarach $2^n \times 2^n$:

$$U_D = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & u_{11} & u_{12} \\ 0 & 0 & \dots & 0 & u_{21} & u_{22} \end{bmatrix}$$

gdzie liczby zespolone u_{ij}, $i,j=1,2$ tworzą macierz unitarną o wymiarach 2×2, reprezentującą wybraną kwantową bramkę logiczną dla jednego qubitu. Przykładowo, mogą to być macierze o następującej postaci:

$$F = \begin{bmatrix} e^{i\pi/4}\cos(\pi/8) & e^{i\pi/4}\sin(\pi/8) \\ -e^{-i\pi/4}\sin(\pi/8) & e^{-i\pi/4}\cos(\pi/8) \end{bmatrix}$$

$$G = \begin{bmatrix} \cos(\pi/8) & -\sin(\pi/8) \\ \sin(\pi/8) & \cos(\pi/8) \end{bmatrix}$$

$$H = \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

$$J = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix}$$

Każda z przedstawionych macierzy unitarnych reprezentuje obrót o pewien ustalony kąt wokół początku układu współrzędnych w zespolonej przestrzeni Hilberta H^2. Ogólnie, dowolny obrót (rotacja) w przestrzeni H^2 może być przedstawiony za pomocą następującej macierzy unitarnej o wymiarach 2×2:

$$V(\theta,\phi) = \begin{bmatrix} \cos(\theta/2) & -ie^{-i\phi}\sin(\theta/2) \\ -ie^{i\phi}\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$

Działanie ciągu kolejnych n-qubitowych operacji kwantowych można przedstawić w postaci iloczynu macierzy unitarnych odpowiadających poszczególnym operacjom lub - podobnie jak w klasycznej teorii automatów - w postaci schematu połączeń.

Ilustracją powyższych rozważań teoretycznych niech będą dwa poniższe proste przykłady liczbowe. Rozpatrzmy efekt działania bramki kwantowej U_H reprezentowanej macierzą:

$$U_H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 0 & 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$$

Załóżmy, że stan kwantowy $|\psi\rangle \in H^4$ jest superpozycją stanów kwantowych $|10\rangle \in H^4$ oraz $|11\rangle \in H^4$ o postaci:

$$|\psi\rangle = 1/\sqrt{2}\left(|10\rangle + |11\rangle\right) = 1/\sqrt{2}\left(|1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right) =$$

$$= 1/\sqrt{2}\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) =$$

$$= 1/\sqrt{2}\left(\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}\right) = 1/\sqrt{2}\begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \in H^4$$

Działanie bramki kwantowej U_H na stan kwantowy $|\psi\rangle \in H^4$ odpowiada wykonaniu mnożenia:

$$U_H|\psi\rangle = 1/\sqrt{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 0 & 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}\begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle \in H^4$$

Rozpatrzmy teraz działanie tej samej bramki kwantowej U_H, lecz tym razem na inny stan kwantowy $|\Phi\rangle \in H^4$, który jest superpozycją stanów kwantowych $|10\rangle \in H^4$ oraz $|11\rangle \in H^4$ o postaci:

$$|\psi\rangle = 1/\sqrt{2}\left(|10\rangle - |11\rangle\right) = 1/\sqrt{2}\left(|1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle\right) =$$

$$= 1/\sqrt{2}\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) =$$

$$= 1/\sqrt{2}\left(\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}\right) = 1/\sqrt{2}\begin{bmatrix} 0 \\ 0 \\ 1 \\ -1 \end{bmatrix} \in H^4$$

Działanie bramki kwantowej U_H na stan kwantowy $|\Phi\rangle \in H^4$ odpowiada wykonaniu mnożenia:

$$U_B|\phi\rangle = 1/\sqrt{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 0 & 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}\begin{bmatrix} 0 \\ 0 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle \in H^4$$

Powyższe dwa przykłady ilustrują bardzo istotny dla konstrukcji algorytmów obliczeń kwantowych efekt redukcji pewnych stanów kwantowych w wyniku wykonywania operacji kwantowych reprezentowanych bramkami kwantowymi.

Istotnym pojęciem związanym z dowolnym układem n qubitów jest tak zwane zawikłanie (ang. *entanglement*) [2,13, 22]. Zawikłanie zwane również splątaniem jest bezpośrednim efektem wykonania iloczynu tensorowego na 2-wymiarowych wektorach reprezentujących poszczególne qubity. Ze znanych własności iloczynu tensorowego wynika, że na podstawie znajomości wektora będącego iloczynem tensorowym dwóch lub więcej wektorów nie można, poza szczególnymi przypadkami (ortonormalne wektory bazowe), jednoznacznie wyznaczyć wektorów stanowiących czynniki tego iloczynu tensorowego.

Zawikłanie oznacza zatem, że dany stan kwantowy $|\psi\rangle \in H^{2^n}$ nie może być przedstawiony jednoznacznie w postaci iloczynu tensorowego n stanów kwantowych $|\psi_i\rangle \in H^2$, $i=1,2,\ldots,n$. Oznacza to, że między poszczególnymi stanami kwantowymi $|\psi_i\rangle$ istnieją wzajemne korelacje. Przykładowo, niech:

$$|\psi\rangle = 1/\sqrt{2}\left(|01\rangle - |10\rangle\right) \in H^4$$

Wektor ten reprezentuje stan kwantowy będący wynikiem zawikłania, gdyż nie można znaleźć dwóch stanów kwantowych $|\psi_1\rangle \in H^2$ oraz $|\psi_2\rangle \in H^2$, takich że:

$$|\psi\rangle = |\psi_2\rangle \otimes |\psi_2\rangle.$$

Pojęcie zawikłania wiąże się bezpośrednio z tak zwaną bazą ortogonalną Bella, którą w zespolonej przestrzeni Hilberta H^4 tworzą następujące cztery wzajemnie ortogonalne wektory bazowe:

$$|00\rangle+|11\rangle \in H^4, |00\rangle-|11\rangle \in H^4, |01\rangle+|10\rangle \in H^4, |01\rangle-|10 \in H^4.$$

Dowolny układ kwantowy złożony z dwóch qubitów jest zawikłany poprzez pewną macierz unitarną o wymiarach 4×4. Można dowieść, że zawikłanie układu kwantowego złożonego z trzech lub ogólnie z większej liczby qubitów może być zawsze rozpatrywane jako superpozycja zawikłań układów kwantowych złożonych z dwóch qubitów.

Kwantowa bramka logiczna oddziałująca na cały układ n qubitów może być przedstawiona jako macierz unitarna o wymiarach $2^n \times 2^n$, będąca iloczynem tensorowym macierzy unitarnych o wymiarach 4×4. Macierz ta zawiera podmacierz jednostkową o wymiarach $2^{n-2} \times 2^{n-2}$.

Informacje dotyczące kwantowych bramek logicznych zamieszczone są także w pracach [40, 42, 46, 60].

4.3. Kwantowa teleportacja

Kwantowa teleportacja związana jest z przesyłem wektorów odpowiadających układom n qubitów. Załóżmy, że dany wektor jest superpozycją dwóch wektorów składowych, to znaczy powstał w wyniku wykonania iloczynu tensorowego na dwóch wektorach składowych. Nadawca oraz odbiorca informacji znają jeden ze składowych wektorów. W procesie teleportacji nadawca przesyła jedynie drugi ze składników iloczynu tensorowego ten, który nie jest znany odbiorcy. Odbiorca informacji dokonuje superpozycji obu wektorów, to znaczy wyznacza iloczyn tensorowy tych wektorów, otrzymując w efekcie cały wektor. Zatem, w kwantowej teleportacji źródłem informacji jest zjawisko zawikłania.

Zjawisko kwantowej teleportacji przedstawimy na następującym przykładzie. Załóżmy, że nadawca oraz odbiorca informacji dysponują tym samym wektorem odpowiadającym stanowi kwantowemu $|\psi\rangle = |00\rangle + |11\rangle \in H^4$. Wektor ten jest superpozycją, czyli iloczynem tensorowym dwóch wektorów odpowiadających dwom pojedynczym qubitom. Nadawca informacji chce przesłać do odbiorcy informację zawartą w pojedynczym qubicie będącym w stanie kwantowym $|\phi\rangle = a|0\rangle + b|1\rangle \in H^2$, gdzie a oraz b są dowolnymi zespolonymi współczynnikami. Nadawca informacji dysponuje stanem początkowym $|\varphi\rangle = |\psi\rangle \otimes |\phi\rangle \in H^8$, który jest superpozycją trzech qubitów, to znaczy iloczynem tensorowym wektorów $|\psi\rangle$ oraz $|\phi\rangle$ o postaci następującej:

$$|\varphi\rangle = |\psi\rangle \otimes |\phi\rangle = (|00\rangle + |11\rangle) \otimes (a|0\rangle + b|1\rangle) =$$

$$= a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle$$

Nadawca informacji dokonuje pomiaru w bazie ortogonalnej Bella dwóch qubitów, a mianowicie, qubitu $|\phi\rangle$ oraz jednego qubitu występującego w stanie kwantowym $|\psi\rangle$, wykorzystując w tym celu bramki kontrolowanej negacji CNOT oraz bramki Hadamarda H. Następnie dwa qubity są mierzone i przesyłane do odbiorcy informacji, który za pomocą takich samych bramek kwantowych przetwarza je uzyskując w efekcie qubit $|\phi\rangle$. Zjawisko teleportacji kwantowej jest szczególnie użyteczne w przypadku przesyłania informacji w obecności zewnętrznych zakłóceń. Informacje dotyczące teleportacji kwantowej zamieszczone są w pracach [12, 14, 15,16].

5. Perspektywiczny uniwersalny komputer kwantowy

Perspektywiczny uniwersalny komputer kwantowy przedstawiony ogólnie na rys.8 powinien umożliwić analizę i przetwarzanie informacji kwantowej zawartej w układach qubitów. Formalnie kwantowy komputer jest układem n qubitów, na których można przeprowadzać odpowiednie operacje kwantowe reprezentowane bramkami kwantowymi lub macierzami unitarnymi odpowiednich wymiarów. Teoretyczne podstawy działania komputera kwantowego oparte są na następujących ogólnych zasadach [6, 20, 23, 39, 45, 54, 59]:

1. Każdy pojedynczy qubit może być przedstawiony za pomocą znanego stanu zmierzonego w bazie ortonormalnej $\{|0\rangle,|1\rangle\}$.
2. Każda uniwersalna bramka kwantowa o odpowiedniej liczbie wejść, reprezentowana macierzą unitarną, może być użyta do przetworzenia dowolnego ustalonego podzbioru qubitów.
3. Qubity mogą być przetwarzane jedynie za pomocą uniwersalnych bramek kwantowych.

Z powyższych ogólnych zasad działania komputera kwantowego wynika, że jego modelem matematycznym jest model sieciowy, w którym ciąg kwantowych uniwersalnych bramek logicznych przetwarza pewne podzbiory n-elementowego zbioru qubitów. Bez utraty ogólności można założyć, że początkowy stan kwantowy n-elementowego zbioru qubitów odpowiada wektorowi bazowemu $|0,0,0,\ldots,0\rangle \in H^{2^n}$, który następnie jest sekwencyjnie przetwarzany przez dowolny ciąg uniwersalnych kwantowych bramek logicznych.

Ogólnie można też przyjąć, że początkowy stan n-elementowego zbioru qubitów odpowiada pewnemu wektorowi bazowemu o postaci $|1,1,\ldots,1,0,0,\ldots,0\rangle \in H^{2^n}$, to znaczy, że początkowy wektor bazowy zawiera jedynki na k pierwszych pozycjach oraz zera na $(n-k)$ ostatnich pozycjach.

W wyniku działania ciągu odpowiednio dobranych kwantowych bramek logicznych na początkowy stan kwantowy otrzymuje się w efekcie n-qubitowy końcowy stan kwantowy $W \in H^{2^n}$, który jest wektorem o normie 1 w 2^n -wymiarowej zespolonej przestrzeni Hilberta. Wektor $W = \sum_s \alpha_s v_s$, gdzie indeks s przebiega zbiór wszystkich możliwych 2^n -wymiarowych stanów bazowych, $v_s \in H^{2^n}$ jest 2^n -wymiarowym wektorem bazowym, współczynniki $\alpha_s \in C$, oraz $\sum_s |\alpha_s|^2 = 1$. Każda kwantowa bramka logiczna reprezentowana jest odpowiednią macierzą unitarną, a cały proces obliczeniowy można przedstawić za pomocą jednej macierzy unitarnej będącej iloczynem poszczególnych macierzy składowych.

Współczynniki zespolone α_s noszą nazwę *amplitud prawdopodobieństwa*, natomiast wektor W jest kombinacją liniową wektorów bazowych V_s. Projekcja ortogonalna wektora W na wektor V_s zachodzi z prawdopodobieństwem $|\alpha_s|^2$. Po wykonaniu wszystkich kwantowych operacji przeprowadza się pomiar końcowego stanu kwantowego reprezentowanego wektorem $W \in H^{2^n}$, natomiast nie dokonuje się pomiarów pośrednich wyników obliczeń kwantowych.

Należy wyraźnie zaznaczyć, że kwantowe obliczenia mają charakter probabilistyczny, gdyż mimo deterministycznego działania poszczególnych bramek kwantowych końcowy pomiar wektora W daje nam informacje probabilistyczne.

Należy zaznaczyć, że w trakcie wykonywania operacji za pomocą bramek kwantowych najczęściej dochodzi do zawikłania wynikowego wektora W. Jest to istotna cecha operacji kwantowych.

Informacje dotyczące ogólnej struktury komputerów kwantowych oraz obliczeń kwantowych zamieszczone są w pracach [3, 11, 24, 25, 26, 27, 32, 39, 44, 47, 52, 57, 58]. Natomiast szeroko rozumiane zagadnienia kodowania informacji kwantowej poruszane są między innymi w następujących pracach: [8, 9, 16, 17, 18, 19, 21, 25, 29, 30, 31, 35, 36, 37, 40, 42, 48, 49, 53, 55, 56].

6. Algorytmy kwantowe

W niniejszym rozdziale przedstawimy dwa wybrane algorytmy kwantowe: algorytm poszukiwań Grovera oraz algorytm faktoryzacji Shora. Omówimy też dyskretną transformację Fouriera.

6.1. Algorytm poszukiwań Grovera

W roku 1997 Grover zaproponował [34, 35] kwantowy algorytm wyszukiwania informacji w dużych zbiorach danych. Problem polega na wyszukaniu w nieuporządkowanym zbiorze danych $\{x_i, i=1,2,3,...,N\}$ określonego elementu $x_j=v$. Przykładowo, może to być wyszukanie w spisie telefonów danego numeru telefonu, nie znając nazwiska abonenta.

Klasyczne algorytmy poszukiwań potrzebują średnio $N/2$ kroków na wyszukanie danej informacji w zbiorze danych zawierającym N elementów. Algorytm kwantowy poszukiwań zaproponowany przez Grovera jest w tym przypadku znacznie bardziej efektywny i potrzebuje na wyszukanie właściwego elementu średnio jedynie $\sqrt{N}$ kroków.

O ogromnej efektywności algorytmu poszukiwań Grovera najlepiej świadczy następujący przykład. W zagadnieniach klasycznej kryptografii przy dekodowaniu nieznanych szyfrów występuje konieczność wyszukiwania zadanych elementów w zbiorze zawierającym około $N=10^{16}$ nieuporządkowanych elementów. Najszybszy z istniejących klasycznych komputerów wykonałby taką czynność w czasie około tysiąca lat. Natomiast komputer kwantowy wykorzystujący wspomniany powyżej algorytm poszukiwań Grovera wyznaczyłby poszukiwany element zbioru w ciągu około czterech minut.

Algorytm Grovera może być uogólniony i zastosowany do jednoczesnego poszukiwania kilku wybranych elementów w nieuporządkowanym zbiorze danych, oraz do wyszukiwania największego lub najmniejszego elementu w zbiorze danych.

6.2. Algorytm faktoryzacji Shora

W roku 1993 Shor zaproponował [10, 30, 41, 46, 49, 50, 51, 52] kwantowy algorytm umożliwiający faktoryzację liczb naturalnych o wielomianowej złożoności obliczeniowej. Jest to najważniejszy algorytm kwantowej informatyki, umożliwiający znaczne przyspieszenie wielu procesów obliczeniowych. Podstawą tego algorytmu jest fakt, że problem faktoryzacji jest równoważny wyznaczaniu okresów pewnej funkcji okresowej. Niech N będzie dowolną liczbą naturalną. Należy wyznaczyć jej rozkład na czynniki pierwsze $N=pq$. Zagadnienie to redukuje się do wyznaczania okresu następującej funkcji $f_{a,N}(x) = a^x \bmod N$, gdzie a jest przypadkowo wybraną liczbą naturalną mniejszą od N, nie posiadającą wspólnych czynników z liczbą N. W szczególnym przypadku, gdy liczba a posiada wspólny dzielnik z liczbą N, wówczas wyznaczając największy wspólny dzielnik $nwd(a,N)$ liczb a oraz N dokonuje się faktoryzacji liczby N.

Można wykazać, że przewaga algorytmu kwantowego nad algorytmem klasycznym wzrasta wraz ze wzrostem liczby N, która podlega faktoryzacji.

6.3. Kwantowa transformacja Fouriera

Kwantowa dyskretna transformacja Fouriera należy do podstawowych kwantowych operacji [7, 50, 51]. Niech a będzie liczbą naturalną taką, że $0 \le a < q$ dla pewnej liczby naturalnej q. Dyskretna transformacja Fouriera reprezentowana jest macierzą unitarną A_q o wymiarach q×q, której element o indeksie $d_{a,c}$, ma postać:

$$d_{a,c} = q^{-1/2}\exp(2\pi iac/q) \qquad c = 0,1,2,\ldots,q-1$$

Dyskretna kwantowa transformacja Fouriera przetwarza stan kwantowy $|a\rangle$ na stan kwantowy:

$$|w\rangle = q^{-1/2} \sum_{c=0}^{c=q-1} |c\rangle \exp(2\pi i a c / q)$$

Obecnie przedstawimy konstrukcję macierzy unitarnej A_q reprezentującej dyskretną kwantową transformację Fouriera. Niech $q=2^m$ oraz stan kwantowy $|a\rangle$ odpowiadający liczbie naturalnej a ma następujące przedstawienie binarne: $|a_{m-1}a_{m-2}...a_1a_0\rangle$. Macierz A_q jest zbudowana jedynie z dwóch podstawowych rodzajów bramek kwantowych, a mianowicie:

1) kwantowych bramek Hadamarda H_j działających na j-ty qubit oraz reprezentowanych macierzą unitarną o wymiarach 2×2

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

2) kwantowych bramek $S_{j,k}$ działających na parę qubitów o indeksach j oraz k dla $j<k$ oraz reprezentowanych macierzą unitarną o wymiarach 4×4 następującej postaci:

$$S_{j,k} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \exp(i\theta_{k-j}) \end{bmatrix}$$

gdzie $\theta_{k-j} = \pi/2^{k-j}$.

Kwantowa transformacja Fouriera realizowana jest za pomocą następującej sekwencji bramek kwantowych stosowanych w kierunku od prawej do lewej.

$$H_{m-1}S_{m-2,m-1}H_{m-2}S_{m-3,m-1}S_{m-3,m-2}H_{m-3}...H_1S_{0,m-1}S_{0,m-2}...S_{0,2}S_{0,1}H_0$$

Zatem bramki kwantowe H_j stosuje się w odwrotnej kolejności, zaczynając od bramki kwantowej H_{m-1}, a kończąc na bramce kwantowej H_0. Natomiast bramki kwantowe $S_{j,k}$ występują pomiędzy bramkami kwantowymi H_{j+1} oraz H_j dla indeksów $k>j$.

LITERATURA

1. Barenco A.: A universal two-bit gate for quantum computation, Proceedings of the Royal Society of London, vol.449, 1995, pp.679-683.
2. Barenco A., Ekert A.: Dense coding based on quantum entanglement, Journal Modern Optimization, vol.42, 1995, pp.1253-1259.
3. Barenco A., Deutsch D., Ekert A.: Universality in quantum computation, Proceedings of the Royal Society of London, vol.449, 1995, pp.669-677.

4. Barenco A., Deutsch D., Ekert A., Jozsa R.: Conditional quantum dynamics and quantum gates, Physical Review Letters, vol.74, 1995, pp.4083-4086.
5. Barenco A., Bennett C., Cleve R., DiVincenzo D., Margolus N., Shor P., Sleator T., Smolin J., Weinfurter H.: Elementary gates for quantum computation, Physical Reviews, vol.52, 1995, pp.3457-3467.
6. Barenco A.: Quantum physics and computers, Contemporary Physics, vol.37, 1996, pp.375-389.
7. Barenco A., Ekert A., Suominen K., Torma P.: Approximate quantum Fourier transform and decoherence, Physical Reviews, vol.54, 1996, pp.139-146.
8. Barenco A., Brun T., Schak R., Spiller T.: Effects of noise on quantum error correction algorithms, Physical Reviews, vol.56, 1997, pp.1177-1188.
9. Barnum H., Fuchs C., Jozsa R., Schumacher B.: A general fidelity limit for quantum channels, Physical Reviews, vol. 54, 1996, pp.4707-4711.
10. Beckman D., Chari A., Devabhaktuni S., Preskill J.: Efficient networks for quantum factoring, Physical Reviews, vol.54, 1996, pp.1034-1063.
11. Bennett C., *Quantum information and computation*, Physics Today, vol.48, 1995, pp.24-30.
12. Bennett C., Brassard G., Popescu S., Schumacher B., Smolin J., Wootters W.: Purification of noisy entanglement and faithful teleportation via noisy channels, Physical Review Letters, vol.76, 1996, pp.722-725.
13. Bennett C., DiVincenzo D., Smolin J., Wootters W.: Mixed state entanglement and quantum error corection, Physical Reviews, vol. 54, 1996, pp.3825-3829.
14. Bennett C., Brassard G., Crepeau C., Jozsa R., Peres A., Wootters W.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Physical Review Letters, vol.70, 1993, pp.1895-1899.
15. Braunstein S., Mann A.: Measurement of the Bell operator and quantum teleportation, Physical Review Letters, vol.51, 1995, pp.1727-1730.
16. Calderbank A., Shor P.: Good quantum error-correcting codes exist, Physical Reviews, vol.54, 1996, pp.1098-1105.
17. Calderbank A., Rains E., Shor P., Sloane N.: Quantum error correction and orthogonal geometry, Physical Review Letters, vol.78, 1997, pp.405-408.
18. Chuang I., Laflamme R., Shor P., Zurek W.: Quantum computers, factoring, and decoherence, Science, vol. 270, 1995, pp.1633-1635.
19. Chuang I., Yamamoto L.: Creation of a persistent qubit using error correction, Physical Reviews, vol.55, 1997, pp.114-127.

20. Cirac J., Zoller P.: Quantum computations with cold trapped ions, Physical Review Letters, vol.74, 1995, pp.4091-4094.
21. Cirac J., Pellizari T., Zoller P.: Enforcing coherent evolution in dissipative quantum dynamics, Science, vol.273, 1996, pp.1207-1209.
22. Cirac J., Kimble H., Mabuchi H., Zoller P.: Quantum state transfer and entanglement distribution among distant nodes of a quantum network, Physical Review Letters, vol.78, 1997, pp.3221-3223.
23. Cleve R., DiVincenzo D.: Schumacher's quantum data compression as a quantum computation, Physical Reviews, vol.54, 1996, pp.2636-2639.
24. Deutsch D.: Quantum theory, the Church-Turing principle and the universal quantum computer, Proceedings of the Royal Society of London, vol.400, 1985, pp.97-117.
25. Deutsch D.: Quantum computational networks, Proceedings of the Royal Society of London, vol.425, 1989, pp.73-90.
26. Deutsch D., Jozsa R.: Rapid solution of problems by quantum computation, Proceedings of the Royal Society of London, vol.439, 1992, pp.553-558.
27. DiVincenzo D.: Two-bit gates are universal for quantum computation, Physical Reviews, vol.51, 1995, pp.1015-1022.
28. DiVincenzo D.: Quantum computation, Science, vol.270, 1995, pp.255-261.
29. DiVincenzo D., Shor P.: Fault-tolerant error correction with efficient quantum codes, Physical Review Letters, vol.77, 1996, pp.3260-3263.
30. Ekert A., Jozsa R.: Quantum computation and Shor's factoring algorithm, Reviews of Modern Physics, vol.68, 1996, pp.733-739.
31. Ekert A., Macchiavello C.: Quantum error correction for communication, Physical Review Letters, vol.77, 1996, pp.2585-2588.
32. Gershenfeld N., Chuang I.: Bulk spin-resonance quantum compuattion, Science, vol.275, 1997, pp.350-356.
33. Gottesman D.: Class of quantum error-correcting codes saturating the quantum Hamming bounds, Physical Reviews, vol.54, 1996, pp.1862-1868.
34. Grover L.K.: Quantum mechanics helps in searching for a needle in a haystack, Physical Review Letters, vol.79, 1997, pp.325-328.
35. Grover L.K.: A fast quantum mechanical algorithm for database search, Proceedings of the 28th ACM Symposium on Theory of Computations, 1996, pp.212-219.
36. Knill E., Laflamme R.: A theory of quantum error-correcting codes, Physical Reviews, vol.55, 1997, pp.900-911.
37. Laflamme R., Miquel C., Paz J., Zurek W.: Perfect quantum error correcting code, Physical Review Leters, vol.77, 1996, pp.198-201.

38. Lloyd S.: Almost any quantum logic gate is universal, Physical Review Letters, vol.75, 1995, pp.346-349.
39. Lloyd S.: Universal quantum simulators, Science, vol.273, 1996, pp.1073-1078.
40. Mattle K., Weinfurther H., Kwiat P., Zeilinger A.: Dense coding in experimental quantum communication, Physical Review Letters, vol.76, 1996, pp.4656-4659.
41. Miquel C., Paz J., Perazzo P.: Factoring in a dissipative quantum computer, Physical Reviews, vol.54, 1996, pp.2605-2613.
42. Miquel C., Paz J., Zurek W.: Quantum computation with phase drift errors, Physical Review Letters, vol.78, 1997, pp.3971-3974.
43. Monroe C., Meekhof D., King B., Itano W., Wineland D.: Demonstration of a universal quantum logic gate, Physical Review Letters, vol.75, 1995, pp.4714-4717.
44. Nielsen M., Chuang I.: Programmable quantum gate arrays, Physical Review Letters, vol.79, 1997, pp.321-324.
45. Palma G., Suominen K., Ekert A.: Quantum computers and dissipation, Proceedings of the Royal Society of London, vol.452, 1996, pp.567-584.
46. Plenio M., Knight P.: Realistic lower bounds for the factorisation time of large numbers on a quantum computer, Physical Reviews, vol.53, 1996, pp.2986-2990.
47. Schumacher B.: Quantum coding, Physical Reviews, vol.51, 1995, pp.2738-2747.
48. Schumacher B., Nielsen M.: Quantum data processing and error correction, Physical Reviews, vol.54, 1996, pp.2629-2631.
49. Shor P.: Scheme for reducing decoherence in quantum computer memory, Physical Reviews, vol.52, 1995, pp.2493-2496.
50. Shor P.: Polynomial-time algorithms for prime factorisation and discrete logarithms on a quantum computer, SIAM Journal on Computing, vol.26, 1997, pp.1484-1509.
51. Shor P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe, 20-22.11.1994. pp.124-134.
52. Shor P.: Quantum computing, Journal Documenta Mathematica, Extra Volume ICM 1998.
53. Shor P., Laflamme R.: Quantum analog of the MacWilliams identities for classical coding theory, Physical Review Letters, vol.78, 1997, pp.1600-1602.
54. Simon D.: On the power of quantum computation, SIAM Journal on Computing, vol.26, 1997, pp.1474-1483.
55. Steane A.: Error correcting codes in quantum theory, Physical Review Letters, vol.77, 1996, pp.793-797.
56. Steane A.: Simple quantum error-correcting codes, Physical Reviews, vol.54, 1996, pp.4741-4751.

57. Steane A.: Active stabilisation, quantum computation, and quantum state synthesis, Physical Review Letters, vol.78, 1997, pp.2252-2255.
58. Turchette Q., Hood C., Lange W., Mabushi H., Kimble H.: Measurement of conditional phase shift for quantum logic, Physical Review Letters, vol.75, 1995, pp.4710-4713.
59. Unruh W.: Maintaining coherence in quantum computers, Physical Reviews, vol.51, 1995, pp.992-997.
60. Vedral V., Barenco A., Ekert A.: Quantum networks for elementary arithmetic operations, Physical Reviews, vol.54, 1996, pp.147-153.

Recenzent: Dr inż. Przemysław Szmal

Wpłynęło do Redakcji 29 marca 2000 r.

Abstract

The particular behavior of atomic spin called nuclear magnetic resonance is a fundamental physical phenomenon taken into account in recent research on quantum computers. This phenomenon is based on resonance absorbency of electromagnetic energy taking place in some solid bodies, liquids and gases placed in constant external magnetic field and perturbed by impulsive varying magnetic field with properly chosen frequencies. In the case of atoms creating molecules, the behavior of their spins depends on the neighboring atoms. It enables to create logic gates, which are used to organize quantum computation processes in quantum computers.

The subject of quantum computing brings together ideas from classical information theory, computer science and quantum physics. In the paper fundamental elements of quantum computer and mathematical backgrounds of quantum computation processes are presented. The elementary unit of quantum information is quantum bit called shortly qubit. A quantum system of n qubits can be considered as an element of a complex Hilbert space of appropriate dimension. Simple unitary operations on a given set of qubits are called quantum logic gates. The universal quantum gate is the quantum equivalent of the well known classical universal logic gate. The universal quantum gate can be represented by a suitable defined unitary matrix of appropriate dimensions. Especially Toffoli gate and Hadamard gate are two fundamental quantum logic gates. These two quantum gates play a central role in networks for quantum computations. A quantum computer is a finite set of qubits and a network of quantum fundamental operations. Computation algorithms for such a quantum computer should be specially con-

structed, for example for finding the period of a function, prime factorization, and searching a random list.