STUDIA INFORMATICA 2001
Volume 22 Number 1 (43)

Stefan WĘGRZYN, Jerzy KLAMKA
Instytut Informatyki Teoretycznej i Stosowanej PAN

INFORMATYKA KWANTOWA I JEJ MIEJSCE W INFORMATYCE JAKO DYSCYPLINIE NAUKOWEJ

Streszczenie. Określa się informatykę jako dyscyplinę naukową zajmującą się badaniem praw rządzących procesami kodowania, przechowywania i przekazywania informacji. Podaje się określenie systemu informatyki jako systemu złożonego z dwóch podstawowych elementów, a mianowicie środków językowych i odpowiednich środków urządzeniowych, które umożliwiają realizację programów napisanych za pomocą przyjętych środków językowych. Omawia się charakterystyki dwóch istniejących obecnie na ziemi rodzajów systemów informatyki, a mianowicie technicznych systemów informatyki tworzonych przez ludzi od 60 lat i nanosystemów informatyki, które rozwinęły się i rozwijają w organizmach biologicznych od miliardów lat. Na tym tle przedstawia się charakterystyki i podstawowe elementy kwantowych systemów informatyki, tworzonych obecnie przez ludzi, a opartych na elementach mechaniki kwantowej.

THE QUANTUM INFORMATICS AND ITS ROLE IN INFORMATICS AS THE SCIENTIFIC DISCIPLINE

Summary. Informatics is a scientific discipline, which considers the laws of coding processes, preservation and transferring of information. Informatics' system is a system composed of two fundamental means, namely: languages and corresponding installations, which makes possible the realization of programs, which are written using languages. In the paper characteristics of two kind of informatics' systems are given, namely technical system of informatics formed by people for 60 years and nano informatics' systems, which have been developed in biological organism for milliards years. The characteristics of basic quantum elements and informatics systems based on quantum mechanics are also presented.

1. Informatyka jako dyscyplina naukowa

Informatyka jest dyscypliną naukową zajmującą się badaniem praw rządzących procesami kodowania, przechowywania, przetwarzania i przekazywania informacji [6].

Dyscyplina ta stworzyła podstawy projektowania, budowy i rozwoju współczesnych komputerów i zainicjowała w naukach ścisłych i technicznych, w których koncentrowano się dotychczas przede wszystkim na badaniach praw rządzących ruchem oraz przetwarzaniem mas i energii, koncentrację prac na badaniach praw rządzących ruchem i przetwarzaniem informacji.

Podstawową zasadą informatyki jest następująca sekwencja działań:

- opracowanie algorytmu,
- napisanie programu,
- przygotowanie struktury urządzeniowej, do której program może być wprowadzony i zrealizowany,
- realizacja programu.

Przeprowadzenie tej sekwencji działań wymaga dysponowania językami, umożliwiającymi zapisanie treści algorytmów w postaci programów, które mogą być wprowadzone, a następnie zrealizowane w przygotowanych strukturach urządzeniowych.

W rozwiązywaniu problemów metodami informatyki występują więc dwa podstawowe elementy:

zbiór **środków językowych** umożliwiających zapisywanie algorytmów w postaci programów,

zbiór **środków urządzeniowych** umożliwiających realizację tych programów.

Te dwa elementy tworzą wzajemnie uzupełniającą się całość, którą można nazwać **systemem informatyki**.

Dobór dwóch podstawowych elementów systemu - a więc języka programowania i struktury części urządzeniowej, w której przygotowane programy mogą być realizowane - wynika z celów, którym system informatyki ma służyć.

2. Techniczne i biologiczne (nano) systemy informatyki

Według obecnie posiadanej wiedzy można mówić o istnieniu na ziemi dwóch rodzajów systemów informatyki, a mianowicie technicznych systemów informatyki, które opracowali i zbudowali ludzie, a których reprezentantami są elektroniczne komputery, oraz zajmujących dziesiątki milionów razy mniejsze objętości niż komputery techniczne biologicznych sys-

temów informatyki, czyli systemów informatyki istniejących w organizmach biologicznych, które stworzyła natura, a których reprezentantem może być ziarno zboża zawierające dziesiątki Mb informatycznego programu rozwoju tej rośliny i jej samoreplikacji.

Różnice między technicznymi systemami informatyki a systemami informatyki istniejącymi w organizmach biologicznych wynikają z celów, które dzięki nim mają być uzyskiwane.

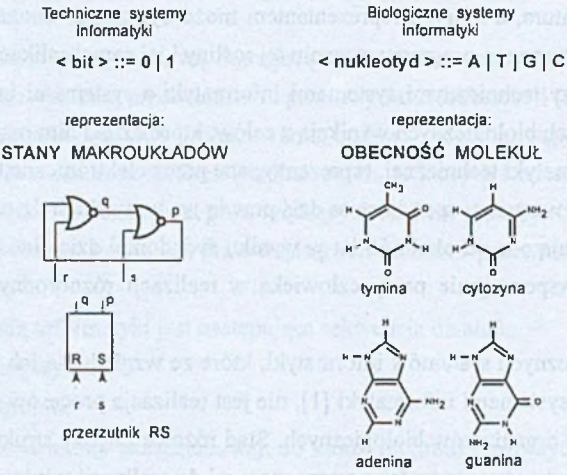
Systemy informatyki technicznej, reprezentowane przez elektroniczne komputery cyfrowe i ich urządzenia zewnętrzne, spotykane są dziś prawie we wszystkich dziedzinach działalności ludzkiej. Powstają one od około 60 lat w wyniku świadomej działalności człowieka, a zadaniem ich jest wspomaganie pracy człowieka w realizacji różnorodnych procesów obliczeniowych.

Celem biologicznych systemów informatyki, które ze względu na ich wymiary będziemy nazywali też nanosystemami informatyki [1], nie jest realizacja procesów obliczeniowych ale realizacja budowy organizmów biologicznych. Stąd różnice między strukturami części urządzeniowych obu rodzajów systemów przeznaczonymi do realizacji właściwych dla każdego z nich podstawowych operacji elementarnych.

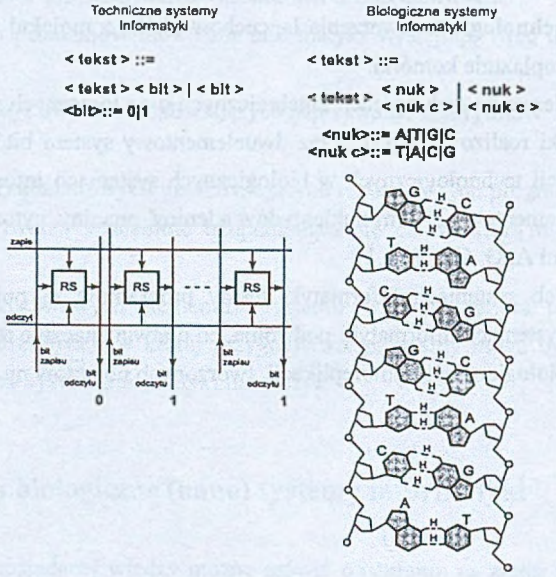
W pierwszym przypadku, systemów informatyki technicznej, są to **elementarne operacje algebraiczne** i **logiczne** na liczbach sprowadzone do operacji na elementarnych symbolach 0, 1 zwanych bitami. W drugim przypadku, biologicznych systemów informatyki, są to **elementarne operacje technologiczne** tworzenia łańcuchów białka z molekuł aminokwasów znajdujących się w cytoplazmie komórki.

Kodowanie elementarnych operacji algebraicznych oraz logicznych w technicznych systemach informatyki realizowane jest przez dwuelementowy system bitów. Kodowanie elementarnych operacji technologicznych w biologicznych systemach informatyki realizowane jest przez czteroelementowy system nukleotydów adeniny, guaniny, cytozyny i tyminy, oznaczonych symbolami A, G, C, T (rys.1).

W technicznych systemach informatyki teksty programów są pojedyncze, natomiast w biologicznych systemach informatyki podwójne, co ułatwia znacznie realizację, występującej w systemach biologicznych, samoreplikacji tworzonych obiektów np. na poziomie komórek (rys.2).



Rys. 1. Symbole terminalne tekstów w biologicznych i technicznych systemach informatyki
Fig. 1. Terminal symbols of texts in biological and technical systems of informatics



Rys. 2. Formaty tekstów w biologicznych i technicznych systemach informatyki
Fig. 2. Formats of programs text in biological and technical systems of informatics

Charakterystyki technicznych i biologicznych systemów informatyki przedstawia niniejsza tabela.

Nazwa	Wiek	Elementarne jednostki informacji	Reprezentacja elementarnych jednostek informacji
Techniczne systemy informatyki	60 lat	bit::=0|1	Obecność w danym miejscu tekstu makroukładu reprezentującego bit
Nanosystemy informatyki	miliardy lat	nukleotyd ::= A|G|C|T	Obecność w danym miejscu tekstu molekuł A,G,C,T reprezentujących nukleotydy

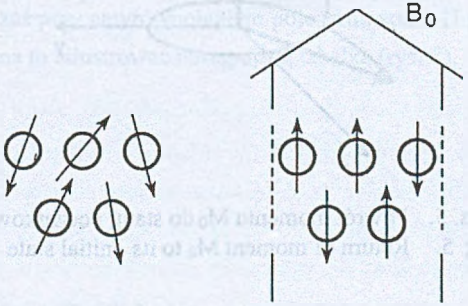
3. Koncepcje kwantowych systemów informatyki i ich fizyczne podstawy

W technicznych systemach informatyki symbole kodów, w których zapisane są teksty programów, reprezentują stany makroukładów o charakterze przerzutników lub wyróżnionych domen magnetycznych.

W nanosystemach informatyki symbole kodów informatycznych reprezentują pojedyncze molekuły i atomy.

W obecnie podjętych pracach nad zupełnie nowym typem systemów informatyki, tak zwanymi kwantowymi systemami informatyki, symbole kodów informatycznych reprezentują spiny atomów umieszczonych w zewnętrznym stałym polu magnetycznym o indukcji B_0 pobudzanych zewnętrznymi impulsami elektromagnetycznymi.

Wprowadzenie zewnętrznego stałego pola magnetycznego uporządkowuje kierunki spinów tak, że przyjmują one położenie równoległe lub antyrównoległe do kierunku linii pola magnetycznego B_0 (rys. 3).

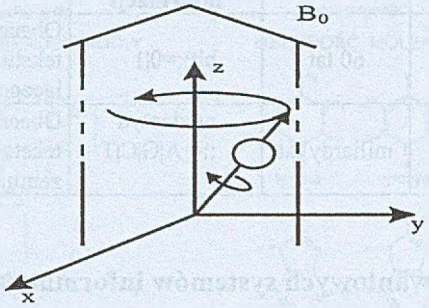


Rys. 3. Kierunki spinów przed i po wprowadzeniu stałego pola magnetycznego
Fig. 3. Directions of spins without and within static magnetic field

W przypadku zewnętrznego stałego pola magnetycznego występuje też zjawisko precesji (rys. 4) o częstotliwościach Larmora:

$$f_0 = \gamma B_0/2\pi \quad \text{lub} \quad \omega_0 = \gamma B_0,$$

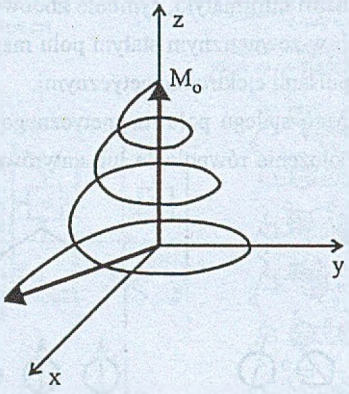
gdzie γ – stała żyromagnetyczna.



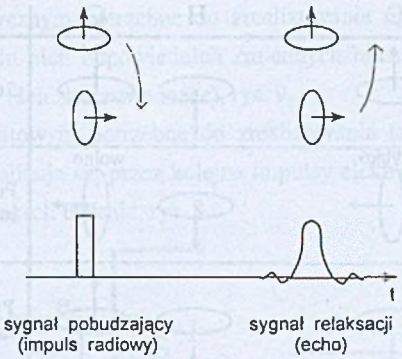
Rys. 4. Precesja wektora momentu magnetycznego
Fig. 4. Precession of magnetic momentum vector

Jeżeli na taki atom skierujemy impuls zmiennego pola elektromagnetycznego o częstotliwości Larmora, to może on zmienić swój poziom energetyczny, zmieniając położenie osi ruchu precesyjnego, np. o 90°, to znaczy przechodząc z położenia równoległego na prostopadłe do kierunku B_0.

Po zaniku impulsu kierunek spinu wraca do poprzedniego, zaś atom emituje wcześniej pochłoniętą energię w postaci tak zwanego *sygnału echa* (rys. 5, 6).



Rys. 5. Powrót momentu M_0 do stanu początkowego
Fig. 5. Return of moment M_0 to its initial state



Rys. 6. Sygnał pobudzający i jego echo
Fig. 6. Exciting signal and its echo

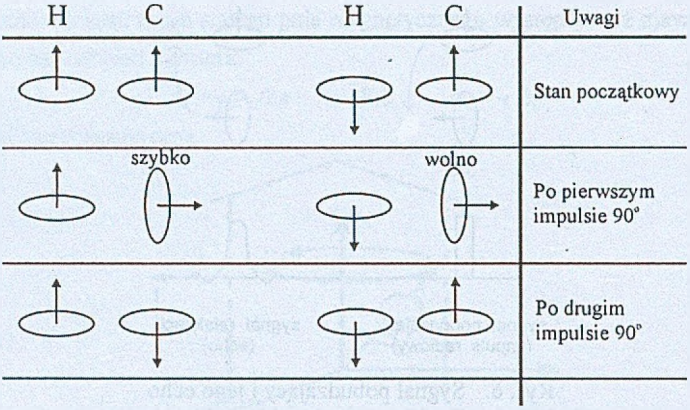
Jeżeli atomy tworzą molekuły, to zachowanie się ich spinów jest uzależnione od stanów sąsiednich atomów.

W pracach doświadczalnych N.Gershenfelda i I.Chuanga [4] wykorzystany był chloroform ($CHCl_3$), a więc ciecz o molekułach złożonych z atomów węgla (C), wodoru (H) i chloru (Cl). Z uwagi na to, że węgiel ^{12}C nie ma spinu, 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, oddziałujące na położenie spinu C.

Pierwszy odchyla położenie spinu C o 90°, drugi natomiast odchyla go o dalsze 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. 7).



Rys. 7. Zależność między spinami wodoru H i tlenu C w molekule chloroformu w reakcji na dwa kolejne zewnętrzne sygnały
Fig. 7. Dependences between spin of hydrogen H and carbon C in chloroform molecule in response to external signals

Zachowanie się spinów atomów węgla C oraz wodoru H można opisać 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:

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

Zatem po dwóch kolejnych impulsach elektromagnetycznych stan spinu węgla C, oznaczony przez b1, można zapisać w następujący sposób:

$$b_1 = b \oplus a, \tag{1}$$

gdzie symbol $\oplus$ oznacza sumę modulo 2.

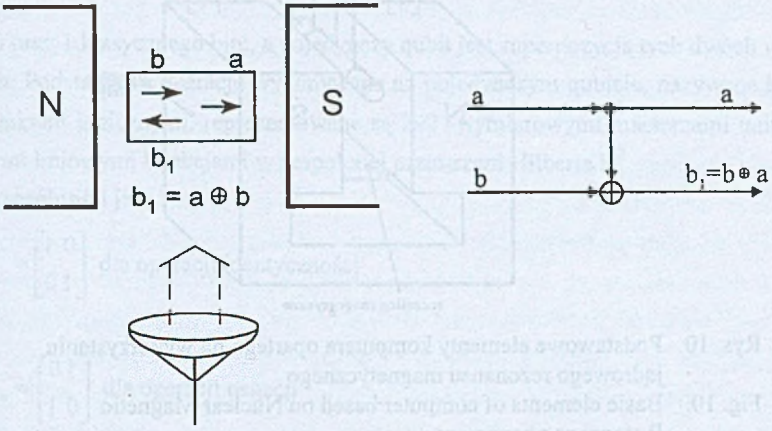
W równaniu (1) b1 jest wynikiem tak zwanej operacji logicznej XOR, realizowanej przez bramkę XOR, której działanie można zilustrować tak, jak to przedstawiono na rys. 8.

Bramka kwantowa 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. 9.

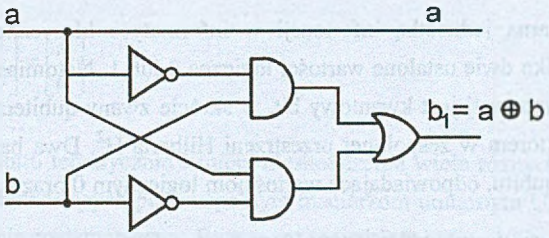
Porównując dwa rozwiązania bramki XOR, a więc kwantowe przedstawione na rys.8 i klasyczne przedstawione na rys. 9 możemy powiedzieć, że:

- w rozwiązaniu klasycznym potrzebne do zrealizowania operacje rozmieszcza się w **przestrzeni**, a przepływ do nich odpowiednich zmiennych binarnych realizuje się poprzez przeprowadzone przewody (ścieżki prowadzące), rys. 9,

- w rozwiązaniu kwantowym potrzebne do zrealizowania takiej bramki operacje rozmieszcza się w **czasie** i realizuje się przez kolejne impulsy elektromagnetyczne o odpowiednich częstotliwościach i czasach trwania, rys. 8.



Rys. 8. Bramka XOR w realizacji kwantowej i jej symboliczne oznaczenie
Fig. 8. Quantum circuit of the gate XOR and its symbolic representation



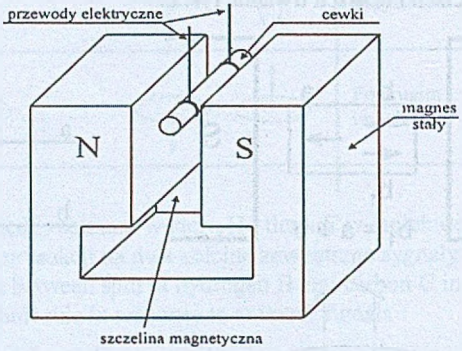
Rys. 9. Bramka XOR w realizacji klasycznej
Fig. 9. Classic circuit of the gate XOR

Prowadzone badania mają na celu wykorzystanie metod jądrowego rezonansu magnetycznego do realizacji właściwych informatyce procesów kodowania i przekształcania danych.

W szczególności bada się możliwości konstrukcji komputera kwantowego [4] według ogólnej idei przedstawionej na rys. 10.

W układzie doświadczalnym przedstawionym na rys.10 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 poddanie wybranej cieczy znajdującej się w rurce działaniu serii impulsów elektromagnetycznych o odpowiednio dobranych częstotliwościach i czasach trwania oraz odczytanie wyniku.



Rys. 10. Podstawowe elementy komputera opartego na wykorzystaniu jądrowego rezonansu magnetycznego
Fig. 10. Basic elements of computer based on Nuclear Magnetic Resonance phenomena

4. Matematyczne podstawy kwantowych systemów informatyki

Elementarną jednostką informacji w informatyce klasycznej jest bit, który może przyjmować tylko dwie ustalone wartości logiczne 0 lub 1. Natomiast elementarną jednostką informatyki kwantowej jest kwantowy bit, w skrócie zwany qubitem, reprezentowany unormowanym wektorem w zespolonej przestrzeni Hilberta H^2. Dwa bazowe ortogonalne stany pojedynczego qubitu, odpowiadające wartościom logicznym 0 oraz 1, tworzą bazę ortogonalną $\left\{\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right\}$ w przestrzeni H^2.

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 prawdopodobieństwa, a wektor $|\Psi\rangle$ jest znormalizowany. Jest więc

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

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 [2], [1].

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, a pojedynczy qubit jest superpozycją tych dwóch wartości logicznych. 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.

W szczególności jest

$$U_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ dla operacji identyczności}$$

$$U_n = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ dla operacji negacji} \tag{3}$$

Mamy wtedy

$$U_i \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{4}$$

oraz

$$U_n \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \tag{5}$$

Dla pojedynczego qubitu teoretycznie istnieje nieskończenie wiele różnych kwantowych bramek logicznych, odpowiadających poszczególnym macierzom unitarnym U, realizujących zadaną kwantową operację matematyczną. Wystarczy jednak posługiwać się tylko kilkoma odpowiednio wybranymi podstawowymi kwantowymi bramkami logicznymi, którym odpowiadają pewne macierze unitarne.

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 informatyki kwantowej operacje te są reprezentowane macierzami unitarnymi.

W przypadku układu kwantowego złożonego z 2 qubitów podstawowe operacje reprezentowane są 4×4 -wymiarowymi macierzami unitarnymi. W tym przypadku spośród wszystkich możliwych podstawowych operacji wykonywanych na parze qubitów w przestrzeni H^4 szcze-

gólne znaczenie ma operacja oznaczona symbolem XOR lub symbolem CNOT. Operacja ta nosi nazwę "sterowalnej bramki negacji", gdyż operacja wykonywana na drugim qubicie zależy od tego, w jakim stanie kwantowym jest pierwszy qubit. W klasycznej algebrze Boole'a dowolną funkcję logiczną można zrealizować za pomocą odpowiednio połączonych bramek logicznych XOR. Mając do dyspozycji odpowiednią liczbę kwantowych bramek logicznych XOR można również realizować dowolne funkcje logiczne [2], [7].

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 $2^n \times 2^n$ -wymiarowe. Zatem macierze te 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 $2^n \times 2^n$-wymiarowymi macierzami unitarnymi. Niemniej podstawową kwantową bramką logiczną dla układu kwantowego zawierającego n qubitów jest tak zwana bramka Toffoli, reprezentowana $2^n \times 2^n$ -wymiarową macierzą unitarną. Okazuje się, że n-wejściowa kwantowa bramka Toffoli jest bramką uniwersalną, za pomocą której można zrealizować dowolną n-argumentową funkcję logiczną.

Szczególnym przypadkiem bramki Toffoli dla n = 2 jest omówiona uprzednio bramka sterowalnej negacji XOR.

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.

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. Zatem przestrzeń stanów dla n qubitów posiada 2^n wzajemnie ortogonalnych stanów bazowych. Elementami tej przestrzeni są wszystkie możliwe superpozycje stanów kwantowych reprezentowane iloczynami tensorowymi 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 reprezentowany znormalizowanym wektorem w przestrzeni H^{2^n} może być przedstawiony w postaci liniowej kombinacji 2^n ortonormalnych wektorów bazowych.

Istotną cechą n-qubitowego komputera kwantowego jest zjawisko zwane superpozycją stanów kwantowych poszczególnych qubitów. Superpozycja stanów kwantowych poszczególnych qubitów oznacza, że układ n qubitów może istnieć w wielu stanach jednocześnie i w tym samym czasie można równolegle dokonywać operacji kwantowych na każdym ze stanów. Zatem komputer kwantowy może wykonywać bardzo dużą liczbę operacji matematycznych równolegle wykorzystując do tego celu jeden procesor kwantowy.

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

Interesującą cechą odróżniającą układy kwantowe od klasycznych układów liczących jest też tak zwane zjawisko uwikłania. Uwikłanie zwane również splątaniem związane jest z dowolnym układem n-qubitów i jest bezpośrednim efektem wykonania iloczynu tensorowego na 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. Zjawisko uwikłania powoduje, że układy kwantowe wchodzą ze sobą we wzajemne związki, które w komputerze kwantowym odgrywają rolę kabla łączącego poszczególne qubity. Ten sam efekt uwikłania leży u podstaw zjawiska kwantowej teleportacji, związanej z przesyłaniem informacji kwantowej.

5. Algorytmy i programowanie komputerów kwantowych

Kwantowe bramki logiczne są podstawowymi elementami uniwersalnego komputera kwantowego. Uniwersalny komputer kwantowy powinien umożliwić analizę i przetwarzanie informacji kwantowej zawartej w układach qubitów. Formalnie kwantowy komputer jest układem n qubitów, na których można przeprowadzić odpowiednie operacje kwantowe reprezentowane bramkami kwantowymi lub macierzami unitarnymi odpowiednich wymiarów.

Z 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.

W istocie program obliczeń w komputerze kwantowym zakodowany jest w postaci ciągu impulsów zewnętrznego pola elektromagnetycznego o odpowiednich częstotliwościach. Efektywny okres jednego cyklu komputera kwantowego określa najdłuższy czas potrzebny na to, aby poszczególne spiny jądrowe obróciły się o odpowiedni kąt. Prędkość działania komputera kwantowego wynika głównie z równoległości wykonywanych obliczeń wynikającej bezpośrednio z liczby wykorzystywanych qubitów.

Należy jednak wyraźnie podkreślić, że wykonywanie obliczeń na komputerze kwantowym wymaga odpowiednich algorytmów obliczeniowych, dostosowanych do specyfiki działania komputera kwantowego. Algorytmy te umożliwiają wielokrotne przyspieszenie obliczeń w stosunku do rezultatów osiąganych za pomocą algorytmów stosowanych do tej pory w klasycznych komputerach.

Podstawowym zagadnieniem związanym z obliczeniami wykonanymi za pomocą komputerów jest zaproponowanie odpowiedniego algorytmu obliczeniowego. Komputer kwantowy przeprowadza obliczenia w oparciu o specjalne algorytmy obliczeniowe, nie stosowane w informatyce klasycznej. Algorytmy te dostosowane do możliwości obliczeniowych komputera kwantowego w istotny sposób wykorzystują podstawowe prawa mechaniki kwantowej, a w szczególności zjawisko superpozycji stanów kwantowych.

Istotnym zagadnieniem klasycznej teorii algorytmów jest określenie złożoności obliczeniowej danego algorytmu. Ogólnie klasyczne algorytmy obliczeniowe dzieli się na dwie podstawowe grupy: algorytmy o wielomianowej złożoności obliczeniowej oraz algorytmy o wykładniczej złożoności obliczeniowej. W przypadku algorytmów kwantowych różnica pomiędzy tymi dwoma złożonościami obliczeniowymi nie ma tak istotnego znaczenia jak w przypadku algorytmów klasycznych.

Do najważniejszych algorytmów informatyki kwantowej należą: algorytm faktoryzacji liczb naturalnych zaproponowany w 1994 roku przez Shora oraz algorytm poszukiwań opracowany przez Grovera w 1996 roku.

W roku 1994 Shor zaproponował [5] kwantowy algorytm umożliwiający faktoryzację liczb naturalnych o wielomianowej złożoności obliczeniowej. Jest to jeden z najważniejszych algorytmów informatyki kwantowej, umożliwiający znaczne przyspieszenie wielu procesów obliczeniowych. W algorytmie Shora problem faktoryzacji dowolnej liczby naturalnej N został sprowadzony do zagadnienia znajdowania okresu pewnej funkcji periodycznej. Każdy krok tego algorytmu z wyjątkiem znajdowania okresu funkcji periodycznej ma wielomianową złożoność obliczeniową.

W roku 1996 Grover zaproponował [3] kwantowy algorytm wyszukiwania informacji w dużych zbiorach danych. Problem polega na wyszukaniu w nieuporządkowanym zbiorze danych {xi, i=1,2,3,...,N}, zawierającym N elementów określonego elementu xi=v. Przykładowo, może to być wyszukanie w spisie telefonów danego numeru telefonu, gdy nie jest znane nazwisko 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 w zbiorze N elementów średnio jedynie $\sqrt{N}$ kroków.

Należy zaznaczyć, że 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. Podsumowanie

W okresie ostatnich kilku lat jesteśmy świadkami rosnącego zainteresowania rozwojem kwantowych systemów informatyki [7], [8], [9], [10].

W niniejszej pracy przedstawiono charakterystykę oraz kierunki prac badawczych w tej dziedzinie. Zmierzają one poprzez prace teoretyczne i badania doświadczalne do stworzenia dla potrzeb własnych całej nauki naukowych podstaw informatycznych przekształceń kwantowych i ich wykorzystania w konstrukcjach komputerów kwantowych oraz informatycznych struktur urządzeniowych.

LITERATURA

1. Cempel Cz.: Nanotechnologie, źródła i perspektywy. Nauka 1999, nr 3, str. 178-186.
2. Deutsch D.: Quantum computational networks. Proceedings of the Royal Society of London, vol. 425, 1989, pp. 73-90.
3. 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.
4. Gershenfeld N., Chuang I.: Bulk spin-resonance quantum computation. Science, vol. 275. 1997, pp. 350-356.
5. Shor P.: Polynominal-time algorithms for prime factorization and discrete logarithms on a quantum computer. Proceedings of the 35th Annual Symposium on Fundations of Computer Science, Santa Fe, 20-22.11.1994, pp.124-134.

6. Węgrzyn S.: Informatics Science. Archiwum Informatyki Teoretycznej i Stosowanej, tom 11 z. 2/1999, s.107-119..
7. Węgrzyn S., Klamka J.: Kwantowe systemy informatyki. Instytut Informatyki Teoretycznej i Stosowanej PAN, Gliwice 2000.
8. Węgrzyn S., Klamka J.: Quantum computing. Archiwum Informatyki Teoretycznej i Sto sowanej, tom 12 (2000), z. 3, pp. 235-246.
9. Węgrzyn S., Klamka J.: Kwantowe systemy informatyki. Studia Informatica, vol. 21, nr1, 2000, str. 15-45.
10. Węgrzyn S., Klamka J.: Kwantowe systemy informatyki. Nauka, nr 3, 2000, str. 71-82.

Recenzent: Dr inż. Przemysław Szmal

Wpłynęło do Redakcji 31 marca 2001 r.

Abstract

In the development of computer science as a scientific discipline there was a time period during which experimental research was 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.

Recently, it was realized that some properties of quantum mechanics might speed up certain computations. The application of quantum physical principles to the field of computing leads directly to the concept of quantum computer. Quantum computations can be modeled formally by defining quantum Turing machine, which is able to be in the superposition of many states. It now appears that, at least theoretically, quantum computations may be much faster than classical computations for solving certain problems including for example prime factorization. Moreover, it should be pointed out, that the quantum computations offer powerful methods of encoding and manipulating information that are not possible within a classical framework.

The potential applications of these quantum information-processing methods include for example cryptography, rapid integer factoring and quantum simulation.

The quantum analogy to the classical bit is the quantum bit named shortly qubit. Physically qubit can be represented as a spin of a particle. A particle in one spin state can be pushed towards another by a frequency pulse in external magnetic field. Therefore, the par-

ticular 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 forming molecules the behavior of their spins depends on the neighboring atoms. It enables an implementation of logical quantum gates, which are used to organize quantum computation processes in quantum computers.

Quantum computers are hypothetical machine that use principles of quantum mechanics for their basic operations. There are a number of differences between quantum and classical computers. In particular, a property of quantum systems that plays a crucial role is the so called entanglement or non-classical correlation between quantum systems. In other words this means, that the quantum state cannot be written as a product of states of individual qubits. Another important property is the high dimensionality of quantum systems. The quantum computation algorithms make critical use of this extra dimensionality.

Finally, it should be pointed out that quantum computers will solve computational problems and carry out simulations that are basically impossible on conventional computers.