Komputer kwantowy na kropkach kwantowych

Janusz Adamowski
Wydział Fizyki i Techniki Jądrowej, Akademia Górniczo-Hutnicza, Kraków
email: adamowski@ftj.agh.edu.pl

Streszczenie *W wykładzie tym omawiane są podstawy obliczeń kwantowych oraz ich możliwa realizacja przy użyciu kropek kwantowych. Dyskutowane jest wykorzystanie spinu elektronu uwięzionego w kropce kwantowej do zapisu/odczytu bitu kwantowego oraz do wykonywania operacji logicznych.*

1. Wstęp

W ostatnich latach następuje szybki rozwój teorii obliczeń kwantowych. Ponadto intensywnie badane są możliwe fizyczne realizacje obliczeń kwantowych. Teoria obliczeń kwantowych opiera się na bezpośrednim zastosowaniu praw mechaniki kwantowej do obliczeń. Zgodnie z obecnym stanem wiedzy mechanika kwantowa opisuje w sposób kompletny strukturę i własności mikroświata, czyli obiektów o rozmiarach mniejszych lub porównywalnych z rozmiarami molekuł. W szczególności kwantowa teoria atomów i cząstek elementarnych, takich jak elektron czy foton, niezwykle precyzyjnie opisuje ich własności podlegające weryfikacji eksperymentalnej. Kwantowe algorytmy obliczeniowe złożone są z ciągów operacji wykonywanych na stanach kwantowych i wykorzystują skwantowanie (przyjmowanie wartości dyskretnych) podstawowych wielkości fizycznych, takich jak energia i moment pędu. Kwantową jednostką informacji jest bit kwantowy, zwany qubitem, będący stanem kwantowym w dwuwymiarowej przestrzeni Hilberta. Reprezentacją qubitu może być np. superpozycja dwóch stanów spinowych elektronu lub fotonu. Qubity mogą służyć do zapisu (odczytu) informacji kwantowej. Ponadto na qubitach mogą być wykonywane kwantowe operacje logiczne, wykorzystywane zarówno do obliczeń jak i przetwarzania oraz przesyłania informacji kwantowej. Operacje te są opisywane matematycznie za pomocą transformacji unitarnych pomiędzy stanami kwantowymi.

Równolegle z rozwojem teorii obliczeń kwantowych badane są obecnie sposoby fizycznej realizacji qubitów o określonych własnościach i przeprowadzania kontrolowanych transformacji pomiędzy nimi. Znaczna część z tych badań uwieńczona została sukcesem. Przewiduje się, że obliczenia kwantowe będzie można wykonywać na wielu różnych układach fizycznych, np. na pojedynczych jonach, atomach i fotonach w pułapkach jonowych i atomowych, na układach wielu molekuł w aparaturze do badania magnetycznego rezonansu jądrowego (NMR), na parach Coopera w nadprzewodniku. Szczególnie obiecująco wygląda możliwość zapisu i przetwarzania informacji kwantowej przy użyciu nanostruktur półprzewodnikowych, a zwłaszcza kropek kwantowych. Zaletą układów półprzewodnikowych jest fakt, iż technologia ich otrzymywania stanowi naturalne rozwinięcie dotychczas stosowanych technologii w przemyśle komputerowym, a dodatkowo możliwe jest sterowanie ich własnościami przy użyciu współczesnej elektroniki.

Omawiane w tym wykładzie kropki kwantowe są laboratoryjnie wytwarzanymi w ciałach stałych strukturami o rozmiarach nanometrowych, w których ruch nośników ładunku (elektronów i dziur) jest ograniczony w trzech kierunkach przestrzennych. Są to najmniejsze sztucznie otrzymywane struktury, których własności elektronowe mogą być kontrolowane za pomocą nowoczesnych ukła-

dów elektronicznych. Należy zauważyć, że kropki kwantowe stanowią granicę dotychczasowego trendu miniaturyzacji urządzeń elektronicznych, który polega na wytwarzaniu przez człowieka coraz mniejszych układów elektronicznych. Mniejszymi od nich obiektami, możliwymi do wykorzystania w przyszłej elektronice, są naturalne atomy i molekuły. Kropki kwantowe, nazywane są sztucznymi atomami, ponieważ elektrony (dziury) uwięzione w nich tworzą stany kwantowe o własnościach podobnych do własności atomów naturalnych. W szczególności poziomy energetyczne odpowiadające stanom kwantowym uwięzionych nośników ładunku są dyskretne. Ze względu na możliwość zmian w szerokim zakresie własności elektronowych za pomocą zewnętrznego pola elektromagnetycznego, kropki kwantowe stanowią obiecujące elementy konstrukcyjne do budowy przyszłych komputerów kwantowych.

Komputery kwantowe, których pojedyncze elementy logiczne są dopiero w fazie badań laboratoryjnych, należy odróżnić od nanokomputerów, które wchodzą już do fazy produkcyjnej. Podstawowe elementy nanokomputerów, czyli nanotranzystory polowe (NFET) i nano-obwody scalone (nanoIC), osiągają obecnie rozmiary poniżej 100 nm, a więc ujawniają się już w nich zjawiska kwantowe. Jednakże zasada działania nanokomputerów opiera się na wykorzystaniu praw fizyki klasycznej, chociaż pewne efekty kwantowe, np. zasada nieoznaczoności, pełnią rolę ograniczającą ich zdolności obliczeniowe i muszą być uwzględnione przy ich konstrukcji. Zupełnie odmienną rolę pełnią zjawiska kwantowe w komputerach kwantowych, w których to właśnie efekty kwantowe umożliwiają wykonywanie obliczeń. Należy zauważyć, że niektóre, inne niż kropki kwantowe, realizacje fizyczne kwantowych bramek logicznych, np. pułapki jonowe i atomowe, układy NMR, posiadają rozmiary centymetrowe, co sugeruje, iż możliwe w przyszłości wprowadzenie do eksploatacji komputerów kwantowych wcale nie będzie musiało oznaczać dalszej miniaturyzacji maszyn obliczeniowych. Będzie natomiast prowadziło do znacznego zwiększenia mocy obliczeniowej.

Historia obliczeń kwantowych zaczyna się od prac Feynmana [1, 2], który zaproponował bezpośrednie zastosowanie praw mechaniki kwantowej do realizacji algorytmów obliczeniowych. Komputery kwantowe odróżnia od komputerów klasycznych właśnie to bezpośrednie wykorzystanie własności kwantowych do obliczeń. Działanie komputerów klasycznych, w tym także nanokomputerów, opiera się na prawach fizyki klasycznej, w szczególności na równaniach Maxwella, stanowiących podstawę elektrodynamiki klasycznej. Wprawdzie w skład budowanych obecnie komputerów wchodzą tranzystory, których działanie opiera się na wykorzystaniu kwantowej struktury elektronowej półprzewodników, to jednak w trakcie obliczeń mamy do czynienia z procesami opisanymi za pomocą równań fizyki klasycznej. Na przykład, zapis lub odczyt jednego bitu klasycznego wymaga przepływu od miliona do miliarda elektronów. Natomiast do zapisu lub odczytu bitu kwantowego wystarczy przepływ jednego elektronu.

Podstawowe idee obliczeń kwantowych zostały wprowadzone i rozwinięte w pracach [3, 4, 5, 6, 7, 8, 9]. Model obliczeń kwantowych i opis uniwersalnego komputera kwantowego jako kwantowej maszyny Turinga zostały opracowane przez Deutscha [3]. Shor [4] wprowadził kwantowe algorytmy faktoryzacji liczb całkowitych. Grover [5] opracował szybki kwantowy algorytm przeszukiwania baz danych. Wooters i Żurek [6] wykazali ważne twierdzenie o niemożliwości klonowania bitów kwantowych. Calderbank i Shor [8] opracowali kwantową metodę korekcji błędów. Teoria obliczeń kwantowych jest obecnie teorią dojrzałą, łączącą w sobie elementy fizyki, matematyki i informatyki [10, 11].

W wykładzie tym omówię możliwości zastosowania kropek kwantowych do wykonywania obliczeń kwantowych. Wykład jest zorganizowany następująco: w rozdziale 2. przedstawione są postulaty mechaniki kwantowej oraz wprowadzenie do obliczeń kwantowych, rozdział 3. zawiera zwięzłą prezentację podstawowych własności fizycznych kro-

pek kwantowych, w rozdziale 4. omówione są możliwe realizacje qubitów i operacji logicznych przy użyciu kropek kwantowych, a rozdział 5. zawiera podsumowanie.

2. Obliczenia kwantowe

2.1. Postulaty mechaniki kwantowej

Obliczenia kwantowe bazują na prawach mechaniki kwantowej, które zostały sformułowane w postaci postulatów. W podrozdziale tym przedstawię te postulaty, które są najważniejsze z punktu widzenia obliczeń kwantowych. W tym celu użyję notacji Diraca, zgodnie z którą wektory stanów kwantowych należące do d-wymiarowej przestrzeni Hilberta $\mathcal{H}^d$ zapisywane są za pomocą nawiasów ostrych (ang. *bracket*), czyli $\rangle$ lub $\langle$. W zapisie Diraca symbole $|\psi\rangle, |\varphi\rangle, |\chi\rangle, \ldots$ oznaczają wektory stanów typu ket, a $\langle\psi|, \langle\varphi|, \langle\chi|, \ldots$ oznaczają sprzężone względem nich po hermitowsku wektory stanów typu bra. Iloczyn wewnętrzny (skalarny) wektora $|\psi\rangle$ razy wektor $|\varphi\rangle$ zapisujemy jako $\langle\psi|\varphi\rangle$; jego wartość jest liczbą zespoloną. Natomiast iloczyn zewnętrzny zapisany jako $|\psi\rangle\langle\varphi|$ jest operatorem, który działając na dowolny wektor $|\chi\rangle$ przekształca go w wektor $\langle\varphi|\chi\rangle|\psi\rangle$.

Postulat I: Dowolny izolowany układ fizyczny opisany jest w sposób kompletny za pomocą wektora stanu $|\psi\rangle \in \mathcal{H}^d$. Wektor ten na ogół zależy od czasu, co zapisujemy jako $|\psi\rangle = |\psi(t)\rangle$, a ponadto $\forall t$ jest unormowany, czyli $\langle\psi|\psi\rangle = 1$. Znaczenie fizyczne kompletności opisu wyjaśnione zostanie w kolejnych postulatach.

Qubit jest wektorem stanu należącym do dwuwymiarowej przestrzeni Hilberta $\mathcal{H}^2$. Jeżeli wektory $|0\rangle$ i $|1\rangle$ tworzą bazę ortonormalną zupełną w tej przestrzeni, to qubit można zapisać jako

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \,, \qquad (1)$$

przy czym liczby zespolone c_0 i c_1, zwane amplitudami prawdopodobieństwa, spełniają warunek unormowania $|c_0|^2 + |c_1|^2 = 1$. Ortonormalna baza stanów $\{|0\rangle, |1\rangle\}$ nazywana jest *bazą obliczeniową*.

Równoważny opis można uzyskać za pomocą *funkcji falowej*, którą dla układu N cząstek definiujemy jako

$$\psi(\xi_1, \ldots, \xi_N; t) = \langle\xi_1, \ldots, \xi_N|\psi(t)\rangle \,, \qquad (2)$$

gdzie zbiór $\xi_i = (x_i, y_i, z_i, \sigma_i)$ zawiera współrzędne przestrzenne (x_i, y_i, z_i) i dyskretną zmienną spinową σ_i cząstki i-tej ($i = 1, \ldots, N$), a $\langle\xi_1, \ldots, \xi_N|$ jest stanem kwantowym o określonych wartościach ξ_i wszystkich cząstek.

Postulat II: Jeżeli $|\psi\rangle \equiv |\nu\rangle$ jest stanem własnym operatora hermitowskiego Ω, czyli jeżeli spełnione jest równanie własne,

$$\Omega|\psi\rangle = \omega_\nu|\psi\rangle \,, \qquad (3)$$

to wynikiem pomiaru wielkości fizycznej, której odpowiada operator Ω, jest – z prawdopodobieństwem równym 1 – wartość własna ω_ν (liczba rzeczywista). Jeżeli natomiast $|\psi\rangle$ nie jest wektorem własnym operatora Ω, czyli $|\psi\rangle \neq |\nu\rangle$, to wynikiem pomiaru rzutowego wielkości fizycznej opisanej operatorem Ω może być wartość własna ω_ν z prawdopodobieństwem $p_\nu = |\langle\psi|\nu\rangle|^2 < 1$. Powiedzmy, że w wyniku pomiaru rzutowego otrzymaliśmy wartość własną ω_ν, to stan układu tuż po wykonaniu pomiaru dany jest przez

$$\frac{\langle\nu|\psi\rangle|\nu\rangle}{|\langle\nu|\psi\rangle|} \,, \qquad (4)$$

gdzie $|\nu\rangle$ jest wektorem własnym operatora Ω przynależnym do wartości własnej ω_ν.

Zastosujmy postulat II do pomiaru qubitu (1) w bazie obliczeniowej $\{|0\rangle, |1\rangle\}$. Operatory pomiarów rzutowych mają postać: $M_0 = |0\rangle\langle 0|$ i $M_1 = |1\rangle\langle 1|$. Przypuśćmy, że stan układu przed pomiarem dany jest przez kombinację liniową (1). W tym przypadku prawdopodobieństwo otrzymania w wyniku pomiaru wartości 0, której odpowiada stan własny $|0\rangle$, wynosi $p(0) = |\langle\psi|0\rangle|^2 = |c_0|^2$. Natomiast prawdopodobieństwo otrzymania wartości 1, której odpowiada stan własny $|1\rangle$, jest równe $p(1) = |\langle\psi|1\rangle|^2 = |c_1|^2$. Stan układu po wykonaniu pomiaru określony jest przez $(c_0/|c_0|)|0\rangle$ i $(c_1/|c_1|)|1\rangle$ odpowiednio w pierwszym i drugim przypadku.

Własności pomiarowe stanów kwantowych, zawarte w postulacie II, pozwalają nam

na przedyskutowanie zawartości informacyjnej qubitu. W odróżnieniu od bitu klasycznego, który jest w stanie klasycznym 0 lub 1 w każdym przypadku z prawdopodobieństwem 1, qubit przyjmuje kontinuum wartości, określonych przez amplitudy c_0 i c_1, które jednak nie są mierzalne. Oznacza to, iż przed wykonaniem pomiaru nie posiadamy żadnej informacji o stanie kwantowym. Jeżeli wykonamy pomiar qubitu (1), to otrzymamy wynik 0 z prawdopodobieństwem $|c_0|^2$ lub wynik 1 z prawdopodobieństwem $|c_1|^2$, przy czym $|c_0|^2 + |c_1|^2 = 1$. Istotną kwantową cechą qubitu jest dychotomia pomiędzy nieobserwowalnym stanem qubitu i dokładnym wynikiem pomiaru w stanie własnym. Cecha ta jest niezwykle ważna w obliczeniach kwantowych i przetwarzaniu informacji kwantowej.

Postulat III: Ewolucja w czasie izolowanego układu kwantowego opisana jest transformacją unitarną U, czyli

$$|\psi(t_2)\rangle = U(t_1, t_2)|\psi(t_1)\rangle \ , \qquad (5)$$

przy czym $U^{-1} = U^\dagger$, gdzie symbol † oznacza sprzężenie hermitowskie, a transformacja U zależy od chwil czasowych t_1 i t_2.

Postulat III można sformułować w równoważnej postaci za pomocą równania Schrödingera

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle \ , \qquad (6)$$

gdzie $\hbar$ jest stałą Plancka ($\hbar = 1.0546 \times 10^{-34}$ Js), a H jest operatorem Hamiltona (hamiltonianem) układu. Związek pomiędzy oboma równoważnymi sformułowaniami (5) i (6) postulatu III uzyskamy znajdując jawną postać operatora ewolucji w czasie. Jest to operator

$$U(t_1, t_2) = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right] \ . \qquad (7)$$

W realizacji qubitów ważna rolę odgrywają stany stacjonarne o postaci

$$|\psi_\nu\rangle = \exp(-iE_\nu t/\hbar)|\nu\rangle \ , \qquad (8)$$

gdzie E_ν jest wartością (energią) własną operatora H, spełniającą równanie własne

$$H|\nu\rangle = E_\nu|\nu\rangle \ . \qquad (9)$$

2.2. Stany dwu-qubitowe

Stan kwantowy układu złożonego z N cząstek jest iloczynem tensorowym stanów jednocząstkowych, czyli jeżeli układy numerowane wskaźnikiem i ($i = 1, \ldots, N$) znajdują się w stanach jednocząstkowych $|\psi_i\rangle$, to stan N-cząstkowy dany jest przez $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_N\rangle$. W obliczeniach kwantowych szczególnie ważny jest stan dwu-qubitowy, który można utworzyć dysponując dwoma cząstkami (obiektami) kwantowymi o stanach bazy $\{|0\rangle, |1\rangle\}$. Zgodnie z własnościami iloczynu tensorowego stanami bazy układu złożonego z dwóch qubitów są następujące stany: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, przy czym użyta została skrócona notacja do zapisu stanów dwu-qubitowych, np. $|00\rangle \equiv |0\rangle|0\rangle \equiv |0\rangle \otimes |0\rangle$.

Wśród stanów dwu-qubitowych szczególną rolę pełnią tzw. *stany Bella*, zwane inaczej stanami EPR (od nazwisk Bell [12] oraz Einstein, Podolsky, Rosen [13], którzy pierwsi wskazali na ich dziwne własności). Stany te definiujemy jako

$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \ , \qquad (10)$$

$$|\psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \ , \qquad (11)$$

$$|\psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \ , \qquad (12)$$

$$|\psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \ . \qquad (13)$$

Matematycznie szczególna własność stanów Bella polega na ich nieseparowalności, co oznacza, że żaden ze stanów Bella nie może być zapisany w postaci iloczynu stanów jednoqubitowych $|\beta_0\rangle$ i $|\beta_1\rangle$, czyli $|\psi_{ij}\rangle \neq |\beta_i\rangle|\beta_j\rangle$, gdzie $|\beta_i\rangle \equiv |i\rangle$ oraz $i = 0, 1$. Stan kwantowy o tej własności nazywamy *stanem splątanym* (ang. *entangled state*). Fizycznie stany Bella posiadają następującą, pozornie paradoksalną, własność polegającą na tym, że wykonując pomiar na jednym qubicie stanu Bella – po wcześniejszym przygotowaniu układu w pewnym określonym stanie Bella – możemy przewidzieć *bez wykonania pomiaru* wartości drugiego qubitu z prawdopodobieństwem równym 1. Ta niezwykła własność stanów

Bella prowadzi do wielu ich zastosowań nie tylko w obliczeniach kwantowych, lecz także w kwantowej teleportacji i kryptografii. Należy podkreślić, że w mikroświecie istnienie stanów Bella jest raczej regułą niż wyjątkiem.

2.3. Qubity spinowe

Do fizycznej realizacji qubitu bardzo dobrze nadaje się spin, który można rozumieć jako wewnętrzny moment pędu cząstki. Spin jest czysto kwantową cechą cząstki. Przyjmuje on wartości dyskretne $0, 1/2, 1, 3/2, \ldots$ (w jednostkach $\hbar$). Qubity można utworzyć ze stanów spinowych pojedynczego elektronu lub jądra atomowego, a także związanej pary elektron-dziura (ekscytonu) oraz układu wielu elektronów uwięzionych w kropce kwantowej. Ze względu na ważną rolę spinu w zapisie informacji kwantowej, przedstawię najważniejsze własności spinu pojedynczej cząstki. Zajmę się cząstką o spinie $1/2$, dla której rzut spinu na wybraną oś, np. z, może przyjmować dwie wartości $\pm(\hbar/2)$. Operatorem z-owej składowej spinu jest

$$s_z = \frac{\hbar}{2}\sigma_z \,, \tag{14}$$

gdzie σ_z jest macierzą Pauliego

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \,. \tag{15}$$

Równania własne składowej z-owej spinu mają postać

$$s_z|0\rangle = +\frac{\hbar}{2}|0\rangle \,, \tag{16}$$

$$s_z|1\rangle = -\frac{\hbar}{2}|1\rangle \,, \tag{17}$$

przy czym stany własne można zapisać w postaci macierzowej jako tzw. spinory

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \,. \tag{18}$$

Ze spinem związany jest *spinowy magnetyczny moment dipolowy*, którego składowa z-owa wyraża się wzorem

$$\mu_z = -\frac{1}{2}g^\star \mu_B \sigma_z \,, \tag{19}$$

gdzie μ_B jest magnetonem Bohra ($\mu_B = 0.927 \times 10^{-23}$ Am^2), $g^\star$ jest efektywnym czynnikiem Landego, który w materiałach półprzewodnikowych może przyjmować wartości zarówno dodatnie jak i ujemne, np. dla elektronu w Si $g^\star = 1.998$, w Ge $g^\star = 1.563$, w GaAs $g^\star = -0.44$, natomiast dla elektronu w próżni $g^\star = 2.0$. Eksperymentalna detekcja spinu polega najczęściej na wykorzystaniu oddziaływania spinowego dipola magnetycznego z zewnętrznym polem magnetycznym $\mathbf{B}$. Dla $\mathbf{B} = (0, 0, B)$ operator tego oddziaływania ma postać

$$H_{int} = -\mu_z B = \frac{1}{2}g^\star \mu_B \sigma_z B \,. \tag{20}$$

Zgodnie z (14), (16) i (17) wartościami własnymi operatora σ_z są $+1$ i -1 odpowiednio w stanach $|0\rangle$ i $|1\rangle$. Zatem oddziaływanie z polem magnetycznym powoduje rozszczepienie każdego poziomu energetycznego E_ν na dwa poziomy spinowe

$$E_{\nu\pm} = E_\nu \pm \frac{1}{2}g^\star \mu_B B \,, \tag{21}$$

przy czym znak $+$ odpowiada stanowi $|0\rangle$ o spinie $+\hbar/2$, a znak $-$ odpowiada stanowi $|1\rangle$ o spinie $-\hbar/2$. Efekt opisany wzorem (21), zwany spinowym efektem Zeemana, może być obserwowany za pomocą odpowiednio czułych metod spektroskopowych. Typowa energia rozszczepienia spinowego np. w Si dla $B = 10$ T wynosi $\sim$0.6 meV, czyli odpowiada promieniowaniu o długości fali $\sim$2 mm.

2.4. Kwantowe bramki logiczne

Do wykonywania operacji na qubitach służą kwantowe bramki (operacje) logiczne, realizowane za pomocą operatorów unitarnych U, które przekształcają stan początkowy $|\psi_i\rangle$ w stan końcowy $|\psi_f\rangle$ według przepisu

$$|\psi_f\rangle = U|\psi_i\rangle \,. \tag{22}$$

Zgodnie z własnościami transformacji unitarnych w operacjach tych zachowane są wartości własne wektora własnego i unormowanie wektorów stanu. Ponadto transformacja unitarna jest liniowa, czyli $U(c_1|\psi_1\rangle + c_2|\psi_2\rangle) = c_1(U|\psi_1\rangle) + c_2(U|\psi_2\rangle)$.

Kwantowe bramki logiczne mogą być jedno-qubitowe lub wielo-qubitowe w zależności od tego, na jakie qubity działają. Jedno-qubitową bramką logiczną, będącą odpowiednikiem klasycznej bramki NOT, jest kwantowa bramka NOT, która jest zdefiniowana za pomocą macierzy

$$U_{NOT} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . \qquad (23)$$

Jeżeli stan jedno-qubitowy $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ zapiszemy w postaci macierzowej jako

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} , \qquad (24)$$

to wynikiem działania bramki NOT na pojedynczy qubit jest

$$U_{NOT} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_0 \end{pmatrix} , \qquad (25)$$

czyli stany bazy $\{|0\rangle, |1\rangle\}$ ulegają zamianie $|0\rangle \leftrightarrow |1\rangle$. Przykładami innych użytecznych w obliczeniach kwantowych bramek logicznych są bramka Z

$$U_Z \equiv \sigma_z , \qquad (26)$$

czyli z-owa macierz Pauliego, oraz bramka Hadamarda o postaci

$$U_H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \qquad (27)$$

Ważną dwu-qubitową bramką logiczną jest bramka kontrolowanej negacji U_{CN} (ang. *controlled*-NOT lub CNOT), która działa na stan dwu-qubitowy $|\beta_1, \beta_2\rangle \equiv |\beta_1\rangle|\beta_2\rangle$, przy czym pierwszy qubit ($|\beta_1\rangle$) jest qubitem kontrolnym, a drugi qubit ($|\beta_2\rangle$) jest qubitem wynikowym (ang. *target qubit*). Bramkę tę można zdefiniować określając jej działanie na stany bazy dwu-qubitowej

$$\begin{aligned} U_{CN}|00\rangle &= |00\rangle , \quad U_{CN}|01\rangle = |01\rangle , \\ U_{CN}|10\rangle &= |11\rangle , \quad U_{CN}|11\rangle = |10\rangle , \end{aligned} \qquad (28)$$

czyli wynikiem działania bramki U_{CN} jest zmiana stanu drugiego qubitu wtedy i tylko wtedy gdy pierwszy qubit znajduje się w stanie $|1\rangle$.

Pokazano [7], że zbiór operacji logicznych, który zawiera wszystkie bramki jedno-qubitowe oraz bramkę dwu-qubitową U_{CN} jest *uniwersalny* w tym sensie, że wszystkie operacje unitarne na stanach N-qubitowych, gdzie N jest dowolne, można wyrazić przez różne kompozycje tych bramek. Niezwykle istotną własnością algorytmów kwantowych jest ich *równoległość*, która polega na tym, że pojedyncza operacja unitarna może działać równocześnie na wszystkie qubity w układzie. Równoległość obliczeń kwantowych jest immanentną cechą układu kwantowego, w więc do jej realizacji nie są konieczne żadne dodatkowe rozwiązania technologiczne.

2.5. Kwantowa maszyna Turinga

Najbardziej popularnym modelem matematycznym klasycznego komputera jest model uniwersalnej maszyny Turinga. Okazuje się, że odpowiednio uogólniona klasyczna teoria obliczeń może stanowić podstawę modelu komputera kwantowego. W tym podrozdziale przedstawię zwięźle koncepcję klasycznej maszyny Turinga, a następnie jej uogólnienie na przypadek kwantowy.

Klasyczna maszyna Turinga jest urządzaniem złożonym z procesora w postaci głowicy zapisu/odczytu i pamięci o nieograniczonej pojemności w postaci nieskończonej taśmy. Taśma jest podzielona na dyskretne komórki. W każdej komórce może być zapisany jeden symbol z pewnego skończonego alfabetu, np. jeden bit klasyczny. Głowica skanuje taśmę w dyskretnych krokach czasowych. W każdym kroku czasowym głowica znajduje się w jednym ze stanów $h \in \{h_0, h_1, \ldots, h_n\}$. Działanie maszyny Turinga polega na wykonywaniu dyskretnych kroków, przy czym każdy krok jest określony przez dwa warunki początkowe: aktualny stan głowicy h i symbol t zapisany w aktualnie skanowanej komórce taśmy. Dla określonej pary warunków początkowych (h, t) maszyna otrzymuje trzy-częściową instrukcję dotycząca kolejnego kroku. Pierwsza część instrukcji określa kolejny stan głowicy h', druga jej część określa symbol t', który głowica zapisuje w skanowanej aktualnie komórce taśmy, a trzecia część instrukcji specyfikuje, zgodnie z wartością zmiennej d, kolejny

ruch głowicy: przejście do kolejnej komórki w lewo ($d = -1$), w prawo ($d = +1$), lub brak ruchu ($d = 0$). Opis matematyczny *deterministycznej maszyny Turinga* uzyskujemy definiując funkcję

$$w = f(h, t, h', t', d) \ . \qquad (29)$$

Obliczenia nie muszą przebiegać w sposób deterministyczny. W działaniu maszyny Turinga można dopuścić przypadkowość w wyborze kolejnych kroków. Takie probabilistyczne obliczenia można sobie wyobrazić w postaci rozgałęziającego się grafu, którego każdy węzeł odpowiada pewnemu stanowi maszyny, a każdy odcinek łączący kolejne węzły odpowiada kolejnemu krokowi obliczeniowemu. Obliczenia zaczynają się w pewnym węźle początkowym, który reprezentuje warunki początkowe, i rozgałęziają się na inne węzły osiągane z pewnymi niezerowymi prawdopodobieństwami p_i. Działanie *probabilistycznej maszyny Turinga* polega na wykonywaniu każdej kolejnej instrukcji z prawdopodobieństwem p_i, które zależy od tych samych zmiennych, co funkcja f występująca we wzorze (29), czyli

$$p_i = p_i(h, t, h', t', d) \ . \qquad (30)$$

Algorytmy probabilistyczne mogą rozwiązywać niektóre problemy, np. znajdowanie ekstremum funkcji wielu zmiennych, szybciej niż znane algorytmy deterministyczne.

Przedstawiony powyżej model klasycznej probabilistycznej maszyny Turinga można w sposób naturalny uogólnić do modelu *kwantowej maszyny Turinga*. W modelu kwantowym prawdopodobieństwo p_i wykonania i-tej instrukcji zastępujemy amplitudą prawdopodobieństwa a_i, która zależy od tych samych zmiennych co p_i [wzór (30)], czyli

$$a_i = a_i(h, t, h', t', d) \ , \qquad (31)$$

przy czym a_i jest na ogół liczbą zespoloną. Zgodnie z postulatami mechaniki kwantowej prawdopodobieństwo p_i wykonania i-tej instrukcji dane jest przez

$$p_i = |a_i|^2 \ . \qquad (32)$$

Przejście do amplitud kwantowych prowadzi do wielu nowych efektów. Jednym z nich jest *interferencja kwantowa*, polegająca na tym, że dodawanie prawdopodobieństw osiągnięcia określonego stanu kwantowego po dwóch możliwych drogach odbywa się zgodnie ze wzorem interferencyjnym

$$|a_{12}|^2 = |a_1|^2 + |a_2|^2 + 2|a_1||a_2| \cos\theta \ , \quad (33)$$

gdzie θ jest różnicą faz amplitud a_1 i a_2. Interferencja kwantowa prowadzi do ciekawej nowej własności komputera kwantowego, która polega na tym, że obliczenia kwantowe mogą przebiegać wieloma różnymi drogami obliczeniowymi, a ich wynik zależy od interferencji amplitud. Taki przebieg obliczeń kwantowych jest istotnie różny od przebiegu obliczeń w klasycznej probabilistycznej maszynie Turinga, w której wybierana jest wyłącznie jedna droga obliczeń.

Należy zaznaczyć, że – ze względu na daleko posuniętą idealizację – model kwantowej maszyny Turinga, podobnie jak jego odpowiednik klasyczny, stanowi jedynie ilustrację idei działania komputera kwantowego. W szczególności, żadnego z modeli maszyny Turinga nie można użyć w praktyce jako planu konstrukcji komputera.

2.6. Warunki realizacji fizycznej obliczeń kwantowych

Przy konstrukcji komputera kwantowego, czyli aparatury fizycznej wykonującej obliczenia kwantowe, musimy się zmierzyć przede wszystkim z problemem utrzymania kontrolowanej ewolucji unitarnej układu kwantowego do czasu zakończenia obliczeń. Taka kontrolowana ewolucja jest możliwa pod warunkiem całkowitej izolacji układu kwantowego od otoczenia. Pełna izolacja układu kwantowego uniemożliwia jednak procesy zapisu/odczytu informacji kwantowej. Tak więc pewne niewielkie oddziaływanie układu z otoczeniem jest konieczne. Oddziaływanie to prowadzi do niekorzystnych z punktu widzenia obliczeń kwantowych procesów rozpadu i dekoherecji stanu qubitowego.

W procesie *rozpadu* układ kwantowy w bardzo krótkim czasie przechodzi do nowego

stanu oddając przy tym swoją energię do otoczenia, np. dla spinu zmianie stanu $|0\rangle \rightarrow |1\rangle$ towarzyszy emisja fotonu o odpowiedniej energii. *Dekoherencja* jest zjawiskiem subtelniejszym, w którym (z zachowaniem energii) zmianie ulega względna faza różnych składników kwantowej superpozycji stanów, np. qubit ulega następującej zmianie:

$$|\psi\rangle \rightarrow c_0|0\rangle + e^{i\theta}c_1|1\rangle \ , \qquad (34)$$

gdzie liczba rzeczywista θ oznacza względną fazę. Pojawienie się względnej różnicy faz pomiędzy stanami bazy obliczeniowej może prowadzić do istotnych zmian w statystyce pomiarów. Czas dekoherencji t_{decoh} jest na ogół znacznie krótszy od czasu rozpadu stanu kwantowego, zatem będzie on określał stosowalność różnych technologii do konstrukcji komputera kwantowego. Ilościową miarą użyteczności wybranej technologii do obliczeń kwantowych jest stosunek czasu dekoherencji t_{decoh} do czasu elementarnej operacji t_{oper}, czyli

$$R = \frac{t_{decoh}}{t_{oper}} \ . \qquad (35)$$

Dla różnych obecnie rozważanych technologii wartość tego stosunku zmienia się w granicach: $10^3 \leq R \leq 10^{13}$. Wartość R jest bardzo przybliżoną miarą liczby kwantowych operacji logicznych, które komputer kwantowy może wykonać zanim pojedynczy qubit ulegnie dekoherencji.

Poza koniecznością uwzględnienia rozpadu i dekoherencji qubitów technologia obliczeń kwantowych musi spełniać następujące warunki: (i) realizowalność fizyczna qubitów; (ii) możliwość precyzyjnego przygotowania początkowego stanu qubitu; (iii) wykonalność kontrolowalnej ewolucji unitarnej qubitu; (iv) możliwość wykonania pomiaru stanu końcowego qubitu. Rozważając układ fizyczny wybrany do realizacji obliczeń kwantowych musimy podać, jakie własności fizyczne posłużą nam do realizacji qubitów (może to być np. spin elektronu, jądra atomowego lub fotonu) oraz jakie procesy fizyczne umożliwią nam zapis i odczyt qubitów (mogą to być np. przejścia promieniste z emisją/absorpcją fotonów).

3. Kropki kwantowe

Półprzewodnikowe kropki kwantowe są strukturami o wszystkich trzech rozmiarach przestrzennych poniżej 1 μm. Typowe rozmiary kropek kwantowych zawarte w przedziale od $\sim$10 nm do $\sim$100 nm. W nanostrukturach tych wytworzony jest potencjał ograniczający ruch nośników ładunku (tzw. potencjał uwięzienia) o zasięgu porównywalnym z rozmiarami przestrzennymi kropki i skończonej głębokości. Typowa głębokość potencjału uwięzienia, czyli położenie minimum energii potencjalnej elektronu mierzone względem dna pasma przewodnictwa materiału otaczającego kropkę, jest rzędu od $\sim$0.1 eV do $\sim$ 1 eV), co prowadzi do różnic energii poziomów jednoelektronowych rzędu kilku meV. Te odległości energetyczne prowadzą do dodatkowego warunku wykonalności obliczeń kwantowych, którym jest brak wzbudzeń termicznych. Oznacza to, że w otrzymywanych obecnie nanostrukturach musi być zachowana temperatura poniżej 1 K.

Najczęściej badanymi obecnie kropkami kwantowymi są tzw. kropki samozorganizowane i kropki elektrostatyczne. *Kropki samozorganizowane (samorosnące)* wytwarzane są w procesie wzrostu warstw w technologii epitaksji z wiązek molekularnych (MBE). Przy wzroście półprzewodnika typu A na podłożu złożonym z półprzewodnika typu B, wskutek naprężeń spowodowanych różnicą stałych sieci pomiędzy materiałami A i B, powstaje struktura wyspowa o uporządkowanym rozkładzie wysp o regularnych kształtach i rozmiarach. Każda wyspa, której kształt jest najczęściej piramoidalny lub słupkowy, stanowi kropkę kwantową. Kolejne nanoszone warstwy (półprzewodnikowe i metaliczne) umożliwiają podłączenie kropek do zewnętrznego układu elektronicznego. W kropkach samozorganizowanych potencjał uwięzienia powstaje wskutek różnicy położeń na skali energii dna pasma przewodnictwa (wierzchołka pasma walencyjnego) pomiędzy półprzewodnikami A i B. Potencjał ten modyfikowany jest przez naprężenia wewnętrzne w kropce i modulację składu kropki wskutek dyfuzji atomów pomiędzy materiałami A i B.

Kropki elektrostatyczne (sterowane bramką) wytwarzane są najczęściej z uzyskanych wcześniej metodą MBE warstw półprzewodnikowych tworzących studnie kwantowe (pojedyncze lub wielokrotne) w złożonym procesie technologicznym kolejnego wytrawiania i nakładania elektrod metalicznych. W rezultacie powstają pojedyncze nanostruktury zwykle o kształcie słupków cylindrycznych lub prostopadłościennych. Każdy słupek może zawierać pojedynczą izolowaną kropkę kwantową lub wielokrotne sprzężone kropki kwantowe, oddzielone od siebie barierami potencjału. W kropce elektrostatycznej istnieje możliwość naniesienia dodatkowej elektrody (bramki) na powierzchnię boczną słupka, co znacznie zwiększa możliwości sterowania polem elektrostatycznym wewnątrz kropki. Potencjał uwięzienia wytworzony jest zarówno przez różnice w położeniu ekstremów pasm jak i przez zewnętrzne pole elektrostatyczne bramki. Znajomość tego potencjału jest istotna do poznania i modelowania własności elektronowych kropki kwantowej. Potencjału tego nie można bezpośrednio zmierzyć, natomiast może on być obliczony z pierwszych zasad elektrostatyki przez rozwiązanie równania Poissona dla całej nanostruktury. Obliczenia takie wykonano [15, 16] dla dwóch typów elektrostatycznych kropek kwantowych różniących się kształtem. Były to kropki kwantowe o symetrii cylindrycznej i kształcie pionowych słupków [14] oraz kropki w strukturze warstwowej przykrytej kapturkiem [17]. Uzyskane wyniki [16] pokazują, że potencjał uwięzienia V można sparametryzować za pomocą funkcji Gaussa [18] lub funkcji potęgowo-wykładniczej [19] o postaci

$$V = -V_0 \exp[-(r/R)^p - (|z|/Z)^p] \,, \quad (36)$$

gdzie $V_0 > 0$ jest głębokością jamy potencjału, $r = \sqrt{x^2 + y^2}$, $p > 1$, a R oraz Z są miarami zasięgu potencjału uwięzienia odpowiednio w kierunkach x, y oraz z. Dla $p = 2$ otrzymujemy potencjał gaussowski, a dla $p > 10$ potencjał uwięzienia przypomina prostokątną studnię potencjału.

Elektrony uwięzione w kropce kwantowej tworzą zlokalizowane stany związane o dyskretnych poziomach energetycznych. Stany te wykazują jakościowe podobieństwo do stanów elektronów związanych w atomach naturalnych, stąd nazwa *sztuczny atom*. Dwie kropki kwantowe oddzielone barierą potencjału tworzą *sztuczną molekułę* [20]. Własności elektronowe sztucznych atomów i molekuł są przedmiotem intensywnych badań eksperymentalnych i teoretycznych. Z punktu widzenia zastosowań do obliczeń kwantowych istotną rolę odgrywa transport jednoelektronowy przez kropkę kwantową. Głównym kanałem tego transportu jest proces tunelowania sekwencyjnego, w którym w kolejnych chwilach czasu przez kropkę tunelują pojedyncze elektrony, jeżeli spełnione są warunki transportu [21]. Metodą transportu jednoelektronowego odkryte zostały niezwykłe własności kropek kwantowych: zapełnianie powłok elektronowych sztucznego atomu [14] i kwantowa blokada kulombowska [22]. Ilościowy opis teoretyczny tych zjawisk został podany w pracy [15]. Słupkowa kropka kwantowa sterowana bramką [14] stanowi prototyp tranzystora jednoelektronowego, w którym możemy kontrolować przepływ pojedynczych elektronów. W perspektywie zastosowanie tranzystorów jednoelektronowych dałoby znaczne zwiększenie szybkości działania urządzeń elektronicznych przy znacznie zmniejszonych stratach energii.

Ostatnio szeroko badane są możliwości wykonywania obliczeń kwantowych na kropkach kwantowych. Do zapisu/odczytu informacji mogą być wykorzystywane stany kwantowe elektronów uwięzionych w kropkach kwantowych, a w szczególności elektronowe stany spinowe. Wydaje się, że zwłaszcza elektrostatyczne kropki kwantowe bardzo dobrze nadają się do realizacji fizycznej qubitów oraz operacji na nich, ponieważ własności elektronowe tych kropek mogą być modelowane przez odpowiedni dobór parametrów nanostruktury oraz sterowane przez zmianę napięć zewnętrznych przyłożonych do elektrod. Umożliwia to zarówno uzyskiwanie pożądanych własności stanów kwanto-

wych (inżynieria kwantowa) jak i przeprowadzanie na nich kontrolowanych operacji logicznych. Ponadto technologia otrzymywania kropek kwantowych stanowi rozwinięcie znanych i dobrze opanowanych technologii warstwowych przyrządów półprzewodnikowych (tranzystory FET). W związku z tym jest znacznie łatwiejsza do wprowadzenia do produkcji niż np. otrzymywane dotąd wyłącznie na skalę laboratoryjną pułapki jonowe i atomowe. Ważna jest też możliwość podłączenia układu kropek kwantowych do odpowiednio czułej aparatury elektronicznej.

4. Realizacja qubitu i bramek logicznych w kropkach kwantowych

W kropkach kwantowych qubitami mogą być stany ekscytonowe lub stany spinowe elektronów. Ekscyton, czyli układ związany elektron-dziura, powstaje w wyniku absorpcji światła o energii porównywalnej z energią przerwy wzbronionej półprzewodnika. Po upływie czasu życia rzędu mikrosekund ekscyton ulega rekombinacji z emisją fotonu. Qubit ekscytonowy może być zrealizowany w prosty sposób: istniejącemu ekscytonowi w związanym stanie podstawowym można przypisać stan $|1\rangle$, a układowi po rekombinacji, czyli brakowi ekscytonu, można przypisać stan $|0\rangle$. Wadą tej koncepcji jest krótki czas rozpadu (czas życia) ekscytonu, natomiast zaletą jest łatwy zapis/odczyt informacji za pomocą fotonów światła widzialnego w procesach absorpcji/emisji. Badane jest również możliwe zastosowanie biekscytonów, czyli układów związanych dwóch ekscytonów, jako qubitów [23].

Obecnie wydaje się, że najbardziej obiecujące jest wykorzystanie spinu elektronu do konstrukcji qubitów i kontrolowanych operacji na nich. Zaletami stanów elektronowych o określonym spinie są: bardzo długi czas życia (teoretycznie brak rozpadu), dość długi czas dekoherencji (nieco poniżej mikrosekundy) [24], oraz możliwość manipulowania spinem, np. za pomocą zewnętrznego pola magnetycznego. Badanie zastosowania spinu jako nowego nośnika informacji jest przedmiotem nowej dziedziny elektroniki opartej na spinie, tzw. *spintroniki* [25, 26]. Spin może być użyty do konstrukcji qubitów i operacji na nich bądź bezpośrednio z wykorzystaniem sprzężenia spinowego magnetycznego momentu dipolowego z polem magnetycznym (podrozdział 2.3) bądź pośrednio z wykorzystaniem własności symetrii wieloelektronowej funkcji falowej (2). Pośrednie wykorzystanie spinu do reprezentacji qubitu opiera się na zmianie znaku (antysymetrii) funkcji falowej (2) przy zamianie współrzędnych przestrzenno-spinowych dwóch elektronów. Własność ta, która stanowi podstawę statystyki kwantowej, prowadzi do określonej symetrii stanów spinowych w podprzestrzeni stanów o określonym spinie. Na przykład, w układzie dwóch elektronów spinowy stan singletowy (antysymetryczny względem zamiany zmiennych spinowych) posiada różną (na ogół niższą) energię od stanów trypletowych (symetrycznych przy zamianie zmiennych spinowych). Rozszczepienie energetyczne singlet-tryplet może być wykorzystane do rozróżnienia tych stanów i operacji logicznych na nich.

W rozdziale tym przedstawię nieco dokładniej bezpośredni sposób wykorzystania stanów spinowych elektronów uwięzionych w kropce kwantowej do realizacji obliczeń kwantowych. W tym przypadku bazę obliczeniową mogą stanowić stany własne składowej z-owej spinu (podrozdział 2.3). Ze względu na uniwersalny charakter bramki logicznej kontrolowanej negacji (CNOT), przedyskutuję jej możliwą realizację za pomocą sprzężonych kropek kwantowych. Działanie bramki CNOT na stany bazy dwu-qubitowej podaje układ równań (28). Rozważmy układ dwóch elektronów w dwóch sprzężonych kropkach kwantowych, numerowanych wskaźnikiem $j = 1, 2$. Przypuśćmy, że w każdej kropce uwięziony jest jeden elektron. Jeżeli każda kropka zbudowana jest z innego materiału półprzewodnikowego, to efektywne czynniki Landego się różnią $g_1^\star \neq g_2^\star$. Zgodnie z (21) prowadzi to do różnej energii Zeemana elektronu w każdej z kropek. Podobny efekt można osiągnąć stosując niejednorodne pole magnetyczne (różne w każdej z kropek, które w tym przypadku mogą mieć jedna-

kowy skład). Skład i rozmiary bariery pomiędzy kropkami dobieramy tak, aby zapewnione było słabe sprzężenie pomiędzy spinami obu elektronów.

Hamiltonian układu można zapisać w postaci

$$H = H_1 + H_2 + H_{int} \ , \tag{37}$$

gdzie H_j $(j = 1, 2)$ jest hamiltonianem jednocząstkowym elektronu o spinie $s_{z,j}$ w zewnętrznym polu magnetycznym, czyli

$$H_j = \omega_j s_{z,j} \ , \tag{38}$$

przy czym $\omega_j = g_j^\star \mu_B B_j/\hbar$ [por. równanie (20)], B_j jest polem magnetycznym w j-tej kropce. Hamiltonian oddziaływania dany jest wzorem

$$H_{int} = (4/\hbar)\Omega s_{z,1} s_{z,2} \ , \tag{39}$$

gdzie parametr Ω charakteryzuje sprzężenie pomiędzy spinami elektronów w różnych kropkach. Operatory $s_{z,j}$ spełniają równania własne

$$s_{z,1}|0,k\rangle == +\frac{\hbar}{2}|0,k\rangle \tag{40}$$

oraz

$$s_{z,1}|1,k\rangle = -\frac{\hbar}{2}|1,k\rangle \ , \tag{41}$$

gdzie $k = 0, 1$. Podobne dwa równania są spełnione dla $s_{z,2}$. Zgodnie z założonymi powyżej warunkami $\omega_1 \neq \omega_2$.

Przy braku sprzężenia $(\Omega = 0)$ hamiltonian (37) posiada następujące wartości własne: $\epsilon_1 = -(\hbar/2)(\omega_1 + \omega_2)$ w stanie $|1,1\rangle$, $\epsilon_2 = -(\hbar/2)(\omega_1 - \omega_2)$ w stanie $|1,0\rangle$, $\epsilon_3 = (\hbar/2)(\omega_1 - \omega_2)$ w stanie $|0,1\rangle$ i $\epsilon_4 = (\hbar/2)(\omega_1 + \omega_2)$ w stanie $|0,0\rangle$. Brak sprzężenia może być zrealizowany przez odpowiednie zwiększenie szerokości bariery pomiędzy kropkami. Każdy stan spinowy może być zmieniany w sposób selektywny w procesach absorpcji lub emisji fotonów o odpowiedniej częstości. Na przykład, w procesie absorpcji foton o częstości ω_1 działa wyłącznie na pierwszy qubit zmieniając go ze stanu $|1,k\rangle$ (o spinie w dół) w stan $|0,k\rangle$ (o spinie w górę). Możliwa jest też zmiana odwrotna, tzn. $|0,k\rangle \rightarrow |1,k\rangle$, w procesie emisji wymuszonej. Procesy te zachodzą dla każdego k $(k = 0, 1)$, czyli dla dowolnego stanu drugiego qubitu. Podobnie foton o częstości ω_2 będzie zmieniał wyłącznie stan drugiego qubitu.

Przypadek włączonego sprzężenia pomiędzy spinami $(\Omega > 0)$ można opisać korzystając z rozwiązań równania własnego hamiltonianu (37), który jest diagonalny w bazie stanów

$$\{|1,1\rangle, |1,0\rangle, |0,1\rangle, |0,0\rangle\} \ . \tag{42}$$

W kolejnych stanach bazy (42) odpowiednie wartości własne energii są teraz równe: $E_1 = \epsilon_1 + \hbar\Omega$, $E_2 = \epsilon_2 - \hbar\Omega$, $E_3 = \epsilon_3 - \hbar\Omega$, $E_4 = \epsilon_4 + \hbar\Omega$. Oznacza to, że po włączeniu oddziaływania energie własne ulegają zmianie o $\pm\hbar\Omega$, natomiast stany własne pozostają niezmienione. Umożliwia to wymuszanie wybranych przejść pomiędzy stanami bazy (42). Padające na układ kropek kwantowych promieniowanie o dokładnie dobranej częstości rezonansowej powoduje selektywne przełączanie pomiędzy stanami bazy połączone ze zmianą jednego qubitu w zależności od stanu drugiego qubitu. Na przykład foton o częstości $\omega_2 - 2\Omega$ powoduje przełączanie wyłącznie pomiędzy stanami $|1,0\rangle$ i $|1,1\rangle$ zachowując stany $|0,0\rangle$ i $|0,1\rangle$ bez zmian. Tak więc w procesach z udziałem tego fotonu realizowana jest operacja CNOT.

Powyższa propozycja realizacji bramki logicznej CNOT jest modelem uproszczonym ze względu na uproszczony opis oddziaływania pomiędzy spinami. Z drugiej strony hamiltonian oddziaływania (39) posiada postać hamiltonianu Heisenberga, który jest uniwersalnym hamiltonianem oddziaływania. Może on być stosowany do opisu różnych obiektów fizycznych obdarzonych spinem, np. jonów, jąder atomowych, par Coopera w nadprzewodniku. Podany model bramki logicznej CNOT może być zrealizowany zarówno w sprzężonych kropkach kwantowych jak i w układzie NMR.

Należy dodać, że badane są też inne sposoby zapisu/odczytu informacji kwantowej z wykorzystaniem spinu elektronu uwięzionego w kropce kwantowej [25]. Są to: (i) pomiar magnetyzacji spontanicznej kropki kwanto-

wej, (ii) pomiar spinu przez pomiar ładunku (wykorzystywany jest przy tym tzw. filtr spinowy, który pozwala na wytworzenie w półprzewodniku prądu elektronów o określonym spinie), (iii) elektronowy rezonans spinowy, (iv) pomiar rozszczepienia singlet-tryplet za pomocą rotacji Faradaya.

5. Podsumowanie

Mechanika kwantowa dostarcza fizycznych podstaw do wykonywania obliczeń według nowych (kwantowych) algorytmów oraz zapisu informacji w postaci bitów kwantowych. Kwantowe podejście do obliczeń posiada obecnie solidne podstawy teoretyczne, będące połączeniem teorii fizycznych, matematycznych i informatycznych. Kwantowa teoria obliczeń pokazuje [10], że możliwe jest bezpośrednie wykorzystanie kwantowej natury mikroświata do niezwykle gęstego upakowania informacji i bardzo szybkiego jej przetwarzania. Badane są różne fizyczne realizacje obliczeń kwantowych: pułapki jonowe i atomowe, jądrowy rezonans magnetyczny, nadprzewodniki oraz kropki kwantowe. Do zapisu informacji kwantowej w postaci qubitów szczególnie dobrze nadaje się spin cząstek. Mogą być w tym celu wykorzystywane elektrony, fotony i jądra atomowe. Użycie spinu elektronu (zamiast jego ładunku) do zapisu informacji jest obecnie niezwykle intensywnie badane. Badania te doprowadziły do powstania nowej gałęzi elektroniki: elektroniki spinowej (spintroniki). Projektowana konstrukcja przyrządów spintroniki przy użyciu nanostruktur półprzewodnikowych stanowi naturalną kontynuację dotychczasowego trendu rozwoju elektroniki, ale z wykorzystaniem nowych jakościowo zjawisk. W badaniach tych szczególną rolę odgrywają kropki kwantowe, które są nanostrukturami półprzewodnikowymi bardzo obiecującymi z punktu widzenia możliwej realizacji zarówno obliczeń kwantowych jak i tranzystora jednolektronowego. Niezwykle korzystną w zastosowaniach cechą kropek kwantowych możliwość sterowania ich własnościami elektronowymi za pomocą zewnętrznych pól elektromagnetycznych, co pozwala na uzyskiwanie pożądanych charakterystyk oraz ich zmianę w bardzo krótkim czasie. Wydaje się, że dzięki swej elastyczności kropki kwantowe staną się podstawowymi elementami przyszłych komputerów kwantowych.

Podsumowując, obecny stan wiedzy w zakresie komputerów kwantowych charakteryzuje się zaawansowaną fazą rozwoju teorii obliczeń kwantowych. Natomiast możliwe konstrukcje komputera kwantowego są dopiero w fazie badań laboratoryjnych.

6. Podziękowania

Autor dziękuje dr. hab. Stanisławowi Bednarkowi i dr. Bartłomiejowi Szafranowi za inspirujące dyskusje naukowe.

Literatura

[1] R.P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[2] R.P. Feynman, Foundations of Physics, **16**, 507 (1986) [tłum. polskie: Postępy Fizyki **39**, 411 (1988)].

[3] D. Deutsch, Proc. Royal Soc. London A **400**, 97 (1985).

[4] P.W. Shor, Proc. 35th Annual Symposium on Foundations of Computer Science, ed. S. Goldwasser (IEEE Computer Society, Los Alamos, CA, 1994), p. 124.

[5] L.K. Grover, Proc. 28th Annual ACM Symposium on the Theory of Computing (ACM Press, New York, 1996), p. 212.

[6] W.K. Wooters, W.H Żurek, Nature **299**, 802 (1982).

[7] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolib, H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[8] A.R. Calderbank, P.W. Shor, Phys. Rev. A **54**, 1098 (1996).

[9] A. Ekert, R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996).

[10] M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, UK, 2000).

[11] M. Hirvensalo, *Quantum Computing* (Springer-Verlag, Berlin, 2001).

[12] J.S. Bell, Physics **1**, 195 (1964).
[13] A. Einstein, B. Podolsky, N. Rosen, Phys. Rev. **47**, 777 (1935).
[14] S. Tarucha, D.G. Austing, T. Honda, R.J. van der Hage, L.P. Kouwenhoven, Phys. Rev. Lett. **77**, 3613 (1996).
[15] S. Bednarek, B. Szafran, J. Adamowski, Phys. Rev. B **64**, 195303 (2001).
[16] S. Bednarek, B. Szafran, K.Lis, J. Adamowski, Phys. Rev. B (2003) - w druku.
[17] R.C. Ashoori, H.L. Stormer, J.S. Weiner, L.N. Pfeiffer, K.W. Baldwin, K.W. West, Phys. Rev. Lett. **71**, 613 (1993).
[18] J. Adamowski, M. Sobkowicz, B. Szafran, S. Bednarek, Phys. Rev. B **62**, 4234 (2000).
[19] M. Ciurla, J. Adamowski, B. Szafran, S. Bednarek, Physica E **15**, 261 (2002).
[20] S. Bednarek, T. Chwiej, J. Adamowski, B. Szafran, Phys. Rev. B **67**, 205316 (2003).
[21] J. Adamowski, S. Bednarek, B. Szafran, Acta Phys. Polon. A **100**, 145 (2001).
[22] L.P. Kouwenhoven, T.H. Oosterkamp, M.W.S. Danoesastro, M. Eto, D.G. Austing, T. Honda, S. Tarucha, Science **278**, 1788 (1997).
[23] O. Gywat, G. Burkard, D. Loss, cond-mat/0109223.
[24] J.M. Kikkawa, D.D. Awschalom, Phys. Rev. Lett. **80**, 4313 (1998).
[25] *Semiconductor Spintronics and Quantum Computation*, eds. D.D. Awschalom, D. Loss, N. Samarth (Springer-Verlag, Berlin, 2002).
[26] S.A. Wolf, A.Y. Chtchelkanova, D.M. Treger, "Spintronics – Spin-Based Electronics", *Handbook of Nanoscience, Engineering, and Technology*, eds. W.A. Goddard III, D.W. Brenner, S.E. Lyshevski, G.J. Iafrate (CRC Press, Boca Raton, 2003).