Podstawy informatyki kwantowej

Jerzy KLAMKA

1. Wprowadzenie

2. Qubity

2.1. Qubity w zapisie wektorowym

W klasycznej informatyce pojedynczy bit może przyjmować tylko dwie ustalone wartości logiczne to znaczy 0 lub 1. Natomiast elementarną jednostką kwantowej informatyki jest kwantowy bit zwany qubitem oraz oznaczony symbolem $|\psi\rangle$.

W opisie matematycznym pojedynczy qubit $|\psi\rangle$ jest dwuwymiarowym znormalizowanym (o długości 1), wektorem o współczynnikach zespolonych, a więc jest elementem 2-wymiarowej zespolonej przestrzeni $\mathbf{C}^2$. Dwa ortogonalne stany dla pojedynczego qubitu są postaci $\{|0\rangle,|1\rangle\}$ i tworzą one bazę ortogonalną

$$\left\{\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right\}$$

w 2-wymiarowej zespolonej przestrzeni $\mathbf{C}^2$.

W zapisie tym wektory bazowe

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}\in\mathbf{C}^2 \qquad\qquad |1\rangle=\begin{bmatrix}0\\1\end{bmatrix}\in\mathbf{C}^2$$

reprezentują odpowiednio wartości logiczne 0 oraz 1 klasycznego bitu algebry Boole'a.

Dowolny qubit $|\psi\rangle \in C^2$ może być przedstawiony w postaci liniowej kombinacji wektorów bazowych

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \alpha|1\rangle + \beta|0\rangle ,$$

gdzie liczby zespolone α oraz β nazywane są amplitudami prawdopodobieństwa, natomiast wektor $|\psi\rangle$ jest wektorem znormalizowanym o długości 1 to znaczy $|\alpha|^2 + |\beta|^2 = 1$ [1], [3], [8].

Oznacza to, że qubit $|\psi\rangle \in C^2$ przyjmuje wartość logiczną 0 z prawdopodobieństwem $|\alpha|^2$ oraz wartość logiczną 1 z prawdopodobieństwem $|\beta|^2$.

Przestrzenią stanów kwantowych dla 2 qubitów jest iloczyn tensorowy (oznaczony symbolem ⊗) przestrzeni stanów kwantowych dla pojedynczych qubitów. W przypadku 2 qubitów jest to 4-wymiarowa przestrzeń zespolona $C^4=C^2 \otimes C^2$. Przykładowo, iloczyn tensorowy dwóch dowolnych qubitów postaci

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle=\begin{bmatrix}\alpha\\ \beta\end{bmatrix}\in C^2$$

oraz

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle=\begin{bmatrix}\gamma\\ \delta\end{bmatrix}\in C^2,$$

będący wektorem w 4-wymiarowej zespolonej przestrzeni C^4 jest dany następującym wzorem:

$$|\psi\phi\rangle = |\psi\rangle \otimes |\phi\rangle = \alpha|0\rangle+\beta|1\rangle \otimes \alpha|0\rangle+\beta|1\rangle =$$

$$=\left(\alpha\begin{bmatrix}1\\0\end{bmatrix}+\beta\begin{bmatrix}0\\1\end{bmatrix}\right)\otimes\left(\gamma\begin{bmatrix}1\\0\end{bmatrix}+\delta\begin{bmatrix}0\\1\end{bmatrix}\right)=\begin{bmatrix}\alpha\\ \beta\end{bmatrix}\otimes\begin{bmatrix}\gamma\\ \delta\end{bmatrix}=$$

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

$$=\alpha\gamma|0\rangle + \alpha\delta|1\rangle + \beta\gamma|2\rangle + \beta\delta|3\rangle=$$

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

Iloczyn tensorowy wektorów jest działaniem łącznym ale nie jest przemienny to znaczy

$$|\psi\rangle \otimes |\varphi\rangle \neq |\varphi\rangle \otimes |\psi\rangle$$

Ogólnie, układ kwantowy złożony z n qubitów można rozpatrywać jako wektor w 2^n-wymiarowej zespolonej przestrzeni C^{2^n}, która jest iloczynem tensorowym n 2-wymiarowych przestrzeni zespolonych C^2, czyli

$$C^{2^n} = \underbrace{C^2 \otimes C^2 \otimes ... \otimes C^2}_{n-razy}$$

która zawiera 2^n wzajemnie ortogonalnych stanów postaci

$\{|0\rangle,|1\rangle,...,|i\rangle,...,|2^n-1\rangle\}$,

gdzie i jest liczbą naturalną przedstawioną za pomocą n-bitowego kodu binarnego, i=0,1,2,...,2^n-1.

W tym przypadku stosuje się również równoważny zapis wykorzystujący bezpośrednio wagowy kod binarny liczby naturalnej

$$i = \sum_{k=0}^{k=n-1} a_k 2^k ,$$

to znaczy

$|i\rangle=|a_{n-1}a_{n-2}...a_k...a_1a_0\rangle$

gdzie a_k, k=0,1,2,...,(n-1) przyjmujące wartości 0 lub 1 są współczynnikami odpowiadającymi wagom 2^k, k=0,1,2,...,(n-1).

Zatem, wektor $|i\rangle \in C^{2^n}$ posiada 1 na (i+1) pozycji a zera na wszystkich pozostałych. Wykorzystując iloczyn tensorowy wektor $|i\rangle$ można przedstawić w następującej postaci

$$|i\rangle = |a_{n-1}a_{n-2}\ldots a_k\ldots a_1a_0\rangle = |a_{n-1}\rangle \otimes |a_{n-2}\rangle \otimes \ldots \otimes |a_k\rangle \otimes \ldots \otimes |a_1\rangle \otimes |a_0\rangle$$

Ponadto, 2^n-wymiarowe wektory postaci

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

tworzą bazę ortogonalną w zespolonej przestrzeni C^{2^n}.

Układ kwantowy n qubitów jest znormalizowanym wektorem $|\psi\rangle$ w przestrzeni C^{2^n}, który może być przedstawiony w postaci liniowej kombinacji 2^n wzajemnie ortogonalnych wektorów bazowych

$|0\rangle$, $|1\rangle$, $|2\rangle$,..., $|i\rangle$,..., $|2^n-1\rangle$.

Stąd:

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

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

Przykładowo, dla układu kwantowego złożonego z 2 qubitów 4 wektory bazowe wzajemnie ortogonalne

$\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}=\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$

w 4-wymiarowej zespolonej przestrzeni C^4 są postaci następującej:

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

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

$$|2\rangle = |10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \in C^4$$

$$|3\rangle = |11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \in C^4$$

Rejestr kwantowy jest zbudowany z qubitów z wykorzystaniem superpozycji stanów kwantowych oraz operacji iloczynu tensorowego. Niech $|\psi_k\rangle \in C^2$, k=0,1,..,n-1, będzie danym zbiorem n qubitów. Rejestr kwantowy jest iloczynem tensorowym n qubitów postaci

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_k\rangle \otimes \ldots \otimes |\psi_{n-1}\rangle$$

2.2. Notacja Diraca.

Symbol

$$|\psi\rangle = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_i \\ \vdots \\ c_n \end{bmatrix}$$

$c_i \in C$, i=1,2,...,n oznacza n-wymiarowy wektor kolumnowy o elementach zespolonych, natomiast symbol

$$\langle\psi| = \begin{bmatrix} c_1^* & c_2^* & \dots & c_i^* & \dots & c_n^* \end{bmatrix},$$

$c_i^* \in C$, i=1,2,...,n oznacza n-wymiarowy wektor wierszowy o sprzężonych elementach zespolonych. Elementy zespolonych wektorów znormalizowanych o długości 1 spełniają równość

$$\sum_{i=1}^{i=n} |c_i|^2 = |c_1|^2 + |c_2|^2 + \dots + |c_i|^2 + \dots + |c_n|^2 = 1$$

Iloczyn skalarny $\langle\psi|\varphi\rangle$ n-wymiarowych wektorów $\langle\psi|$ oraz $|\varphi\rangle$ dany jest wzorem

$$\langle\psi|\varphi\rangle = \begin{bmatrix} c_1^* & c_2^* & \dots & c_i^* & \dots & c_n^* \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_i \\ \vdots \\ d_n \end{bmatrix} = \sum_{i=1}^{i=n} c_i^* d_i$$

Stąd

$$\langle\varphi|\varphi\rangle = \begin{bmatrix} c_1^* & c_2^* & \dots & c_i^* & \dots & c_n^* \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_i \\ \vdots \\ c_n \end{bmatrix} = \sum_{i=1}^{i=n} c_i^* c_i = \sum_{i=1}^{i=n} |c_i|^2$$

Niech w przestrzeni C^n będzie dana baza ortonormalna złożona z wektorów jednostkowych $\{e_1, e_2, \dots, e_i, \dots e_n\}$. Wówczas

$$|\varphi\rangle = \sum_{i=1}^{1=n} \langle e_i|\varphi\rangle |e_i\rangle = \sum_{i=1}^{i=n} c_i |e_i\rangle$$

$$\langle\varphi|\psi\rangle = \langle\varphi| \sum_{i=1}^{i=n} |e_i\rangle\langle e_i|\psi\rangle = \langle\varphi| \sum_{i=1}^{i=n} |e_i\rangle\langle e_i| \sum_{i=1}^{i=n} |e_i\rangle\langle e_i|\psi\rangle$$

Iloczyn $|\varphi\rangle\langle\psi|$ jest n×n wymiarową macierzą o elementach zespolonych, której rząd wynosi 1.

2.3. Macierze gęstości.

Macierz ρ n×n-wymiarowa nazywa się macierzą gęstości jeżeli jest macierzą dodatnio określoną o śladzie równym 1.

Szczególnym przypadkiem macierzy gęstości jest macierz rzutowania na dany wektor q oznaczona symbolem P_q, której rząd jest równy 1. Macierze gęstości nie będące macierzami rzutowania mają zawsze rząd większy od 1.

Każdemu wektorowi $q \in C^n$ można przyporządkować w sposób jednoznaczny operator rzutowania P_q, który rzutuje dowolny wektor $w \in C^n$ na 1-wymiarową podprzestrzeń liniową generowaną przez dany wektor *q*.

$$P_q|w\rangle = \langle q|w\rangle\langle q|$$

Operator rzutowania reprezentowany jest *nxn*-wymiarową hermitowską (symetryczną) macierzą

$$P_q = |q\rangle\langle q|$$

i jak łatwo można sprawdzić spełnia warunek rzutowania

$$P_q P_q = P_q.$$

Przestrzenią stanów jest 2^n-wymiarowa przestrzeń C^{2^n}

$$C^{2^n} = C^2 \otimes C^2 \otimes \ldots \otimes C^2$$

W przestrzeni C^{2^n} czyste stany kwantowe są reprezentowane znormalizowanymi wektorami o długości *1*.

Niech symbol $B=\{0,1\}$ oznacza zbiór dwuelementowy oraz $B^n=\{0,1\}^n$ zbiór będący iloczynem kartezjańskim *n* zbiorów $B=\{0,1\}$. Ponadto, niech $x_i \in B$ dla *i=1,2,...,n*. Wówczas 2^n-wymiarowe znormalizowane wektory postaci

$$\left|x_1, x_2, \ldots, x_i, \ldots, x_n\right\rangle = \left|x_1\right\rangle \otimes \left|x_2\right\rangle \otimes \ldots \otimes \left|x_i\right\rangle \otimes \ldots \otimes \left|x_n\right\rangle$$

tworzą bazę ortonormalną w zespolonej przestrzeni stanów kwantowych C^{2^n}.

Zatem dowolny stan kwantowy $q \in C^{2^n}$ układu kwantowego złożonego z *n* qubitów można przedstawić w postaci kombinacji liniowej stanów bazowych

$$\left|q\right\rangle = \sum_{(x_1, x_2, \ldots, x_i, \ldots, x_n) \in B^n} c_{x_1, x_2, \ldots, x_i, \ldots, x_n} \left|x_1, x_2, \ldots, x_i, \ldots, x_n\right\rangle$$

gdzie zespolone współczynniki $c_{x_1, x_2, \ldots, x_i, \ldots, x_n}$ spełniają równość

$$\sum_{(x_1, x_2, \ldots, x_i, \ldots, x_n) \in B^n} \left| c_{x_1, x_2, \ldots, x_i, \ldots, x_n} \right|^2 = 1$$

Zespolone współczynniki $c_{x_1, x_2, \ldots, x_i, \ldots, x_n}$ noszą nazwę amplitud prawdopodobieństwa względem bazy ortonormalnej

Współczynniki $c_{x_1,x_2,...,x_i,...,x_n}$ mają interpretację fizyczną, a mianowicie kwadraty ich modułów $\left|c_{x_1,x_2,...,x_i,...,x_n}\right|^2$ reprezentują prawdopodobieństwa znalezienia się układu kwantowego w stanie bazowym

$$\left|x_1, x_2, ..., x_i, ..., x_n\right\rangle \in C^{2^n}.$$

W przypadku, gdy układ kwantowy składa się z dwóch podukładów kwantowych odpowiednio o przestrzeniach stanów C^{k^2} oraz C^{m^2}, wówczas jego *2^n*-wymiarowa, (*n=k+m*) przestrzeń stanów C^{n^2} jest iloczynem tensorowym

$$C^{2^n} = C^{2^k} \otimes C^{2^m}.$$

Wykorzystując postać wektora $|q\rangle$, można zdefiniować odpowiadający mu operator rzutowania reprezentowany następującą $2^n \times 2^n$-wymiarową, hermitowską (symetryczną), dodatnio określoną, macierzą rzutowania

$$P_q = \left|q\right\rangle \otimes \left\langle q\right|$$

Ponadto ślad macierzy rzutowania $\mathrm{Tr}(P_q)=1$.

Macierz rzutowania P_q reprezentuje operator rzutowania na jednowymiarową podprzestrzeń generowaną przez wektor $|q\rangle$.

Zatem istnieje wzajemna odpowiedniość pomiędzy danym qubitem $|q\rangle$ w postaci *2^n*-wymiarowego wektora, a dopowiadającym mu operatorem gęstości P_q w postaci macierzy rzutowania (gęstości).

W mechanice kwantowej występują:

stany kwantowe czyste reprezentowane wektorami lub macierzami rzutowania, oraz

stany kwantowe mieszane będące wypukłymi kombinacjami liniowymi stanów czystych reprezentowane macierzami gęstości.

Dowolny samosprzężony, dodatnio określony operator $\rho : C^{2^n} \to C^{2^n}$**, reprezentowany** $2^n \times 2^n$**-wymiarową macierzą gęstości, której ślad** $tr\rho = 1$**, nazywa się stanem układu kwantowego złożonego z** ***n*** **qubitów.**

Macierzy gęstości ρ jest $2^n \times 2^n$**-wymiarową macierzą hermitowską (symetryczną), dodatnio określoną, posiadającą** 2^n **rzeczywistych pojedynczych lub wielokrotnych wartości własnych** $\{s_1, s_2, ..., s_i, ..., s_{2^n}\}$**, którym odpowiadają rzeczywiste** 2^n**-wymiarowe wektory własne** $\{w_1, w_2, ..., w_i, ..., w_{2^n}\}$**, a jej ślad**

$$Tr(P_q) = \sum_{i=1}^{i=2^n} s_i = 1$$

Wykorzystując wartości własne s_i**,** $i=1,2,...,2^n$ **oraz odpowiadające im wektory własne** w_i**,** $i=1,2,...,2^n$**, macierz gęstości ρ można przedstawić w postaci liniowej kombinacji macierzy rzutowania na** 2^n **wektorów własnych**

$$\rho = \sum_{i=1}^{i=2^n} s_i \left| w_i \right\rangle \otimes \left\langle w_i \right|$$

Należy jednak zaznaczyć, że powyższe przedstawienie macierzy gęstości ρ **jest jednoznaczne jedynie w przypadku pojedynczych wartości własnych.**

W tym przypadku wartości własne s_i, $i=1,2,...,2^n$ reprezentują prawdopodobieństwa znalezienia się układu kwantowego w stanie kwantowym odpowiadającym wektorowi własnemu w_i, $i=1,2,...,2^n$ lub równoważnie macierzy rzutowania $|w_i\rangle\otimes\langle w_i|$, $i=1,2,...,2^n$.

W przypadku, gdy

$$Tr(\rho^2)=Tr(|z\rangle\langle z|)=\sum_{i=1}^{i=2^n}|z_i z_i^*|=1$$

macierz gęstości jest jednocześnie macierzą rzutowania $\rho=P_q$ na wektor *q* oraz odpowiadający tej macierzy stan kwantowy nazywa się czystym stanem kwantowym. Natomiast w pozostałych przypadkach macierz gęstości reprezentuje tak zwany mieszany stan kwantowy.

Rozróżnianie stanów kwantowych czystych i mieszanych jest możliwe poprzez badanie śladu kwadratu macierzy gęstości. Dla czystych stanów kwantowych mamy:

$$Tr(\rho^2)=Tr(\rho)=Tr(P_q)=Tr(|q\rangle\langle q|)=\sum_{i=1}^{i=2^n}|q_i q_i^*|=1$$

co wynika z normalizacji wektora *q*, którego długość wynosi *1* Zatem w tym przypadku $\rho=P_q=\rho^2$.

W przypadku mieszanych stanów kwantowych, odpowiadające im wektory zespolone *q* znajdują się wewnątrz kuli jednostkowej w przestrzeni C^2, a zatem ich długość jest zawsze mniejsza od *1*. W tym przypadku ślad kwadratu macierzy gęstości ρ^2 reprezentujący kwadrat długości wektora q jest mniejszy od jedności i wynosi

$$Tr(\rho^2)=Tr(|q\rangle\langle q|)=\sum_{i=1}^{i=2^n}|z_i z_i^*|<1$$

2.4. Stany kwantowe splątane.

Niech $|i\rangle_A$ oraz $|j\rangle_B$ będą bazami ortonormalnymi odpowiednio dla n-wymiarowego układu kwantowego A oraz m-wymiarowego układu kwantowego B. Zatem dla stanów kwantowych $|\psi\rangle_A$ oraz $|\varphi\rangle_B$ mamy

$$|\psi\rangle_A = \sum_{i=1}^{i=n} a_i |i\rangle_A \text{ oraz} \qquad |\varphi\rangle_B = \sum_{j=1}^{j=m} b_j |j\rangle_B$$

Stąd iloczyn tensorowy tych stanów kwantowych jest postaci

$$|\psi\rangle_A \otimes |\varphi\rangle_B = \sum_{i=1}^{i=n}\sum_{j=1}^{j=m} a_i b_j |i\rangle_A |j\rangle_B = \sum_{i=1}^{i=n}\sum_{j=1}^{j=m} c_{ij} |i\rangle_A |j\rangle_B$$

gdzie $c_{ij} = a_i b_j$, i=1,2,…,n, j=1,2,…,m są dowolnymi współczynnikami zespolonymi. W ogólnym przypadku faktoryzacja ta nie jest możliwa i wówczas stan kwantowy reprezentowany wektorem nm-wymiarowym w przestrzeni C^{nm} nie posiadający tej faktoryzacji nazywa się stanem splątanym.

Przykładowo stan kwantowy

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right)$$

jest stanem kwantowym splątanym.

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

Przykładowo, niech

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

Wektor ten reprezentuje stan kwantowy będący wynikiem splątania, gdyż nie można znaleźć dwóch stanów kwantowych $|\psi_1\rangle \in \mathbf{C}^2$ oraz $|\psi_2\rangle \in \mathbf{C}^2$ takich, że

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

Pojęcie splątania wiąże się bezpośrednio z tak zwaną bazą ortogonalną Bella, którą w zespolonej przestrzeni $\mathbf{C}^4$ tworzą następujące 4 wzajemnie ortogonalne wektory bazowe:

$|\mathbf{00}\rangle + |\mathbf{11}\rangle \in \mathbf{C}^4$**,**

$|\mathbf{00}\rangle - |\mathbf{11}\rangle \in \mathbf{C}^4$**,**

$|\mathbf{01}\rangle + |\mathbf{10}\rangle \in \mathbf{C}^4$**,**

$|\mathbf{01}\rangle - |\mathbf{10}\rangle \in \mathbf{C}^4$**.**

2.5. Obserwable.

Niech Q będzie $2^n \times 2^n$-wymiarową, macierzą hermitowską, to znaczy Q = Q*, reprezentującą obserwablę Q. Wówczas wartość liczbowa obserwabli oznaczona symbolem $\langle Q \rangle$ dla qubitu $q \in C^{2^n}$ jest postaci:

$$\langle Q \rangle = \langle q | Q | q \rangle$$

Z drugiej strony wykorzystując znane z algebry pojęcie śladu macierzy otrzymuje się równość

$$Tr(QP_q) = Tr\left(Q | q \rangle \langle q |\right)$$

Zatem po wykonaniu odpowiednich przekształceń macierzowych wartość liczbową obserwabli Q można wyrazić wzorem:

$$\langle Q \rangle = \langle q | Q | q \rangle = Tr(QP_q)$$

gdzie P_q jest macierzą rzutowania na 2^n-wymiarowy wektor q.

W szczególnym przypadku, gdy wektor q jest wektorem własnym obserwabli Q, wówczas wartośc liczbowa obserwabli jest wartością własną odpowiadająca wektorowi własnemu q.

W szczególnym przypadku obserwabla może być reprezentowana operatorem rzutowania lub kombinacją liniową operatorów rzutowania.

$$\langle Q \rangle = \langle z | P_q | z \rangle$$

gdzie P_q jest macierzą rzutowania na 2^n-wymiarowy wektor q.

3. Bramki kwantowe

3.1. Bramki 1-qubitowe.

Kwantowymi bramkami logicznymi są wszystkie operacje kwantowe wykonywane w przestrzeni stanów kwantowych. Podstawowe operacje kwantowe wykonywane na pojedynczym qubicie nazywane jedno-qubitowymi kwantowymi bramkami logicznymi reprezentowane są 2×2-wymiarowymi macierzami unitarnymi U będącymi liniowymi wzajemnie odwracalnymi odwzorowaniami w zespolonej przestrzeni C^2.

Macierze unitarne spełniają następującą podstawową równość: $U^{-1} = U^*$, gdzie U^{-1} jest macierzą odwrotną, natomiast w przypadku rzeczywistych macierzy unitarnych $U^{-1} = U^T$, gdzie U^T jest macierzą transponowaną. Macierze unitarne reprezentują w zespolonej przestrzeni C^2 obroty o pewien kąt wokół początku układu współrzędnych, które nie zmieniają długości poszczególnych wektorów. Ponieważ istnieje nieskończenie wiele 2×2-wymiarowych macierzy unitarnych, zatem dla pojedynczego qubitu teoretycznie istnieje nieskończenie wiele różnych kwantowych bramek logicznych, odpowiadających poszczególnym macierzom unitarnym U, oraz realizujących zadaną kwantową operację matematyczną [1], [4], [8].

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

$$U_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$ **dla operacji identyczności I, oraz**

$$U_{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$ **dla operacji negacji NOT.**

Przykładowo, działanie bramki NOT dla ortogonalnych wektorów bazowych

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \in \mathbf{C^2}$ **oraz** $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \in \mathbf{C^2}$

można przedstawić następująco: $|0\rangle \rightarrow |1\rangle$, oraz $|1\rangle \rightarrow |0\rangle$, gdzie symbol $\rightarrow$ oznacza transformację wektora.

$$U_{NOT}|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$U_{NOT}|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

Biorąc pod uwagę postać macierzy unitarnej U_{NOT} reprezentującej kwantową operację negacji oraz stosując standardowy zapis wektorowy otrzymuje się następującą zależność:

$$U_{NOT}|\psi\rangle = U_{NOT}(\alpha|0\rangle + \beta|1\rangle) = U_{NOT}(\alpha\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta\begin{bmatrix} 0 \\ 1 \end{bmatrix}) =$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = (\beta\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha\begin{bmatrix} 0 \\ 1 \end{bmatrix}) = (\beta|0\rangle + \alpha|1\rangle) = |\neg\psi\rangle$$

Zatem, działanie kwantowej bramki NOT dla dowolnego znormalizowanego stanu kwantowego $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbf{C^2}$ reprezentowanego wektorem o współczynnikach zespolonych α, β, można przedstawić następująco:

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

gdzie symbol $\neg$ oznacza negację w zapisie kwantowym, to znaczy zamianę współczynników α oraz.β.

Bramka kwantowa Hadamarda H jest reprezentowana następującą 2×2-wymiarową macierzą unitarną

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

Działanie bramki Hadamarda H dla ortogonalnych wektorów bazowych $|0\rangle \in \mathbf{C}^2$ oraz $|1\rangle \in \mathbf{C}^2$ można przedstawić następująco:

$$|0\rangle \rightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \in \mathbf{C}^2,$$

oraz

$$|1\rangle \rightarrow \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \in \mathbf{C}^2.$$

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

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

Istotną rolę w obliczeniach kwantowych odgrywają 2 × 2-wymiarowe hermitowskie unitarne macierze Pauliego postaci

$$\sigma_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_3 = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ogólnie liczby zespolone u_{ij}, i,j=1,2 tworzą 2×2-wymiarową macierz unitarną

$$U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}$$

Przykładowo, mogą to być macierze postaci:

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

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

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

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

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

3.2. Bramki 2-qubitowe.

W przypadku układu kwantowego złożonego z dwóch qubitów podstawowe operacje kwantowe reprezentowane są 4×4-wymiarowymi macierzami unitarnymi działającymi w przestrzeni $\mathbf{C}^4$. Szczególne znaczenie ma operacja, której działanie można przedstawić za pomocą następującej 4×4-wymiarowej unitarnej macierzy:

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

gdzie $$D = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}$$

jest dowolną operacją kwantową na pojedynczym qubicie, reprezentowaną 2×2-wymiarową unitarną macierzą D.

Operacja ta nosi nazwę "sterowanej bramki D", gdyż operacja wykonywana na drugim qubicie reprezentowana macierzą D zależy od tego czy pierwszy qubit jest w stanie kwantowym $|0\rangle \in \mathbf{C}^2$ czy też w stanie kwantowym $|1\rangle \in \mathbf{C}^2$. W przypadku, gdy pierwszy qubit jest w stanie kwantowym $|0\rangle \in \mathbf{C}^2$, wówczas drugi qubit pozostaje bez zmian, natomiast gdy pierwszy qubit jest w stanie kwantowym $|1\rangle \in \mathbf{C}^2$, wówczas na drugim qubicie wykonywana jest operacja kwantowa reprezentowana 2×2-wymiarową macierzą unitarną D.

W szczególnym przypadku gdy macierz unitarna D jest macierzą odpowiadającą operacji negacji NOT, to znaczy $D=U_{NOT}$ uzyskuje się bramkę kwantową o nazwie "sterowana negacja" oznaczanej symbolem CNOT (ang. controlled NOT), której odpowiada 4×4-wymiarowa unitarna macierz U_{CNOT}.

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

Działanie 2-qubitowej bramki kwantowej CNOT dla czterech ortonormalnych wektorów bazowych jest następujące:

$|0\rangle = |\mathbf{00}\rangle \in \mathbf{C^4}$, $|1\rangle = |\mathbf{01}\rangle \in \mathbf{C^4}$, $|2\rangle = |\mathbf{10}\rangle \in \mathbf{C^4}$, $|3\rangle = |\mathbf{11}\rangle \in \mathbf{C^4}$

można przedstawić następująco:

$|0\rangle = |\mathbf{00}\rangle \rightarrow |\mathbf{00}\rangle = |0\rangle$,

$|1\rangle = |\mathbf{01}\rangle \rightarrow |\mathbf{01}\rangle = |1\rangle$,

$|2\rangle = |\mathbf{10}\rangle \rightarrow |\mathbf{11}\rangle = |3\rangle$,

$|3\rangle = |\mathbf{11}\rangle \rightarrow |\mathbf{10}\rangle = |2\rangle$.

Zatem działanie 2-qubitowej bramki CNOT dla dowolnego stanu kwantowego

$$|\Psi\rangle = \alpha|\mathbf{00}\rangle + \beta|\mathbf{01}\rangle + \gamma|\mathbf{10}\rangle + \delta|\mathbf{11}\rangle \in \mathbf{C^4}$$

reprezentowanego wektorem odpowiednio o współczynnikach zespolonych α, β, γ, δ, można przedstawić następująco:

$$|\Psi\rangle = \alpha|\mathbf{00}\rangle + \beta|\mathbf{01}\rangle + \gamma|\mathbf{10}\rangle + \delta|\mathbf{11}\rangle \rightarrow \alpha|\mathbf{00}\rangle + \beta|\mathbf{01}\rangle + \delta|\mathbf{10}\rangle + \gamma|\mathbf{11}\rangle$$

4. Perspektywiczny uniwersalny komputer kwantowy

Formalnie kwantowy komputer jest układem n qubitów, na których można przeprowadzać odpowiednie operacje kwantowe reprezentowane bramkami kwantowymi czyli macierzami unitarnymi odpowiednich wymiarów.

Bez utraty ogólności można założyć, że początkowy stan kwantowy n-elementowego układu qubitów odpowiada wektorowi bazowemu $|0,0,0,...,0\rangle \in C^{2^n}$, który następnie jest sekwencyjnie przetwarzany przez dowolny ciąg bramek kwantowych.

W wyniku działania ciągu odpowiednio dobranych kwantowych bramek logicznych na początkowy stan kwantowy otrzymuje się w efekcie n-qubitowy końcowy stan kwantowy W, który jest wektorem o długości 1 w 2^n-wymiarowej zespolonej przestrzeni C^{2^n}. Końcowy pomiar wektora W daje nam informacje probabilistyczne.

5. Algorytmy kwantowe

Do najważniejszych algorytmów kwantowych należą:

1. **algorytm poszukiwań opracowany przez Grovera w 1997 roku,**
2. **algorytm faktoryzacji liczb naturalnych zaproponowany w 1993 roku przez Shora,**

5.1. Algorytm poszukiwań Grovera

W 1997 roku Grover zaproponował [5], [6] kwantowy algorytm wyszukiwania informacji w dużych zbiorach danych. Problem polega na wyszukaniu w nieuporządkowanym zbiorze danych $\{d_i, i=1,2,3,...,N\}$ zawierającym N elementów określonego elementu $d_j=y$.

Klasyczne algorytmy poszukiwań potrzebują średnio $^N/_2$ kroków na wyszukanie danej informacji w zbiorze danych zawierającym N elementów. Algorytm kwantowy poszukiwań Grovera znacznie bardziej efektywny i potrzebuje średnio jedynie $\sqrt{N}$ kroków.

Przykładowo dla $N=10^{16}$ nieuporządkowanych elementów. klasyczny komputer wykonałby taką czynność w czasie około kilkuset lat. Natomiast komputer kwantowy wykorzystujący algorytm poszukiwań Grovera wyznaczyłby poszukiwany element zbioru w ciągu około kilku minut.

5.2. Algorytm faktoryzacji Shora

W 1993 roku Shore zaproponował [7] efektywny kwantowy algorytm umożliwiajacy faktoryzację liczb naturalnych to znaczy znajdowanie jej podzielników. Algorytm ten posiada wielomianową złożoność obliczeniową. Należy zanaczyć, że jest to najważniejszy opracowany do tej pory algorytm kwantowej informatyki umożliwiający znaczne przyspieszenie wielu istotnych procesów obliczeniowych, wystepujacych głównie w kryptografii.

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

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. **Deutsch D., Quantum computational networks, Proceedings of the Royal Society of London, vol.425, 1989, pp.73-90.**
3. **Bugajski S., Klamka J., Węgrzyn S., Foundations of quantum computing. Part I, Archiwum Informatyki Teoretycznej i Stosowanej, vol.13, no1, 2001, str. 97-142.**
4. **Bugajski S., Klamka J., Węgrzyn S., Foundations of quantum computing. Part II, Archiwum Informatyki Teoretycznej i Stosowanej, vol.13, no1, 2001, str. 137-149.**
5. **Grover L.K., A fast quantum mechanical algorithm for database search, Proceedings of the 28th ACM Symposium on Theory of Computations, 1996, pp.212-21.**
6. **Klamka J., "Quantum search algorithm", Studia Informatica, vol.23, no 2, 2002, str.95-102.**
7. **Shore 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.**
8. **Węgrzyn S., Klamka J., Kwantowe systemy informatyki, Instytut Informatyki Teoretycznej i Stosowanej PAN, Gliwice, 2000.**
9. **Węgrzyn S., Klamka J., "Kwantowe systemy informatyki", Studia Informatica, vol.21, no.1, 2000, str.15-45.**
10. **Węgrzyn S., "Kwantowe systemy informatyki", Nauka, 2000, no.3, str.71-82,**
11. **Węgrzyn S., Klamka J., "Quantum computing", Archiwum Informatyki Teoretycznej i Stosowanej, tom 12, zeszyt 3, 2000, pp.235-246.**
12. **Węgrzyn S., "Informatyka kwantowa i jej miejsce w informatyce jako dyscyplinie naukowej", Studia Informatica, vol.22, no.1, pp.11-27.**