

Wprowadzenie do teorii komputerów kwantowych

mgr inż. Olga Siedlecka

olga@icis.pcz.pl

Instytut Informatyki Teoretycznej i Stosowanej

Plan seminarium

- Wstęp
- Historia
- Fizyka klasyczna
- Układy probabilistyczne
- Mechanika kwantowa
- Informacja kwantowa
- Algorytm Grovera

Wstęp

Teoria komputerów kwantowych zawiera piękno niezależnie od tego czy uda się kiedyś zrealizować ją w praktyce.

N.D. Mermin

Historia

- Richard Feynman - symulacja ewolucji układów kwantowych na klasycznych maszynach,
- Rolf Laundauer, Charles H. Bennet - udowodnili, że wszystkie algorytmy, które przeprowadza zwykła maszyna Turinga, mogą być przeprowadzone w taki sposób, aby były odwracalne,
- lata 80 - te, Paul Benioff wykazał, że komputer może działać opierając się jedynie o operacje kwantowo - mechaniczne,
- David Deutsch - podał dwa modele obliczeń kwantowych: uniwersalną kwantową maszynę Turinga i sieć bramek kwantowych

Historia

- 1994r. Peter W. Shor - algorytm rozkładu liczby na czynniki pierwsze przy użyciu zjawisk splątania i superpozycji,
- 1995r. Lov Grover - zaproponował kwantowy algorytm wyszukiwania informacji w dużych zbiorach danych.
- 1995r. konferencja w Turynie (we Włoszech) - projekty budowy obwodów kwantowych,
- 1996r. Christopher R. Monroe, David J. Wineland, H. Jeff Kimble - zbudowali niektóre prototypowe elementy mogące posłużyć do budowy komputera kwantowego,

Fizyka klasyczna

- Fizyka klasyczna jest nauką empiryczną, zatem teoria zostaje uznana za prawdziwą, gdy jej przewidywania zgodzą się z wynikami doświadczalnymi. Pojęcie obserwabli (zmiennych dynamicznych) ma w niej ogromne znaczenie. Przykładami obserwabli związanych z układem fizycznym jest położenie i pęd. Pełny opis układu nazywamy **stanem układu**.

Fizyka klasyczna

- Fizyka klasyczna jest nauką empiryczną, zatem teoria zostaje uznana za prawdziwą, gdy jej przewidywania zgodzą się z wynikami doświadczalnymi. Pojęcie obserwabli (zmiennych dynamicznych) ma w niej ogromne znaczenie. Przykładami obserwabli związanych z układem fizycznym jest położenie i pęd. Pełny opis układu nazywamy **stanem układu**.
- Układ fizyczny jest opisany wektorem stanu $\mathbf{x} \in \mathbb{R}^k$ dla danego k . Zbiór możliwych stanów układu nazywamy **przestrzenią fazową** układu.

Fizyka klasyczna

- Fizyka klasyczna jest nauką empiryczną, zatem teoria zostaje uznana za prawdziwą, gdy jej przewidywania zgodzą się z wynikami doświadczalnymi. Pojęcie obserwabli (zmiennych dynamicznych) ma w niej ogromne znaczenie. Przykładami obserwabli związanych z układem fizycznym jest położenie i pęd. Pełny opis układu nazywamy **stanem układu**.
- Układ fizyczny jest opisany wektorem stanu $\mathbf{x} \in \mathbb{R}^k$ dla danego k . Zbiór możliwych stanów układu nazywamy **przestrzenią fazową** układu.
- Jeżeli stan układu zależy od czasu możemy używać oznaczenia $\mathbf{x}(t)$ lub $\mathbf{x}_t$.

Fizyka klasyczna

- Fizyka klasyczna jest nauką empiryczną, zatem teoria zostaje uznana za prawdziwą, gdy jej przewidywania zgodzą się z wynikami doświadczalnymi. Pojęcie obserwabli (zmiennych dynamicznych) ma w niej ogromne znaczenie. Przykładami obserwabli związanych z układem fizycznym jest położenie i pęd. Pełny opis układu nazywamy **stanem układu**.
- Układ fizyczny jest opisany wektorem stanu $\mathbf{x} \in \mathbb{R}^k$ dla danego k . Zbiór możliwych stanów układu nazywamy **przestrzenią fazową** układu.
- Jeżeli stan układu zależy od czasu możemy używać oznaczenia $\mathbf{x}(t)$ lub $\mathbf{x}_t$.
- Jeżeli dwa układy są opisane stanami $\mathbf{x}$ oraz $\mathbf{y}$, to stan układu powstałego z ich połączenia będzie iloczynem kartezjańskim wektorów stanu podukładów $(\mathbf{x}, \mathbf{y})$.

Układy probabilistyczne

- W wypadku układów probabilistycznych nie znamy stanu układu z całkowitą pewnością, znamy jedynie rozkład prawdopodobieństwa dla stanów: układ może znajdować się w stanach $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ z prawdopodobieństwem odpowiednio $p_1, p_2, \dots, p_n$, takimi że $p_1 + p_2 + \dots + p_n = 1$.

Układy probabilistyczne

- W wypadku układów probabilistycznych nie znamy stanu układu z całkowitą pewnością, znamy jedynie rozkład prawdopodobieństwa dla stanów: układ może znajdować się w stanach $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ z prawdopodobieństwem odpowiednio $p_1, p_2, \dots, p_n$, takimi że $p_1 + p_2 + \dots + p_n = 1$.
- Wyrażenie $p_1[\mathbf{x}_1] + p_2[\mathbf{x}_2] + \dots + p_n[\mathbf{x}_n]$, gdzie $p_i \geq 0$ oraz $p_1 + p_2 + \dots + p_n = 1$, reprezentuje rozkład prawdopodobieństwa i oznacza, że układ znajduje się w stanie $\mathbf{x}_i$ z prawdopodobieństwem p_i . Powyższy rozkład jest nazywany **stanem mieszanym**, natomiast stany $\mathbf{x}_i$ są tzw. **stanami czystymi**.

Układy probabilistyczne

- W wypadku układów probabilistycznych nie znamy stanu układu z całkowitą pewnością, znamy jedynie rozkład prawdopodobieństwa dla stanów: układ może znajdować się w stanach $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ z prawdopodobieństwem odpowiednio $p_1, p_2, \dots, p_n$, takimi że $p_1 + p_2 + \dots + p_n = 1$.
- Wyrażenie $p_1[\mathbf{x}_1] + p_2[\mathbf{x}_2] + \dots + p_n[\mathbf{x}_n]$, gdzie $p_i \geq 0$ oraz $p_1 + p_2 + \dots + p_n = 1$, reprezentuje rozkład prawdopodobieństwa i oznacza, że układ znajduje się w stanie $\mathbf{x}_i$ z prawdopodobieństwem p_i . Powyższy rozkład jest nazywany **stanem mieszanym**, natomiast stany $\mathbf{x}_i$ są tzw. **stanami czystymi**.
- Każdy układ można uczynić probabilistycznym przy użyciu układu pomocniczego. W taki sposób są konstruowane algorytmy probabilistyczne: algorytm sam w sobie jest ściśle deterministyczny, natomiast korzysta on z bitów losowych.

Układy probabilistyczne

- Załóżmy, że ewolucja czasowa układu ze stanami czystymi $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ zależy od układu pomocniczego ze stanami czystymi $\mathbf{o}$ oraz $\mathbf{r}$, w taki sposób, że stan układu złożonego $(\mathbf{x}_i, \mathbf{o})$ przechodzi w ustalonym przedziale czasu w stan $(\mathbf{x}_{o(i)}, \mathbf{o})$, natomiast stan $(\mathbf{x}_i, \mathbf{r})$ przechodzi w $(\mathbf{x}_{r(i)}, \mathbf{r})$, gdzie $o, r : \{1, \dots, n\} \longrightarrow \{1, \dots, n\}$ są pewnymi funkcjami. Układ ze stanami $\mathbf{o}$ oraz $\mathbf{r}$ jest układem sterującym, który w stanie mieszanym nazywamy **randomizerem**.

Układy probabilistyczne

- Załóżmy, że ewolucja czasowa układu nie jest deterministyczna i układ zmienia się w taki sposób, iż każdy stan przechodzi w rozkład

$$\mathbf{x}_i \longrightarrow p_{1i}[\mathbf{x}_1] + p_{2i}[\mathbf{x}_2] + \dots + p_{ni}[\mathbf{x}_n]$$

gdzie $p_1 + p_2 + \dots + p_n = 1$ dla każdego i . Wielkość p_{ji} jest prawdopodobieństwem, że układ znajdujący się w stanie $\mathbf{x}_i$ przejdzie do stanu $\mathbf{x}_j$. W danym przedziale czasu rozkład $p_1[\mathbf{x}_1] + p_2[\mathbf{x}_2] + \dots + p_n[\mathbf{x}_n]$ przechodzi w

$$\begin{aligned} & p_1(p_{11}[\mathbf{x}_1] + \dots + p_{n1}[\mathbf{x}_n]) + \dots + p_n(p_{1n}[\mathbf{x}_1] + \dots + p_{nn}[\mathbf{x}_n]) = \\ & = (p_{11}p_1 + \dots + p_{1n}p_n)[\mathbf{x}_1] + \dots + (p_{n1}p_1 + \dots + p_{nn}p_n)[\mathbf{x}_n] = \\ & = p'_1[\mathbf{x}_1] + p'_2[\mathbf{x}_2] + \dots + p'_n[\mathbf{x}_n], \\ & p'_i = p_{i1}p_1 + \dots + p_{in}p_n. \end{aligned}$$

Układy probabilistyczne

- Prawdopodobieństwa p_i oraz p'_i związane są zależnością:

$$\begin{bmatrix} p'_1 \\ p'_2 \\ \vdots \\ p'_n \end{bmatrix} = \begin{bmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \dots & p_{nn} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}$$

Przy czym zachodzi $p_{1i} + p_{2i} + \dots + p_{ni} = 1$, co zapewnia spełnienie równości $p'_1 + p'_2 + \dots + p'_n = p_1 + p_2 + \dots + p_n$. Macierz o takiej własności nazywa się **macierzą Markowa**, natomiast układ probabilistyczny zmieniający się w czasie w sposób opisany powyżej - **łańcuchem Markowa**.

Mechanika kwantowa

- W mechanice kwantowej stan n -poziomowego układu jest reprezentowany przez wektor jednostkowy w n -wymiarowej zespolonej przestrzeni wektorowej H_n , którą nazywamy **przestrzenią stanów** układu. Wybierzmy w przestrzeni stanów H_n bazę ortonormalną $\{|\mathbf{x}_1\rangle, |\mathbf{x}_2\rangle, \dots, |\mathbf{x}_n\rangle\}$. Wektory bazowe $|\mathbf{x}_i\rangle$ nazywamy **stanami bazowymi**. Dowolny stan układu kwantowego można przedstawić w postaci **superpozycji** stanów bazowych:

$$\alpha_1|\mathbf{x}_1\rangle + \alpha_2|\mathbf{x}_2\rangle + \dots + \alpha_n|\mathbf{x}_n\rangle$$

gdzie α_i są liczbami zespolonymi nazywanymi **amplitudami prawdopodobieństwa** względem wybranej bazy. Warunek unormowania wektora stanu wymaga, by spełniały one równanie $|\alpha_1|^2 + |\alpha_2|^2 + \dots + |\alpha_n|^2 = 1$. Prawdopodobieństwo zaobserwowania własności $\mathbf{x}_i$ wynosi $|\alpha_i|^2$.

Informacja kwantowa - qubity

Bitem kwantowym (qubitem) nazywać będziemy dwupoziomowy układ kwantowy. W dwuwymiarowej zespolonej przestrzeni wektorowej H_2 wybierzmy bazę ortonormalną $B = \{|0\rangle, |1\rangle\}$, tzw. bazę obliczeniową. Stany $|0\rangle$ i $|1\rangle$ nazywamy stanami bazowymi. Dowolny stan qubitu można przedstawić w postaci superpozycji stanów bazowych:

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

o jednostkowej normie, tzn. $|\alpha_0|^2 + |\alpha_1|^2 = 1$, liczby α_0 i α_1 są amplitudami stanów bazowych, odpowiednio $|0\rangle$ i $|1\rangle$. Mówimy, że obserwacja (odczyt) qubitu daje wynik $|0\rangle$ lub $|1\rangle$ z prawdopodobieństwem odpowiednio $|\alpha_0|^2$ i $|\alpha_1|^2$.

Informacja kwantowa - unarne bramki kwantowe

Unarną (jednoargumentową) bramką kwantową nazywamy operację na qubicie, której odpowiada unitarne odwzorowanie $U : H_2 \longrightarrow H_2$. Unarna bramka kwantowa definiuje liniową operację

$$|0\rangle \longrightarrow a|0\rangle + b|1\rangle$$

$$|1\rangle \longrightarrow c|0\rangle + d|1\rangle$$

taką, że macierz: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ jest unitarna, tzn.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Informacja kwantowa - unarne bramki kwantowe

■ Bramka kwantowej negacji:

$$M_{\neg} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad M_{\neg}|0\rangle = |1\rangle \quad M_{\neg}|1\rangle = |0\rangle$$

Informacja kwantowa - unarne bramki kwantowe

■ Bramka kwantowej negacji:

$$M_{\neg} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad M_{\neg}|0\rangle = |1\rangle \quad M_{\neg}|1\rangle = |0\rangle$$

■ Pierwiastek kwadratowy z negacji:

$$\sqrt{M_{\neg}} = \begin{bmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{bmatrix} \quad \sqrt{M_{\neg}}\sqrt{M_{\neg}} = M_{\neg}$$

$$\sqrt{M_{\neg}}|0\rangle = \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \quad \sqrt{M_{\neg}}|1\rangle = \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle$$

Informacja kwantowa - unarne bramki kwantowe

■ Bramka Hadamarda-Walsha:

$$W_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

$$W_2|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad W_2|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$W_2 W_2 |0\rangle = |0\rangle \text{ interferencja konstruktywna}$$

$$W_2 W_2 |1\rangle = |1\rangle \text{ interferencja destruktywna}$$

Informacja kwantowa - unarne bramki kwantowe

■ Bramka Hadamarda-Walsha:

$$W_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

$$W_2|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad W_2|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$W_2 W_2 |0\rangle = |0\rangle \text{ interferencja konstruktywna}$$

$$W_2 W_2 |1\rangle = |1\rangle \text{ interferencja destruktywna}$$

■ Bramka zmiany fazy:

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

Informacja kwantowa - pary qubitów

Stany układu dwóch bitów kwantowych tworzą czterowymiarową przestrzeń Hilberta $H_4 = H_2 \otimes H_2$ z bazą ortonormalną $\{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\}$. Stan układu dwóch qubitów jest wektorem:

$$\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$$

o jednostkowej normie, tzn. $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$.

Odczyt układu dwóch qubitów daje wynik $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ z prawdopodobieństwem odpowiednio $|\alpha_0|^2, |\alpha_1|^2, |\alpha_2|^2, |\alpha_3|^2$. Jeżeli chcemy odczytać stan jednego z qubitów, to dla pierwszego otrzymamy $|0\rangle$ z prawdopodobieństwem $|\alpha_0|^2 + |\alpha_1|^2$, zaś $|1\rangle$ z prawdopodobieństwem $|\alpha_2|^2 + |\alpha_3|^2$. Analogicznie dla drugiego qubit.

Informacja kwantowa - splątanie

Stan układu dwóch qubitów $\mathbf{z} \in H_4$ jest **rozkładalny**, jeżeli można go przedstawić za pomocą w postaci iloczynu tensorowego stanów z przestrzeni H_2 , $\mathbf{z} = \mathbf{x} \otimes \mathbf{x}$. Stan, który nie jest rozkładalny, jest **splątany**.

Stan $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ jest rozkładalny:

$$\frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Stan $\frac{1}{2}(|00\rangle + |11\rangle)$ jest splątany, odczyt każdego qubitów z osobna da wynik $|0\rangle$ lub $|1\rangle$ z jednakowym prawdopodobieństwem. Odczyt układu jako całości da zawsze qubity o jednakowej wartości. Para takich qubitów jest nazywana parą **EPR** (Einstein, Podolski, Rosen).

Informacja kwantowa - bramki binarne

Binarną bramką kwantową nazywamy operację na parach qubitów, której odpowiada unitarne odwzorowanie $U : H_4 \longrightarrow H_4$.

■ Bramka sterowanej negacji:

$$M_{cnot} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$M_{cnot}|00\rangle = |00\rangle \quad M_{cnot}|01\rangle = |01\rangle$$

$$M_{cnot}|10\rangle = |11\rangle \quad M_{cnot}|11\rangle = |10\rangle$$

Informacja kwantowa - bramki binarne

■ Bramka Hadamarda-Walsha:

$$W_4 = W_2 \otimes W_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Dla dowolnych $x_0, x_1 \in \{0, 1\}$ zachodzi

$$\begin{aligned} W_4 |x_0 x_1\rangle &= \frac{1}{2} (|0\rangle + (-1)^{x_0} |1\rangle) (|0\rangle + (-1)^{x_1} |1\rangle) = \\ &= \frac{1}{2} (|00\rangle + (-1)^{x_1} |01\rangle + (-1)^{x_0} |10\rangle + (-1)^{x_0+x_1} |11\rangle) \end{aligned}$$

Informacja kwantowa - rejestry

Uporządkowany układ m qubitów będziemy nazywać **rejestrem kwantowym** o długości m . Przestrzeń stanów takiego układu jest m -krotnym iloczynem tensorowym $H_{2^m} = H_2 \otimes \dots \otimes H_2$, natomiast stany bazowe mają postać

$$\{|\mathbf{x}\rangle : \mathbf{x} \in \{0, 1\}^m\}$$

Jeżeli $\mathbf{x} = x_1 \dots x_m$ utożsamimy z liczbą zapisaną w systemie dwójkowym, to można powiedzieć, że stany bazowe mają postać

$$\{|a\rangle : a \in \{0, 1, \dots, 2^m - 1\}\}$$

Stan układu m -qubitów ma postać:

$$\alpha_0|0\rangle + \alpha_1|1\rangle + \dots + \alpha_{2^m-1}|2^m - 1\rangle$$

Informacja kwantowa - nieklonowanie

Rozważmy układ kwantowy o n stanach bazowych $|a_1\rangle, \dots, |a_n\rangle$. Wyróżnijmy stan $|a_1\rangle$ jako stan, na którym będziemy dokonywać zapisu informacji. Unitarne odwzorowanie w przestrzeni $H_n \otimes H_n$ nazywamy **kwantową maszyną kopiującą**, jeżeli dla dowolnego stanu $|x\rangle \in H_n$ zachodzi $U(|x\rangle|a_1\rangle) = |x\rangle|x\rangle$.

Twierdzenie o nieklonowaniu: Dla $n > 1$ kwantowa maszyna kopiująca nie istnieje.

Możliwe jest jedynie otrzymanie kopii stanów bazowych.

Informacja kwantowa - obserwacja

Postulat rzutowania: po dokonaniu pomiaru układ znajduje się w jednym ze swoich stanów bazowych.

Założmy, że przeprowadzamy pomiar na układzie w stanie:

$$\alpha_1|\mathbf{x}_1\rangle + \alpha_2|\mathbf{x}_2\rangle + \dots + \alpha_n|\mathbf{x}_n\rangle$$

Otrzymaliśmy w wyniku $\mathbf{x}_k$, co za tym idzie układ jest w stanie bazowym $|\mathbf{x}_k\rangle$.

Informacja kwantowa - obserwacja

Rozpatrzmy układ złożony:

$$\sum_{i=1}^n \sum_{j=1}^m \alpha_{ij} |\mathbf{x}_i\rangle |\mathbf{y}_j\rangle$$

obserwacja pierwszego podukładu dała w wyniku $\mathbf{x}_k$ z prawdopodobieństwem $P(k) = \sum_{j=1}^m |\alpha_{kj}|^2$, zatem układ znajduje się w stanie:

$$\frac{1}{\sqrt{P(k)}} \sum_{j=1}^m \alpha_{kj} |\mathbf{x}_k\rangle |\mathbf{y}_j\rangle$$

Przejście pierwszego ze stanów w drugi jest nieodwracalne, a zatem niezgodne z zasadą **ewolucji unitarnej**. Proponowane rozwiązanie to wprowadzenie układu pomocniczego, do którego kopiujemy stany bazowe $|\mathbf{x}_i\rangle |\mathbf{x}_1\rangle \longrightarrow |\mathbf{x}_i\rangle |\mathbf{x}_i\rangle$.

Informacja kwantowa - teleportacja

Założmy, że Alicja i Bob, to dwie komunikujące się ze sobą strony, Alicja jest w posiadaniu qubitów $a|0\rangle + b|1\rangle$, który chce teleportować. Teleportacja kwantowa jest możliwa, jeżeli obie strony posiadają qubity splątane ze sobą, np. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Przyjmijmy, że qubit lewy należy do Alicji, zaś prawy do Boba. Stan złożonego układu ma postać:

$$\begin{aligned} & (a|0\rangle + b|1\rangle) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \\ &= \frac{a}{\sqrt{2}}|0\rangle|00\rangle + \frac{a}{\sqrt{2}}|0\rangle|11\rangle + \frac{b}{\sqrt{2}}|1\rangle|00\rangle + \frac{b}{\sqrt{2}}|1\rangle|11\rangle = \\ &= \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}}|111\rangle \end{aligned}$$

Informacja kwantowa - teleportacja

Protokół teleportacji:

- Alicja wykonuje na swoich qubitach operację sterowanej negacji:

$$\frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|110\rangle + \frac{b}{\sqrt{2}}|101\rangle$$

Informacja kwantowa - teleportacja

Protokół teleportacji:

- Alicja wykonuje na swoich qubitach operację sterowanej negacji:

$$\frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|110\rangle + \frac{b}{\sqrt{2}}|101\rangle$$

- Alicja wykonuje transformatę Hadamarda-Walsha na lewym qubicie:

$$\frac{a}{\sqrt{2}} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |00\rangle + \frac{a}{\sqrt{2}} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |11\rangle +$$

$$\frac{b}{\sqrt{2}} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) |10\rangle + \frac{b}{\sqrt{2}} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) |01\rangle =$$

$$\frac{a}{2}|000\rangle + \frac{a}{2}|100\rangle + \frac{a}{2}|011\rangle + \frac{a}{2}|111\rangle + \frac{b}{2}|010\rangle - \frac{b}{2}|110\rangle + \frac{b}{2}|001\rangle - \frac{b}{2}|101\rangle$$

Informacja kwantowa - teleportacja

- Wydzielamy qubit Boba:

$$\frac{1}{2}|00\rangle a|0\rangle + \frac{1}{2}|10\rangle a|0\rangle + \frac{1}{2}|01\rangle a|1\rangle + \frac{1}{2}|11\rangle a|1\rangle +$$
$$\frac{1}{2}|01\rangle b|0\rangle - \frac{1}{2}|11\rangle b|0\rangle + \frac{1}{2}|00\rangle b|1\rangle - \frac{1}{2}|10\rangle b|1\rangle =$$

Informacja kwantowa - teleportacja

- Wydzielamy qubit Boba:

$$\frac{1}{2}|00\rangle a|0\rangle + \frac{1}{2}|10\rangle a|0\rangle + \frac{1}{2}|01\rangle a|1\rangle + \frac{1}{2}|11\rangle a|1\rangle +$$

$$\frac{1}{2}|01\rangle b|0\rangle - \frac{1}{2}|11\rangle b|0\rangle + \frac{1}{2}|00\rangle b|1\rangle - \frac{1}{2}|10\rangle b|1\rangle =$$

■

$$\frac{1}{2}|00\rangle(a|0\rangle + b|1\rangle) + \frac{1}{2}|01\rangle(a|1\rangle + b|0\rangle) +$$

$$\frac{1}{2}|10\rangle(a|0\rangle - b|1\rangle) + \frac{1}{2}|11\rangle(a|1\rangle - b|0\rangle)$$

Informacja kwantowa - teleportacja

- Wydzielamy qubit Boba:

$$\frac{1}{2}|00\rangle a|0\rangle + \frac{1}{2}|10\rangle a|0\rangle + \frac{1}{2}|01\rangle a|1\rangle + \frac{1}{2}|11\rangle a|1\rangle +$$

$$\frac{1}{2}|01\rangle b|0\rangle - \frac{1}{2}|11\rangle b|0\rangle + \frac{1}{2}|00\rangle b|1\rangle - \frac{1}{2}|10\rangle b|1\rangle =$$



$$\frac{1}{2}|00\rangle(a|0\rangle + b|1\rangle) + \frac{1}{2}|01\rangle(a|1\rangle + b|0\rangle) +$$

$$\frac{1}{2}|10\rangle(a|0\rangle - b|1\rangle) + \frac{1}{2}|11\rangle(a|1\rangle - b|0\rangle)$$

- Alicja przeprowadza obserwacje stanu swoich dwóch qubitów i przesyła jej wynik do Boba.

Informacja kwantowa - teleportacja

- Jeżeli Bob otrzymał 00, nie musi nic robić, jego qubit jest już w stanie $a|0\rangle + b|1\rangle$.

Informacja kwantowa - teleportacja

- Jeżeli Bob otrzymał 00, nie musi nic robić, jego qubit jest już w stanie $a|0\rangle + b|1\rangle$.
- Jeżeli Bob otrzymał 01, wykonuje na swoim qubicie operację negacji.

Informacja kwantowa - teleportacja

- Jeżeli Bob otrzymał 00, nie musi nic robić, jego qubit jest już w stanie $a|0\rangle + b|1\rangle$.
- Jeżeli Bob otrzymał 01, wykonuje na swoim qubicie operację negacji.
- Jeżeli Bob otrzymał 10, wykonuje operację zmiany fazy.

Informacja kwantowa - teleportacja

- Jeżeli Bob otrzymał 00, nie musi nic robić, jego qubit jest już w stanie $a|0\rangle + b|1\rangle$.
- Jeżeli Bob otrzymał 01, wykonuje na swoim qubicie operację negacji.
- Jeżeli Bob otrzymał 10, wykonuje operację zmiany fazy.
- Jeżeli Bob otrzymał 11, wykonuje operację negacji, a następnie zmiany fazy.

Informacja kwantowa - kodowanie supergęste

Założmy, że Alicja tym razem nie chce przesłać stanu dodatkowego qubitu, ale zwykłą parę bitów. Jest to operacja komplementarna do teleportacji, a nazywamy ją **kodowaniem supergęstym**.

Alicja posiada dwa klasyczne bity b_1 i b_2 oraz lewy qubit pary EPR, Bob posiada prawy qubit pary EPR:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Informacja kwantowa - kodowanie supergęste

Protokół kodowania supergęstego:

- Alicja wykonuje operacje na swoim qubicie w zależności od wartości bitów b_1 i b_2

b_1	b_2	Operacja wykonana przez Alicję
0	0	$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
0	1	$\frac{1}{\sqrt{2}}(10\rangle + 01\rangle)$
1	0	$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
1	1	$\frac{1}{\sqrt{2}}(10\rangle - 01\rangle)$

Informacja kwantowa - kodowanie supergęste

Protokół kodowania supergęstego:

- Alicja wykonuje operacje na swoim qubicie w zależności od wartości bitów b_1 i b_2

b_1	b_2	Operacja wykonana przez Alicję
0	0	$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
0	1	$\frac{1}{\sqrt{2}}(10\rangle + 01\rangle)$
1	0	$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
1	1	$\frac{1}{\sqrt{2}}(10\rangle - 01\rangle)$

- Alicja przesyła swój qubit Bobowi

Informacja kwantowa - kodowanie supergęste

- Bob wykonuje na obu qubitach bramkę kwantową zdefiniowaną przez macierz:

$$B = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}$$

Informacja kwantowa - kodowanie supergęste

- Bob wykonuje na obu qubitach bramkę kwantową zdefiniowaną przez macierz:

$$B = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}$$

- Bob po wykonaniu operacji otrzymuje wartości bitów b_1 i b_2

Algorytm wyszukiwania Grovera

Dany jest nieuporządkowany zbiór S zawierający 2^n -elementów, szukamy w nim elementu $\mathbf{y}$. Dana jest również funkcja $f : S \longrightarrow \{0, 1\}$,

w przypadku wyszukiwania kwantowego funkcja f ma postać:

$f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, gdzie $\mathbb{F}_2$ jest ciałem o dwóch elementach 0 i 1.

Dodawanie i mnożenie zdefiniowane są następująco:

$$0 + 0 = 1 + 1 = 0, \quad 0 + 1 = 1, \quad 0 * 0 = 0 * 1 = 0, \quad 1 * 1 = 1$$

Funkcja f jest określona:

$$f(\mathbf{x}) = \begin{cases} 1 & \mathbf{x} = \mathbf{y} \\ 0 & \mathbf{x} \neq \mathbf{y} \end{cases}$$

Algorytm wyszukiwania Grovera

Algorytm Grovera, to algorytm wyszukiwania probabilistycznego, tzn. nie będziemy wymagać, aby algorytm zawsze znajdował taki $\mathbf{x}$, że $f(\mathbf{x}) = 1$, chcemy jedynie, aby dawał poprawny wynik z niezerowym prawdopodobieństwem ($0 < p \leq 1$).

Algorytm ma charakter iteracyjny, w każdym kroku stan bazowy odpowiadający szukanemu elementowi ma zmienianą fazę, poza tym następuje obrót wokół średniej wszystkich amplitud, a także wzmocnienie amplitudy szukanego stanu.

Algorytm wyszukiwania Grovera

Etapy algorytmu wyszukiwania Grovera:

- Posługując się transformatą Hadamarda H_n normalizujemy rejestr $|\phi\rangle = |0^{(n)}\rangle$:

$$H_n|\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{\mathbf{x}\mathbf{y}} |\mathbf{y}\rangle \quad |\phi_0\rangle = H_n|0^{(n)}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} |\mathbf{x}\rangle$$

Algorytm wyszukiwania Grovera

Etapy algorytmu wyszukiwania Grovera:

- Posługując się transformatą Hadamarda H_n normalizujemy rejestr $|\phi\rangle = |0^{(n)}\rangle$:

$$H_n|\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{\mathbf{x}\mathbf{y}} |\mathbf{y}\rangle \quad |\phi_0\rangle = H_n|0^{(n)}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} |\mathbf{x}\rangle$$

- Stosujemy operator G_n (operator Grovera), $\frac{1}{4}\Pi 2^{\frac{n}{2}}$ razy, gdzie

$$G_n = -H_n R_n H_n V_f$$

H_n - transformata Hadamarda

R_n - operator kwantowy,

V_f - zmodyfikowany operator sprawdzenia

Algorytm wyszukiwania Grovera



$$G_n = -H_n R_n H_n V_f$$

$$H_n |\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{\mathbf{x}\mathbf{y}} |\mathbf{y}\rangle$$

$$R_n |0\rangle = -|0\rangle, \quad R_n |\mathbf{x}\rangle = |\mathbf{x}\rangle, \quad \text{gdy } \mathbf{x} \neq 0 \quad R_n = \begin{bmatrix} -1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$V_f |\mathbf{x}\rangle = (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle$$

Algorytm wyszukiwania Grovera



$$G_n = -H_n R_n H_n V_f$$

$$H_n |\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{\mathbf{x}\mathbf{y}} |\mathbf{y}\rangle$$

$$R_n |0\rangle = -|0\rangle, \quad R_n |\mathbf{x}\rangle = |\mathbf{x}\rangle, \quad \text{gdy } \mathbf{x} \neq 0 \quad R_n = \begin{bmatrix} -1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$V_f |\mathbf{x}\rangle = (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle$$

■ Dokonujemy pomiaru.

Źródła

- E. Riffel, W. Polak, *An introduction to quantum computation for non physics*, ACM Computer Surveys, vol. 32, issue 3, Sept.2000
- L. K. Grover, *A fast quantum-mechanical algorithm for database search*, Proceedings of the 28th Annual ACM Symposium on the Theory of Computing - STOC, 212 - 219 (1996)
- M. Hirvensalo, *Algorytmy kwantowe*, Wydawnictwa Szkolne i Pedagogiczne S.A., Warszawa 2004
- S. Węgrzyn, J. Klamka, J.A. Miszczak, *Kwantowe systemy informatyki*, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2003