

Modele obliczeń kwantowych

Jakub Zieliński

Wydział Elektroniki i Technik Informatycznych
Politechnika Warszawska

Notacja Diraca, "bra-ket"

Używana do opisu wektorów z tzw. przestrzeni dualnej ($\langle bra|$ jest hermitowskim sprzężeniem $|ket\rangle$).

Jeżeli $|ket\rangle$ jest wektorem kolumnowym

$$(\alpha_1 \quad \alpha_2 \quad \cdots \quad \alpha_{n-1} \quad \alpha_n)^T$$

to $\langle bra|$ jest wektorem w postaci rzędu

$$(\beta_1 \quad \beta_2 \quad \cdots \quad \beta_{n-1} \quad \beta_n)$$

Podstawowe opercje

- 1 iloczyn skalarny $\langle bra|ket\rangle$
- 2 rzutowanie na wektor $|v_1\rangle\langle v_1|v_2\rangle$ (rzut v_2 na v_1)
- 3 zapis wektora w bazie

$$|V\rangle = \sum_{i=1}^n \alpha_i |v_i\rangle$$

Przykład nr 1

Wektor w bazie o wymiarze $n = 3$ możemy zapisać w następujący sposób:

$$|\psi\rangle = \alpha|001\rangle + \beta|010\rangle + \gamma|100\rangle$$

$|001\rangle, |010\rangle, |100\rangle$ są wyłącznie etykietami.

Przykład nr 2

Weźmy wektor $|V\rangle = \sum_{i=1}^n \alpha_i |v_i\rangle$.

Rzutujemy wektor $|V\rangle$ na wektor bazowy $|v_1\rangle$.

$$|v_1\rangle\langle v_1||V\rangle = \alpha_1|v_1\rangle\langle v_1|v_1\rangle + \alpha_2|v_1\rangle\langle v_1|v_2\rangle + \dots + \alpha_n|v_1\rangle\langle v_1|v_n\rangle$$

Otrzymujemy $|v_1\rangle\langle v_1||V\rangle = \alpha_1|v_1\rangle\langle v_1|v_1\rangle = \alpha_1|v_1\rangle$

Czym jest kubit?

Opis matematyczny

Układ opisany dwuwymiarową przestrzenią Hilberta. Kubit jest superpozycją 2 podstawowych stanów własnych $|0\rangle$ i $|1\rangle$.

$$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$$

Gdzie α^2 i β^2 są prawdopodobieństwami wystąpienia odpowiednich stanów własnych oraz

$$\|\alpha\|^2 + \|\beta\|^2 = 1$$

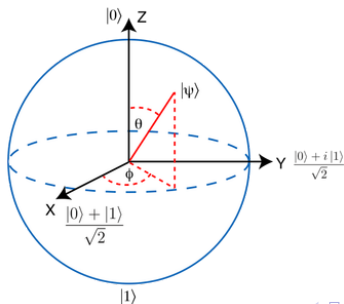
Sfera Blocha

Kubit może być również przy pomocy funkcji trygonometrycznych.

$$|\psi_0\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle$$

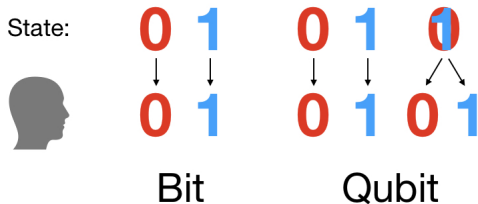
gdzie $0 \leq \phi \leq \pi$ i $0 \leq \theta \leq 2\pi$

Pozwala to na przedstawienie kubit jako sfery Blocha.



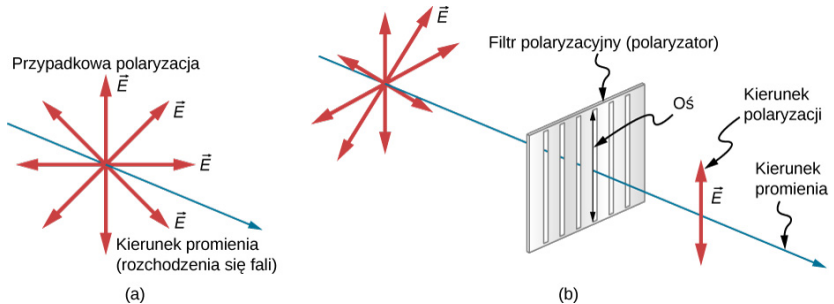
Pomiar stanu kubitu

Na wynik pomiaru stanu kubitu wpływa jego opis w przestrzeni Hilberta, tzn. wartości współczynników α i β . Co więcej, pomiar powoduje zmianę stanu układu. Następuje *collapse* i stan układu przyjmuje wartość pomiaru. $np. |\phi\rangle \longrightarrow |1\rangle$



Pomiar stanu kubit

Jeżeli jako fizyczny model naszego kubit użnamy foton, to pomiar stanu możemy sobie wyobrazić jako przepuszczenie przez polaryzator.



Podstawowe operacje na kubitach

Zdefiniujmy wektory własne $|0\rangle$ i $|1\rangle$ odpowiednio jako $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ i $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Łatwo sprawdzić, że wektory są ortonormalne, czyli

$$\langle 0|0\rangle = 1 \qquad \langle 1|1\rangle = 1 \qquad \langle 1|0\rangle = 0 \qquad \langle 0|1\rangle = 0$$

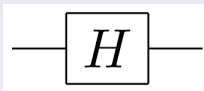
Bramka Hadamarda

Jedno-kubitowa bramka oznaczana \hat{H} , opisana macierzą

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



Alternatywna baza

$\hat{H}|0\rangle$ oznaczamy przez $|+\rangle$, a $\hat{H}|1\rangle$ przez $|-\rangle$.

$|+\rangle$ i $|-\rangle$ są ortogonalne, więc również wyznaczają bazę.

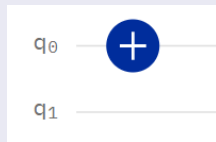
Bramka NOT, \hat{X}

Bramka neguje stan kwantowy, podobnie jak klasyczny NOT.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

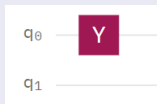
$$\hat{X}(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$$

Warto zauważyć że $\hat{X}\hat{X}$ jest macierzą I .



Bramka \hat{Y}

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$



$$\hat{Y}(\alpha|0\rangle + \beta|1\rangle) = -i\beta|0\rangle + i\alpha|1\rangle$$

$\hat{Y}\hat{Y}$ jest macierzą I .

Bramka \hat{Z}

Bramka zmiany fazy o π .

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



$$\hat{Z}(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

$\hat{Z}\hat{Z}$ jest macierzą I .

Notacja Diraca opisuje też stany wielokubitowe.

Iloczyn tensorowy

Przy jego pomocy można złożyć dwa stany w jeden wypadkowy.

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix} \otimes |\psi_B\rangle = \begin{pmatrix} \alpha_A |\psi_B\rangle \\ \beta_A |\psi_B\rangle \end{pmatrix} = \begin{pmatrix} \alpha_A \alpha_B \\ \alpha_A \beta_B \\ \beta_A \alpha_B \\ \beta_A \beta_B \end{pmatrix}$$

Stany dwukubitowe

Przy pomocy iloczynu tensorowego możemy wyznaczyć wektory reprezentujące stany własne układu.

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Bramka CNOT

Bramka dwukubitowa. Wyróżniamy kubit *control* i *target*.
Control decyduje o negacji *target*.

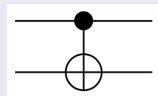
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\hat{CNOT}|00\rangle = |00\rangle$$

$$\hat{CNOT}|01\rangle = |01\rangle$$

$$\hat{CNOT}|10\rangle = |11\rangle$$

$$\hat{CNOT}|11\rangle = |10\rangle$$



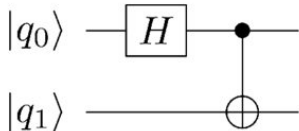
Stan splątany

- 1 Stanu układu nie da się "rozsupłać".
- 2 Zmiana jednego z kubitów wpływa na drugi.
- 3 Wystarczy zmierzyć jeden z kubitów, by poznać stan obu.

Jak splątać kubity?

Przepuśćmy stan $|00\rangle$ przez poniższy obwód kwantowy.

$$|00\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



Wszystkie przypadki "wejścia"

$$\begin{aligned} |00\rangle &\longrightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |01\rangle &\longrightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |10\rangle &\longrightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |11\rangle &\longrightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}$$

Stany Bell'a

Tworzą alternatywną bazę dla układów 2 kubitowych.

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

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Dowód splątania

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

Aby zachodziła równość, $\alpha\gamma = \beta\delta = \frac{1}{\sqrt{2}}$, a $\alpha\delta = \beta\gamma = 0$

Ten warunek jest nie do spełnienia.

Analogicznie dla reszty przypadków.

Cel procedury

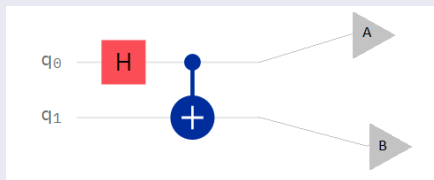
Zakodowanie dwu-bitowej informacji w jednym kubicie.

Procedura

- 1 Przygotowanie splątanego układu
- 2 Kodowanie w A
- 3 Przesył kubitów z A do B
- 4 Dekodowanie w B

Krok nr 1

Splątanie kubitów w laboratorium i przekazanie kubitów do punktów A i B.



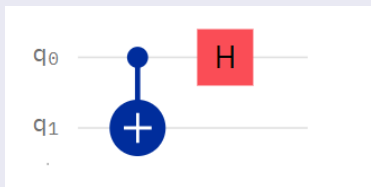
Krok nr 2

W punkcie A wykonujemy jedną z 4 operacji. Które kodujemy klasycznie.

Informacja	Operacja	Stan układu
00	\hat{I}	$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
01	\hat{X}	$\frac{1}{\sqrt{2}}(10\rangle + 01\rangle)$
10	\hat{Z}	$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
11	$\hat{X}\hat{Z}$	$\frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

Krok nr 3

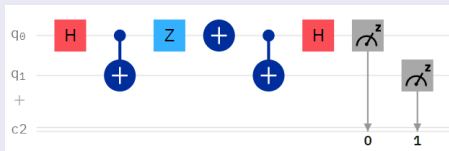
Przekazanie kubitów z A do B i wykonanie dekodowania obwodem odwrotnym do obwodu splątującego.



Krok nr 4

Wykonanie pomiaru na kubitach w punkcie B.

Funkcja opisująca kubit jest postaci $|AB\rangle$, co daje 100% szansę na odczytanie zakodowanej wiadomości.



Cel procedury

Transport informacji o kubicie, czyli jego stanu kwantowego, do wskazanego miejsca.

Procedura

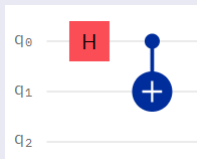
- 1 Umieszczenie splątanych kubitów w A i B.
- 2 Wykonanie pomiaru w bazie Bella, na kubitach z A.
- 3 Klasyczny transport informacji o wyniku pomiaru do B.
- 4 Dekodowanie kubit w B.

Krok 1

Splątana parę kubitów rozdzielamy do punktów A i B.
W punkcie A znajduje się również kubit $|\psi\rangle$, którego stan przeniesiemy do B.

Stan układu :

$$(\alpha|0\rangle + \beta|1\rangle) \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$



Krok 2

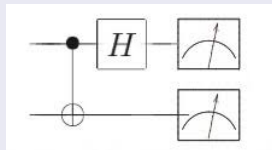
Przedstawmy stan 2 kubitów z A (2 pierwsze) w bazie Bell'a.

$$|00\rangle = |\phi^+\rangle + |\phi^-\rangle$$

$$|01\rangle = |\psi^+\rangle + |\psi^-\rangle$$

$$|10\rangle = |\psi^+\rangle - |\psi^-\rangle$$

$$|11\rangle = |\phi^+\rangle - |\phi^-\rangle$$

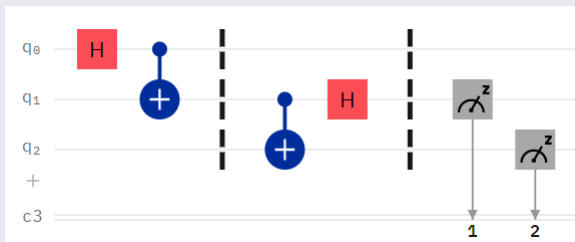


Przy pomocy powyższych zależności otrzymujemy:

$$\left(\frac{1}{\sqrt{2}}\right)^2 \left[|\phi^+\rangle (\alpha|0\rangle + \beta|1\rangle) + |\psi^+\rangle (\alpha|1\rangle + \beta|0\rangle) + |\phi^-\rangle (\alpha|0\rangle - \beta|1\rangle) + |\psi^-\rangle (\alpha|1\rangle - \beta|0\rangle) \right]$$

Krok 3

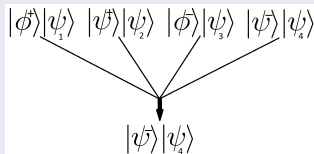
W zależności o wyniku pomiaru do B zostaje przekazana informacja o sposobie przywrócenia informacji o $|\psi\rangle$ na kubicie pozostającym w B.



Krok 4

Dzięki informacji z A, wiemy w jakim stanie jest układ po pomiarze. Na kubicie z B wykonujemy jedną z operacji: \hat{I} , \hat{X} , \hat{Z} , $\hat{X}\hat{Z}$.

Założmy, że pomiar w A dał wynik $|\psi^-\rangle$. Zachodzi *collapse* funkcji falowej do postaci: $|\psi^-\rangle(\alpha|1\rangle - \beta|0\rangle)$



Protokoły kwantowe - kwantowa "teleportacja"

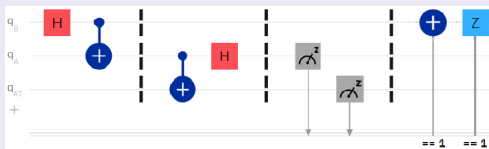
Krok 4

Dzięki informacji z A, wiemy w jakim stanie jest układ po pomiarze. Na kubicie z B wykonujemy jedną z operacji: \hat{I} , \hat{X} , \hat{Z} , $\hat{X}\hat{Z}$.

Zauważmy, że $|\psi^-\rangle(\alpha|1\rangle - \beta|0\rangle)$ to nic innego jak $\hat{Z}\hat{X}|\psi\rangle$.

Podsumowanie

Operacja $\hat{X}\hat{Z}$
ustawia stan $|\psi\rangle$,
tym samym kończąc
protokół.



Sformułowanie problemu

Istnieje funkcja postaci $f : N \rightarrow \{0, 1\}$, dana wzorem

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

Chcemy poznać wartość x_s .

Podjęście klasyczne

Iterujemy po wszystkich możliwych wartościach x i sprawdzamy czy $f(x_i)$ jest równe 1.

Złożoność oczywiście : $O(N)$



Podejście "kwantowe"

Algorytm bazuje na iteracyjnym "wzmacnianiu amplitudy" prawdopodobieństwa szukanego stanu $|x_s\rangle$. Proces osiągamy poprzez odpowiednie manipulowanie rejestrem kwantowym.

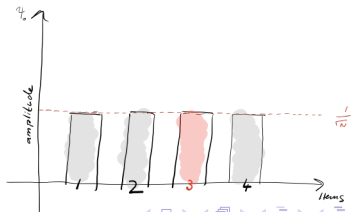
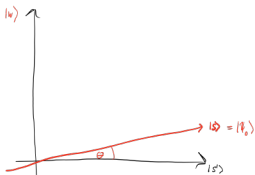
Krok 1 - Przygotowanie rejestru

Niech rejestr kwantowy będzie dany funkcją falową :

$$|\phi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N-1} |\omega_i\rangle$$

gdzie $N = 2^n$, a n to ilość kubitów.

Wybieramy taką postać wejściową, ponieważ nie faworyzuje żadnego ze stanów.



Krok 2 - Manipulacje na rejestrze

Korzystamy z dwóch operacji (bramek). Nazwijmy je \mathcal{A} i \mathcal{B} .

Po każdej iteracji stan rejestru to:

$$|\phi_{n+1}\rangle = \mathcal{B}\mathcal{A}|\phi_n\rangle$$

gdzie:

$$\mathcal{A} = \mathcal{I} - 2|\omega_0\rangle\langle\omega_0|$$

$$\mathcal{B} = 2|\phi_0\rangle\langle\phi_0| - \mathcal{I}$$

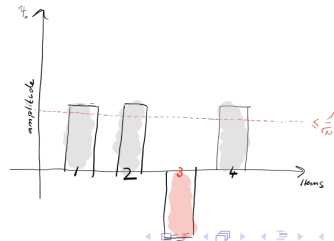
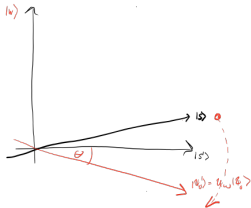
Powtarzamy odpowiednią ilość razy.

Operacja \mathcal{A} - "oracle"

Działanie operatora \mathcal{A} na stan bazowy $|\omega_i\rangle$:

$$\mathcal{A}|\omega_i\rangle = (\mathcal{I} - 2|\omega_0\rangle\langle\omega_0|)|\omega_i\rangle = |\omega_i\rangle - 2|\omega_0\rangle \cdot \begin{cases} 0, & \omega_i \neq \omega_0 \\ 1, & \omega_i = \omega_0 \end{cases}$$

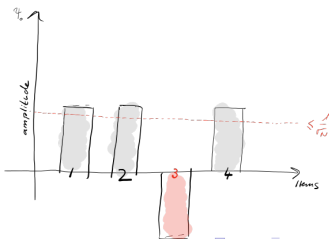
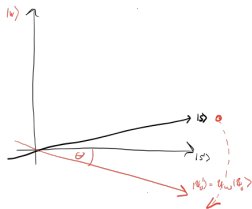
$$\mathcal{A}|\omega_i\rangle = \begin{cases} |\omega_i\rangle, & \omega_i \neq \omega_0 \\ -|\omega_i\rangle, & \omega_i = \omega_0 \end{cases}$$



Operacja \mathcal{A} - "oracle"

Działanie operatora \mathcal{A} na rejestr kwantowy:

$$\mathcal{A}|\phi\rangle = \mathcal{A}\left(\sum_{\omega=0}^{N-1} \alpha_{\omega} |\omega\rangle\right) = -\alpha_{\omega_0} |\omega_0\rangle + \sum_{\substack{\omega=0 \\ \omega \neq \omega_0}}^{N-1} \alpha_{\omega} |\omega\rangle$$

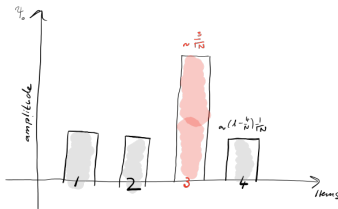
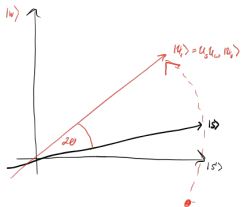


Operacja \mathcal{B}

Działanie operatora \mathcal{B} na stan bazowy $|\omega_i\rangle$:

$$\mathcal{B}|\omega_i\rangle = (2|\phi_0\rangle\langle\phi_0| - \mathcal{I})|\omega_i\rangle = 2|\phi_0\rangle \underbrace{\langle\phi_0|\omega_i\rangle}_{=\frac{1}{\sqrt{N}}} - |\omega_i\rangle = \frac{2}{\sqrt{N}}|\phi_0\rangle - |\omega_i\rangle$$

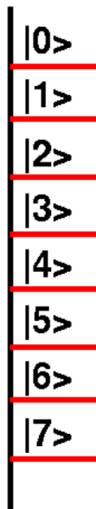
$$\langle\phi_0|\omega_i\rangle = \left(\frac{1}{\sqrt{N}} \quad \frac{1}{\sqrt{N}} \quad \cdots \quad \frac{1}{\sqrt{N}} \quad \frac{1}{\sqrt{N}}\right) \cdot (0 \quad 1 \quad \cdots \quad 0 \quad 0)^T = \frac{1}{\sqrt{N}}$$

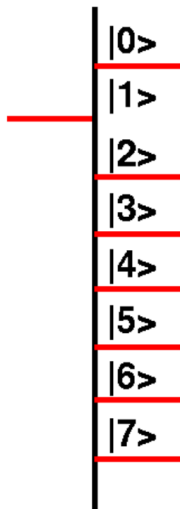


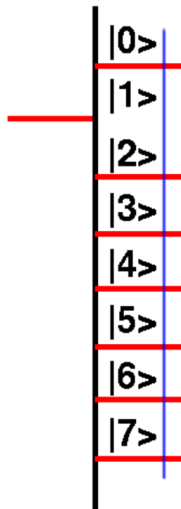
Operacja \mathcal{B}

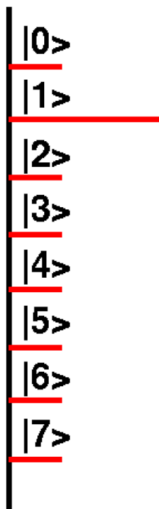
Działanie operatora \mathcal{B} na rejestr kwantowy:

$$\begin{aligned}\mathcal{B}|\phi\rangle &= \mathcal{B}\left(\sum_{\omega=0}^{N-1} \alpha_{\omega}|\omega\rangle\right) = \sum_{\omega=0}^{N-1} \alpha_{\omega} \left(\frac{2}{\sqrt{N}}|\phi_0\rangle - |\omega\rangle\right) \\&= \frac{2}{\sqrt{N}} \sum_{\omega=0}^{N-1} \alpha_{\omega} \left(\frac{1}{\sqrt{N}} \sum_{\omega=0}^{N-1} |\omega\rangle\right) - \sum_{\omega=0}^{N-1} \alpha_{\omega} |\omega\rangle \\&= \underbrace{\frac{2}{N} \sum_{\omega=0}^{N-1} \alpha_{\omega} \sum_{\omega=0}^{N-1} |\omega\rangle}_{\alpha_{avg}} - \sum_{\omega=0}^{N-1} \alpha_{\omega} |\omega\rangle \\&= \sum_{\omega=0}^{N-1} (2\alpha_{avg} - \alpha_{\omega}) |\omega\rangle = \sum_{\omega=0}^{N-1} \left(\alpha_{avg} + (\alpha_{avg} - \alpha_{\omega})\right) |\omega\rangle\end{aligned}$$





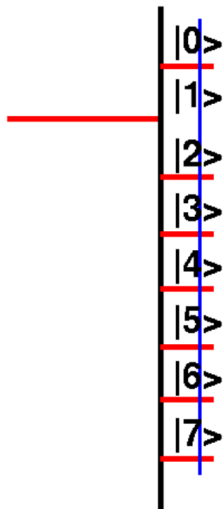


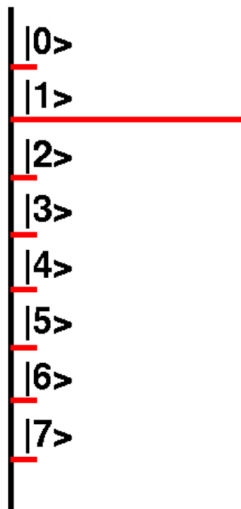


Algorytmy kwantowe - Algorytm Groovera



Algorytmy kwantowe - Algorytm Groovera



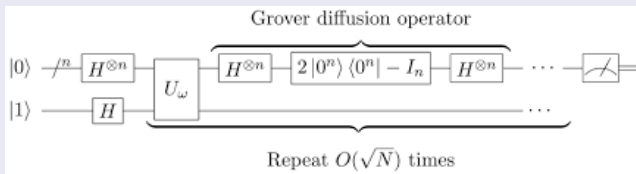


Podsumowanie i implementacja

Ilość operacji \mathcal{BA} to: $\lfloor \frac{\pi}{4} \sqrt{N} - \frac{1}{2} \rfloor \implies O(\sqrt{N})$

Po wykonanych operacjach algorytm kończy się pomiarem.

Prawdopodobieństwo sukcesu $P(\checkmark) \approx 1 - \frac{1}{N}$



Praktyczne zastosowanie

Praktyczne zastosowanie

- 1 skrypt "kubity.pdf", dr inż. Tomasz Gradowski
- 2 nagrania YT "Wszechnica CFT PAN: Części 1-12", mgr K. Kowalczyk-Muryńska
- 3 Wikipedia
- 4 "Algorytm Grovera", Dr Robert Nowotniak

Dziękuję za uwagę.
Proszę o **proste** pytania.