Modele obliczeń kwantowych

Jakub Zieliński

Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska

Notacja Diraca, "bra-ket"

Używana do opisu wektorów z tzw. przestrzeni Hilberta oraz przy korzystaniu z operatora sprzężenia hermitowskiego: $|ket\rangle \longrightarrow \langle ket|$

gdzie $|ket\rangle$ jest wektorem kolumnowym

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} & \alpha_n \end{pmatrix}^T$$

$\langle ket|$ jest wektorem w postaci rzędu

$$\begin{pmatrix} \alpha_1^* & \alpha_2^* & \cdots & \alpha_{n-1}^* & \alpha_n^* \end{pmatrix}$$

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 - Rozkład w bazie

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 - Rzutowanie

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

Rzutujmy wektor $|V\rangle$ na ortonormalny wektor bazowy $|v_1\rangle$.

$$|v_1\rangle\langle v_1||V\rangle = \alpha_1|v_1\rangle \overbrace{\langle v_1|v_1\rangle}^{1} + \alpha_2|v_1\rangle \overbrace{\langle v_1|v_2\rangle}^{0} + \ldots + \alpha_n|v_1\rangle \overbrace{\langle v_1|v_n\rangle}^{0}$$

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 $\|\alpha\|^2$ i $\|\beta\|^2$ są prawdopodobieństwami wystąpienia odpowiednich stanów własnych oraz

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

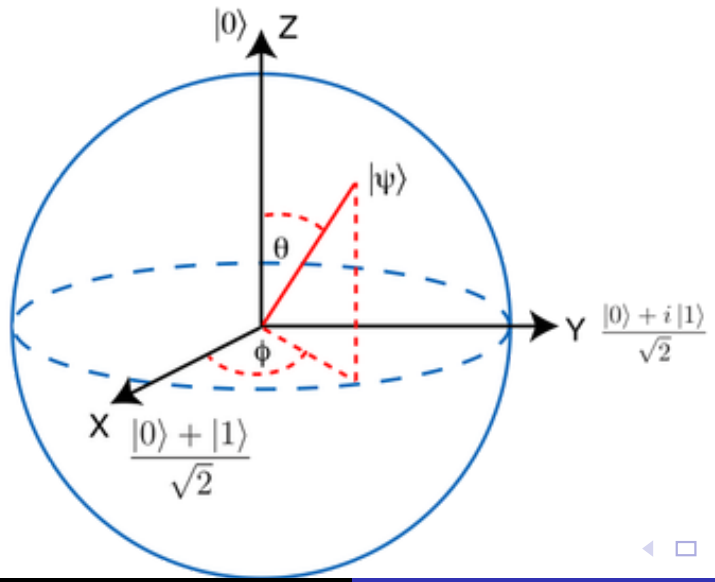
Sfera Blocha

Kubit może być również opisany przy pomocy funkcji trygonometrycznych.

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

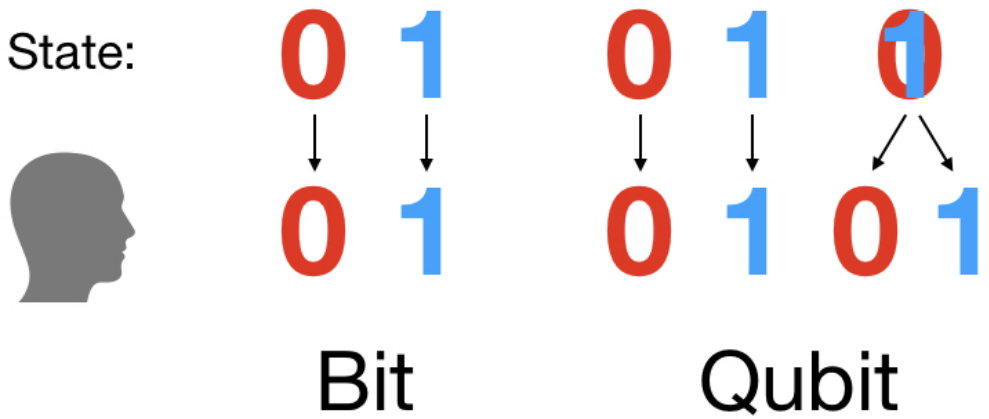
gdzie $0 \leq \phi \leq \pi$ i $0 \leq \theta \leq 2\pi$

Pozwala to na przedstawienie kubitu jako sfery Blocha.



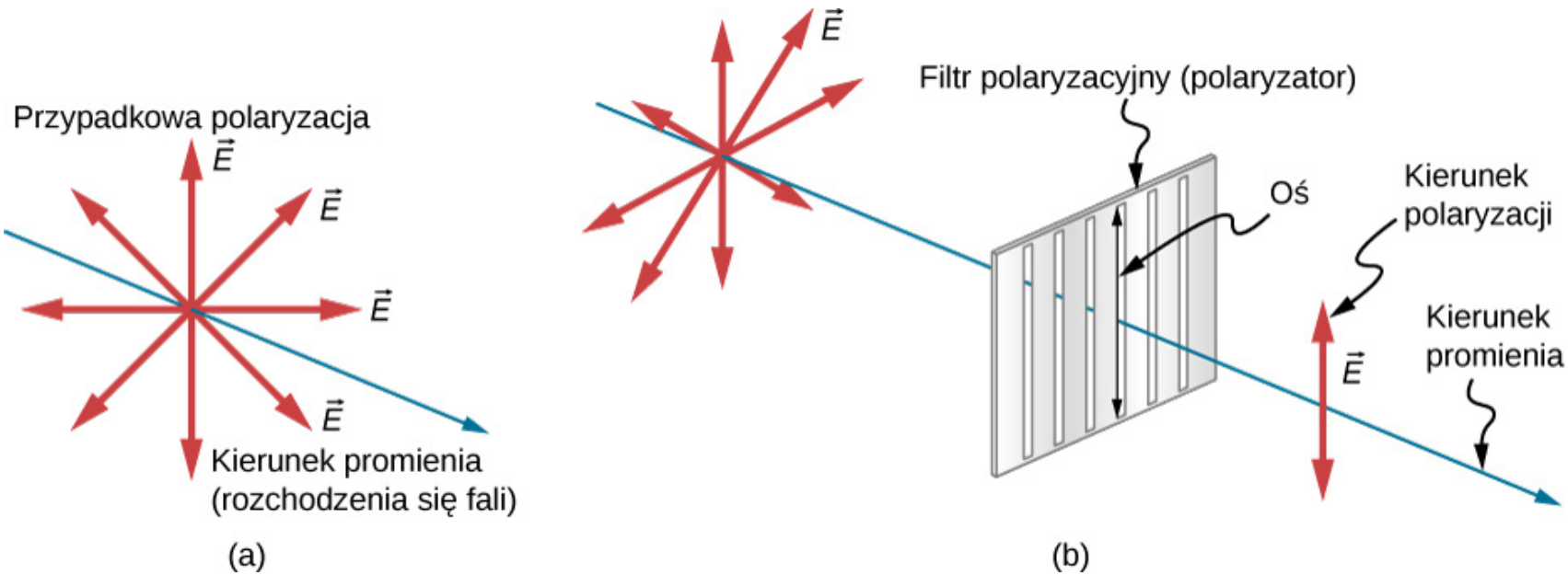
Pomiar stanu kubitu

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 przyjmuj wartość pomiaru. *np.* $|\phi\rangle \longrightarrow |1\rangle$



Pomiar stanu kubitu

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

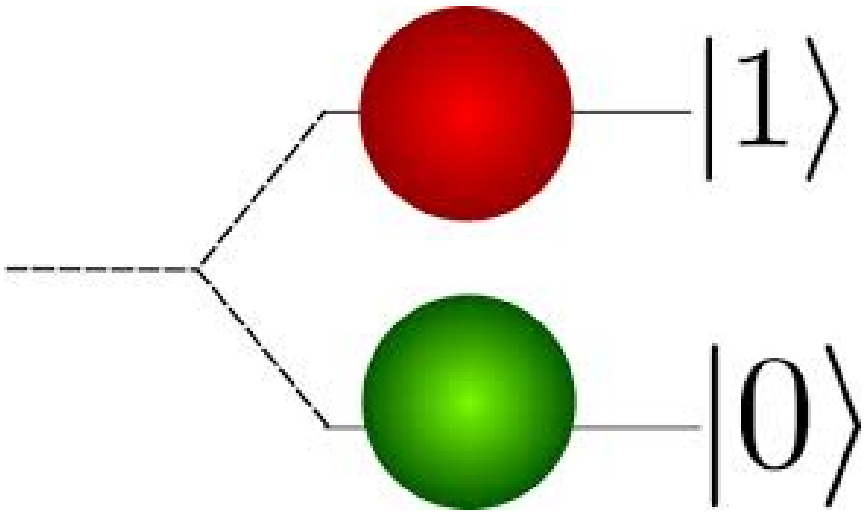


Podstawowe operacje na kubitach

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

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

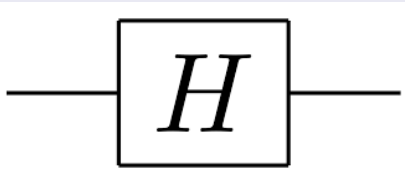


Bramka Hadamarda

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.

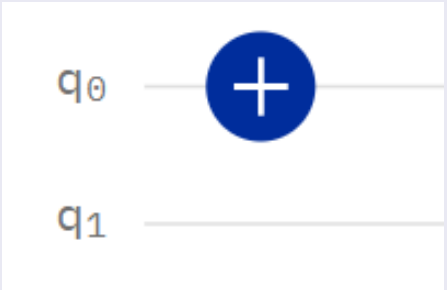
Bramka NOT, $\hat{X}$

Bramka neguje stan kwantowy, podobnie jak klasyczny NOT.

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

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

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



Bramka $\hat{Y}$

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

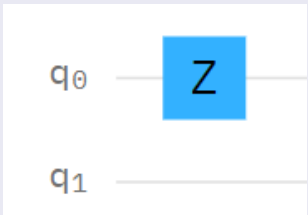
$$\hat{Y}\left(\alpha|0\rangle+\beta|1\rangle\right) = -i\beta|0\rangle+i\alpha|1\rangle$$

$\hat{Y}\hat{Y}$ jest macierzą I.

Bramka $\hat{Z}$

Bramka zmiany fazy o π.

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



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

$\hat{Z}\hat{Z}$ jest macierzą I.

Stany wielokubitowe

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 dwukubtitowe

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

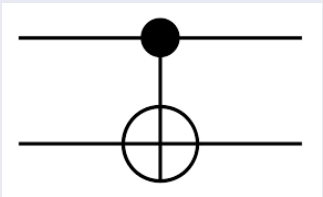
$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Bramka CNOT

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

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

$$\hat{CNOT}|00\rangle = |00\rangle$$
$$\hat{CNOT}|01\rangle = |01\rangle$$
$$\hat{CNOT}|10\rangle = |11\rangle$$
$$\hat{CNOT}|11\rangle = |10\rangle$$



Splątanie kwantowe

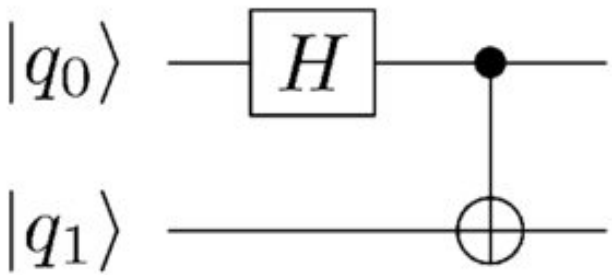
Stan splątany

1. Stanu układu nie da się "rozsupłać".
2. Zmiana stanu 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.

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



Wszystkie przypadki "wejścia"

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

Stany Bell'a

Tworzą alternatywną bazę dla układów 2 kubitowych.

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \qquad |\phi^-\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big) \qquad |\psi^-\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$$

Dowód splątania

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

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.

Protokoły kwantowe - gęste kodowanie

Cel procedury

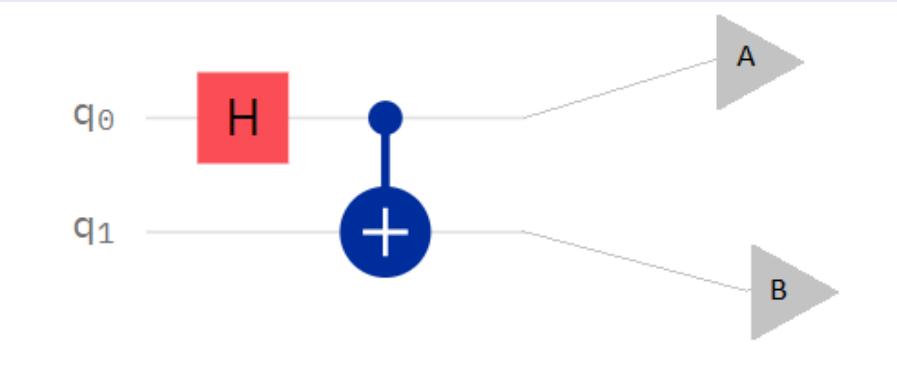
Zakodowanie dwu-bitowej informacji w jednym kubicie.

Procedura

1. Przygotowanie splątanego układu
2. Kodowanie w A
3. Przesył kubitu z A do B
4. Dekodowanie w B

Krok nr 1

Splątanie kubitów $|0_A\rangle$ i $|0_B\rangle$w laboratorium i przekazanie ich do punktów A i B.



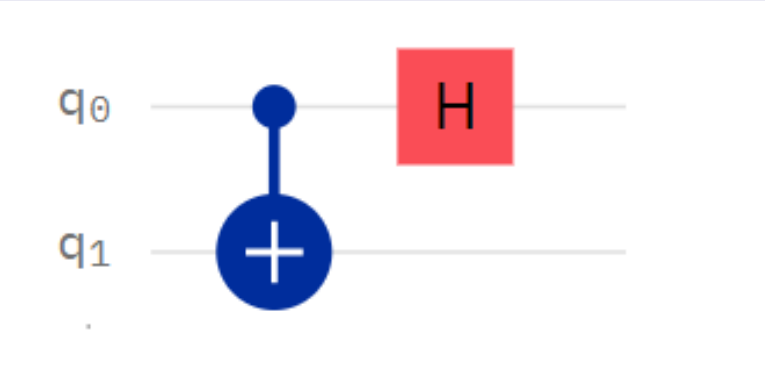
Krok nr 2

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

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

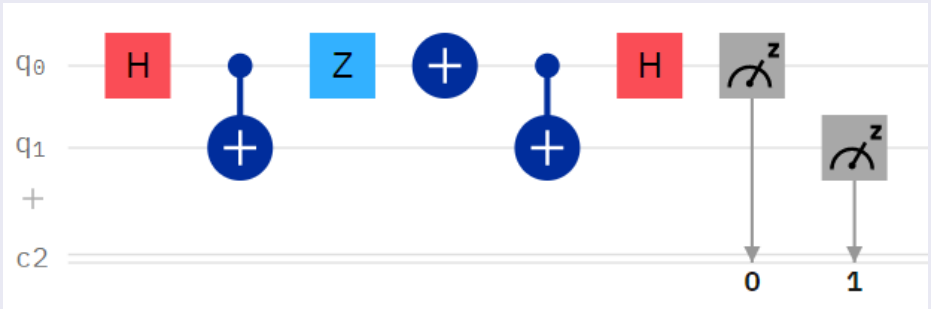
Krok nr 3

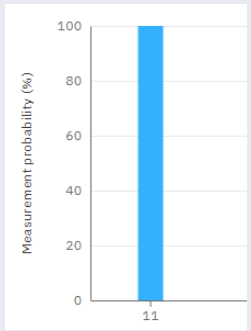
Przekazanie kubitu z A do B i wykonanie dekodowania obwodem odwrotnym do obwodu splątującego.



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.





Protokoły kwantowe - kwantowa "teleportacja"

Cel procedury

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

Procedura

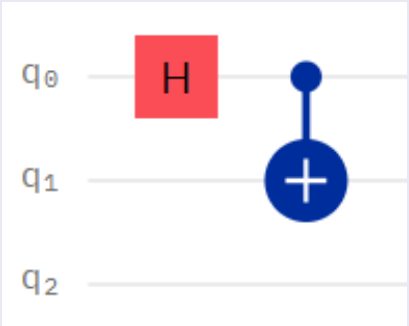
1. Umieszczenie splątanych kubitów w A i B.
2. Wykonanie pomiaru w bazie Bella, na kubitach z A.
3. Klasyczny transport informacji o wyniku pomiaru do B.
4. Dekodowanie kubitu w B.

Krok 1

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

Stan układu :

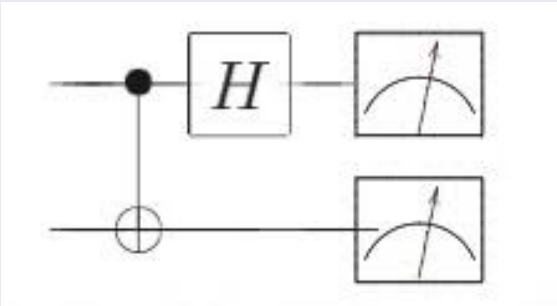
$$(\alpha|0\rangle+\beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)=\frac{1}{\sqrt{2}}(\alpha|000\rangle+\alpha|011\rangle+\beta|100\rangle+\beta|111\rangle)$$



Krok 2

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

$$
\begin{aligned}
|00\rangle &= |\phi^+\rangle + |\phi^-\rangle \\
|01\rangle &= |\psi^+\rangle + |\psi^-\rangle \\
|10\rangle &= |\psi^+\rangle - |\psi^-\rangle \\
|11\rangle &= |\phi^+\rangle - |\phi^-\rangle
\end{aligned}
$$

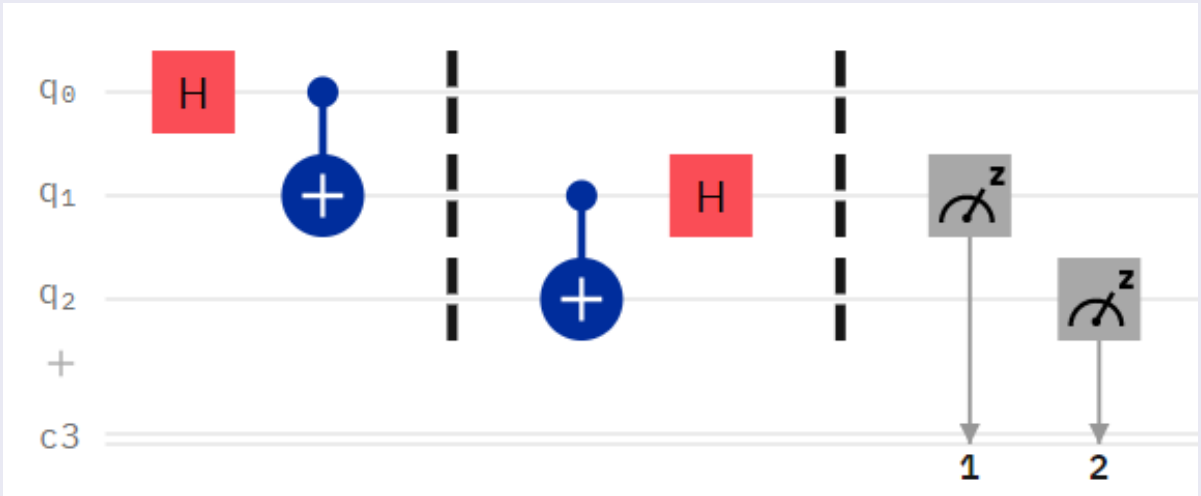


Przy pomocy powyższych zależności otrzymujemy:

$$
\begin{aligned}
\left(\tfrac{1}{\sqrt{2}}\right)^2 \Big[&|\phi^+\rangle\big(\alpha|0\rangle + \beta|1\rangle\big) + |\psi^+\rangle\big(\alpha|1\rangle + \beta|0\rangle\big) + \\
&|\phi^-\rangle\big(\alpha|0\rangle - \beta|1\rangle\big) + |\psi^-\rangle\big(\alpha|1\rangle - \beta|0\rangle\big) \Big]
\end{aligned}
$$

Krok 3

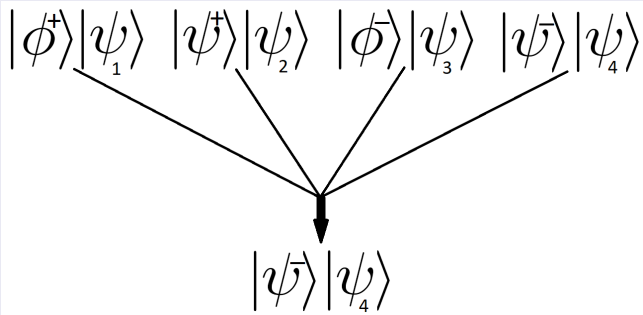
W zależności o wyniku pomiaru do B zostaje przekazana informacja o sposobie przywrócenia informacji o $|\psi\rangle$ na kubicie pozostającym w B.



Krok 4

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

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



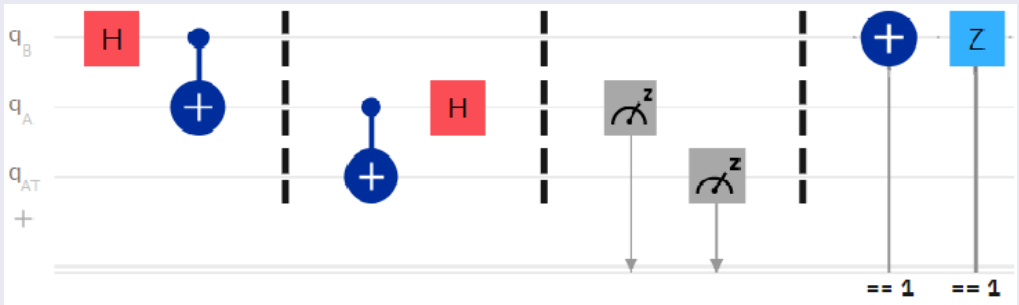
Krok 4

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 $|\psi^-\rangle\big(\alpha|1\rangle - \beta|0\rangle\big)$ 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 $f : N \to \{0, 1\}$, dana wzorem

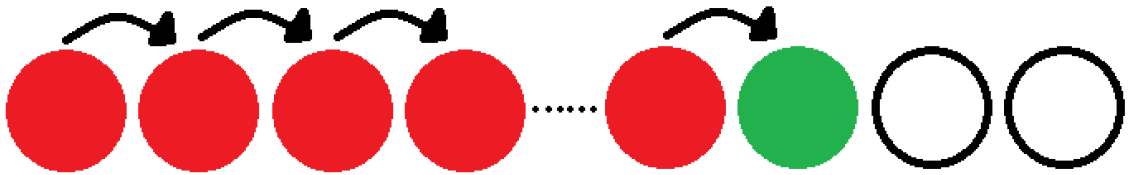
$$f(x) = \begin{cases} 0, & x \neq x_s \\ 1, & x = x_s \end{cases}$$

Chcemy poznać wartość x_s.

Podejście 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.

1. Przygotowanie rejestru
2. "Oracle" wskazuje szukany element
2. Wzmacniamy amplitudę szukanego elementu
3. Pomiar

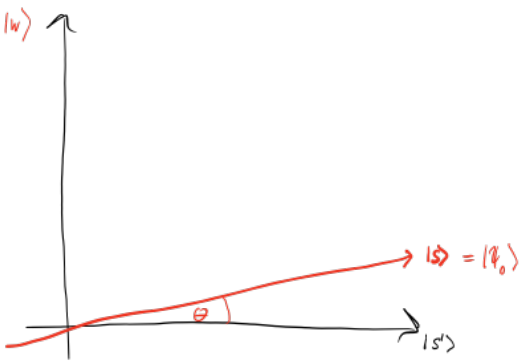
Krok 1 - Przygotowanie rejestru

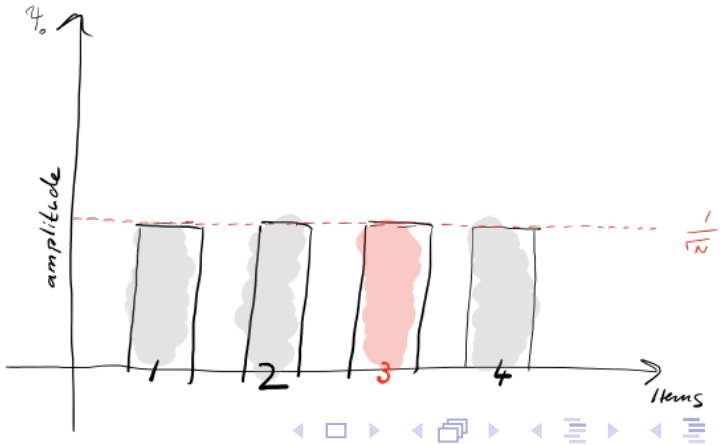
Niech rejestr kwantowy będzie dany funkcją falową :

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

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

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





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:

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

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

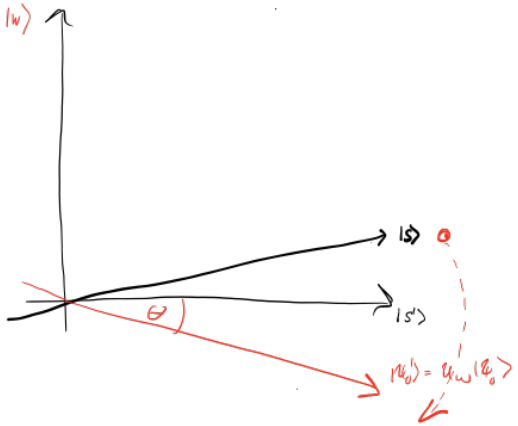
Powtarzamy odpowiednią ilość razy.

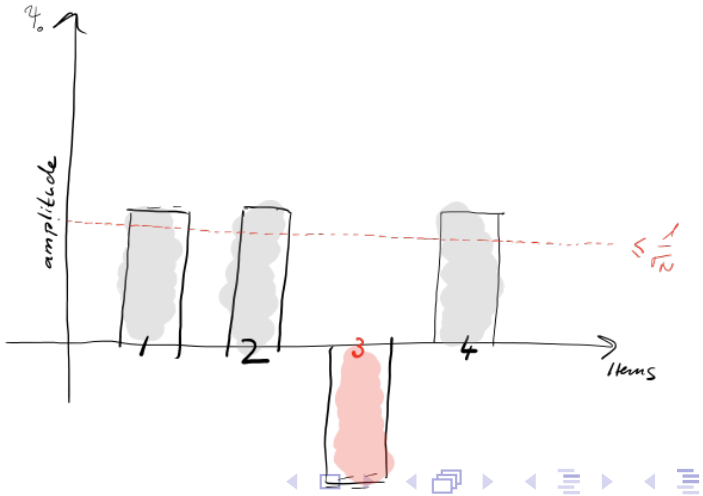
Operacja $\mathcal{A}$ - "oracle"

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

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

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

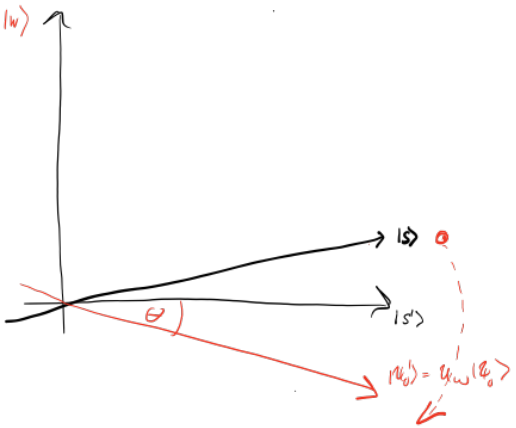


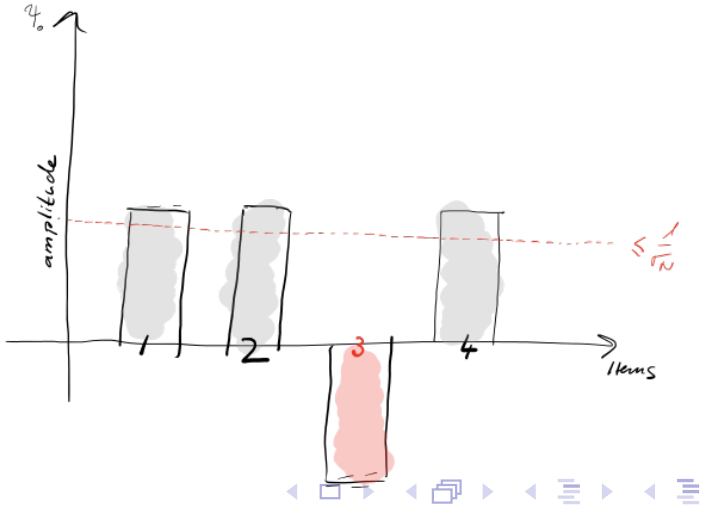


Operacja $\mathcal{A}$ - "oracle"

Działanie operatora $\mathcal{A}$ na rejestr kwantowy:

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



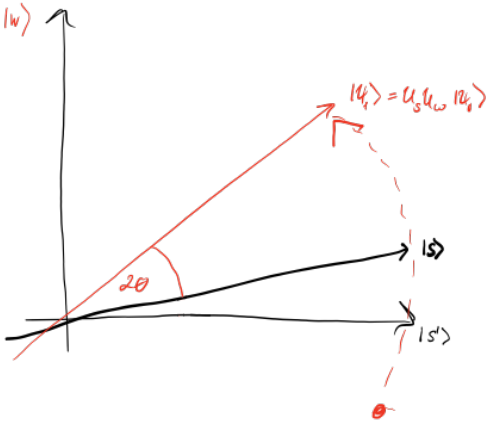


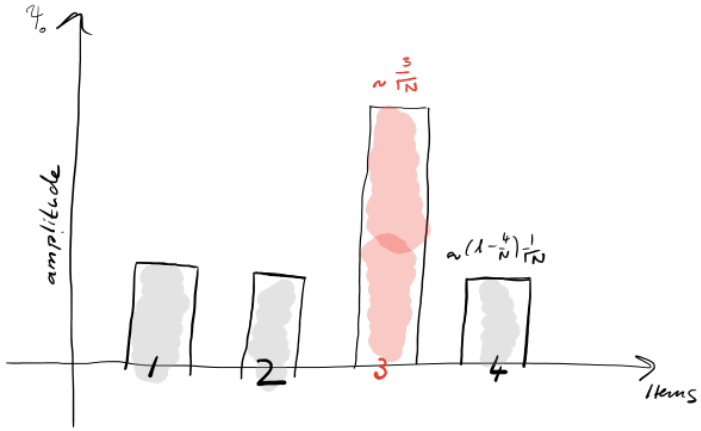
Operacja $\mathcal{B}$

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

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

$$\langle\phi_0|\omega_i\rangle = \begin{pmatrix} \frac{1}{\sqrt{N}} & \frac{1}{\sqrt{N}} & \cdots & \frac{1}{\sqrt{N}} & \frac{1}{\sqrt{N}} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \end{pmatrix}^T = \frac{1}{\sqrt{N}}$$





Operacja $\mathcal{B}$

Działanie operatora $\mathcal{B}$ na rejestr kwantowy:

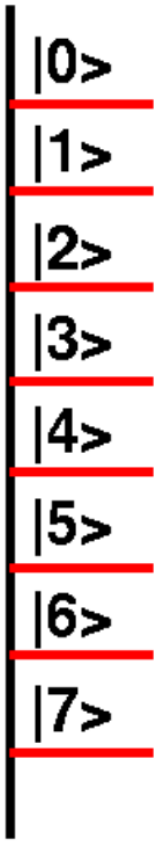
$$\mathcal{B}|\phi\rangle = \mathcal{B}\Big(\sum_{\omega=0}^{N-1}\alpha_\omega|\omega\rangle\Big) = \sum_{\omega=0}^{N-1}\alpha_\omega\Big(\frac{2}{\sqrt{N}}|\phi_0\rangle - |\omega\rangle\Big)$$

$$= \frac{2}{\sqrt{N}}\sum_{\omega=0}^{N-1}\alpha_\omega\Big(\frac{1}{\sqrt{N}}\sum_{\omega=0}^{N-1}|\omega\rangle\Big) - \sum_{\omega=0}^{N-1}\alpha_\omega|\omega\rangle$$

$$= 2\underbrace{\frac{1}{N}\sum_{\omega=0}^{N-1}\alpha_\omega}_{\alpha_{avg}}\sum_{\omega=0}^{N-1}|\omega\rangle - \sum_{\omega=0}^{N-1}\alpha_\omega|\omega\rangle$$

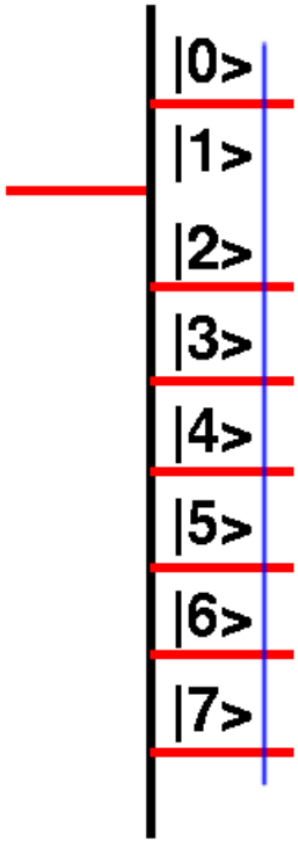
$$= \sum_{\omega=0}^{N-1}\big(2\alpha_{avg} - \alpha_\omega\big)|\omega\rangle = \sum_{\omega=0}^{N-1}\Big(\alpha_{avg} + (\alpha_{avg} - \alpha_\omega)\Big)|\omega\rangle$$

Algorytmy kwantowe - Algorytm Groovera



Algorytmy kwantowe - Algorytm Groovera

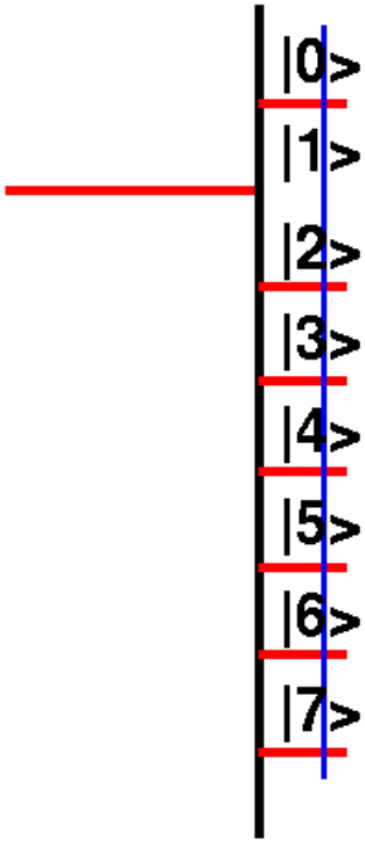
Algorytmy kwantowe - Algorytm Groovera



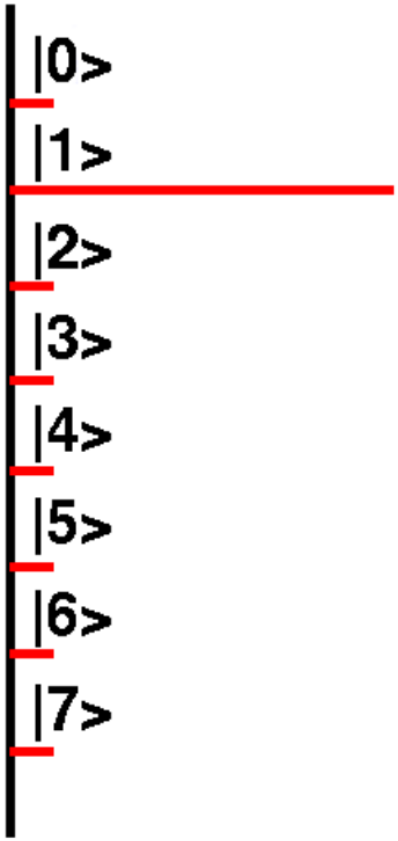
Algorytmy kwantowe - Algorytm Groovera

Algorytmy kwantowe - Algorytm Groovera

Algorytmy kwantowe - Algorytm Groovera



Algorytmy kwantowe - Algorytm Groovera

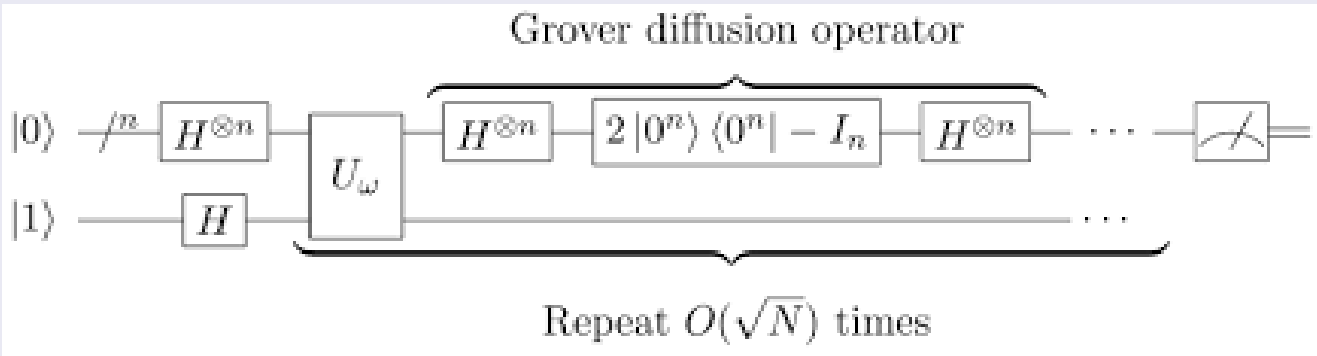


Podsumowanie i implementacja

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

Jeżeli przygotujemy "Oracle", który bedzię miał do danych recordu, naturalnym jest użycie algorytmu przy obsłudze baz danych.

Pros:

1. Osiągnięcie kwantowego przyspieszenia
2. Bardzo użyteczne dla IoT

Cons:

1. Kosztowny "Oracle" : $O(N)$
2. Zmiana elementu szukanego $\longrightarrow$ nowy "Oracle"
3. Rozmiar układu rośnie wraz z N
4. Trzeba być **niezłym** fizykiem

Bibliografia

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

Koniec

Dziękuję za uwagę.
Proszę o proste pytania.