Komputer kwantowy
Zasady funkcjonowania

Dr hab. inż. Krzysztof Giaro
Politechnika Gdańska
Wydział ETI

Obliczenia kwantowe.

R. Feynman [1985]

• symulację zachowania układu kwantowego należy przeprowadzić na "maszynie" kwantowej.

D. Deutsch [1985,1989]

• modele obliczeń: kwantowa maszyna Turinga i "sieć" q–bramek.

P. Shor [1995]

• pierwszy kwantowy algorytm: faktoryzacja. Czas $O(n^3)$.

L. Grover [1996]

• wyszukiwanie spośród N elementów jednego o pewnej własności. Liczba sprawdzeń $O(N^{1/2})$.

Kryptografia kwantowa.

Protokoły zdalnego uzgadniania klucza.

• Użytkownicy A i B chcą ustalić wspólny losowy ciąg binarny (klucz) mogący posłużyć do bezpiecznego kodowania korespondencji transmitowanej kanałem publicznym.

• Zasady fizyki kwantowej gwarantują poufność (podsłuch wykluczony) – ewentualna ingerencja osoby trzeciej wprowadza obserwowalne zaburzenie widoczne dla A i B.

- *BB84*: C. Bennett, G. Brassard [1984]
- Z wykorzystaniem *stanów splątanych*, A. Ekert [1991]

☺ **Pierwsze zastosowania komercyjne**

• Bity reprezentują dwa rodzaje polaryzacji fotonów przesyłanych światłowodami.

• Obecny zasięg rzędu 100km.

Fizyka klasyczna a kwantowa

Fizyka klasyczna

• zgodna z intuicją wizja świata,

• **determinizm**: “dalsze losy” cząstki są jednoznacznie wyznaczone przez jej bieżące położenie i pęd.

Fizyka kwantowa

• prawa natury okazują swój niecodzienny, **probabilistyczny** charakter,

• zasada **nieoznaczoności** (Heisenberg):

1. nie można jednocześnie wyznaczyć położenia i pędu cząstki,
2. nie ma “delikatnych” pomiarów, obserwacja zaburza układ
3. uzyskiwane wyniki mają charakter losowy.

Fizyka klasyczna a kwantowa

Przykład. Ruch cząstki w zewnętrznym polu.

Obraz klasyczny:

• współrzędne (x_1,x_2,x_3),

• ich wartości zmieniają się w czasie zgodnie z równaniami ruchu (determinizm).

$$\frac{\partial^2 x_i}{\partial t^2} = -\frac{1}{m}\frac{\partial V(x_1,x_2,x_3)}{\partial x_i},$$

$$i = 1,2,3.$$

Obraz kwantowy:

• zespolona **funkcja falowa** $\psi(x_1,x_2,x_3)$,

• zmienia się ona w czasie zgodnie z **równaniem Schrödingera** (determinizm).

$$\frac{\partial \psi}{\partial t} = -\frac{2\pi\imath}{h} H\psi$$

• $|\psi(x_1,x_2,x_3)|^2$ – gęstość prawdopodobieństwa wykrycia cząstki w punkcie (losowość).

Stan układu kwantowego, przestrzeń stanów

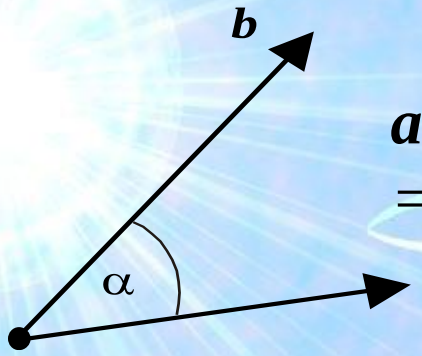
Postulat *I*. ***Z układem fizycznym związana jest tzw.* przestrzeń Hilberta*: przestrzeń liniowa nad ciałem liczb zespolonych z iloczynem skalarnym.***

$\langle\psi|\phi\rangle=\langle\phi|\psi\rangle^*$

$\langle\psi|c\phi+d\gamma\rangle=c\langle\psi|\phi\rangle+d\langle\psi|\gamma\rangle$

$\langle\psi|\psi\rangle\geq 0$

$\langle\psi|\psi\rangle=0 \Leftrightarrow \psi=0$



$\boldsymbol{a}\circ\boldsymbol{b} = |\boldsymbol{a}||\boldsymbol{b}|\cos\alpha = a_x b_x + a_y b_y + a_z b_z$

- Iloczyn skalarny określa **normę** (**długość**) wektora ψ: $|\psi|=\langle\psi|\psi\rangle^{1/2}$.
- Wektory ψ,ϕ są **ortogonalne** ($\psi\perp\phi$), gdy $\langle\psi|\phi\rangle=0$.

Stan układu kwantowego, przestrzeń stanów

Postulat *I*. ... ***Układ może przyjmować stany będące wektorami jednostkowymi jego przestrzeni stanów.***

Przykład.

- Funkcje falowe cząstek.
- Przestrzeń L tworzą funkcje $\psi(x_1,x_2,x_3)$ całkowalne z kwadratem.
- Iloczyn skalarny

$$\langle \psi|\phi\rangle=\int_R{}^3 [\psi(x_1,x_2,x_3)^*]\phi(x_1,x_2,x_3)\, dx_1dx_2dx_3.$$

Stan układu kwantowego, przestrzeń stanów

Przykład. Obliczenia kwantowe przeprowadza się *wyłącznie w przestrzeniach skończonego wymiaru!*

- Układy o skończenie wymiarowej przestrzeni stanów.
- **Przestrzeń C^n** tworzą *n*–tki zespolone.

$$\phi = \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{bmatrix} \quad \psi = \begin{bmatrix} d_1 \\ d_2 \\ \dots \\ d_n \end{bmatrix}$$

Operacje liniowe:

$$c\phi = c\begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{bmatrix} = \begin{bmatrix} cc_1 \\ cc_2 \\ \dots \\ cc_n \end{bmatrix}$$

$$\phi + \psi = \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{bmatrix} + \begin{bmatrix} d_1 \\ d_2 \\ \dots \\ d_n \end{bmatrix} = \begin{bmatrix} c_1 + d_1 \\ c_2 + d_2 \\ \dots \\ c_n + d_n \end{bmatrix}$$

Baza standardowa:

$$\phi_1 = \begin{bmatrix} 1 \\ 0 \\ \dots \\ 0 \end{bmatrix}, \phi_2 = \begin{bmatrix} 0 \\ 1 \\ \dots \\ 0 \end{bmatrix}, \dots, \phi_n = \begin{bmatrix} 0 \\ 0 \\ \dots \\ 1 \end{bmatrix}$$

$$\langle \phi | \psi \rangle = \sum_{j=1}^{n} c_j^* \cdot d_j$$

$$\|\phi\| = \sqrt{\sum_{j=1}^{n} |c_j|^2}$$

Stan układu kwantowego, przestrzeń stanów

Postulat II. ***Ewolucja czasowa izolowanego układu kwantowego jest deterministyczna. Zmiany stanu w czasie opisuje*** **operator** $U(t)$**:** $L \to L$

$$\psi(t) = U(t)\ \psi(0)$$

- ***jest on*** **liniowy:**

$$U(t)(c\psi + d\phi) = cU(t)\psi + dU(t)\phi$$

- **unitarny** **(*nie zmienia iloczynu skalarnego*):**

$$\langle U(t)\psi | U(t)\phi \rangle = \langle \psi | \phi \rangle$$

Stan układu kwantowego, przestrzeń stanów

Postulat *III*. Pomiar kwantowy.

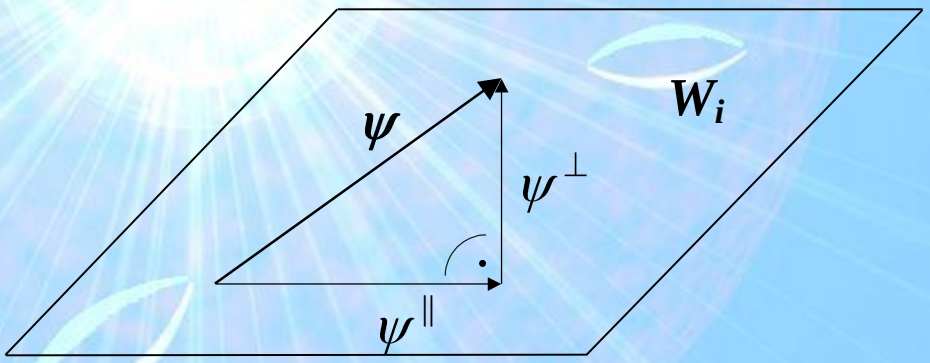
Badamy pewną wielkość fizyczną.

- ***Każdej możliwej jej wartości*** w_i ***odpowiada liniowa podprzestrzeń stanów*** $W_i \subseteq L$***, dla których wielkość ta ma określoną wartość równą*** w_i***,***
- ***przestrzenie odpowiadające różnym wartościom*** $w_i \neq w_j$ ***są prostopadłe*** $(W_i \perp W_j)$***,***

Stan układu kwantowego, przestrzeń stanów

Postulat *III*. Pomiar kwantowy. ...

• ***niech stan*** $\psi = \psi^{\parallel} + \psi^{\perp}$, ***gdzie*** $\psi^{\parallel} \in W_i$, $\psi^{\perp} \perp W_i$. ***Dokonany przez obserwatora pomiar wielkości fizycznej zwróci wynik*** w_i ***z prawdopodobieństwem równym*** $|\psi^{\parallel}|^2$, ***następuje wtedy*** **przeskok kwantowy** $\psi \to \psi^{\parallel}$.



• Stany ortogonalne $\psi \perp \phi$ są **całkowicie rozróżnialne**.

Bity i bramki kwantowe

Bit kwantowy (**qbit**)

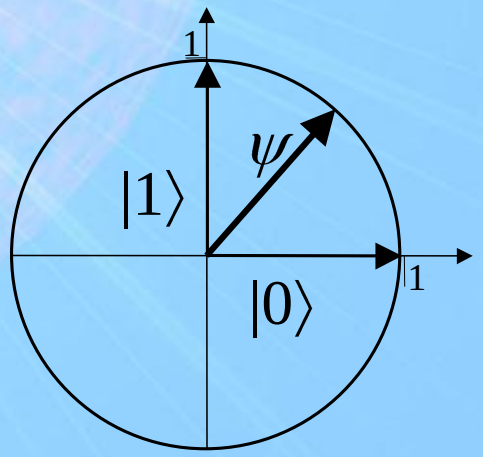
- układ kwantowy o dwuwymiarowej przestrzeni stanów,
- konkretny stan takiego układu,
- wektor z C^2.

Stany bazowe: $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ oczywiście $|0\rangle \perp |1\rangle$.

Dopuszczalnym stanem bitu kwantowego jest dowolny wektor jednostkowy

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

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



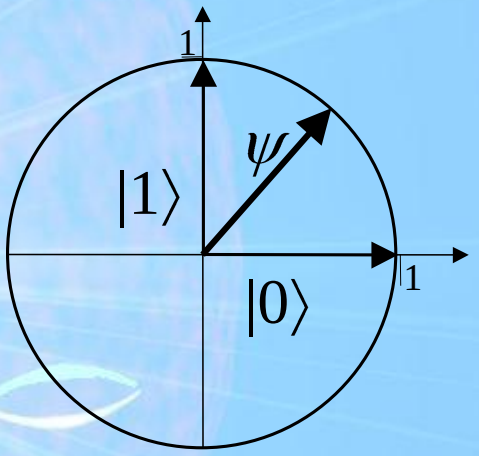
Bity i bramki kwantowe

Bit kwantowy (qbit)

Dopuszczalnym stanem bitu kwantowego jest dowolny wektor jednostkowy

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

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



Pomiar stanu qbitu przez obserwatora:

- prawdopodobieństwo odczytania 0 dla qbitu w stanie ψ (“przeskok” $\psi \rightarrow |0\rangle$) wynosi $|\langle\psi|0\rangle|^2=|\alpha|^2$.
- dla 1 prawdopodobieństwo “przeskoku” $\psi \rightarrow |1\rangle$ wynosi $|\langle\psi|1\rangle|^2=|\beta|^2$.

Bity i bramki kwantowe

Co można robić z bitami kwantowymi?
Łączyć w **rejestry kwantowe**.

Postulat *IV*. Układ złożony. ***Jeśli podukład I ma przestrzeń stanów o k wymiarach a podukład II o l wymiarach, to przestrzeń stanów układu złożonego z obu tych części ma wymiar kl.***

Przykład. Stan układu złożonego wyznaczamy za pomocą tzw. **iloczynu tensorowego**. Jeśli $\psi=[c_1,...,c_k]^T$, $\phi=[d_1,...,d_l]^T$, to całość jest w stanie

$$\psi\otimes\phi=[c_1\phi^T,...,c_k\phi^T]^T =$$
$$= [c_1d_1,\ c_1d_2,\ ...,\ c_1d_l,\quad c_2d_1,\ c_2d_2,...,\ c_2d_l,\ ...$$
$$c_kd_1,\ c_kd_2,...,c_kd_l]^T.$$

Bity i bramki kwantowe

Co można robić z bitami kwantowymi?

Łączyć w **rejestry kwantowe**.

Przykład. Rozważamy dwa q–bity w stanach:

$$\begin{bmatrix}\alpha_1\\ \beta_1\end{bmatrix},\begin{bmatrix}\alpha_2\\ \beta_2\end{bmatrix}$$

$$\begin{bmatrix}\alpha_1\\ \beta_1\end{bmatrix}\otimes\begin{bmatrix}\alpha_2\\ \beta_2\end{bmatrix}=\begin{bmatrix}\alpha_1\alpha_2\\ \alpha_1\beta_2\\ \beta_1\alpha_2\\ \beta_1\beta_2\end{bmatrix}$$

Jaki jest stan rejestru jako całości?

Rejestr **2–bitowy** ma 4–wymiarową przestrzeń stanów.

Baza:

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=|0\rangle\otimes|0\rangle,\quad\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=|0\rangle\otimes|1\rangle,\quad\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=|1\rangle\otimes|0\rangle,\quad\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=|1\rangle\otimes|1\rangle$$

Stan rejestru ma postać: $\alpha|0\rangle\otimes|0\rangle+\beta|0\rangle\otimes|1\rangle+\gamma|1\rangle\otimes|0\rangle+\delta|1\rangle\otimes|1\rangle=\begin{bmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{bmatrix}$

$(|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2=1)$

Bity i bramki kwantowe

Rejestr ***n*–bitowy** ma 2^n–wymiarową przestrzeń stanów.

Baza $|0\rangle$, $|1\rangle$, ..., $|2^n-1\rangle$, przy czym:

$|i\rangle = |i_{n-1}\rangle \otimes |i_{n-2}\rangle \otimes ... \otimes |i_0\rangle =$ $\quad (i_j \in \{0,1\})$

$$= \begin{bmatrix} 0 \\ 0 \\ \dots \\ 0 \\ 1 \\ 0 \\ \dots \\ 0 \\ 0 \end{bmatrix}$$

– pozycja 0
– pozycja 1
– pozycja i
– pozycja 2^n-2
– pozycja 2^n-1

gdzie i jest liczbą o kolejnych bitach rozwinięcia dwójkowego:

$$i_{n-1}, i_{n-2}, \dots, i_0.$$

Bity i bramki kwantowe

Jeden stan może być liniową superpozycją **wielu** różnych "klasycznie rozumianych" wartości rejestru:

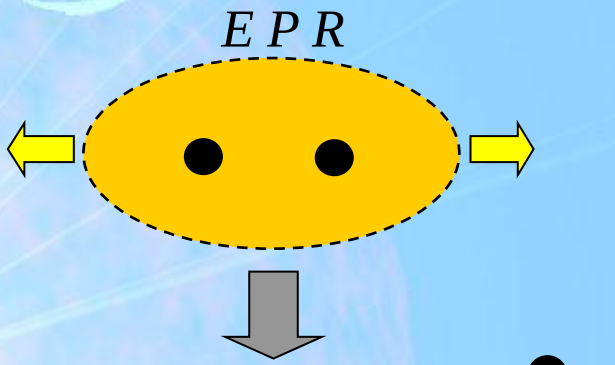
$$\psi = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \dots \\ \dots \\ \dots \\ \alpha_{2^n-2} \\ \alpha_{2^n-1} \end{bmatrix} = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

Pomiar wszystkich bitów rejestru zwróci liczbę i z prawdopodobieństwem $|\alpha_i|^2$ (przeskok $\psi \rightarrow |i\rangle$).

Bity i bramki kwantowe

Przykład. Stan EPR (Einstein-Podolsky-Rosen)

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



Mierzymy drugi bit rejestru.

- wartości 0 odpowiada podprzestrzeń rozpięta na $|0\rangle \otimes |0\rangle$, $|1\rangle \otimes |0\rangle$,
- wartości 1 odpowiada podprzestrzeń rozpięta na $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |1\rangle$.

Z prawd. ½ uzyskujemy 0 ($\Phi^+ \rightarrow |0\rangle \otimes |0\rangle$), z prawd. ½ otrzymamy 1 ($\Phi^+ \rightarrow |1\rangle \otimes |1\rangle$).

Wynik **losowy**, ale **zawsze** oba bity ustawią się jednakowo!

Bity i bramki kwantowe

Proces fizyczny przekształca stany według pewnego operatora $U(t)$. Jest on ***liniowy*** i ***unitarny***.

Bramka kwantowa

- ustalone zjawisko fizyczne mające wpływ na jeden lub kilka bitów rejestru kwantowego,
- dowolny liniowy operator unitarny działający w przestrzeni stanów kilku q–bitów.

Przykład. Negacja klasyczna

$$NOT\,|0\rangle=|1\rangle,\ NOT\,|1\rangle=|0\rangle,$$

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

Bity i bramki kwantowe

Przykład. Tego “klasycznie” zrobić się nie da:

$$\sqrt{NOT} = \frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix} \qquad \sqrt{NOT}\sqrt{NOT} = NOT$$

Przykład. Bramka Hadamarda *Hd*

$$Hd = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad Hd|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^i|1\rangle) \qquad (i \in \{0,1\})$$

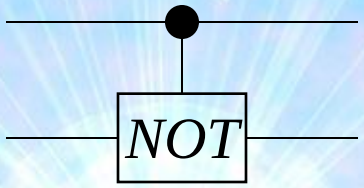
$$Hd^2 = Id$$

Bity i bramki kwantowe

Przykład. Bramka 2–qbitowa *CN*.

$$CN = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$\equiv$



Czyli dla $x,y \in \{0,1\}$ mamy $CN\ |x,y\rangle = |x,x \oplus y\rangle$.

Przykład. Najprostszy program kwantowy. Jak zrealizować zamianę stanu dwóch q–qbitów?

$$SWAP\ \psi \otimes \phi = \phi \otimes \psi$$

Bity i bramki kwantowe

Ograniczenia bramek kwantowych

- liniowość,
- unitarność,
- unitarność implikuje ***odwracalność***.

Przykład. (**Non–Clone Theorem**). Nie można kopiować nieznanego stanu jednego qbitu na drugi.

$$Copy\ \psi\otimes|0\rangle=\psi\otimes\psi$$

dla wszystkich $\psi\in C^2$.

Dowód.

$$Copy\begin{bmatrix}\alpha\\ \beta\end{bmatrix}\otimes|0\rangle=\begin{bmatrix}\alpha\\ \beta\end{bmatrix}\otimes\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}\alpha^2\\ \alpha\beta\\ \alpha\beta\\ \beta^2\end{bmatrix}$$

$$Copy\ (\alpha|0\rangle+\beta|1\rangle)\otimes|0\rangle =$$
$$= \alpha\ Copy|0\rangle\otimes|0\rangle+\beta\ Copy|1\rangle\otimes|0\rangle$$
$$= \alpha|0\rangle\otimes|0\rangle + \beta|1\rangle\otimes|1\rangle$$

Algorytm kwantowy

Struktura **procedury kwantowej**.

1. Obliczenia prowadzone są w rejestrze złożonym z q–bitów (**podrejestry**: wejściowy, wyjściowy, pomocniczy)

$$\psi_{start}=|0...0\rangle\otimes|0...0\rangle\otimes|0...0\rangle$$

2. Wprowadzenie danych

$$\psi_{in}=|dana\rangle\otimes|0...0\rangle\otimes|0...0\rangle$$

3. Układ poddajemy działaniu pewnej serii bramek kwantowych

$$\psi_{stop}=\Sigma_j\ \chi_j\ |dana\rangle\otimes|wynik_j\rangle\otimes|resztki_j\rangle$$

4. Pomiar wartości bitów (algorytm **probabilistyczny**)

$$\psi_{out}=|dane\rangle\otimes|wynik_j\rangle\otimes|resztki_j\rangle$$

Algorytm kwantowy

Na czym polega siła algorytmów kwantowych?

$$\psi_{\text{in}} = |dana\rangle \otimes |0...0\rangle \otimes |0...0\rangle \rightarrow (3)$$
$$\rightarrow \psi_{\text{stop}} = \Sigma_j \chi_j |dana\rangle \otimes |wynik_j\rangle \otimes |resztki_j\rangle$$

Liniowość algorytmu $\Rightarrow$ **kwantowe "zrównoleglenie"**

$$\Sigma_i \alpha_i \psi_{\text{in},i} = (\Sigma_i \alpha_i |dana_i\rangle) \otimes |0...0\rangle \otimes |0...0\rangle \rightarrow (3)$$
$$\rightarrow \Sigma_i \alpha_i \psi_{\text{stop},i} = \Sigma_i \Sigma_j \alpha_i \chi_{i,j} |dana_i\rangle \otimes |wynik_{i,j}\rangle \otimes |resztki_{i,j}\rangle$$

☺ **W tym samym czasie możemy przeprowadzić operacje obliczeniowe tak dla jednej danej wejściowej, jak i dla superpozycji wielu różnych wejść!**

☹ **Problem: jak odzyskać rezultaty z superpozycji???**

Algorytm Grovera

Problem:

Dany jest zbiór Q o rozmiarze $|Q|=N=2^n$ i funkcja obliczalna $f: Q \rightarrow \{0,1\}$ taka, że $\exists!_q\, f(q)=1$.

Znajdź ten unikalny element $q \in Q$.

Algorytm probabilistyczny Grovera znajduje element z prawdopodobieństwem większym od $1-1/N$ wykonując obliczenie wartości funkcji f tylko $O(N^{1/2})$ razy.
Algorytm klasyczny wymagałby $\Omega(N)$ sprawdzeń.

Algorytm Grovera

Rejestr *n*–bitowy przechowuje **numery elementów** z *Q*.

1. Ustaw rejestr w stanie “wyzerowanym”

$$\psi_{\text{pocz}} = |0_{n-1}\rangle \otimes |0_{n-2}\rangle \otimes \ldots \otimes |0_0\rangle = |0\rangle$$

2. Wykonaj na każdym jego bicie bramkę Hadamarda *Hd*

$$\psi_{\approx} = [\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)] \otimes \ldots \otimes [\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)] = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$$

– do rejestru „wpisaliśmy” superpozycję **wszystkich możliwych** numerów *n*-bitowych!

Algorytm Grovera

Rejestr *n*–bitowy przechowuje **numery elementów** z *Q*.

$$\psi_{\approx} = [\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)] \otimes \ldots \otimes [\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)] = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$$

3. Powtarzaj kolejne iteracje:

$$\psi_0 = \psi_{\approx}, \quad \psi_{k+1} = BA\ \psi_k$$

gdzie operatory:

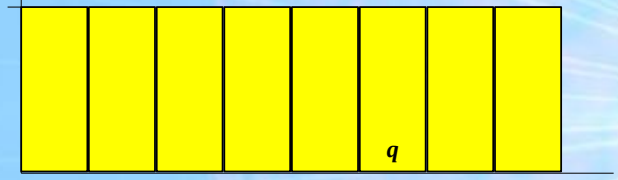
$$A\phi = \phi - 2|q\rangle\langle q|\phi\rangle,$$
$$B\phi = 2|\psi_{\approx}\rangle\langle\psi_{\approx}|\phi\rangle - \phi$$

4. Zakończ dla $k = \lfloor \pi/4 \arcsin(N^{-1/2}) \rfloor \approx \lfloor \pi N^{1/2}/4 \rfloor$. **Zmierz** wartości bitów rejestru odczytując szukane *q*.

Algorytm Grovera

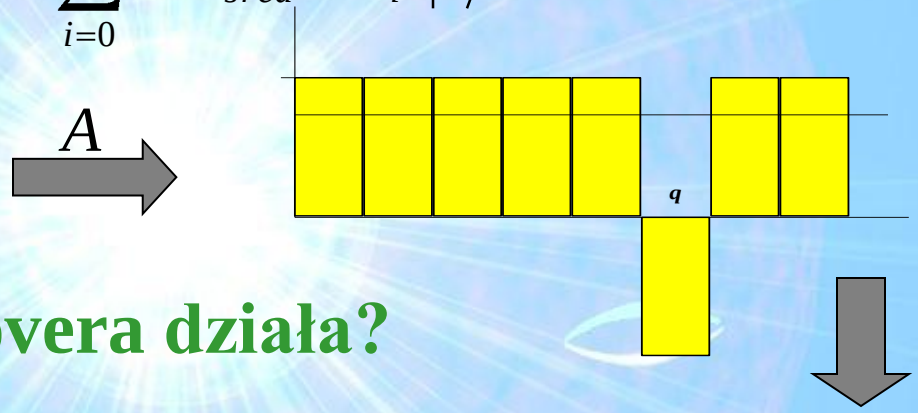
Jak działają *A*, *B*?

$$A\sum_{i=0}^{N-1}\alpha_i|i\rangle=\sum_{i=0}^{N-1}\alpha_i(-1)^{f(i)}|i\rangle$$



$$B\sum_{i=0}^{N-1}\alpha_i|i\rangle=\frac{2}{\sqrt{N}}\sum_{i=0}^{N-1}\alpha_i\left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle\right)-\sum_{i=0}^{N-1}\alpha_i|i\rangle=$$

$$=\sum_{i=0}^{N-1}(2\alpha_{sred}-\alpha_i)|i\rangle$$

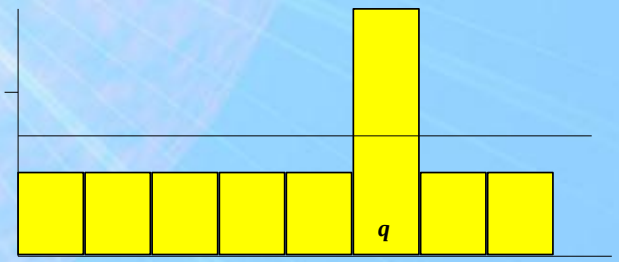


Dlaczego algorytm Grovera działa?

k–ta iteracja:

a_k – współczynnik przy $|q\rangle$

b_k – współczynnik przy $|i\rangle$, $i\neq q$.



$$a_0=b_0=1/N^{1/2}.$$

$$a_{k+1}=(1-2/N)a_k+(2-2/N)b_k$$

$$b_{k+1}=(-2/N)a_k+(1-2/N)b_k$$

Algorytm Grovera

Dlaczego algorytm Grovera działa? Rozwiązanie rekursji:

$$\mathbf{a_k=\sin[(2k+1)\arcsin(N^{-1/2})] \approx \sin((2k+1)/N^{1/2})}$$

$$b_k= (N-1)^{-1/2}\cos[(2k+1)\arcsin(N^{-1/2})]$$

Współczynnik a_k przy szukanym $|q\rangle$ zachowuje się jak **sinusoida**. Należy przerwać pętlę z chwilą, gdy zbliżymy się do **pierwszego maksimum**, tj. $k=\lfloor \pi N^{1/2}/4 \rfloor$.

Fakt. Prawdopodobieństwo sukcesu dla pomiaru wykonanego po k iteracjach algorytmu Grovera spełnia $|a_k|^2>1-1/N$.

Algorytm Grovera

Przepis na operator *A*:

Wykorzystujemy dodatkowy q–bit, “algorytm” obliczający *f*

$$U_f |x\rangle \otimes |0\rangle = |x\rangle \otimes |f(x)\rangle$$

oraz bramkę jednobitową σ_z

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

$$\sigma_z|0\rangle = |0\rangle,\ \sigma_z|1\rangle = -|1\rangle$$

Stosując kolejno na $|x\rangle \otimes |0\rangle$: U_f, σ_z na q–bicie pomocniczym, U_f^{-1} uzyskamy $(-1)^{f(x)}|x\rangle \otimes |0\rangle$.

Algorytm Grovera

Przepis na *B*: $B=Hd^{(n)}\,R\,Hd^{(n)}$, gdzie $Hd^{(n)}$ to bramka *Hd* wykonana na każdym z *n* bitów, a *R* działająca na cały rejestr ma postać:

$$R|i\rangle = \begin{cases} |0\rangle & i = 0 \\ -|i\rangle & i \neq 0 \end{cases}$$

Koszt jednej iteracji:

użyto $O(n)$ bramek kwantowych oraz dwukrotnie obliczono funkcję *f* (algorytm U_f).