1 Do czego służy algorytm Grovera

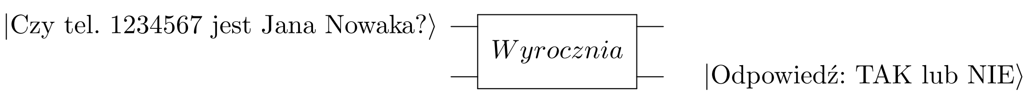
Algorytm Grovera służy do wyszukiwania rekordu w nieposortowanej bazie. Typowy przykład to "problem odwróconej książki telefonicznej" - mamy numer telefonu i chcemy sprawdzić do kogo należy.

Klasyczny algorytm potrzebuje sprawdzić po kolei wszystkie rekordy w książce telefonicznej, więc liczba zapytań jest rzędu $O(N)$, gdzie N - liczba rekordów w książce.

Kwantowy algorytm Grovera pozwala na $O(\sqrt{N})$ zapytań. Jak to robi?

2 Wyrocznia

Podstawowym założeniem algorytmu Grovera, jest założenie o posiadaniu wyroczni, która jest w stanie szybko odpowiedzieć, czy rekord, który znaleźliśmy to ten którego szukamy. Dla problemu odwróconej książki telefonicznej taka wyrocznię można stworzyć stosunkowo łatwo. Można ją np. przedstawić tak:



gdzie:

- na rejestrze wejściowym zadajemy pytanie
- na rejestrze wyjściowym otrzymujemy odpowiedź tak lub nie
- szczegółowe działanie bramki jest takie samo, jak działanie bramki uniwersalnej U_f

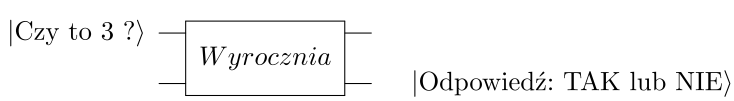
Rozwiązywany problem sprowadza się do odpytania wyroczni możliwie najmniejszą liczbę razy.

Klasycznie uruchamiamy wyrocznię $O(N)$ razy odpytując po kolei o wszystkie możliwe osoby (których jest w sumie N).

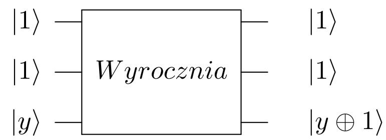
3 Wyrocznia dla prostego przypadku

Dla dokładnego zobrazowania, co dzieje się w algorytmie Grovera skupimy sie na prostym problemie. Mamy zbiór czterech liczb $\{0, 1, 2, 3\}$, z których jedna została przez kogoś wybrana, nie wiemy która. Ten ktoś dał nam wyrocznię, do której możemy zadawać pytania o konkretne liczby np. "Czy to liczba 3 ?"

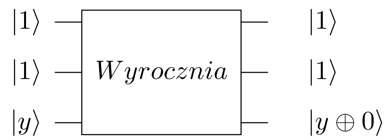
Jak będzie wyglądać taka wyrocznia?



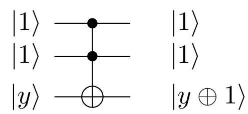
bardziej szczegółowo wyrocznia na TAK:



bardziej szczegółowo wyrocznia na NIE:



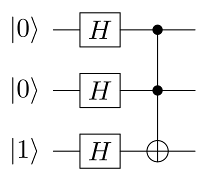
Wyrocznia, która działa odpowiada TAK dla $|11\rangle$, a NIE dla $|00\rangle$, $|01\rangle$, $|10\rangle$ to:



Bazując na tej wyroczni, można dość łatwo zbudować podobne dla $|00\rangle$, $|01\rangle$, $|10\rangle$ (patrz poprzednie zadanie domowe)

4 Jak działa wyrocznia przy zapytaniu kwantowym?

W algorytmie Grovera pytamy o wszystkie możliwości jednocześnie za pomocą bramek H



Wtedy po przejściu przez bramki H mamy

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Rozbijam sumę na składnik zawierający pytania na NIE i pytanie na TAK:

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + \frac{1}{2}|11\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

W przypadku składników na NIE przejscie przez wyrocznię nic nie zmienia, w przypadku składnika na TAK ulegają zamianie stany $|110\rangle$ oraz $|111\rangle$

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + \frac{1}{2}|11\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)$$

$\|\psi\rangle$	$Ctrl_Z \|\psi\rangle$
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|10\rangle$
$\|11\rangle$	$-\|11\rangle$

Tabela 1: Działanie bramki $Ctrl_Z$ dla stanów bazowych

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) - \frac{1}{2}|11\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Teraz mogę z powrotem złożyc składniki:

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Widać, że **wyrocznia zadziałała tak, ze odpowiedź na TAK została wyróżniona** minusem. Oczywiście przy pomiarze nic nam to nie da, konieczne są dalsze przekształcenia tego stanu.

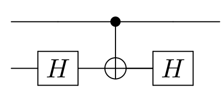
Dla dalszych rozważań oznaczę interesującą nas część wyniku wyroczni jako

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \tag{1}$$

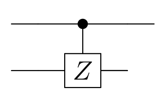
5 Inwersja

Drugą częścią algorytmu Grovera jest inversja, do której przekazujemy stan uzyskany z wyroczni czyli w naszym przykładzie $|\psi\rangle$.

Dla naszego przykładu (n=2) "sercem" inwersji jest bramka



Można pokazać, stosując zasadę HXH=Z, że bramka działa jak:



Działanie bramki na stany bazowe obrazuje tabelka 1.
Można zauważyć, że bramka ta działa tak samo jak operator $1 - 2|11\rangle\langle 11|$ wyliczając jego działanie dla stanów bazowych (działanie na pozostałe stany będzie takie samo z liniowości):

$$(1 - 2|11\rangle\langle 11|)|00\rangle = |00\rangle - 2|11\rangle \underbrace{\langle 11|00\rangle}_{\text{iloczyn skalarny=0}} = |00\rangle - 2|11\rangle \cdot 0 = |00\rangle$$

Iloczyn skalarny $\langle 11|00\rangle$

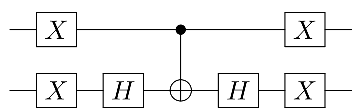
$$\begin{bmatrix}0 & 0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = 0$$

$$(1 - 2\,|11\rangle\,\langle 11|)\,|01\rangle = |01\rangle - 2\,|11\rangle \underbrace{\langle 11|01\rangle}_{\text{iloczyn skalarny=0}} = |01\rangle - 2\,|11\rangle \cdot 0 = |01\rangle$$

$$(1 - 2\,|11\rangle\,\langle 11|)\,|10\rangle = |10\rangle - 2\,|11\rangle \underbrace{\langle 11|10\rangle}_{\text{iloczyn skalarny=0}} = |10\rangle - 2\,|11\rangle \cdot 0 = |10\rangle$$

$$(1 - 2\,|11\rangle\,\langle 11|)\,|11\rangle = |11\rangle - 2\,|11\rangle \underbrace{\langle 11|11\rangle}_{\text{iloczyn skalarny=1}} = |11\rangle - 2\,|11\rangle = -\,|11\rangle$$

Aby zbudować układ inwersji "obkładamy" $Ctrl_Z$ bramkami X



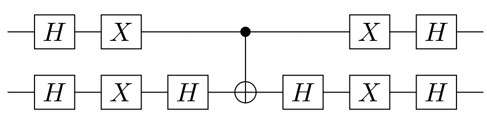
Wyliczamy "skutki obłożenia" stosując operator $1 - 2\,|11\rangle\,\langle 11|$

$$(X \otimes X)(1 - 2\,|11\rangle\,\langle 11|)(X \otimes X) =$$

$$(X \otimes X)(X \otimes X) - 2(X \otimes X)(|11\rangle\,\langle 11|)(X \otimes X) =$$

$$1 - 2(|00\rangle\,\langle 00|)$$

Ostatnim krokiem jest "obłożenie" układu bramkami H



I "skutki obłożenia" stosując operator $1 - 2\,|00\rangle\,\langle 00|$

$$(H \otimes H)(1 - 2\,|00\rangle\,\langle 00|)(H \otimes H) =$$

$$(H \otimes H)(H \otimes H) - 2(H \otimes H)(|00\rangle\,\langle 00|)(H \otimes H) =$$

$$1 - 2(|\phi\rangle\,\langle\phi|)$$

Gdzie $|\phi\rangle = (H \otimes H)\,|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

Teraz zbadamy działanie naszej inwersji $1 - 2(|\phi\rangle\,\langle\phi|)$ na stan $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$ uzyskany z wyroczni.

$$[1 - 2(|\phi\rangle\,\langle\phi|)]\,|\psi\rangle = |\psi\rangle - 2\,|\phi\rangle \underbrace{\langle\phi|\psi\rangle}_{\text{iloczyn skalarny }=\frac{1}{2}} = |\psi\rangle - |\phi\rangle$$

.

Iloczyn skalarny $\langle\phi|\psi\rangle$

$$\begin{bmatrix}\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2}\end{bmatrix} \cdot \begin{bmatrix}\frac{1}{2}\\ \frac{1}{2}\\ \frac{1}{2}\\ -\frac{1}{2}\end{bmatrix} = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} - \frac{1}{4} = \frac{1}{2}$$

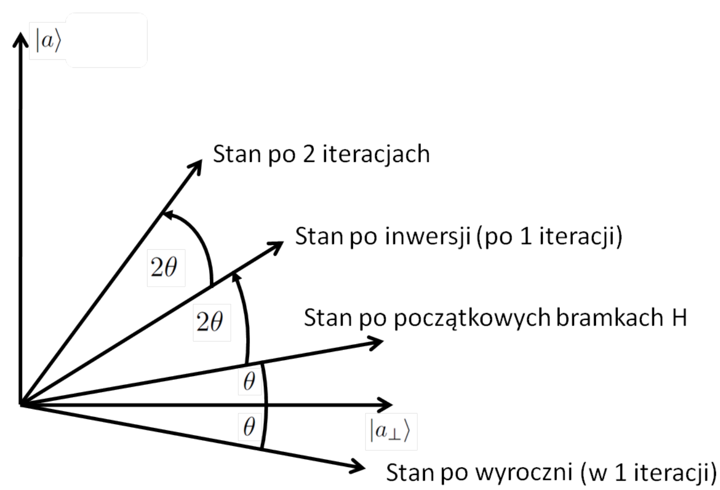
Stan uzyskany po inwersji to: $|\psi\rangle - |\phi\rangle$ czyli:

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

Inwersja wzmocniła amplitudę stanu, który był wyróżniony !

6 Iteracja Grovera

Na iterację Grovera składa się wykonanie jednej wyroczni i jednej inwersji. Jak widać, dla zapytania mieszczącego się na 2 qbitach wystarczy wykonać jedną iterację. W dalszej części będziemy używać oznaczenia n na liczbe qbitów mieszczących nasze zapytanie. Tutaj $n = 2$, ponieważ szukamy wśród liczb $\{0, 1, 2, 3\}$ mieszczących się na 2 qbitach. Dla większych n liczba iteracji rośnie.



Rysunek 1: Graficzna interpretacja algorytmu Grovera dla n qbitów

7 Interpretacja geometryczna

[opis rysunku 1 na filmiku] Jak widać, po każdej iteracji wynik obraca się o kąt 2θ w kierunku przeciwnym do wskazówek zegara.

[opis rysunku 2 na filmiku] Dla n=2 kąt θ obliczamy korzystając z interpretacji geomentycznej iloczynu skalarnego:

$$\langle a|\phi\rangle = ||a|| \cdot ||\phi|| \cdot cos(\alpha)$$

$$\langle a|\phi\rangle = \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \frac{1}{2}$$

Ponieważ długości wektorów stanu są zawsze =1, to:

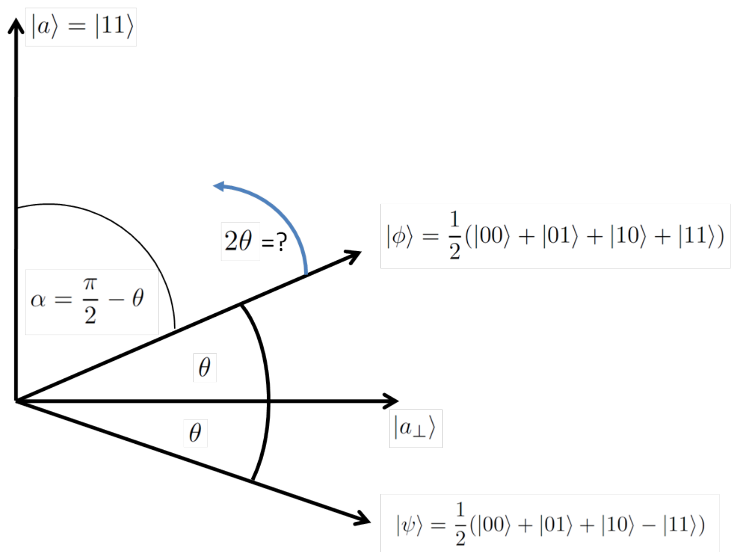
$$cos(\alpha) = \frac{1}{2}$$

$$\alpha = \frac{\pi}{3}$$

$$\theta = \frac{\pi}{2} - \frac{\pi}{3} = \frac{\pi}{6}$$

Po pierwszej iteracji obrócimy stan ϕ o

$$2\theta = 2\frac{\pi}{6} = \alpha$$



Rysunek 2: Graficzna interpretacja algorytmu Grovera dla dwóch qbitów

Czyli znajdziemy się dokładnie w stanie $|a\rangle$

Dla zapytania mieszczącego się na n qbitach liczba iteracji jest większa, mozna ją oszacować z interpretacji geometrycznej. W ogólności dla n-qbitowego zapytania (korzytystając z amplitud dla stanu $H^{\otimes n}|0^{\otimes n}\rangle$) mamy

$$sin(\theta) = cos(\frac{\pi}{2} - \theta) = \langle a|\phi\rangle = \frac{1}{2^{\frac{n}{2}}}$$

Im większe n, tym dokładniej możemy przybliżyć

$$\theta \approx sin(\theta) = \frac{1}{2^{\frac{n}{2}}}$$

Ilość iteracji - szacujemy na podstawie, ile razy 2θ mieści się w $\frac{\pi}{2}$

$$\frac{\frac{\pi}{2}}{2\theta} = \frac{\frac{\pi}{4}}{\theta} = \frac{\frac{\pi}{4}}{\frac{1}{2^{\frac{n}{2}}}} = \frac{\pi}{4}2^{\frac{n}{2}} = \frac{\pi}{4}\sqrt{2^n} = \frac{\pi}{4}\sqrt{N}$$

gdzie $N = 2^n$ liczba możliwych elementów.

[demo algorytmu Grovera]