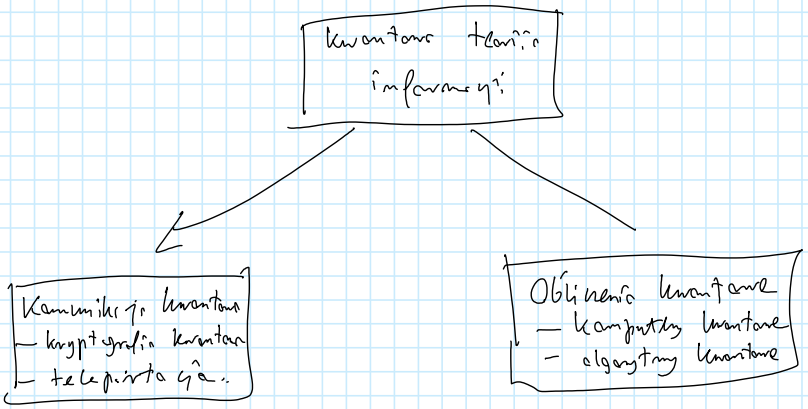
11-obliczenia kwantowe

3 maja 2011 10:47

Obliczenia kwantowe

1. Wstęp

Kwantowa teoria informacji – przetwarzanie informacji kwantowej
2 prawa fizyki kwantowej, operowanie na pojedynczych
układach kwantowych, atomach, fotonach



Dotychczas mówiliśmy głównie o kwantowej
Czas zacząć mówić o obliczeniach.

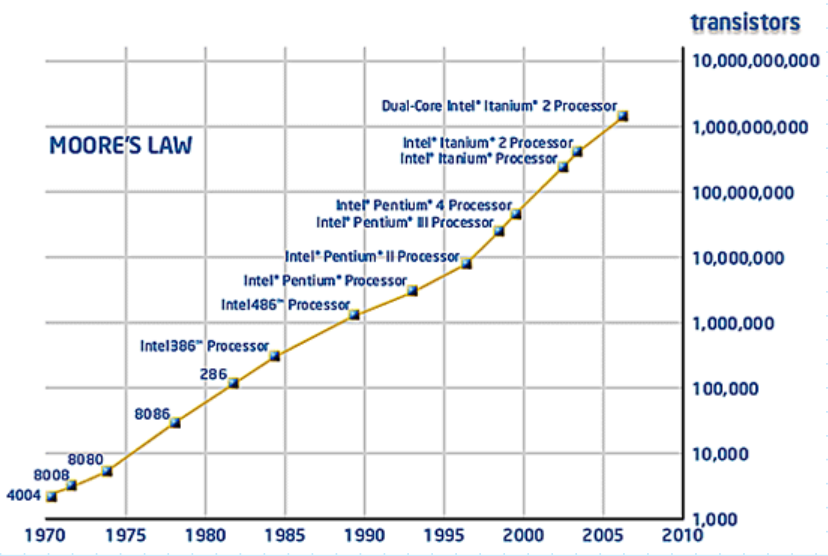
Obecne komputery też używają praw fizyki kwantowej:
struktura półprzewodników, tranzystory, momenty magnetyczne atomów (spiny)

Ale ....

– 1 bit danych na dysku twardym: ($d \approx 0{,}5\,nm$)
$250\,nm \times 250\,nm \times 25\,nm \approx 12{,}5$ mln atomów

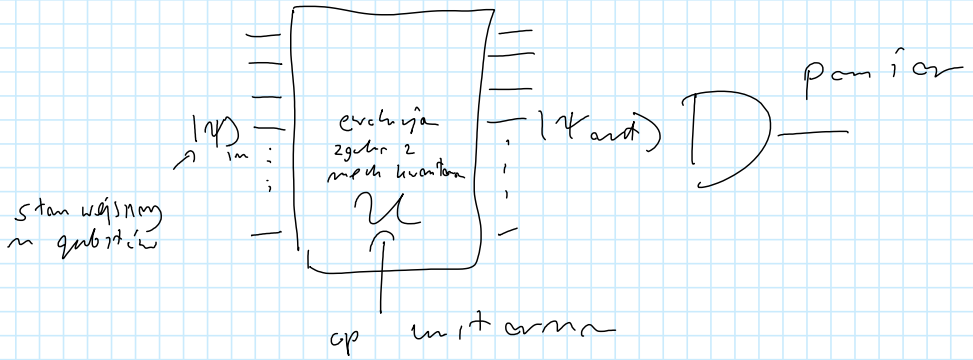
– 1 tranzystor w CPU
$50\,nm \times 50\,nm \times 25\,nm \approx 500$ tys atomów

Wciąż dużo. Nie jesteśmy na etapie żeby używać pojedynczych atomów do obliczeń i wykorzystać pełne możliwości fizyki kwantowej
Kiedyś zejdziemy do poziomu 1 atomu.



Rozmiar tranzystorów zmniejsza się dwa razy co 2 lata
Będzie rozmiar atomu ok roku 2030-2050 ?
Nawet jak to nastąpi nie oznacza to, że mamy
już komputer kwantowy.
Musimy umieć utrzymać kwantowe zjawiska tak
tak aby móc wykonywać potrzebne mech. kwantowej

2. Idea



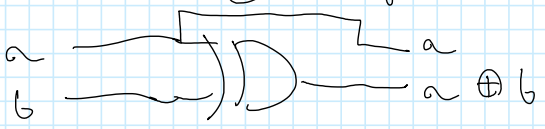
- Klasyczne komputery budujemy zazwyczaj z prostych elementarnych bramek: NOT, AND, OR, XOR ...
Wiadomo, że np. każdy układ logiczny można zbudować z bramki NAND .

- W klasycznych komputerach zazwyczaj używamy bramek nieodwracalnych

(dwóch można również inaczej) 

nie da się odtworzyć wejścia z bitu wyjściowego

- Można by czynić w obliczeniach bramki odwracalnych, wystarczy np.



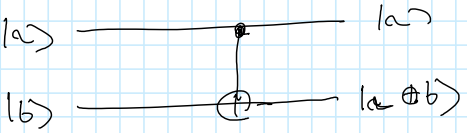
Kosztem komplikacji obwodów, zyskuje się tego nie robi. Pamiętajmy jednak, że liczba w zasadzie jest odwracalna. Nieodwracalność bierze się z tego, że po prostu ignorujemy jakieś stopnie swobody

- Myśląc o komputerach kwantowych mamy operacje unitarne - które są odwracalne. Można oczywiście też zrobić nieodwracalne np. śledząc po pomiarze z wyjściowych qubitów, ale to zazwyczaj niszczy kwantowe superpozycje, więc nadal nie sensu. Ograniczy się więc do operacji unitarnych.

Chcemy modelować elementarne bramki.
Z którymi można zrobić dowolną op. U.
Bramki te muszą być odwracalne.

- Bramka CNOT

$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$
$|0\rangle|1\rangle \longrightarrow |0\rangle|1\rangle$
$|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle$
$|1\rangle|1\rangle \longrightarrow |1\rangle|0\rangle$

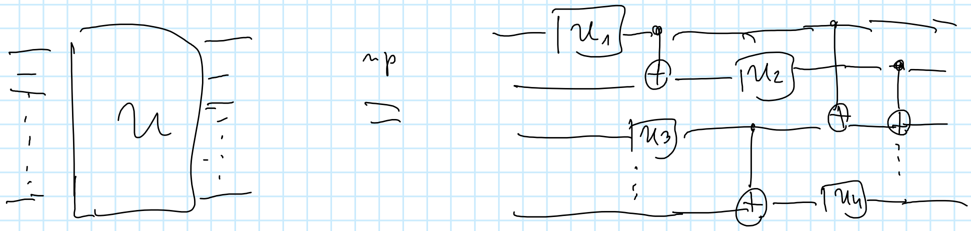


$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

w bazie $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

Mając właściwie to jest taki odwracalny XOR

<u>Fakt</u> Każda wielokubitowa $\mathcal{U}$ może być rozłożona na jednokubitowe op. unitarne i bramki CNOT



W ogólności potrzebujemy wielu bramek jednokubitowych (∞ wiele obrotów sfery Blocha) można np. wybrać:

—[H]— bramka Hadamarda $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ $\Big\}\ H^{\dagger}H = I$

—[φ]— opóźnienie fazowe φ (bramka fazowa) $U_\varphi = \begin{bmatrix}1 & 0\\ 0 & e^{i\varphi}\end{bmatrix}$ (np. $\varphi = \frac{\pi}{2}$ ćwierćfalówka)

3. Kwantowy paralelizm - dlaczego komputer kwantowy ma szansę liczyć szybciej?

Idea: $f: \{0,1\} \to \{0,1\}$ jednobitowa funkcja $f(0), f(1)$

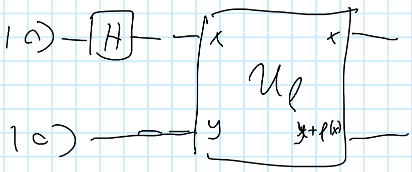
<u>Wyobraźmy</u> sobie że kodujemy funkcję f w bramce kwantowej U_f

$$|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle$$

↑ qubit z argumentem funkcji; ↑ qubit z wynikiem funkcji; ↑ dodawanie mod 2

$$\begin{cases} |0\rangle|0\rangle \\ |0\rangle|1\rangle \\ |1\rangle|0\rangle \\ |1\rangle|1\rangle \end{cases} \xrightarrow{U_f} \begin{array}{l} |0\rangle|0\oplus f(0)\rangle \\ |0\rangle|1\oplus f(0)\rangle \\ |1\rangle|0\oplus f(1)\rangle \\ |1\rangle|1\oplus f(1)\rangle \end{array}$$

jest to op. unitarna



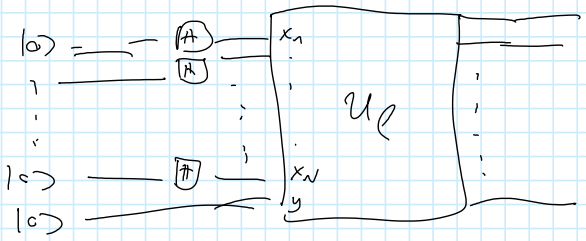
$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\right)$$

$$|0\rangle|0\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle+|1\rangle|0\rangle\right) \xrightarrow{U_f} \frac{1}{\sqrt{2}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\right)$$

Użyliśmy tylko raz obliczenia f a mamy stan $|\psi\rangle$ w którym pełna jest f zarówno dla $f(0)$ i $f(1)$.
„Liczymy równocześnie" $f(0)$ i $f(1)$ dzięki temu, że wymóciliśmy superpozycję.

Ogólniej: $f: \{0,1\}^N \to \{0,1\}$ funkcja na N bitach

$$|x_1, \dots, x_N, y\rangle \xrightarrow{U_f} |x_1 \dots x_N, y \oplus f(x_1, \dots, x_N)\rangle$$



$$|0\rangle^{\otimes N} |0\rangle \xrightarrow{H^{\otimes N} \otimes \mathbb{1}} \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)^{\otimes N} \otimes |0\rangle =$$

$$= \frac{1}{\sqrt{2^N}} \left(|0\rangle \dots |0\rangle + |0\rangle \dots |1\rangle + \dots + |1\rangle \dots |1\rangle\right) \otimes |0\rangle \xrightarrow{U_f}$$

wszystkie liczby N bitowe

$$= \frac{1}{\sqrt{2^N}} \cdot \left(|0\rangle \dots |0\rangle \otimes |f(0,\dots,0)\rangle + |0\rangle \dots |1\rangle \otimes |f(0,\dots,1)\rangle + \dots + |1\rangle \dots |1\rangle \otimes |f(1,\dots,1)\rangle\right)$$

„Policzyliśmy" w jednym obliczeniu wartości funkcji f dla wszystkich 2^N możliwych danych wejściowych.
Nadzieja na wykładniczo przyspieszenie obliczeń!
Ale nie tak szybko – nie istnieje pomiar pozwalający jednocześnie odczytać wszystkie wartości f. Pomiar w bazie $|0,\dots,0\rangle, \dots, |1,\dots,1\rangle$. Stan zmieni się nam na jeden z wyrazów superpozycji i poznamy tylko jedną wartość f...

Ale może są problemy w których chodzi obliczenie wszystkich f jest elementem pośrednim a nie końcowym odczytujemy jakąś funkcję tych f i wystarczy jeden pomiar dający pożądany wynik.

Algorytm Deutscha

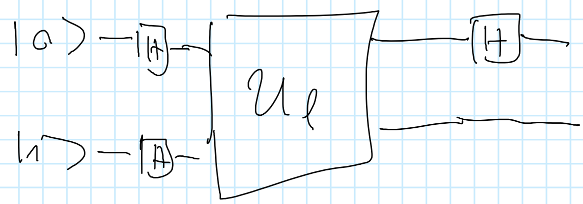
Najprostszy: całkowicie nieprzydatny ale ciekawy dydaktycznie

Rozważmy funkcję $f: \{0,1\} \to \{0,1\}$.

Pytamy się czy funkcja jest różnowartościowa?

Klasycznie funkcję musimy policzyć 2 razy.

A jeśli mamy komputer kwantowy wystarczy raz



$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle$$

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \xrightarrow{U_f} \frac{1}{2}\Big(|0\rangle\big(|f(0)\rangle-|1\oplus f(0)\rangle\big) + |1\rangle\big(|f(1)\rangle-|1\oplus f(1)\rangle\big)\Big) =$$

$$= \frac{1}{2}\Big((-1)^{f(0)}|0\rangle(|0\rangle-|1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle-|1\rangle)\Big) =$$

$$= \frac{1}{2}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)\big(|0\rangle-|1\rangle\big) \xrightarrow{H\otimes I}$$

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

$$= \Big(\underbrace{\frac{1}{2}\Big[(-1)^{f(0)}+(-1)^{f(1)}\Big]}|0\rangle + \underbrace{\frac{1}{2}\Big[(-1)^{f(0)}-(-1)^{f(1)}\Big]}|1\rangle\Big)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

pierwszy nawias: 1 – f. stała, 0 – f. różnowart.

drugi nawias: 1 – f różnowart., 0 – f stała

Mierzymy pierwszy qubit jeśli wynik $|0\rangle \Rightarrow$ f. stała

$|1\rangle \Rightarrow$ f różnowartościowa

Dzięki temu że policzymy jednocześnie dla obu wartości wejściowych wystarczyło tylko raz użyć

notatka -

Algorytm Grovera

Kwantowe przeszukiwanie nieuporządkowanej bazy danych. Niech baza składa się z N ($N=2^n$) elementów.

Niech f będzie funkcją identyfikującą poszukiwany element:

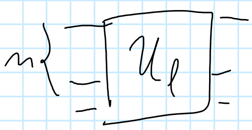
$f(x) = 1$ gdy x jest poszukiwanym elementem

$f(x) = 0$ w przeciwnym razie

Jeśli szukamy jednego elementu, musimy średnio obliczyć funkcję f, $\sim \frac{N}{2}$ razy. Czy kwantowo da się lepiej?

Załóżmy że mamy kwantową wersję f

$$U_f \underbrace{|x\rangle}_{n \text{ qubitów}} \underbrace{|y\rangle}_{1 \text{ qubit}} = |x\rangle|y \oplus f(x)\rangle$$

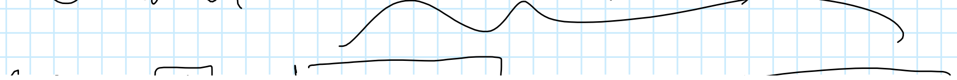


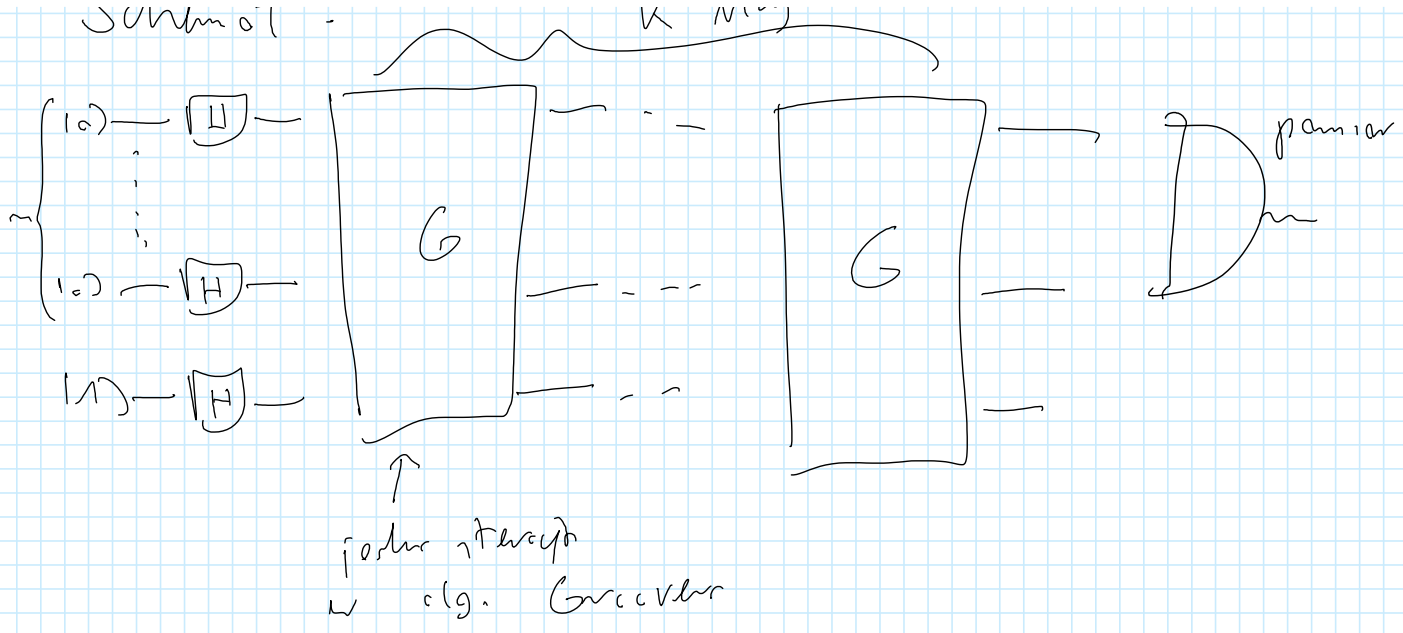
Zauważmy że:

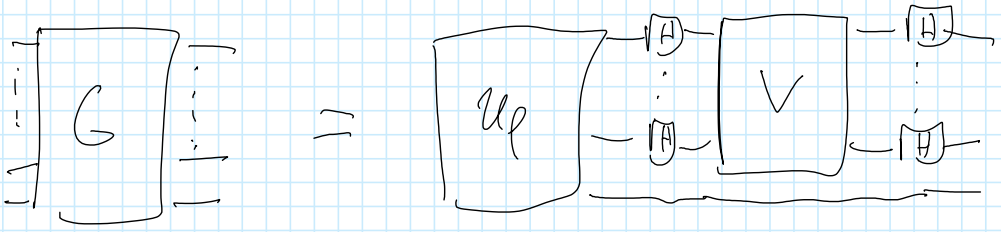
$$U_f |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

W dalszym ciągu mamy ignorować ostatni qubit on cały czas będzie pozostawał w stanie $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Schemat:







V – op unitarny t. że $V|a\rangle = |c\rangle$
$V|x\rangle = -|x\rangle, \quad x > 0$

$$V = 2|c\rangle\langle c| - \mathbb{1}$$

$$H^{\otimes N} V H^{\otimes N} = 2|\psi\rangle\langle\psi| - \mathbb{1}, \text{ gdzie}$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

Czyli: $G = \left(2|\psi\rangle\langle\psi| - \mathbb{1}\right) U_f$

Niech $|x_0\rangle$ – bedzie odpowiadać szukanemu stanowi

Niech $|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$ będzie superpozycją pozostałych stanów.

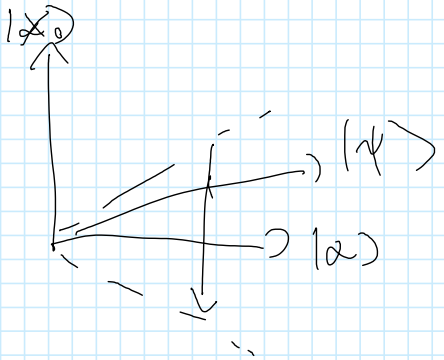
Rozważmy jak działa G na superpozycję $|x_0\rangle$ i $|\alpha\rangle$

Zauważmy że $|\psi\rangle = \sqrt{\frac{N-1}{N}}|\alpha\rangle + \frac{1}{\sqrt{N}}|x_0\rangle$

położenie:

$$G(a|\alpha\rangle + b|x_0\rangle) = (2|\psi\rangle\langle\psi| - \mathbb{1})(a|\alpha\rangle - b|x_0\rangle)$$

odbicie względem $|\alpha\rangle$



$$= 2|\psi\rangle\left(\sqrt{\frac{N-1}{N}}\cdot a - \frac{1}{\sqrt{N}} b\right) - (a|\alpha\rangle - b|x_0\rangle) =$$

odbicie względem $|\psi\rangle$

$$= 2\frac{N-1}{N} a|\alpha\rangle - 2\frac{1}{N} b|x_0\rangle + \frac{2\sqrt{N-1}}{N} a|x_0\rangle - \frac{2\sqrt{N-1}}{N} b|\alpha\rangle$$
$$- (a|\alpha\rangle - b|x_0\rangle) =$$

$$= \left(2a - \frac{2a}{N} - 2\frac{\sqrt{N-1}}{N} b - a\right)|\alpha\rangle + \left(b - \frac{2}{N} b + \frac{2\sqrt{N-1}}{N} a\right)|x_0\rangle$$

$$= \left(a\left(1 - \frac{2}{N}\right) - b\frac{2\sqrt{N-1}}{N}\right)|\alpha\rangle + \left(b\left(1 - \frac{2}{N}\right) + a\frac{2\sqrt{N-1}}{N}\right)|x_0\rangle$$

Czyli przy przejściu obrót o kąt θ:

$$\cos\theta = 1 - \frac{2}{N} \qquad \theta = \arccos\left(1 - \frac{2}{N}\right)$$

$\cos\theta = 1 - \frac{2}{N}$ $\quad \theta = \arccos\left(1 - \frac{2}{N}\right)$

W Alg. Grovera startujemy ze stanu $|\psi\rangle$

$$|\psi\rangle = \sqrt{\frac{N-1}{N}}\,|\alpha\rangle + \frac{1}{\sqrt{N}}\,|x_0\rangle =$$

$$= \cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|x_0\rangle$$

I w kolejnych krokach obracamy się o kąt θ

Czyli po k iteracjach:

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|x_0\rangle$$

Jeśli N bardzo duże $\quad \theta \approx \frac{2\sqrt{N-1}}{N} \approx \frac{2}{\sqrt{N}}$

Chcemy, żeby $\frac{2k+1}{2}\theta \approx \frac{\pi}{2}$

$$(2k+1)\cdot\frac{1}{\sqrt{N}} = \pi \qquad k \approx \sqrt{N}$$

Czyli kwadratowe przyspieszenie w porównaniu z algorytmem klasycznym.