7. Kvantni algoritmi II

Cilj: Spoznajmo "uporabne" kvantne algoritme: Deutsch-Jozsa, Grover, Schor
Navedimo konkretno implementacijo Groverjevega algoritma

7.1) Načini kvantnega računanja

- Kvantna vrata: vsaka unitarna transformacija je lahko predstavljena kot mreža majhnega števila tipov vrat
  Univerzalni set vrat: a) $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$, Phase shift $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$, CNOT
  b) Toffoli in Hadamar
  c) Cliffordova vezja: CNOT, H, S, T vrata.
  Niso univerzalna, a jih lahko učinkovito simuliramo s klasičnim računalnikom

- Adiabatsko kvantno računanje: počasna evolucija začetnega Hamiltonskega operatorja in osnovnega stanja v končni problem. Tipično optimizacijski problemi. (Predavanja Jaka Vodeb)

- Topološka kvantno računanje: uporaba kvazidelca „anion" v 2D, ki se prepletajo v "kitke" in v prepletu zakodiramo še logične operacije. Prednost: zelo stabilno. Problem: anionov še ne znamo ustvariti.

7.2) Kvantni paralelizem

Dvočlenska vrata U_f preslikajo

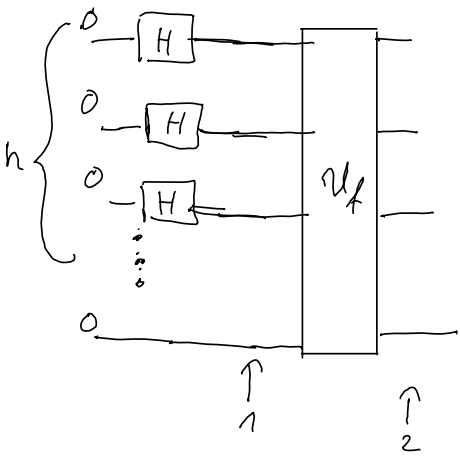
$$|x, y\rangle \to |x, y \oplus f(x)\rangle$$

če pripravimo stanje

$$(|0\rangle + |1\rangle)/\sqrt{2} \otimes |0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2}}|0, f(0)\rangle + \frac{1}{\sqrt{2}}|1, f(1)\rangle$$

Funkcijo f smo izvedli na vseh možnih vhodnih vrednostih

n- kubitov



1) $\frac{1}{2^{n/2}} \sum_{i_1,\ldots,i_n} |i_1,\ldots,i_n\rangle$

2) $\frac{1}{2^{n/2}} \sum_{i_1\ldots i_n} |i_1\ldots i_n\rangle \otimes |f(i_1,\ldots i_n)\rangle$

Kvantni paralelizem: izvrednotimo za vse možne argumente v enem koraku.

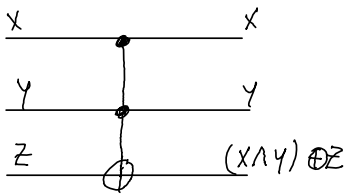
Vprašanja: - kako to uporabimo?
- kako implementiramo U_f vrata?

7.3) Reverzibilnost, AND in Toffoli vrata

	AND
0 0	0
0 1	0
1 0	0
1 1	1

AND ni reverzibilen in ne more biti kvantna vrata

Trik: Uvedi dodatno ("ancilla") vrata



Toffoli vrata

$|x\,y\,z\rangle \to |x\;y\;z \oplus x \wedge y\rangle$

x y z	output
0 0 0	0 0 0
0 0 1	0 0 1
0 1 0	0 1 0
0 1 1	0 1 1
1 0 0	1 0 0
1 0 1	1 0 1
1 1 0	1 1 1
1 1 1	1 1 0

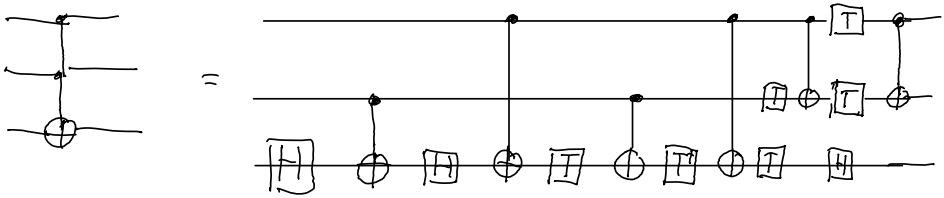
Simulacija AND, če $z=0$.

Transformacija

$$U = \begin{pmatrix} 1 & 0 & & & & & & \\ 0 & 1 & 0 & & & & & \\ & 0 & 1 & 0 & & \emptyset & & \\ & & 0 & 1 & 0 & & & \\ & \emptyset & & 0 & 1 & 0 & & \\ & & & & 0 & 1 & 0 & \\ & & & & & 0 & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix}$$

$U^{-1} U = \mathbb{1}$ Vrata so unitarna.

Možna realizacija:



7.4 Deutsch in Deutsch-Jozsa algoritem

Prvi primer algoritma, ki je hitrejša izvrednitev na kvantnem kot klasičnem.

Naloga: Imamo funkcijo, ki slika iz zaporedja binarnih števil v 0 ali 1 $f(x_1 \dots x_n) = \begin{cases} 0 \\ 1 \end{cases}$. Pokaži, če je funkcija:

a) konstantna $f(x_1 \dots x_n) = 1$ ali $f(x_1 \dots x_n) = 0$ za vsak $x_1 \dots x_n$

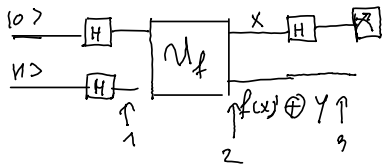
b) Uravnotežena $f(x_1 \dots x_n) = \begin{cases} 0 \\ 1 \end{cases}$ ... polovično verjetnostjo

klasično je vseh možnosti 2^n. V najslabšem primeru: $\frac{2^n}{2} + 1 = 2^{n-1} + 1$ ugibanj.

Funkcijo pravimo funkcijo oračelj.

Predstavimo vrata U_f

Poglejmo, kakšno generacijo izvede vezje



1) $|\psi_1\rangle = H \otimes H\,|01\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

2) $|\psi_2\rangle = \frac{1}{2}\left(|0\rangle\left(|f(0)\oplus 0\rangle - |f(0)\oplus 1\rangle\right) + |1\rangle\left(|f(1)\oplus 0\rangle - |f(1)\oplus 1\rangle\right)\right)$

$\frac{1}{2}\sum_{x=0}^{\hat{}} |x\rangle\left(|f(x)\rangle - |1\oplus f(x)\rangle\right) = \frac{1}{2}\sum_{x=0}^{\hat{}} (-1)^{f(x)}\,|x\rangle\,(|0\rangle - |1\rangle)$

(X) ker $f(x) = \begin{cases} 0 \\ 1 \end{cases}$

$|0\,f(0)\rangle - |0\,1\oplus f(0)\rangle = \begin{cases} |00\rangle - |01\rangle \text{ if } f(0)=0 \\ |01\rangle - |00\rangle \text{ if } f(0)=1 \end{cases} = (-1)^{f(0)}\,|0\rangle(|0\rangle - |1\rangle)$

$|1\,f(1)\rangle - |1,1\oplus f(1)\rangle = \begin{cases} |10\rangle - |11\rangle \\ |11\rangle - |10\rangle \end{cases} = (-1)^{f(1)}\,|1\rangle(|0\rangle - |1\rangle)$

3) Ignoriramo 2. kubit in aplociramo H vrata $\sum_x |x\rangle \xrightarrow{H} \sum_{x,y} (-1)^{xy}\,|y\rangle$

$|\psi_3\rangle = \frac{1}{2}\sum_{x=0}^{\hat{}} (-1)^{f(x)}\left[\sum_{y=0}^{\hat{}} (-1)^{xy}\,|y\rangle\right] = \frac{1}{2}\sum_{y=0}^{\hat{}}\left[\sum_{x=0}^{\hat{}} (-1)^{f(x)}\,(-1)^{xy}\right]|y\rangle$

Verjetnost da izmerimo $P_{|0\rangle} = \left|\frac{1}{2}\sum_{x=0}^{\hat{}} (-1)^{f(x)}\right|^2 = \begin{cases} 1 \text{ ; če } f(x) = \text{konst} \\ 0 \text{ ; če } f(x) = \text{uravnotežena} \end{cases}$

Zakaj deleje:

a) Če je funkcija konstantna, je stanje pred in po oraklju enako. H je inverz samega sebe in tako delimo $|0\rangle$

b) če je funkcija uravnotežena, potem dobi fazo enako stanje in tako je funkcija ortogonalna na input oraklja. Ko dodamo H, dobimo končno stanje, ki je ortogonalno $|0\rangle$.

c) Eno izvrednotenje omogoča rešitev problema. kvantni paralelizem.

d) Posplošitev na več kubitov Deutsch-Jotzsa algoritem. (Na vajah)

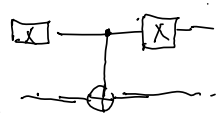
e) Kako implementiramo funkcijo f?

→ $f(x)=0$: $|x,y\rangle \to |x, f(x)\oplus y\rangle = |x,y\rangle$ ne naredimo nič.

→ $f(x)=1$: $|x,y\rangle \to |x, 1\oplus y\rangle = |x,\bar{y}\rangle$ NOT na y, kar pomeni X vrata

→ Uravnotežena $f(x)=x$: $|x,y\rangle \to |x, x\oplus y\rangle$ CNOT vrata

→ Uravnotežena $f(x)=\bar{x}$ $|x,y\rangle \to |x, \overline{x\oplus y}\rangle =$ CNOT + X vrata



Qiskit primer in posplošitev na N-kubitov na vajah.

7.5) Grover algoritem ali "quantum search algorithm" (1996)

Iskanje elementa v neurejenem seznamu, ki izpolnjuje določenem pogoju.

Klasična kompleksnost: $O(N)$, kjer je N število elementov v seznamu. Poiskositi moramo vse rešitve.

Kvantna pospešitev: $O(\sqrt{N})$ kar je kvadratna pospešitev (ne eksponentna kot pri Deutsch)

Pogoj: Dan nam je orakelj U_f, ki "prepozna" rešitev.

Uporaba: iskanja v velikem neurejenem seznamu (praviloma težko, ker je težko narediti orakelj)

- inverzija funkcije $y = f(x)$, kjer v množici X-ov najdemo točnega x^*, ki zadošča $y = f(x^*)$.
- iskanje rešitve, ki zadošča pogoju $y = f(x^*)$

7.5.1) Geometrijska ideja algoritma

Definirajmo: Enakomerno superpozicijo vseh stanj -

$$|E\rangle = \frac{1}{\sqrt{2^N}} \sum_{x_1 \dots x_n} |x_1 \dots x_n\rangle = \frac{1}{\sqrt{2^N}} \sum_{\vec{x}} |\vec{x}\rangle$$

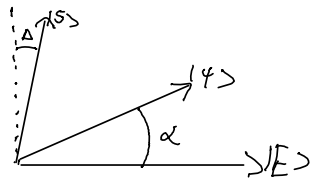
$|\vec{x}\rangle$ .. bitstring

$\Rightarrow |\beta\rangle$ je superpozicija prave rešitve

$\Rightarrow |\psi\rangle$ je začetno stanje

$\langle E|\beta\rangle \propto \frac{1}{\sqrt{N}}$ sta skoraj ortogonalna

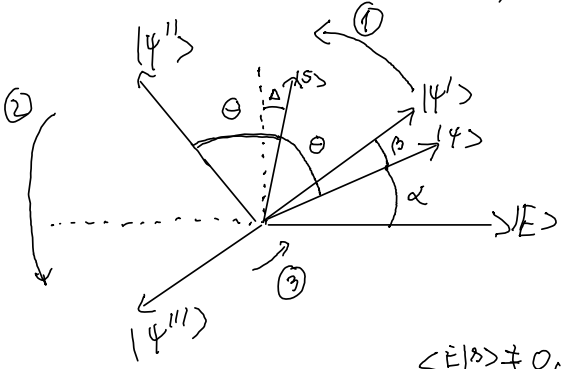
(Samo ena od vseh mala rešitev)



Opravimo rotacije: a) ψ zrcalimo preko $|s\rangle$

b) potem preko $|E\rangle$

c) pomnožimo z (-1)



Zaporedje teh korakov imenujemo Groverjeva iteracija.

$|\psi\rangle$ se preslika v $|\psi'\rangle$, ki je bližje $|s\rangle$, če $\langle E|s\rangle \neq 0$.

$\langle E|s\rangle \neq 0$, ker $|E\rangle$ sestavljajo vse kontinuacije.

Postopek iteriramo dokler se pridemo do $|s\rangle$ z. velika verjetnostjo. Koliko iteracij je potrebnoz?

Kako zrcalimo stanje $|\psi\rangle$ preko stanja $|\varphi\rangle$ v N-dim Hilbertovem prostoru?

a) Razbijemo na vzporedno in pravokotno komponento

b) pravokotno komponento pomnožimo z (-1)

a) $|\psi\rangle = |\varphi\rangle\langle\varphi|\psi\rangle + (1 - |\varphi\rangle\langle\varphi|)|\psi\rangle$

b) $|\psi\rangle = |\varphi\rangle\langle\varphi|\psi\rangle - (1 - |\varphi\rangle\langle\varphi|)|\psi\rangle = \underbrace{(2|\varphi\rangle\langle\varphi| - 1)}_{\text{Groverjev difuzijski operator } U_\varphi}|\psi\rangle$

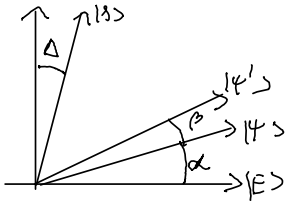
7.5.2 Groverjeva iteracija

$U_s|\psi\rangle = |\psi''\rangle = 2\langle s|\psi\rangle|s\rangle - |\psi\rangle$

$U_E|\psi''\rangle = |\psi'''\rangle = 2\langle E|\psi''\rangle|E\rangle - |\psi''\rangle = 4\langle s|\psi\rangle\langle E|s\rangle|E\rangle - 2\langle E|\psi\rangle|E\rangle - 2\langle s|\psi\rangle|s\rangle + |\psi\rangle$

$$|\psi'\rangle = \left(-4\langle E|s\rangle\langle s|\psi\rangle + 2\langle E|\psi\rangle\right)|E\rangle + 2\langle s|\psi\rangle|s\rangle - |\psi\rangle$$

Growerjeva iteracija slika med $|\psi\rangle, |E\rangle$ in $|s\rangle$!



$$\langle s|\psi'\rangle = |\langle s|s\rangle|\,|\langle\psi|\psi'\rangle|\cos(\pi - (\alpha+\beta+\Delta))$$

za kakšen kot se prevrtenemo iz $|\psi\rangle \to |\psi'\rangle$?

$$\langle s|\psi'\rangle = -4\langle E|s\rangle\langle s|\psi\rangle\langle s|E\rangle + 2\langle E|\psi\rangle\langle s|E\rangle + 2\langle s|\psi\rangle\langle s|s\rangle - \langle s|\psi\rangle =$$

$$= -4|\langle E|s\rangle|^2\langle s|\psi\rangle + 2\langle s|E\rangle\langle E|\psi\rangle + 2\langle s|\psi\rangle\langle s|s\rangle - \langle s|\psi\rangle$$

$$= 2\left(1 - 2|\langle E|s\rangle|^2\right)\langle s|\psi\rangle + 2\langle s|E\rangle\langle E|\psi\rangle - \langle s|\psi\rangle$$

$$\sin(\alpha+\beta+\Delta) = 2(1-2\sin^2(\Delta))\sin(\Delta+\alpha) + 2\sin(\Delta)\cdot\cos(\alpha) - \sin(\Delta+\alpha)$$

$$\sin(\alpha+\beta+\Delta) = 2\cos(2\Delta)\sin(\alpha+\Delta) + \sin(\Delta)\cdot\cos(\alpha) - \sin(\Delta)\cos(\alpha) - \cos(\Delta)\sin(\alpha)$$

$$= 2\cos(2\Delta)\sin(\alpha+\Delta) + \sin(\Delta-\alpha) = \sin(3\Delta+\alpha) - \sin(\Delta+\alpha) + \sin(\Delta-\alpha)$$

$$\sin(\alpha+\beta+\Delta) = \sin(3\Delta+\alpha) \qquad \boxed{\beta = 2\Delta}$$

Vsakič se prevrtenemo 2 Δ proti pravi rešitvi. Kot je neodvisen od iteracije.

Kriterij za zaključek:

a) Predpostavimo, da je ena rešitev

b) Prekrivanje $\langle s|E\rangle = \frac{1}{\sqrt{N}}$, Torej $\sin(\Delta) = \frac{1}{\sqrt{N}}$.

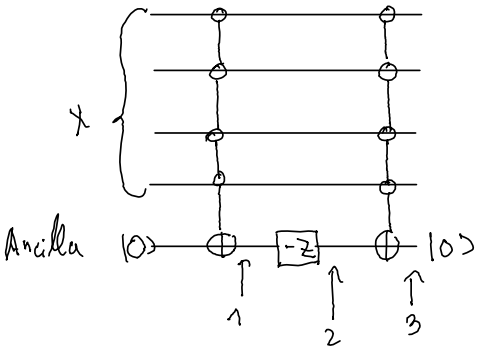
Popolno prekrivanje bo $\sin^2(2r\Delta + \Delta) = 1 \Rightarrow r = \frac{\pi\sqrt{N}}{4}$ / število korakov

c) kompleksnost je $O(\sqrt{N})$ in klasična je $O(N)$.
Lahko dokažemo, da je to optimalno za nestrukturirano iskanje.

d) Večji kot je iskalni Hilbertov prostor N, večja je verjetnost, da najdemo pravo rešitev.

7.5.3 Kako zrcalimo čez stanja

Kako preslikamo čez $|000\ldots0\rangle$? če stanje $|000\rangle$ ohrani
če $|X\rangle \neq |0000\ldots\rangle \Rightarrow |X\rangle \to -|X\rangle$

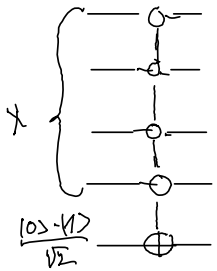


1.) Ancilla $\begin{cases} |1\rangle ; \text{če } |X\rangle = |00\ldots0\rangle \\ |0\rangle ; \text{drugače} \end{cases}$

2.) Ancilla $= \begin{cases} |1\rangle \ ; \text{če ancilla } |1\rangle \\ -|0\rangle \ ; \text{če ancilla } |0\rangle \end{cases}$

3) $\begin{cases} |X,0\rangle ; & \text{če } X = |000\ldots0\rangle \\ -|X,0\rangle ; & \text{drugače} \end{cases}$

Zmanjšajmo število vrat s "trikom s fazo"

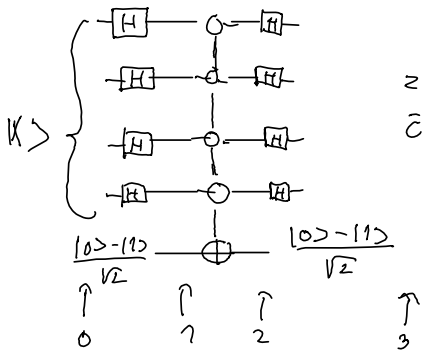


$$\begin{cases} |X\rangle \otimes \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|X\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} ; & \text{če } |X\rangle = |00\ldots0\rangle \\ |X\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \ ; & \text{drugače} \end{cases}$$

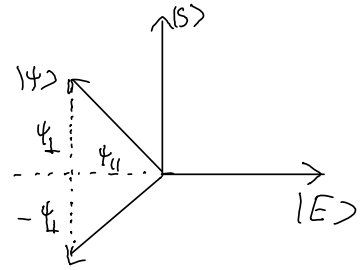
Do globalne faze natančno je to enaka operacija.

Zrcaljenje čez $|E\rangle$: - prenašni $|E\rangle \to |10\ldots0\rangle$
- zrcali čez $|00\ldots0\rangle$
- Prenašni $|000\ldots0\rangle \to |E\rangle$

Pokažimo, da je rezje



ravno zrcaljenje čez $|E\rangle$



$H^{\otimes n}|E\rangle = |000\ldots0\rangle$

0) $|\psi\rangle = (\alpha|E\rangle + \beta|E_\perp\rangle) \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

1) $|\psi\rangle = (\alpha|000\ldots0\rangle + \beta H^{\otimes n}|E_\perp\rangle) \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

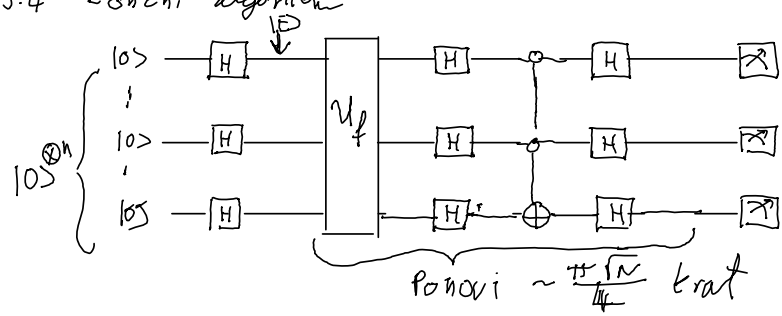
2) $|\psi\rangle = \left(-\alpha|00\ldots0\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} + \beta H^{\otimes n}|E_\perp\rangle\right) \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

3) $|\psi\rangle = -\alpha|E\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} + \beta \underbrace{H^{\otimes n} H^{\otimes n}}_{\mathbb{1}} |E_\perp\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} =$

$= -\left(\alpha|E\rangle - \beta|E_\perp\rangle\right) \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ Ravno zrcaljenje čez $|E\rangle$.

Celotna operacija je $2|E\rangle\langle E| - \mathbb{1}$, kar je zrcaljenje čez $|E\rangle$.

7.5.4 Končni algoritem

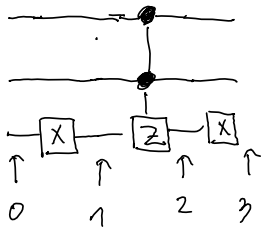


Kako implementiramo oraklelj U_f

$U_f |x\rangle = (-1)^{f(x)} |x\rangle$; kjer je $f(x) = \begin{cases} 1; & x \text{ iskano stanje} \\ 0; & \text{drugače} \end{cases}$

Recimo, da iščemo stanje "110".

Recept: - apliciraj X vrata za g-bit z ničlo
- uporabi kontrol z vrata
- apliciraj X vrata za g-bit z ničlo



0: $|110\rangle$
1: $|111\rangle$
2: $-|111\rangle$
3: $-|110\rangle$
! spremeni fazo !

ali

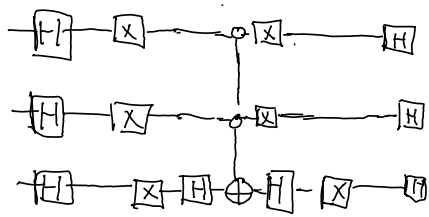
0: $|000\rangle$
1: $|001\rangle$
2: $|001\rangle$
3: $|000\rangle$
Ne spremeni faze.

Groverjev algoritem je primer kvantnega algoritma, ki ima kvadratni pospešek pred klasičnim algoritmom. Lahko pokažemo, da je to asimptotsko optimalno $O(\sqrt{N})$

Glej naloge za problem iskanja "011"

7 komentarji razlike v implementaciji:
- IBM ima ravno obrnjen vrstni red kvbitov
- Globoka struktura enaka
- Preslikava preko $|E\rangle$

giskit



7.6 Shor algoritem ('94)

Algoritem za razcep naravnega števila na praštevila

$15 = 3 \cdot 5$

Klasična kompleksnost $O\left(e^{1.9 (\log N)^{\frac{1}{3}} (\log \log N)^{\frac{2}{3}}}\right) \sim O(2^{N^{\frac{1}{3}}})$,
kjer je N naravno število. Super polinomsko, sub-eksponentno

Kvantna kompleksnost $O(\log^2 N \log\log(N))$ ali $O(M^2)$, kjer je $M = \log N$ število bitov.

Eksponentni pospešek! RSA temelji na predpostavki, da je razcep praštevil oteževan.

Razred BQP: "Bounded error quantum polynomial time"

Maksimalna napaka je 33%.

Primeri s 7-kubiti: $15 = 3 \times 5$ (Jedrska magnetna resonanca 2001 @ IBM

$21 = 3 \times 7$ ('12)

35 - neuspela zaradi prevel napak ('19)

Potrebe po "error-correction"!

Matematični temelji: - kvantna Fourierjeva transformacija

- iskanje reda $x^r \equiv 1 \pmod N$ in poišči najmanjši r.

- splošen problem je problem skrite podgrupe; A je vedno eksponentno zahtevnejši

Obstajajo drugi algoritmi za razcep; npr. $56153 = 241 \times 233$

Minimizacijski algoritmi.